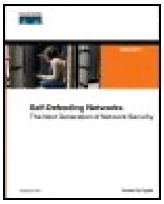


Self-Defending Networks: The Next Generation of Network Security

By Duane De Capite

.....

Publisher: **Cisco Press**
Pub Date: **August 31, 2006**
Print ISBN-10: **1-58705-253-9**
Print ISBN-13: **978-1-58705-253-8**
Pages: **250**

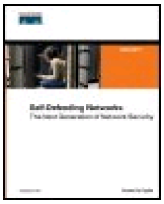
Table of Contents | Index

Overview

Protect your network with self-regulating network security solutions that combat both internal and external threats.

- Provides an overview of the security components used to design proactive network security
- Helps network security professionals understand what the latest tools and techniques can do and how they interact
- Presents detailed information on how to use integrated management to increase security
- Includes a design guide with step-by-step implementation instructions

Self-Defending Networks: The Next Generation of Network Security helps networking professionals understand how to deploy an end-to-end, integrated network security solution. It presents a clear view of the various components that can be used throughout the network to not only monitor traffic but to allow the network itself to become more proactive in preventing and mitigating network attacks. This security primer provides unique insight into the entire range of Cisco security solutions, showing what each element is capable of doing and how all of the pieces work together to form an end-to-end Self-Defending Network. While other books tend to focus on individual security components, providing in-depth configuration guidelines for various devices and technologies, *Self-Defending Networks* instead presents a high-level overview of the entire range of technologies and techniques that comprise the latest thinking in proactive network security defenses. This book arms network security professionals with the latest information on the comprehensive suite of Cisco security tools and techniques. Network Admission Control, Network Infection Containment, Dynamic Attack Mitigation, DDoS Mitigation, Host Intrusion Prevention, and Integrated Security Management are all covered, providing the most complete overview of various security systems. It focuses on leveraging integrated management, rather than including a device-by-device manual to implement self-defending networks.



Self-Defending Networks: The Next Generation of Network Security

By Duane De Capite

.....

Publisher: **Cisco Press**

Pub Date: **August 31, 2006**

Print ISBN-10: **1-58705-253-9**

Print ISBN-13: **978-1-58705-253-8**

Pages: **250**

Table of Contents | Index

Copyright
About the Author
About the Contributing Author
About the Technical Reviewers
Acknowledgments
Icons Used in This Book
Command Syntax Conventions
Foreword
Introduction
Chapter 1. Understanding Types of Network Attacks and Defenses
Categorizing Network Attacks
Understanding Traditional Network Defenses
Introducing Cisco Self-Defending Networks
Summary
References
Chapter 2. Mitigating Distributed Denial-of-Service Attacks
Understanding Types of DDoS Attacks
DDoS Mitigation Overview
Using Cisco Traffic Anomaly Detector
Configuring Cisco Guard
Summary
References
Chapter 3. Cisco Adaptive Security Appliance Overview
Antispoofing
Intrusion Prevention Service
Protocol Inspection Services
HTTP Inspection Engine
Configuring Content Security and Control Security
Summary
References
Chapter 4. Cisco Incident Control Service
Implementing Outbreak Management with Cisco ICS
Displaying Outbreak Reports
Displaying Devices
Viewing Logs
Summary
References
Chapter 5. Demystifying 802.1x

Fundamentals of 802.1x
Introducing Cisco Identity-Based Networking Services
Machine Authentication
Section 802.1. x and NAC
Using EAP Types
VPN and 802.1x
Summary
References
Chapter 6. Implementing Network Admission Control
Network Admission Control Overview
NAC Framework Benefits
NAC Framework Components
Operational Overview
Deployment Models
Summary
References
Chapter 7. Network Admission Control Appliance
NAC Appliance Features
NAC Appliance Manager
Summary
References
Chapter 8. Managing the Cisco Security Agent
Management Center for Cisco Security Agents
Cisco Security Agent
Summary
References
Chapter 9. Cisco Security Manager
Getting Started
Device View
Map View
Policy View
IPS Management
Object Manager
Value Override Per Device
Summary
References
Chapter 10. Cisco Security Monitoring, Analysis, and Response System
Understanding Cisco Security MARS Features
Summary Dashboard
Incidents
Rules
Query/Reports
Management
Admin
Cisco Security Manager Linkages
Summary
References
Index

Copyright

Self-Defending Networks
The Next Generation of Network Security
Duane De Capite

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Printed in the United States of America 1 2 3 4 5 6 7 8 9 0

First Printing September 2006

Library of Congress Cataloging-in-Publication Number: 2005932409

Warning and Disclaimer

This book is designed to provide information about self-defending networks. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc., shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through e-mail at feedback@ciscopress.com. Please be sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Corporate and Government Sales

Cisco Press offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales.

For more information please contact: **U.S. Corporate and Government Sales** 1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside the U.S. please contact: **International Sales** international@pearsoned.com

Trademark Acknowledgments

Publisher	Paul Boger
Cisco Representative	Anthony Wolfenden
Cisco Press Program Manager	Jeff Brady
Executive Editor	Brett Bartow
Managing Editor	Patrick Kanouse
Development Editor	Dayna Isley
Project Editor	Mandie Frank
Copy Editor	Paul Wilson
Technical Editors	Darrin Miller, Chris Tobkin
Team Coordinator	Vanessa Evans
Book and Cover Designer	Louisa Adair
Composition	Mark Shirar
Indexer	Ken Johnson

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www.europe.cisco.com
Tel: 31 0 20 357 1000

Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco.com Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic
Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy
Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA

Dedications

This book is dedicated to Donna, Nicolas, and Annabella: Thank you for making all of my dreams come true.

About the Author

Duane De Capite is a product line manager in the Security and Technology Group (STG) at Cisco Systems, Inc., and has been working with security and management teams for the past five years. Duane has also held marketing and engineering roles in IOS, storage networking, content networking, and management at Cisco. Prior to Cisco, Duane worked at IBM as a software developer. Duane holds an M.B.A. degree from the University of North Carolina at Chapel Hill and a B.S. degree in engineering from North Carolina State University, Summa Cum Laude. Duane has also completed graduate coursework toward an M.S. in engineering at Stanford University. Duane lives with his family in Chapel Hill, North Carolina.

About the Contributing Author

Denise Helfrich is a technical marketing engineer at Cisco Systems, Inc. Denise has been at Cisco since 2000 and in the telecommunications and networking business for more than 20 years, focusing on technical training and technical marketing. She currently works for the World Wide Sales Force Development group, creating and supporting technical training e-labs worldwide for various Unified Communication solutions. During the previous five years, Denise worked for Cisco in the Router Technology and Security Technology business units, developing training and marketing content and supporting various new router and router security products, such as Network Admission Control.

About the Technical Reviewers

Darrin Miller is an engineer in the Security Technology Group at Cisco Systems, Inc. Darrin is responsible for system-level security architecture. Darrin has worked primarily on policy-based admission and incident response programs within Cisco. Prior to that, Darrin conducted security research in the areas of IPv6, SCADA, incident response, and trust models. This work has included protocol security analysis and security architectures for next-generation networks. Darrin has authored and contributed to several books and whitepapers on the subject of network security. Darrin has also spoken around the world at leading network security conferences on a variety of topics. Prior to his eight years at Cisco, Darrin held various positions in the network security community.

Chris Tobkin, CISSP, is a consulting systems engineer for Cisco Systems, Inc., working with Enterprises within the central United States focused on security products and technologies. He has been involved with security technologies since 1996 at the University of Minnesota handling host and network security. After leaving the University of Minnesota in 2000, Chris worked for a security services and training company before joining Check Point Software Technologies as a regional technology leader in 2001. Since 2004, Chris has leveraged his industry knowledge and expertise to become a key liaison between the Cisco field engineering organization and the Security Technologies Group within Cisco Systems.

Acknowledgments

I am very fortunate to work with lots of great people. These people have helped me with insight and by answering all of my many questions. I am also fortunate to have lots of support from people at work as well as at home. This support has enabled me to write this book, and I am very thankful for this opportunity.

This book would not have been possible without the support from my family. It took a long time to write, and I had to promise that I would not start writing another book for at least six months. The process required many long evenings and weekends, and special thanks goes to my wife Donna for providing inspiration, writing feedback, and encouraging me throughout.

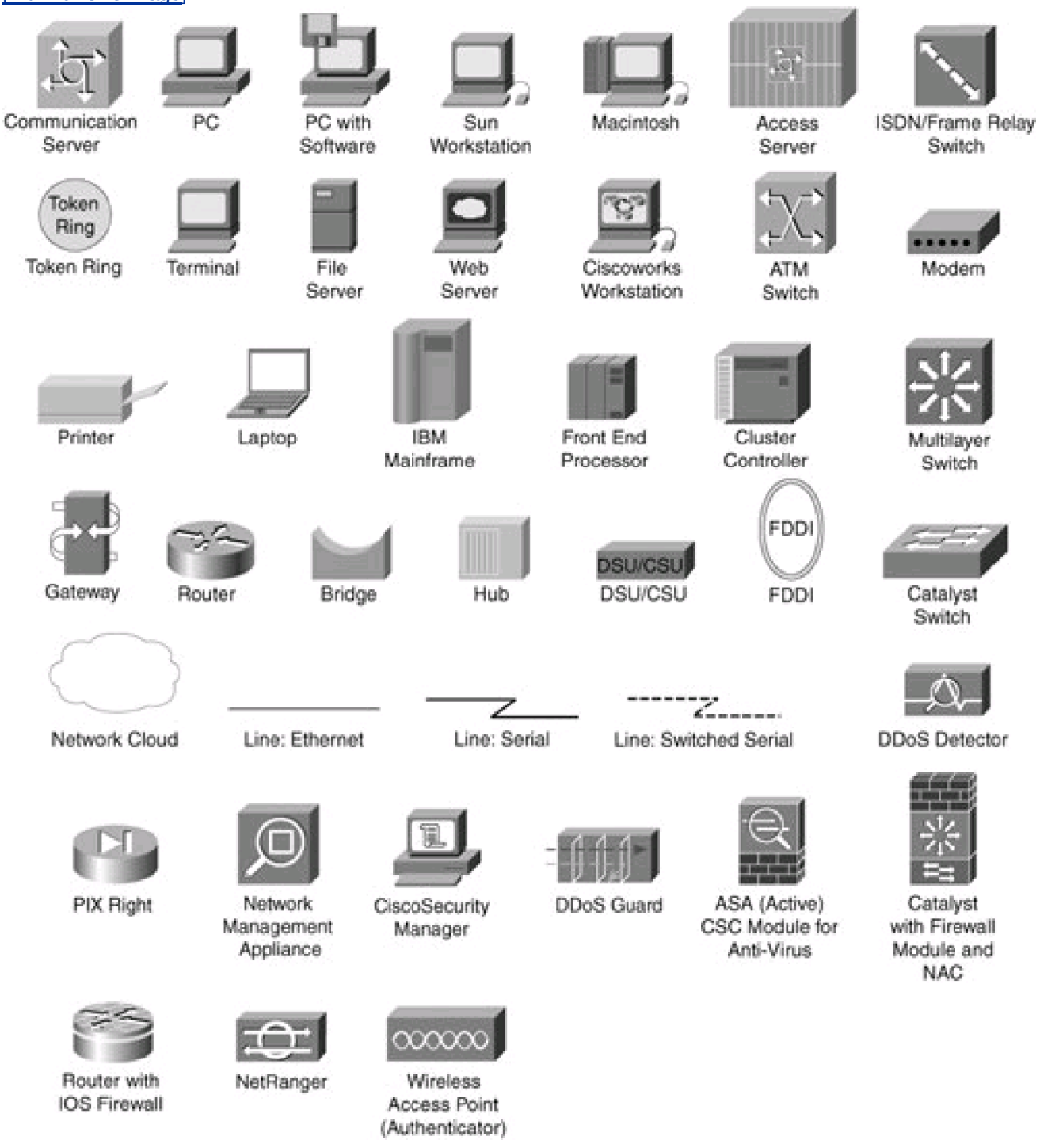
I would like to thank the reviewers, Darrin Miller and Chris Tobkin, for the excellent job and contributions to this book. I would also like to thank Denise Helfrich for authoring portions of this book while managing to coauthor another book for Cisco Press. I would also like to thank the excellent editorial staff at Cisco Press. This book would not be possible without the contributions by Brett Bartow and Dayna Isley.

Dozens of people helped me by answering questions and providing access to equipment. Special thanks goes these individuals, including Nick Chong, Edmund Lam, Steven Lee, Mark Bernier, Francesca Martucci, Steve DeJarnett, Joshua Houston, and Hari Shankar.

I would also like to thank the leadership team in the Security Technology Group for its support and guidance over the years. Special thanks goes to Amrit Patel and Dario Zamarian for giving me the opportunity to work with many of the great product teams in the Security Technology Group and for giving me the opportunity to write this book.

Icons Used in This Book

[View full size image]



Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italics* indicate arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets [ ] indicate optional elements.
- Braces { } indicate a required choice.
- Braces within brackets [{ }] indicate a required choice within an optional element.

Foreword

At Cisco, we strive to turn security from a silo and reactive approach to a proactive and holistic system that provides adaptive layers of defense-in-depth. Increasingly, network attacks are not just "outside-in" at the perimeter but "inside-out," necessitating threat protection and mitigation at every layer. Threats are taking vile and virulent forms and have turned from mere annoyances to menacing and significant losses of millions of dollars to businesses.

In this book, *Self Defending Networks: The Next Generation of Network Security,* the author Duane De Capite reviews not only the different forms of threats and protection, but he also examines the importance of architecting systematic network and information security. The need for risk mitigation, integrating innovative network security technologies such as unified threat management, behavioral day-zero protection, and application security with appropriate monitoring and control, is what makes networks truly *self-defending*. Such an architecture is not possible with point-products only. It calls for dramatic change from the band-aid approach to a thoughtful combination of policy, process, and technology. The author highlights the paramount importance of bridging the gap between classical desktop antivirus options and network security. Network administrators must have plans to integrate security seamlessly into their networks and build more collaborative trust models with Network Admission Control (NAC) across Cisco internetworks and industrywide coalitions and standards.

As we build networks of the 21st century deploying mobile devices, real-time video interactions, Internet telephony, and web applications, it is clear that security can no longer be an afterthought but is at the forefront of all new deployments. I do hope you will enjoy reading and learning the various attributes of security products and technologies that transform self-defending networks to the *reality* of securing information assets, applications, and networks.

Jayshree Ullal
Senior Vice President, Security, Switching and Datacenter Technologies
Cisco Systems

Introduction

Security is one of the fastest-growing areas in the networking and IT industries today. Security is often the top concern of Chief Information Officers (CIOs) and one of the top technology initiatives of many organizations. However, security projects often do not get the focus needed to be approved and deployed. Perhaps, this reticence can be explained by the complexity of security. Cisco has reduced the cost to deploy and manage security by creating a self-defending network. The self-defending network can enable the network to detect and defend itself against certain attacks. This book provides an overview of the attacks that a self-defending network can protect against, introduces the components of a self-defending network, and details how an organization can manage its self-defending network in a centralized and integrated fashion.

This book provides an overview of the components of a self-defending network, including distributed denial-of-service (DDoS) mitigation, Adaptive Security Appliances (ASA), Cisco Incident Control Service (Cisco ICS), NAC framework, NAC appliances (Cisco Clean Access), IEEE 802.1x, Cisco Security Agent (CSA), and integrated, centralized management.

Management is the glue that enables the components of a self-defending network to integrate and share a common defensive plan to thwart network attacks. The Cisco Security Manager and Cisco Security MARS are the bedrock of the Cisco centralized management strategy.

Goals and Methods

The goal of this book is to familiarize you with concepts, benefits, and implementation details of a Cisco self-defending network. This book endeavors to make you more comfortable with the following topics:

- Security threats and risks to IP networks
- Baseline security components of a traditional security network
- Concepts and benefits of a Cisco self-defending network
- Advanced topics in network security, including DDoS mitigation, NAC, and 802.1x
- In-depth coverage of the Cisco centralized management suite, including the Cisco Security Manager and Cisco Security MARS.

This book is not intended to be a one-stop shopping destination or a step-by-step guide to deploy each component of a self-defending network; instead, this book is a first-step to introduce you to the components of the Cisco self-defending network. If this book were a menu item in a restaurant, it would be a sampler platter, not an all-you-can buffet or a complete five-course meal. You can read this book in a day and, in that time, gain the ability to discuss the philosophy and components of a self-defending network at a high-level.

This book is heavily focused on device management and centralized management to show how you can manage a self-defending network. Many chapters of this book contain screenshots from beta or alpha software to get this book to market shortly after the products are released. There may be changes in the device manager and centralized management GUIs from alpha/beta software. There may also be changes in the device managers and centralized management GUIs between the versions used in the book and subsequent versions that are released to the market after the publication of this book.

Who Should Read This Book?

This book is intended for everyone learning about security and next-generation security networks, including Chief Security Officers (CSOs) and CIOs, network engineers and architects, and engineering students. This book is written to enable quick overview coverage of topics like DDoS, while creating a quick reference to enable deep-dives into specific implementation details, like how to deploy an 802.1x network.

How This Book Is Organized

This book is designed to be read as a beginning-to-intermediate overview of Cisco self-defending networks. The chapters cover the following topics:

- **Chapter 1, "Understanding Types of Network Attacks and Defenses"** Starts with an overview of network security threats and then details specific components of a self-defending network.
- **Chapter 2, "Mitigating Distributed Denial-of-Service Attacks"** Discusses the DDoS attack threats to an IP network and the components to mitigate this DDoS thread, including the DDoS service module for the Catalyst 6500/7600 family and the DDoS Device Manager.
- **Chapter 3, "Cisco Adaptive Security Appliance Overview"** Discusses the Cisco security appliance for firewall, IPS, VPN, antivirus, antispam, antiphishing, and URL filtering. This chapter also details how you can use the Adaptive Security Appliance Device Manager (ASDM) to help create a self-defending network.
- **Chapter 4, "Cisco Incident Control Service"** Examines the Cisco ICS product, developed with Trend Micro, that enables IOS routers, IPS Sensors, and the IPS module (AIP-SSM) of the Adaptive Security Appliance to update virus-related IPS signatures. This chapter also details the ability of Cisco ICS to configure access-list rules on IOS routers and ASA security appliances to help to protect the network against network virus infections.
- **Chapter 5, "Demystifying 802.lx"** Examines the underlying technology of the IEEE 802.1x standard, which enables networks to identify, authenticate, and authorize users to the desired VLANs and applications. This chapter also details how 802.1x can be a component of NAC.
- **Chapter 6, "Implementing Network Admission Control"** Provides an overview of the component of a self-defending network that authenticates and quarantines rogue users and users with down-level versions of OS patches and virus-protecting software. This chapter is dedicated to NAC framework, or a NAC solution that uses existing routers and switches.
- **Chapter 7, "Network Admission Control Appliance"** Covers the fundamentals of and configuration of the NAC appliance (Cisco Clean Access) product line. Specifically, this chapter covers how this NAC appliance can provide an alternative to the embedded components of NAC framework that may be attractive to several target markets, including the education market. This chapter also details how 802.1x is not required to implement NAC with the NAC appliance.
- **Chapter 8, "Managing the Cisco Security Agent"** Covers the fundamentals and configuration of the end-point or desktop self-defending component. It also discusses the product to provide end-point or desktop protection for up to 100,000 PCs or laptops with a single management center.
- **Chapter 9, "Cisco Security Manager"** Covers the centralized management product (Cisco Security Manager), which can configure the self-defending network for routers, switches, ASA, and IPS devices. This chapter also details how a management station can manage a self-defending network.
- **Chapter 10, "Cisco Security Monitoring, Analysis, and Response System"** Details how Cisco Security MARS can centrally monitor and provide mitigation for a self-defending network. Cisco Security MARS received monitoring input from many components in the selfdefending network, including routers, switches, ASA devices, IPS devices, databases, hosts, and Cisco Security Agents.

Chapter 1. Understanding Types of Network Attacks and Defenses

Reports of network security attacks have been increasing at an alarming rate. These network attacks fall into a variety of categories, none of them being attractive things that you want on your network. Network uptime, online orders, and productivity from networked applications are your offense, or networked assets. Network security is your defense, or protection of your networked assets, from these ever-increasing network attacks. A self-defending network is the next generation of network security, which introduces a new, innovative security architecture that can provide an additional layer of protection against network attacks.

Categorizing Network Attacks

Network attacks can be categorized based upon the nature of the attack. Categories of network attacks include the following:

- Virus
- Worm
- Trojan Horse
- Denial of service (DoS)
- Distributed denial of service (DDoS)
- Spyware
- Phishing

The next sections describe each of these categories in more detail.

Virus

When I was a software developer for a large systems company in the early 1990s, one of my coworkers liked to tell a story about how his grandmother called him up one day at the office and told him that she was worried about his health because she was concerned that he would catch a computer virus and become sick! A tremendous amount of education and socialization about computer viruses has occurred since the early 1990s. Even television and radio advertisements talk about how Internet services come bundled with antivirus protection to thwart these dastardly viruses. As my coworker had to explain to his grandmother, only computers, not people, can catch these particular viruses.

The term *virus* is credited to University of Southern California professor Frederick Cohen in his 1984 research paper *Computer Viruses: Theory and Experiments*. A computer virus is designed to attack a computer and often to wreak havoc on other computers and network devices. A virus can often be an attachment in an e-mail, and selecting the attachment can cause the executable code to run and replicate the virus. Other examples of executable code that can contain a virus include spreadsheet macros, JavaScript, or a macro in a Microsoft Word document.

Simple text files and .JPG pictures for example do not spread viruses because they are treated as a data form to be viewed and are not executed by the target computer. A virus must be executed or run in memory in order to run and search for other programs or hosts to infect and replicate. As the name implies, a virus needs a host such as a spreadsheet or e-mail in order to attach, infect, and replicate.

There are several common effects of a virus. Some viruses are benign, and simply notify their victim that they have been infected. Viruses can also be malignant and create destruction by deleting files and otherwise wreaking havoc on the infected computer that contains digital assets, such as pictures, documents, passwords, and financial records.

Worm

In this case, *worm* doesn't refer to a hole in the space-time continuum. A *worm* is a destructive software program that scans for vulnerabilities or security holes on other computers in order to exploit the weakness and replicate.

Worms can replicate independently and very quickly. For example, in 2001, the Code Red worm replicated itself over 250,000 times in less than 12 hours. Worms can also be relatively small in size. The SQL Slammer worm from 2003, for example, was only around 400 bytes. Worms can also attack instant messaging technology, as evidenced by an alert from Trend Micro on the Bropia worm, which you can read about at ZDNet (http://news.zdnet.com/2100-1009_22-5562129.html).

Note

Two researchers at Xerox Parc are credited with developing the first computer worm in 1978.

Worms differ from viruses in two major ways:

- Viruses require a host to attach and execute, and worms do not require a host.
- Viruses and worms typically cause different types of destruction.

Viruses, once they are resident in memory, often delete and modify important files on the infected computer. Worms, however, tend to be more network-centric than computer-centric. Worms can replicate quickly by initiating network connections to replicate and send massive amounts of data. Worms, such as SQL Slammer, brought many unsuspecting networks to their knees by initiating large numbers of network connections and data transfers. This type of network attack is also called a *distributed denial-of-service (DDoS)* attack, which is discussed in more detail later in this chapter.

Worms can also contain a piggybacked passenger, or data payload, which can relegate a target computer to the status of a zombie. A *zombie* is a computer that has been compromised and is now under control by the network attacker. Zombies are often used to launch additional network attacks. A large collection of zombies under the control of an attacker is referred to as a "botnet." Botnets can grow to be quite large. Botnets have been identified that were larger than 100,000 zombie computers.

Trojan Horse

A Trojan horse, or Trojan, is pernicious software that attempts to masquerade itself as a trusted application such as a game or screen saver. Once the unsuspecting user attempts to access what appears to be an innocuous game or screen saver, the Trojan can initiate damaging activities such as deleting files or reformatting a hard drive. Trojans are typically not self-replicating.

Network attackers attempt to use popular applications, such as Apple's iTunes, to deploy a Trojan. For example, a network attack sends an e-mail with a purported link to download a free iTunes song. This Trojan would then initiate a connection to an external web server and initiate an attack once the user attempted to download the apparent free song.

Denial-of-Service

A denial-of-service (DoS) attack is a network attack that results in the denial of service by a requested application such as a web server. There are several mechanisms to generate a DoS attack. The simplest method is to generate large amounts of what appears to be valid network traffic. This type of network DoS attack attempts to clog the network pipe so that valid user traffic cannot get through the network

connection. However, this type of DoS typically needs to be distributed because it usually requires more than one source to generate the attack (more on distributed DoS, or DDoS, attacks in the following section).

A DoS attack takes advantage of the fact that target systems such as servers must maintain state information and may have expected buffer sizes and network packet contents for specific applications. A DoS can exploit this vulnerability by sending packet sizes and data values that are not expected by the receiving application.

Several types of DoS attacks exist, including Teardrop attacks and the Ping of Death, which send handcrafted network packets that are different from those the application expects and may provoke the application and server to crash. These DoS attacks on an unprotected server, such as an ecommerce server, can cause the server to crash and prevent users from adding items to their shopping cart.

Distributed Denial-of-Service

A DDoS is similar in intent of a DoS attack, except that a DDoS attack originates from multiple source attack points. In addition to increasing the amount of network traffic from multiple, distributed attackers, a DDoS attack also presents the challenge of requiring the network defense to identify and stop each of the distributed attackers. You learn more about DDoS attacks in the section "DDoS Mitigation."

Several years ago, I was on a customer site visit to a very large online retailer at the very same time they were under a DDoS attack. They were able to stop the DDoS attack without dedicated DDoS mitigation products, but a significant amount of time was involved to identify the sources of the attack. This investigation, as well as the eventual remediation of the attack, involved communication and cooperation from the customer's Internet service provider (ISP). The intended victim was able to stop the attack after several hours, but they also had to stop the flow of valid traffic (in this case sales orders) in order to stop the DDoS attack.

Spyware

Spyware is a class of software applications that can participate in a network attack. Spyware is an application that attempts to install and remain hidden on a target PC or laptop. Once the spyware application has been surreptitiously installed, the spyware captures information about what users are doing with their computers. Some of this captured information includes websites visited, e-mails sent, and passwords used. Attackers can use the captured passwords and information to gain entry to a network to launch a network attack.

In addition to being used to directly participate in a network attack, Spyware can also be used to gather information that can be sold underground. This information, once purchased, can be used by another attacker that is "harvesting data" to be used in planning another network attack.

Phishing

Phishing is a type of network attack that typically starts by sending an e-mail to an unsuspecting user. The phishing e-mail attempts to look like a legitimate e-mail from a known and trusted institution such as a bank or ecommerce site. This false e-mail attempts to convince users that something has happened, such as suspicious activity on their account, and that the user must follow the link in the e-mail and logon to the site to view their user information. The link in this e-mail is often a false copy of the real bank or ecommerce site and features a similar look-and-feel to the real site. The phishing attack is designed to trick users into providing valuable information such as their username and password.

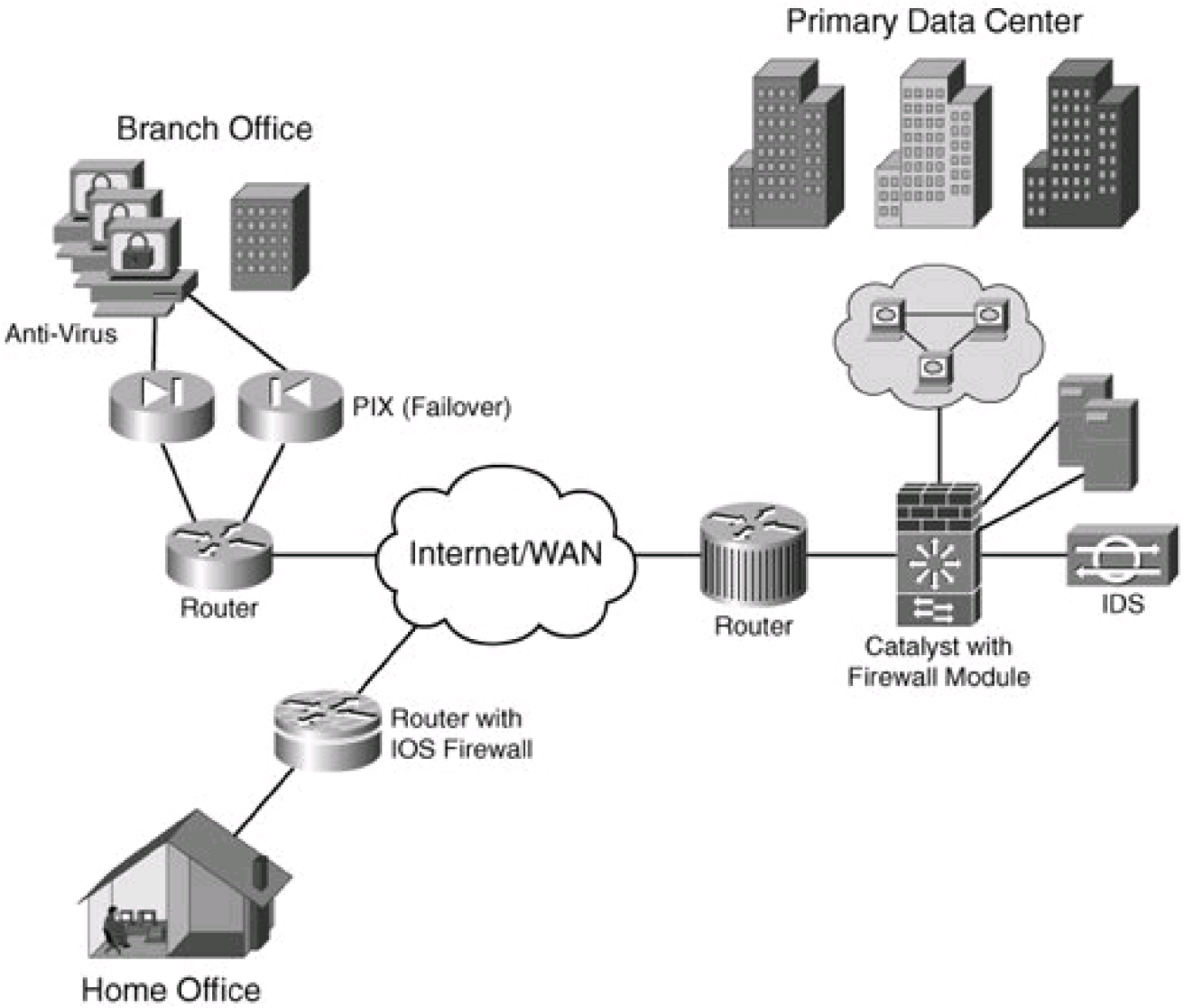
Understanding Traditional Network Defenses

Traditional security networks rely heavily on router access lists, firewalls, and intrusion detection to protect the network against attacks. These products provide a good baseline for network security; however, you can supplement them with other security products to increase network security. These traditional network security products are also typically manually configured, often with different administrators and different graphical user interfaces (GUIs).

The remainder of this chapter discusses traditional network defenses and provides an overview of a self-defending network. This chapter also describes how integrated, centralized management can help to increase network security. Figure 1-1 shows a network with traditional network defense components.

Figure 1-1. Traditional Network Defense

[View full size image]



Traditional network defenses are composed of the following products, which you will learn more about in the next sections:

- Router access lists
- Firewalls
- Intrusion Detection Systems (IDS)
- Virtual Private Networks (VPNs)
- Antivirus programs

Router Access Lists

The access list, or access control list (ACL), is the cornerstone of network security. Access lists permit or deny network traffic based upon parameters including source IP address, destination IP address, and network service or port number. Router access lists are typically stateless, meaning that the router does not a maintain TCP connection state for each connection. Router access lists offer perimeter protection and a base defense because routers are typically both edge devices for perimeter networks and core devices for large networks. In addition to protecting edge and core networks, access lists are also often used to protect the network device itself.

Firewalls

Firewalls are prevalent in perimeter networks and data centers. Firewalls are often found in the perimeter to protect remote sites or edge networks. Network firewalls take their name from the traditional firewalls that can exist on trains and buildings to quarantine or block a fire from spreading from one area to another.

Network firewalls often follow a similar approach by protecting parts of the network from other parts of the network in the event of an attack. Firewalls maintain a TCP state for each connection that passes through the firewall. Firewalls can prevent attacked web servers or zombies from attacking other parts of the network. Network firewalls can also implement a demilitarized zone (DMZ) functionality. Portions or areas of the network can be classified as either outside the network, typically toward the Internet, or inside the network, typically toward the users or servers, or a DMZ. DMZs enable a layer of protection between the untrusted, in this case the outside of the network, and the trusted, or inside, part of the network. Router access lists and firewalls combine to compose the bedrock of traditional network security defenses.

Intrusion Detection Systems

Router access lists and firewalls have been pervasive since the early 1990s. Intrusion detection systems (IDSs) started to become widely deployed toward the end of the 1990s. IDSs are passive devices that monitor a copy of network traffic as it flows through the system. IDSs are often deployed in data centers near critical servers. As the name implies, these IDSs can detect a network attack based upon network traffic signatures or patterns of data in the network traffic.

IDSs typically detect rather than prevent the network attack because they are not inline, as they are operating on a copy of the network traffic. IDSs are highly valuable to network security defense, because they can provide an early warning that a network attack has been initiated.

Virtual Private Networks

VPNs are commonplace in most corporate networks. VPNs are essentially a security layer applied to a public or private network to make the network connection secure. VPNs are also considered to be leased-line or ISDN replacements. VPNs use authentication mechanisms including one-time passwords and encryption such as 3DES (Triple DES, pronounced "dez") or Advanced Encryption Standard (AES) to provide a secure layer on top of a network connection. Because VPNs often replace leased-lines like T1s or ISDN connections, they are often managed by the Network Operations group, or NetOps, rather than the Security Operations, or SecOPs, group. VPNs are not a major focus of this book as they are often managed by the NetOps group for a site-to-site connection or a remote access connection to the corporate data center.

Antivirus Programs

Many organizations have implemented an antivirus program to combat the frequent virus attacks against their network. Antivirus programs often scan received e-mail to identify and remove known virus attacks. While antivirus scanning components are valuable additions to the security of a network, antivirus components are traditionally standalone and not integrated into the network fabric. The ability to embed the antivirus functionality directly into a network enables the network to be self-defending as the security components can be integrated and centrally managed and provides a mechanism for the network to be self-healing and automatically defend itself against certain viruses or viral attacks.

PREV NEXT

Introducing Cisco Self-Defending Networks

Self-defending networks augment and complement the traditional network defense components outlined in the previous section. Self-defending networks differ from traditional network defenses in that self-defending networks have the capability to provide some amount of automatic protection of the network components and end-user workstations in the event of a network attack.

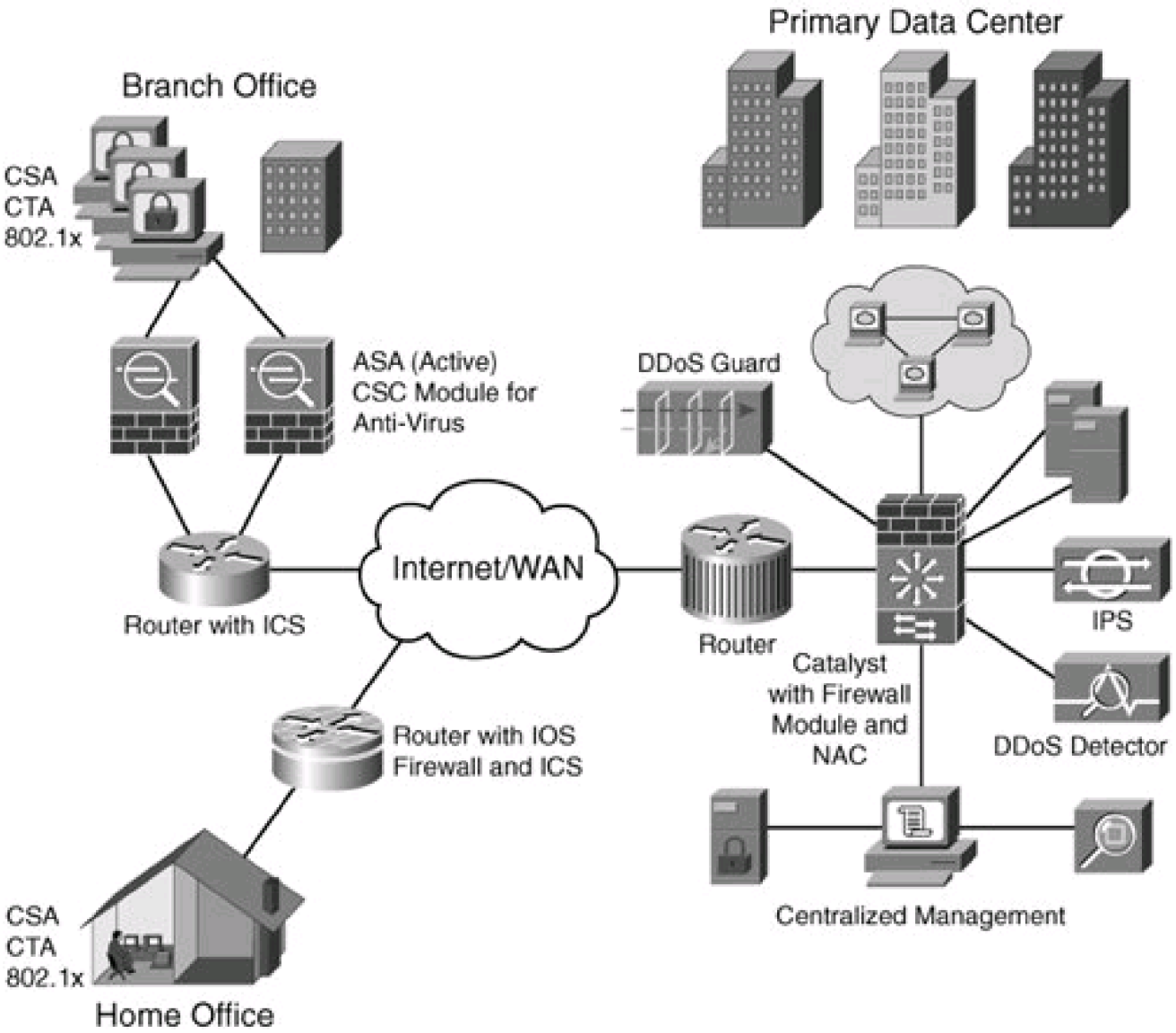
Self-defending networks can also be implemented in layers, in a manner similar to defensive layers of a football or soccer team. The layered self-defending network includes components that can protect the network connections in the data center, at the remote or branch location, and at the desktop. Self-defending networks can either recommend a configuration or automatically apply a configuration to prevent certain network attacks. Self-defending network components include the following:

- DDoS mitigation, including DDoS Guard and DDoS Traffic Anomaly Detector
- Adaptive Security Appliances (ASA)
- Incident Control Service (ICS)
- Network Admission Control (NAC)
- 802.1x
- Host intrusion prevention: Cisco Security Agent (CSA)
- Cisco Security Centralized management

Figure 1-2 displays an example of a network diagram with self-defending components. The next sections describe the components in more detail.

Figure 1-2. Self-Defending Network

[View full size image]



DDoS Mitigation

DDoS attacks can often be among the toughest to defend because they involve large amounts of what appears to be legitimate source traffic and multiple, distributed senders of this source traffic. Automatic or self-defending DDoS mitigation involves the automatic rerouting of the DDoS traffic while maintaining the valid network traffic connections. Cisco Guard and Detector appliances and Catalyst 6500/7600 DDoS service modules can provide this automatic DDoS mitigation by creating a baseline of normal network activity, detecting DDoS attacks and then automatically rerouting the DDoS traffic away from the target servers by updating the routing tables.

In addition to customer-managed DDoS mitigation solutions, there are also ISP-managed DDoS mitigation or clean-pipe solutions. These ISP-managed solutions are implemented with Cisco DDoS mitigation appliances and service modules. The ISP-managed solutions often contain partner products from Arbor Networks, which complement the Cisco DDoS mitigation appliance and linecard products.

Intrusion Prevention Systems

Intrusion Prevention Systems (IPSs) are the successor to IDS products. IDS operates on a copy of network traffic, from a source such as a span port on a LAN switch, so it can detect, but typically cannot prevent, an attack because the original network traffic has already propagated through the network.

IPS operates inline and processes the actual network packet, not a copy of the network traffic. IPSs can detect a network attack based upon network traffic signatures or patterns of data in the network traffic. Since IPS operates inline, IPS has the ability to drop the packets of the attack and prevent a network attack rather than detect a network attack. IPS is an important part of the self-defending network, rather than a traditional network defense, since IPS has the ability to be self-defending and prevent a network attack without manual operator intervention during the attack.

IPS can be implemented as a standalone IPS appliance or service module. IPS can also be implemented as an integrated component with the Adaptive Security Appliance (ASA). This book focuses on IPS as an integrated component with ASA rather than as a standalone product.

Adaptive Security Appliance

ASA is an integrated and extensible security appliance product line from Cisco. ASA is an integration of the PIX firewall, Network IDS/IPS system, and VPN 3000 concentrator. This ASA appliance contains many self-defending characteristics including inline IPS support, application layer inspection/enforcement, and SYN Cookie capabilities. These self-defending features can enable the ASA appliance to drop network attack connections and protect end servers and users from attacks by monitoring, inspecting, and restricting the network connection attempts to target devices. For example, the HTTP application inspection engine in ASA can inspect a specific HTTP connection flow and can drop an HTTP packet that does not conform to the proper packet format. The ASA IPS engine also allows specific IPS signatures to be applied to specific traffic flows. The inline IPS signature engine in ASA can be configured to automatically drop any packets in the traffic flow that match the IPS signature.

The SYN Cookie feature in ASA can prevent a TCP connection attack against a host by creating a cookie for each TCP connection request. This cookie can be used to protect the host by preventing the host from allocating a buffer for each TCP connection attempt. Features like SYN Cookie can be very powerful self-defending mechanisms since many host computers can be crashed or compromised when they run out of buffer spaces like the ones used for each TCP connection.

Incident Control Service

Cisco also offers the ability to contain a worm infection within the network. The Cisco Incident Control Service (ICS) is developed in partnership with Trend Micro. The Cisco ICS provides automatic updates of new vulnerability updates from Trend Micro. The Cisco ICS also provides the ability to automatically update these Outbreak Prevention Signatures on ASA, IOS router, and IPS platforms. In addition to Outbreak Prevention Signature update, Cisco ICS also provides Outbreak Prevention ACL (access list) updates, which can recommend or automatically apply a new ACL to an IOS router or ASA device in the event that a network infection has been identified to the Cisco ICS.

Network Admission Control

Network Admission Control (NAC) can help to create a self-defending network by preventing a rouge or vulnerable user from entering the network, thus reducing the attack risk before the user enters the network. NAC allows network components to check the operating system (OS) service pack (SP) updates, antivirus updates, and Cisco Security Agent (CSA) updates before the user is granted access to the network. Any down-level or at-risk users are quarantined to a safe part of the network until they can be remediated or upgraded with the proper OS, antivirus, or CSA updates required to safely participate on the network.

NAC components can be embedded directly into the framework of routers and switches, or NAC components can be deployed as dedicated, standalone appliances.

The NAC components that are embedded directly in routers and switches require client or agent software on the user computer. This client is known as Cisco Trust Agent (CTA). The standalone NAC framework solution supports an optional software client or agent for the end-station. Both the framework and appliance NAC solution support an audit mode for agentless devices. Audit mode allows information to be gathered about unknown endpoints without an agent and to be used to influence the amount of network access that is granted to these agentless machines. The NAC appliance also leverages an integrated scanner. The scanner probes the network to identify hosts and information about hosts including IP address and OS. In addition to being a dedicated standalone solution, the NAC appliances also do not require IEEE 802.1x authentication.

IEEE 802.1x

IEEE 802.1x is a standard for machine authentication and user authentication. IEEE 802.1x is widely deployed today in wireless LAN environments and can leverage a supplicant that resides on the end-device or host. Cisco's embedded NAC framework solution can leverage IEEE 802.1x to provide the basic authentication prior to more advanced authentication including OS SP patches, antivirus patches, and CSA updates.

Cisco's framework NAC solution leverages a unique end-device supplicant, the Cisco Trust Agent (CTA), to provide the advanced authentication features. CTA includes a base 802.1x supplicant. Many people are confused about exactly what 802.1x is. Chapter 5, "Demystifying 802.1x," reduces the confusion about 802.1x and identity management.

Host Intrusion Prevention: CSA

CSA provides host intrusion protection for users or hosts on the network. CSA can be considered the last line of the layered self-defending network defense because CSA can prevent malicious behavior on a host, including attacks such as buffer overflow. CSA can be automatically and centrally updated with new policies to help protect against new network attacks.

CSA is end-device or host software that monitors the behavior and critical resources of the end-device or host. CSA also contains an option that can implement a personal firewall service. CSA provides "day-zero" protection, which is a fancy way of saying that it can protect against certain attacks before the attack is known. CSA does not require signatures like legacy Host Intrusion Prevention and antivirus products. CSA provides this day-zero protection capability by detecting the symptoms of an attack, rather than the unique identifier of the attack. For example, CSA can prevent the modification of registry keys and can detect a buffer overflow. The ability to detect and prevent the symptom of an attack enables CSA to protect against certain attacks prior to the identification and naming of the attack.

Cisco Security Centralized Management

A good defense is typically a layered defense. This layered defense can be composed of router access lists and firewall service modules to protect the core network and data center, ASA to protect DMZs and the perimeter, NAC to provide secure network access at the perimeter, and CSAs to protect the server, workstations, and laptops. This defense is similar to that of a football team, starting with the front line to protect the servers, all the way to the safeties, or CSAs, as a last line of defense on the workstation or desktop. Like any layered defense, it is imperative to provide coordination and integration among the different layers of defense. This coordination, or coaching, can be implemented in an integrated fashion with centralized management products.

Cisco Security Centralized management can be divided into two main functional areas:

- Configuration
- Monitoring

Components from each of these functional areas are marketed under the Cisco Security Management product suite. The Cisco Security product for centralized configuration is the Cisco Security Manager (CS-Manager), and the centralized monitoring product is the Cisco Security Monitoring, Analysis, and Response System (CS-MARS).

Centralized configuration management products, like the Cisco Security Manager, enable hundreds or thousands of routers and security appliances to be configured with a consistent or coordinated security policy.

Centralized monitoring products, like the Cisco Security MARS, receive monitoring events like syslog, SNMP Traps, IPS Secure Device Event Exchange (SDEE), and Remote Data Exchange Protocol (RDEP) events and can create an end-to-end picture of what is happening in the network based upon the monitoring events from the devices in the network. The Cisco centralized monitoring Cisco Security MARS product also adds a response or self-defending feature where Cisco Security MARS can create a recommendation on how to stop a network attack as well as enable IPS signatures on IOS routers with the Distributed Threat Mitigation (DTM) feature. Cisco Security MARS also includes support for NetFlow to establish a baseline of what network traffic should look like prior to a potential network attack. Network traffic that is far in excess of this baseline can be used to determine that the network is under an attack.

PREV NEXT

Summary

There are several types of network attacks. Some of the most popular network attacks include viruses, worms, Trojans, DoS, DDoS, spyware, and phishing. Viruses are executable software that attack a host by attaching to a program or file such as an e-mail or spreadsheet. Viruses can wreak havoc on the target PC if the virus executes on the user's machine. Worms are more network-centric than viruses and do not require a host to replicate. Worms look for vulnerabilities to attack and initiate other network connections. Trojans attack by attempting to masquerade as something innocuous, such as a screen-saver or game. DoS attacks prevent legitimate network activity by attacking a vulnerability such as an expected packet size or buffer size for an application. A DDoS attack prevents legitimate network traffic by flooding the network with traffic from multiple or distributed sources, such as from zombies or botnets. Spyware is a network attack that monitors or spies on a user's activity, including keystrokes such as usernames or passwords. Phishing is a type of network attack that often sends an e-mail to an unsuspecting user and attempts to trick the user into logging on to a fake website, such as a bank or ecommerce site, through a link in the phishing e-mail. When the user logs on to the fake website, the phishing attack gathers the username and password.

Traditional network security is composed of router access lists, firewalls, and IDS appliances. Self-defending networks complement traditional network security by providing additional layers of security on the network. Self-defending networks have the ability to recommend configurations to stop certain network attacks. Self-defending networks also have the ability to automatically stop certain network attacks, including the automatic update of new configurations to the security devices within the self-defending network.

Components within the self-defending network include DDoS mitigation with Cisco Guard and Detector, the Cisco Adaptive Security Appliance (ASA), Cisco Incident Control Service (Cisco ICS), Network Admission Control (NAC) framework in routers and switches, NAC appliances, 802.1x identity, Cisco Security Agent (CSA), and centralized management. Cisco's core centralized security management products are the Cisco Security Manager (CS-Manager) and Cisco Security Monitoring, Analysis, and Response System (CS-MARS).

References

Computer Hope. Computer History,"History for 19801990." http://www.computerhope.com/history/198090.htm

Computer Virus FAQ for New Users.http://www.faqs.org/faqs/computer-virus/new-users/

Brain, Marshall. How Computer Viruses Work.http://www.howstuffworks.com/virus

Kotadia, Munir. MSN Messenger Hit by Double-Whammy Worm. ZDNet Australia. February 2005.
http://news.zdnet.com/2100-1009_22-5562129.html

Chapter 2. Mitigating Distributed Denial-of-Service Attacks

The Cisco distributed denial-of-service (DDoS) mitigation solution is composed of two key components: Cisco Traffic Anomaly Detector, which is responsible for detecting a DDoS attack, and Cisco Guard, which is responsible for mitigating the attack. Customers can implement a DDoS solution with the Cisco Guard and the Cisco Traffic Anomaly Detector, or they can purchase the DDoS solution from a service provider. The solution from a service provider is often called a *clean pipes* solution. A clean pipes solution is implemented with a variety of products, including the Cisco Guard, Cisco Traffic Anomaly Detector, and partner products from vendors like Arbor Networks.

The Cisco Guard and the Cisco Traffic Anomaly Detector are based upon the patented Multi-Verification Process (MVP) architecture. This MVP architecture enables the Cisco Guard and Cisco Traffic Anomaly Detector to leverage the latest analysis and attack recognition techniques to detect and remove network attack traffic while scrubbing and reinjecting valid network traffic to its proper destination. Before describing the functions and configuration processes for these products, this chapter summarizes various DDoS attacks.

Understanding Types of DDoS Attacks

Table 2-1 describes several varieties of generic DDoS attacks.

Table 2-1. Generic DDoS Attacks

Name of Attack	Flooding Capability	Short Description
Land	TCP SYN	Source and destination IP addresses are the same, causing the TCP response to loop.
SYN	TCP	Sends large numbers of TCP connection initiation requests to the target. The target system must consume resources to keep track of these partially opened connections.
Teardrop	TCP fragments	Sends overlapping IP fragments.
Smurf	Internet Control Message Protocol (ICMP)	Sends ICMP ping requests to a directed broadcast address. The forged source address of the request is the target of the attack. The recipients of the directed broadcast ping request respond to the request and flood the target's network.
Ping of death	ICMP	Brings down a system by sending out more than 65536 ICMP packets.
Open/close	TCP, UDP	Opens and closes connections at a high rate to any port serviced by an external service through inetd. The number of connections allowed is hard coded inside inetd (Internet super daemon, often used to run other services like FTP).
ICMP Unreachable	ICMP	The attacker sends ICMP unreachable packets from a spoofed address to a host. This causes all legitimate TCP connections on the host to be torn down to the spoofed address. This causes the TCP session to retry, and as more ICMP unreachables are sent, a denial-of-service (DoS) condition occurs.
ICMP redirect	ICMP	Causes data overload to the system being targeted.
ICMP Router Discovery Protocol (IRDP)	ICMP	Spoofing IRDP causes fake routing entries to be entered into a Windows machine. IRDP has no authentication. Upon startup, a system running MS Windows 95/98 will always send 3 ICMP Router Solicitation packets to the 224.0.0.2 multicast address. If the machine is NOT configured as a DHCP client, it ignores any Router Advertisements sent back to the host. However, if the Windows machine is configured as a DHCP client, any Router Advertisements sent to the machine will be accepted and processed.
ARP redirect	ARP	Attacks local subnets.
Looping User Datagram Protocol (UDP) ports	UDP	Spoofs two UDP serviceschargen (port 19) and echo (port 7)to send data to each other.
Fraggle	UDP	Same as Smurf, but uses UDP rather than ICMP to broadcast address for amplification.
UDP flood	UDP	Sends large numbers of UDP packets to the target system, thus tying up network resources.
TCP flood	TCP	Repeatedly establishes and abandons TCP connections, enabling a malicious host to tie up significant resources on a server.
UDP reflectors	UDP	All web servers, Domain Name System (DNS) servers, and routers are reflectors, because they will return SYN ACKs or RSTs in response to SYN or other TCP packets; query replies in response to query requests; or ICMP Time Exceeded or Host Unreachable in response to particular IP packets. By spoofing IP addresses from slaves, a massive DDoS attack can be arranged.

Name of Attack	Flooding Capability	Short Description
URL attacks	TCP	Attempts to overload an HTTP server with HTTP bombing (continuous requests for the same homepage or large web page) or by requesting the page with REFRESH to bypass any proxy server. Many of these attacks are not zombie attacks but rather human executedby hundreds simultaneously.
Virtual Private Network (VPN) attacks	TCP	Using specially crafted Generic Routing Encapsulation (GRE) or IP in IP tunnel (IPIP) packets to attack the destination address of a VPN.

Source: Cisco Systems, Inc.

PREV NEXT

DDoS Mitigation Overview

To mitigate DDoS attacks, Cisco offers the Traffic Anomaly Detector and the Guard.

The Traffic Anomaly Detector learns what is a normal traffic pattern for a protected network area, or zone. After the Traffic Anomaly Detector establishes a network traffic baseline, DDoS mitigation policies are constructed and thresholds are tuned in order to configure the Traffic Anomaly Detector to react to various DDoS attack scenarios. In the event of a DDoS attack, the Traffic Anomaly Detector informs the Guard of the DDoS attack. The Guard diverts the traffic from the DDoS attack to the Guard. This DDoS attack diversion is typically implemented by updating the Border Gateway Protocol (BGP) routing table or by other mechanisms including static routes (manual IP routes) and policy-based routes (specific traffic forwarding based upon parameters including application and packet size).

The Guard's ability to update routing tables in the event of an attack allows the Guard to automatically scrub the DDoS attack traffic, while still forwarding or tunneling valid network traffic to the destination zone. The Traffic Anomaly Detector is often deployed upstream from the servers that are being protected in the data center. Figure 2-1 shows the Traffic Anomaly Detector and Guard appliances.

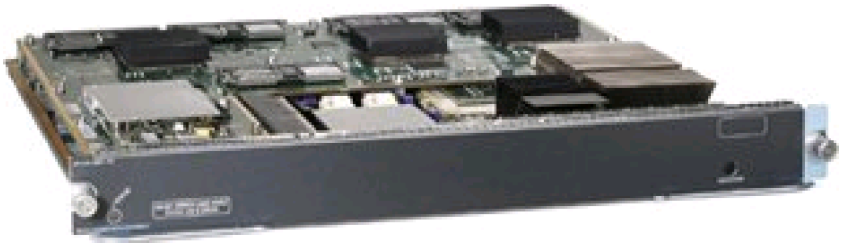
Figure 2-1. Traffic Anomaly Detector and Guard Appliances

Source: Cisco Systems, Inc.

Using Cisco Traffic Anomaly Detector

The two main product options for the Cisco Traffic Anomaly Detector are the appliance and the Traffic Anomaly Detector service module on the Catalyst 6500 and Catalyst 7600 product lines. Figure 2-2 shows the Traffic Anomaly Detector service module.

Figure 2-2. Catalyst 6500/7600 Traffic Anomaly Detector Service Module



Source: Cisco Systems, Inc.

In addition to the Traffic Anomaly Detector, there are several others mechanisms to detect a DDoS attack and inform the Guard of the attack. Some of these mechanisms that detect a DDoS attack and inform the Guard include the DDoS signatures on the intrusion prevention system (IPS) appliances and modules. However, this section focuses on the Traffic Anomaly Detector because this component is frequently deployed and is a very feature-rich component for DDoS mitigation.

The Traffic Anomaly Detector is capable of monitoring gigabit speeds and operates on a copy of the network traffic. This copy of the network traffic is often obtained by using a span port of the Catalyst LAN switch to create a copy of the network traffic. The Traffic Anomaly Detector is designed to monitor the traffic destined to one of more zones. A Zone is a particular server, group of servers, subnet, network, or Internet service provider (ISP) that is being protected from a DDoS attack. The Traffic Anomaly Detector protects a zone by learning the baseline traffic destined to the zone, and then applies policy configuration and threshold tuning to protect the zone from a DDoS attack. The Traffic Anomaly Detector can be configured with command-line interface (CLI) or an easy-to-use web-based device manager (WBM). However, the Traffic Anomaly Detector WBM supports only a subset of the CLI of the Traffic Anomaly Detector.

Configuring the Traffic Anomaly Detector

The Traffic Anomaly Detector must be bootstrapped or configured to allow web-based access to the device. The following CLI commands allow web-based access:

service wbm

permit wbm *ip-addr [ip-mask]*

ip-addr [*ip-mask*] is the IP address of the host the launches the web browser.

Launch the web browser and type the following:

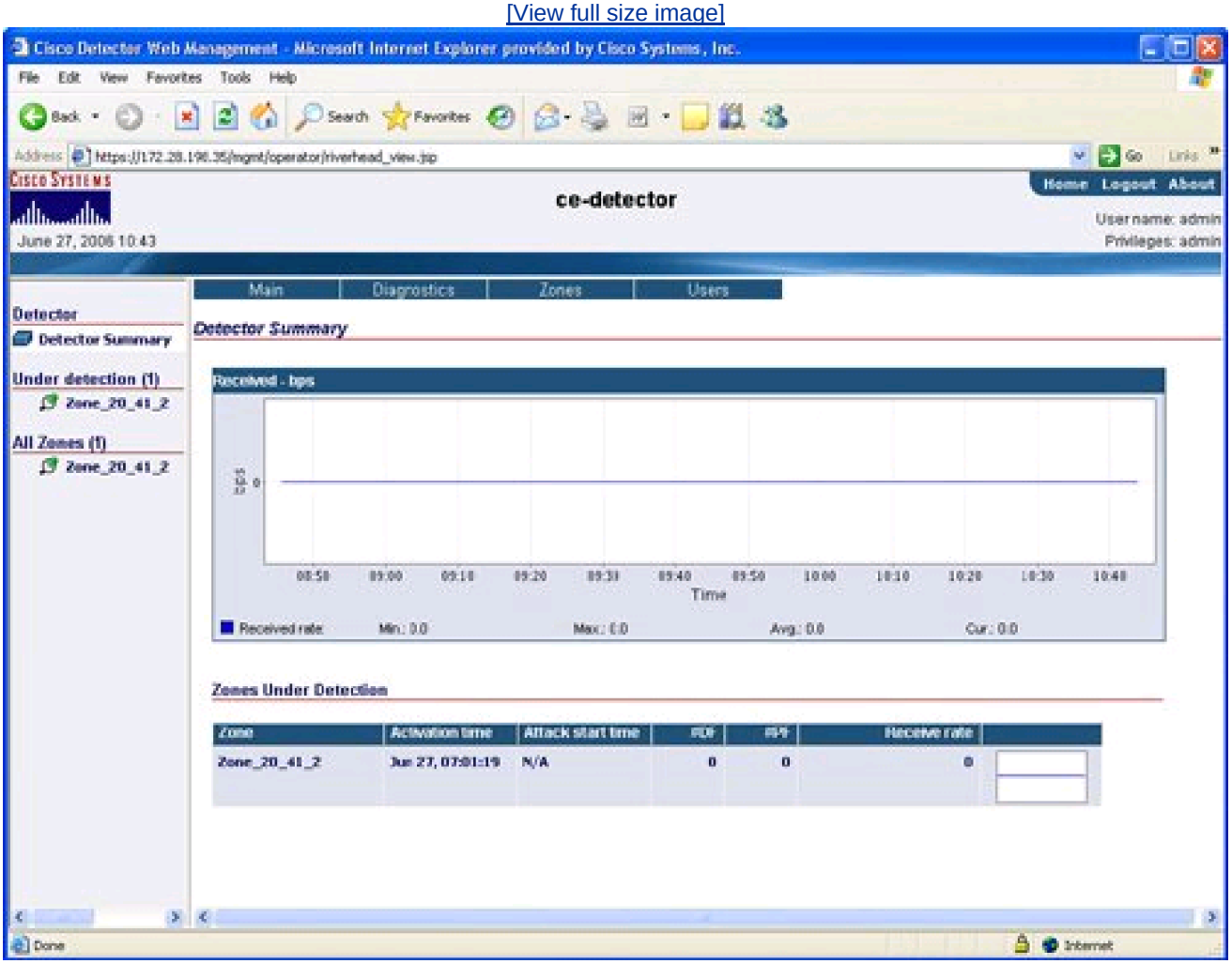
https:// *detector-ip-addr*

detector-ip-addr is the IP address of the Detector.

Enter the username and password for the administrative rights to configure the Traffic Anomaly Detector, and you will see the homepage of the Traffic Anomaly Detector WBM, as shown in Figure 2-3. The Traffic Anomaly Detector WBM features a Detector Summary, which displays the average, minimum, maximum, and current level of network traffic through the Traffic Anomaly Detector in bits per second (bps).

Figure 2-3. Traffic Anomaly Detector WBM Homepage

[View full size image]

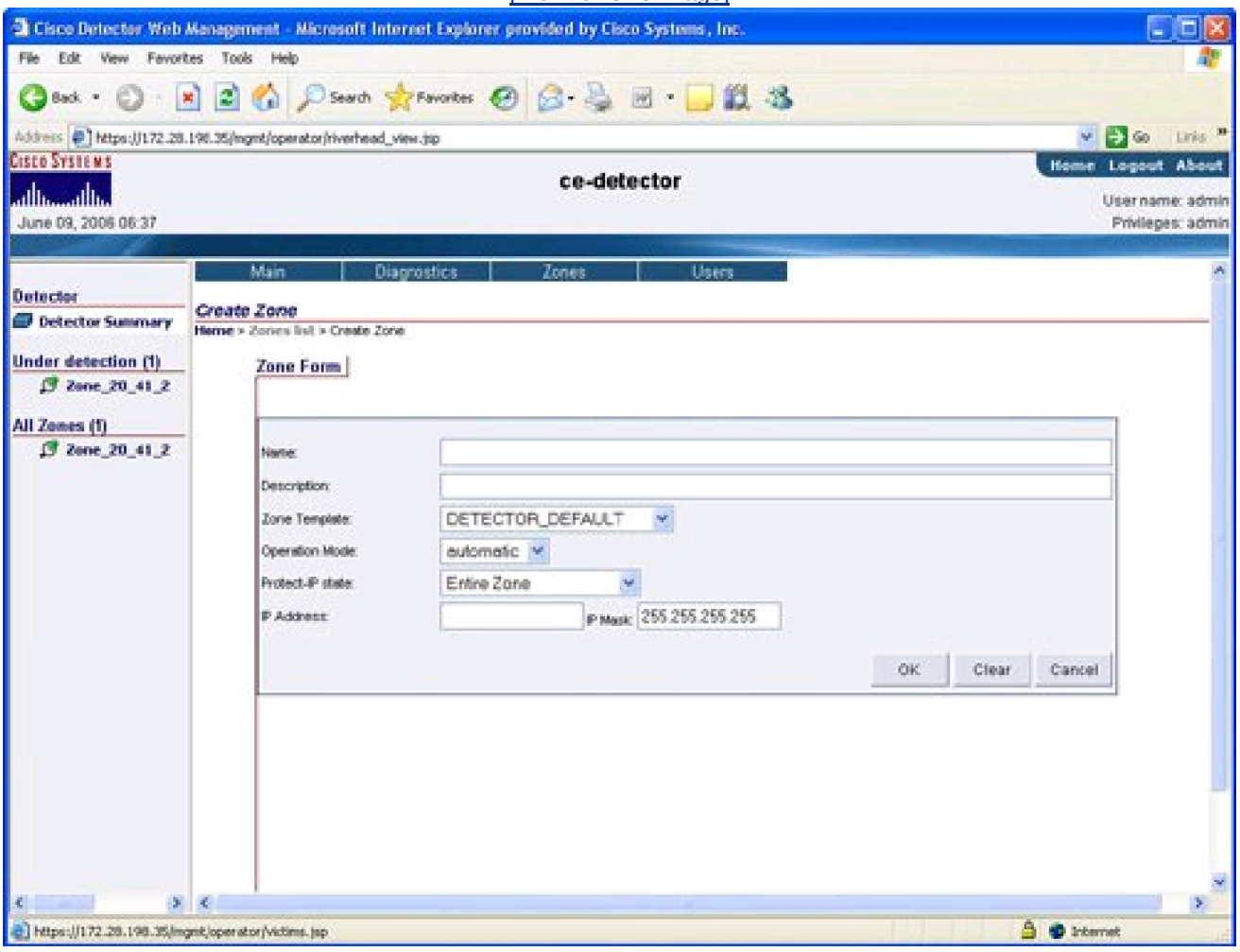


Zone Creation

The Traffic Anomaly Detector attempts to detect a DDoS attack against a particular zone. You can create a zone under the Zones tab by selecting **Create Zone**. Figure 2-4 shows an example of the Create Zone configuration panel.

Figure 2-4. Create Zone Configuration

[View full size image]



You can give a zone a name and template, which contains a list of default DDoS mitigation policies templates to be constructed and tuned for the zone. Default templates are provided to create a base DDoS protection coverage. You can copy and edit these default configuration policies to provide customized configuration policies for more advanced attack protection.

Zones can be created with either a DETECTOR_zone template or a GUARD_zone template. A zone that is created with GUARD_zone template has the ability to be automatically synchronized with the Guard. DETECTOR_zone templates are designed for use when zone information does not need to be synchronized with the Guard.

The Traffic Anomaly Detector can inform the admin of a potential DDoS attack, or a Traffic Anomaly Detector can automatically inform or trigger the Guard to mitigate the attack. Select the automatic operation mode for the Traffic Anomaly Detector to inform the Guard to trigger or automatically protect against the known attack so that the network can be self-defending against a DDoS attack without user

intervention.

Caution

A self-defending network is a very powerful concept. However, be aware that a self-defending network can automatically configure network devices, reroute and deny network traffic, and may result in false positives. A *false positive* is valid network traffic that was dropped, delayed, or otherwise affected due to an incorrect classification that the valid network traffic was in fact part of a network attack.

To configure the IP address of the remote Guard that will protect the Traffic Anomaly Detector's zone, you must use CLI. Example 2-1 shows an example of a base Traffic Anomaly Detector configuration file that details how to configure the IP address of the remote Guard for the Traffic Anomaly Detector. Network connections between the Traffic Anomaly Detector and the remote Guard are secured with Secure Shell (SSH) or Secure Socket Layer (SSL). SSH keys must be generated and applied to both devices to complete the SSH connection. The Traffic Anomaly Detector can generate a private-public SSH key pair and distribute its public key to every Guard listed in the remote-guards list. Multiple Cisco Traffic Anomaly Detectors can report to the same Cisco Guard for a distributed architecture.

Example 2-1. CLI Configuration of the Cisco Traffic Anomaly Detector Service Module

```
hostname ce-detector
timezone America/Los_Angeles

history logs 7
history reports 30
no export packet-dump
boot reactivate-zones
tacacs-server timeout 0
tacacs-server key (null)
no tacacs-server first-hit
aaa authentication login local
aaa authentication enable local
no aaa authorization exec tacacs+
username riverhead dynamic encrypted $1$LVZopVja$8kSY10uykJaSYT325wDDk/
username cleanpipes adm1n09 encrypted 18KLWZvg0DP02
enable password level admin encrypted 18xVodWfkJfOk
enable password level config encrypted 84QiLbAV5gfOA
enable password level dynamic encrypted 161R6GsPeIPWs

snmp community public

snmp trap-dest 172.28.198.22 public debugging
interface eth0
  ip address 172.28.198.35 255.255.255.0
  mtu 1500
  no shutdown
exit
interface giga0
  mtu 1500
  no shutdown
```

```
exit
interface giga1
  mtu 1500
  no shutdown
exit

default-gateway 172.28.198.1
service ntp
service wbm
service internode-comm
service snmp-trap

permit wbm  17.28.198.100
permit ssh  17.28.198.100
permit internode-comm 172.28.198.34

ntp server 171.68.10.150

logging host 172.28.198.22
logging trap informational
logging facility local7


zone Zone_20_41_2 GUARD_DEFAULT interactive

 no learning-params periodic-action
 learning-params threshold-selection max-thresholds
 learning-params threshold-tuned
 learning-params sync accept
 learning-params sync remote-activate
 no packet-dump auto-capture
 packet-dump disk-space 2048
 ip address 20.41.2.0 255.255.255.0

 remote-guard ssl 172.28.198.34
 protect-ip-state  entire-zone
 no bypass-filter *
 no flex-content-filter *



admin@ce-detector-conf#conf t
admin@ce-detector-conf#remote-guard
  ssh                 :  Secure shell
  ssl                 :  Secure socket layer

admin@ce-detector-conf#remote-guard ssl
  <remote-guard-address>:  IP address in dotted-decimal notation (A.B.C.D)
```

Traffic Anomaly Detector Zone Filters

Zone filters enable mirrored network traffic to be managed by the Detector. Zone filters enable the Traffic Anomaly Detector to drop traffic prior to inspection by the Traffic Anomaly Detector. Zone filters also enable the Traffic Anomaly Detector to analyze network traffic

for spikes or anomalies and notify the Guard of these network traffic abnormalities. There are four types of filters:

- **User** User filters are assigned to a Zone that is created with the GUARD_zone template. User filters are used to provide a first layer of defense against the attack until the Guard has analyzed the attack and until the Guard can create custom, dynamic filters for the network attack.
- **Bypass** Bypass filters restrict certain network traffic flows from being directed to the Detector.
- **Flex** Flex filters support the ability to count a specific traffic flow.
- **Dynamic** The Detector creates dynamic filters as the result of an analysis of a traffic flow. The dynamic filter is the mechanism to activate a remote Guard to protect a zone, or an IP address in a zone, in the event of a detected DDoS attack for a specific IP traffic flow. Dynamic filters are temporary and are expected to expire at the end of a DDoS attack.

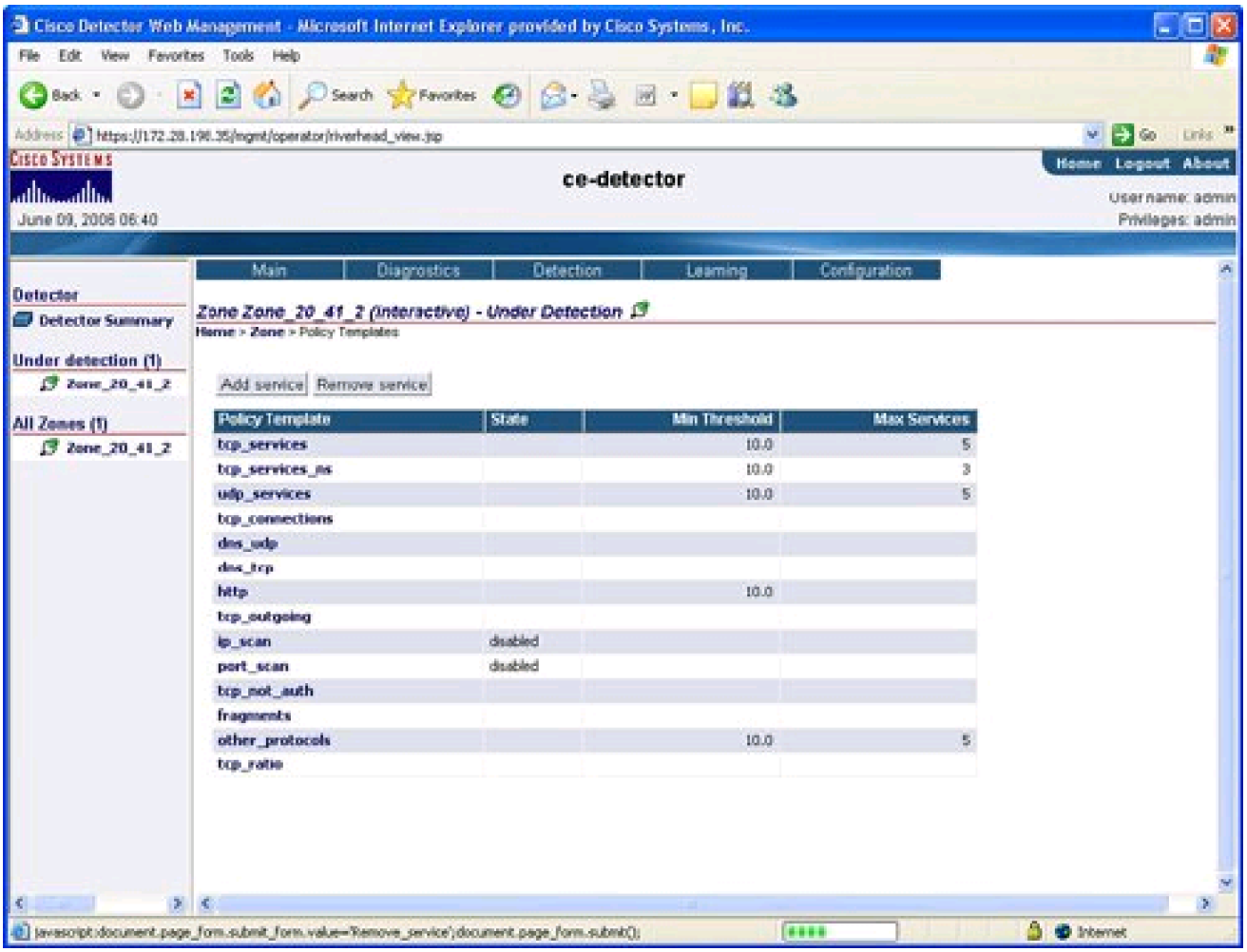
You can configure user, bypass, and flex filters with the Traffic Anomaly Detector WBM. You can create these filters by selecting the Configuration tab for a specific Zone.

Policy Template

A *policy template* is a collection of information that is leveraged during the learning phase of the zone. The policy template provides the basis for creating the zone's detection policies after the normal traffic baseline is established during the learning phase. To configure a policy template for a zone, go to Configuration > Policy template as shown in Figure 2-5.

Figure 2-5. Policy Template Configuration

[View full size image]



You can select and edit the policy templates. The primary parameters or options for each policy template are

- **State** State allows the user to enable or disable/turn-off a policy template. It is strongly cautioned that disabling/turning-off a default policy template can compromise the DDoS protection of a zone because there may be no policies to protect the network traffic that would have been specified in the policy template.
- **Minimum threshold** Minimum threshold refers to packets-per-second (pps) or total number of network connections. The Guard will not create a dynamic filter to mitigate an attack until the traffic flow exceeds the minimum threshold.
- **Maximum services** Maximum services refers to the number of port numbers or service ports that are protected by the Guard for that policy template. Additional memory on the Traffic Anomaly Detector is required for each additional service in the policy templates for each Zone.

Learning Phase

A zone must enter a learning phase in order to establish a baseline of normal network traffic and to provide a mechanism to construct the zone's active policies from the base policy template. The learning phase consists of two processes:

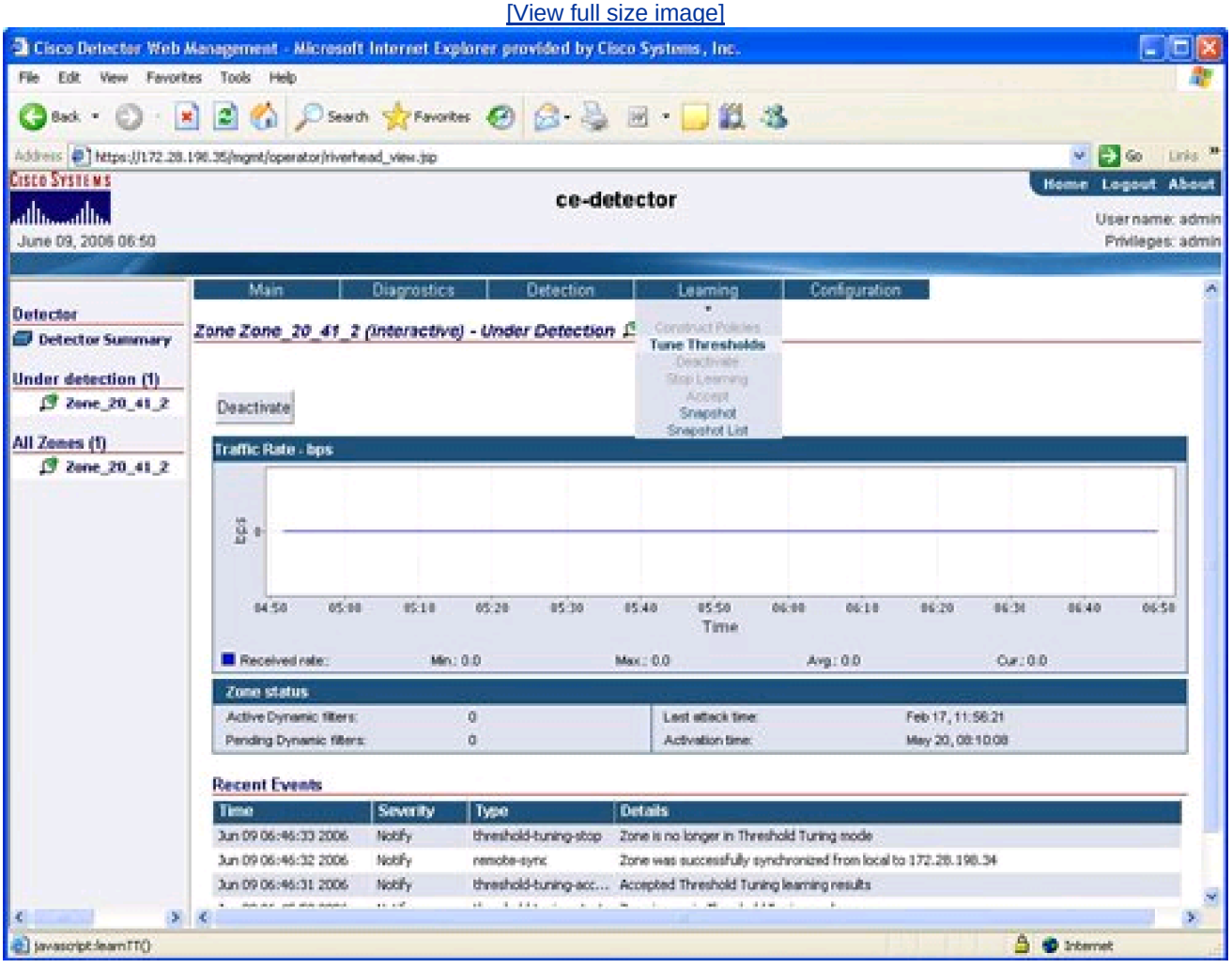
- Policy construction
- Threshold tuning

In the policy construction phase, zone policies are created from the base template. It is recommended that the policy construction phase run for at least two hours to ensure a proper baseline.

The second phase is the threshold-tuning phase. During this tuning phase, the Traffic Anomaly Detector creates a minimum threshold value for the relevant zone policies. This threshold value is used to indicate the minimum level of network traffic for specific network flows that would indicate a potential DDoS attack on the zone. It is recommended that the threshold-tuning phase run for at least 24 hours to improve the computation of the minimum threshold values for each service that will constitute a possible DDoS attack. Zones that were created with the GUARD_zone template cannot initiate the policy construction phase from the Traffic Anomaly Detector. You can initiate the policy construction and the phases for zones created with the DETECTER_zone template through the Traffic Anomaly Detector WBM, as shown in Figure 2-6.

Figure 2-6. Initiating the Learning Phase

[View full size image]



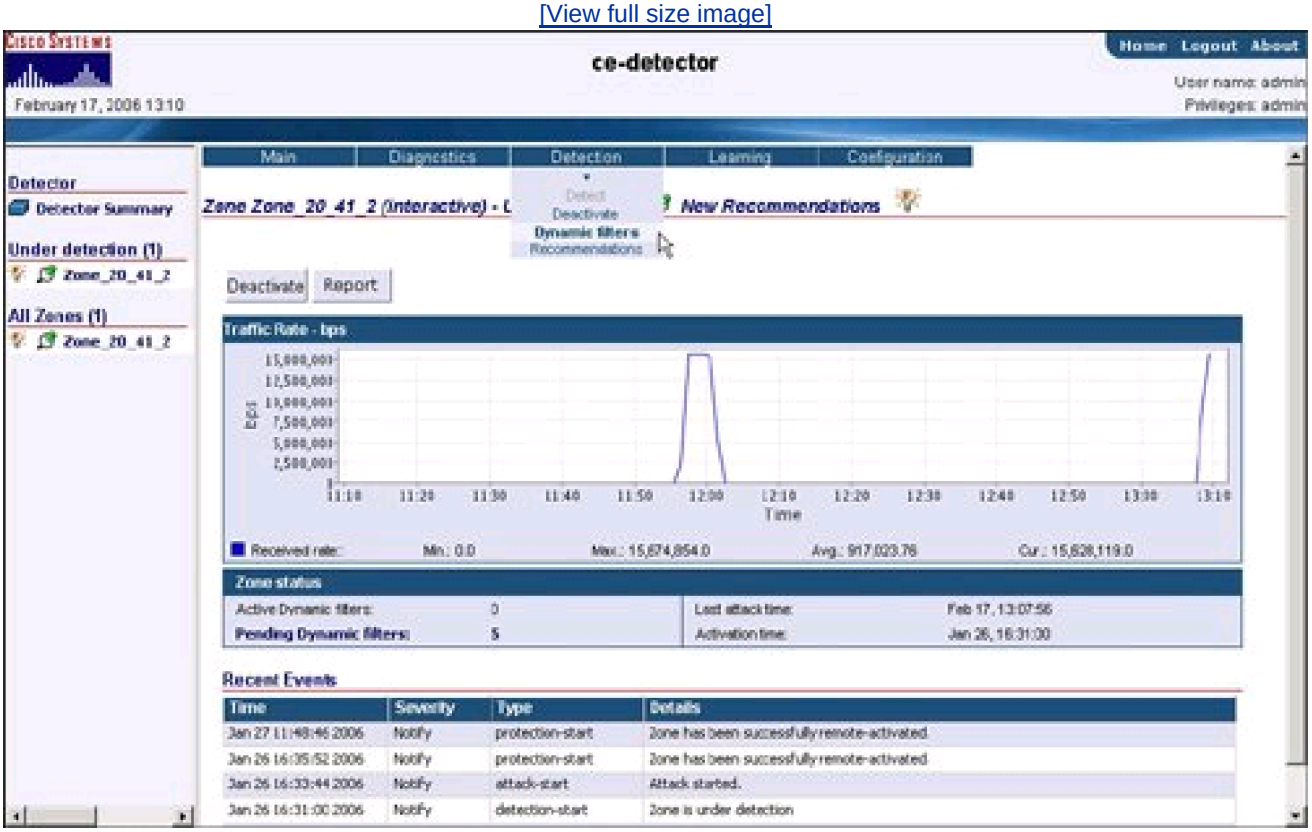
Detecting and Reporting Traffic Anomalies

After you have completed the learning phase, constructed zone policies, and tuned the threshold values, you can enable the zone to detect a traffic anomaly or potential DDoS attack. Figure 2-7 shows an example of the Detection tab in the Traffic Anomaly Detector WBM.

Figure 2-7 also displays the location to view any generated dynamic filters. Dynamic filters are created by the Traffic Anomaly Detector during the detection of a potential DDoS attack. These dynamic filters created by the Traffic Anomaly Detector are used to create a syslog or are used as a trigger to activate the remote Guard to scrub the network traffic.

Figure 2-7. Zone Detection

[View full size image]



The Traffic Anomaly Detector WBM also offers extensive diagnostic information, including counters and attack reports. Figure 2-8 shows an example of an attack report, which indicates what attacks were detected and when they were detected. Attack reports can also be exported in text and XML format.

Figure 2-8. Attack Reports

[View full size image]

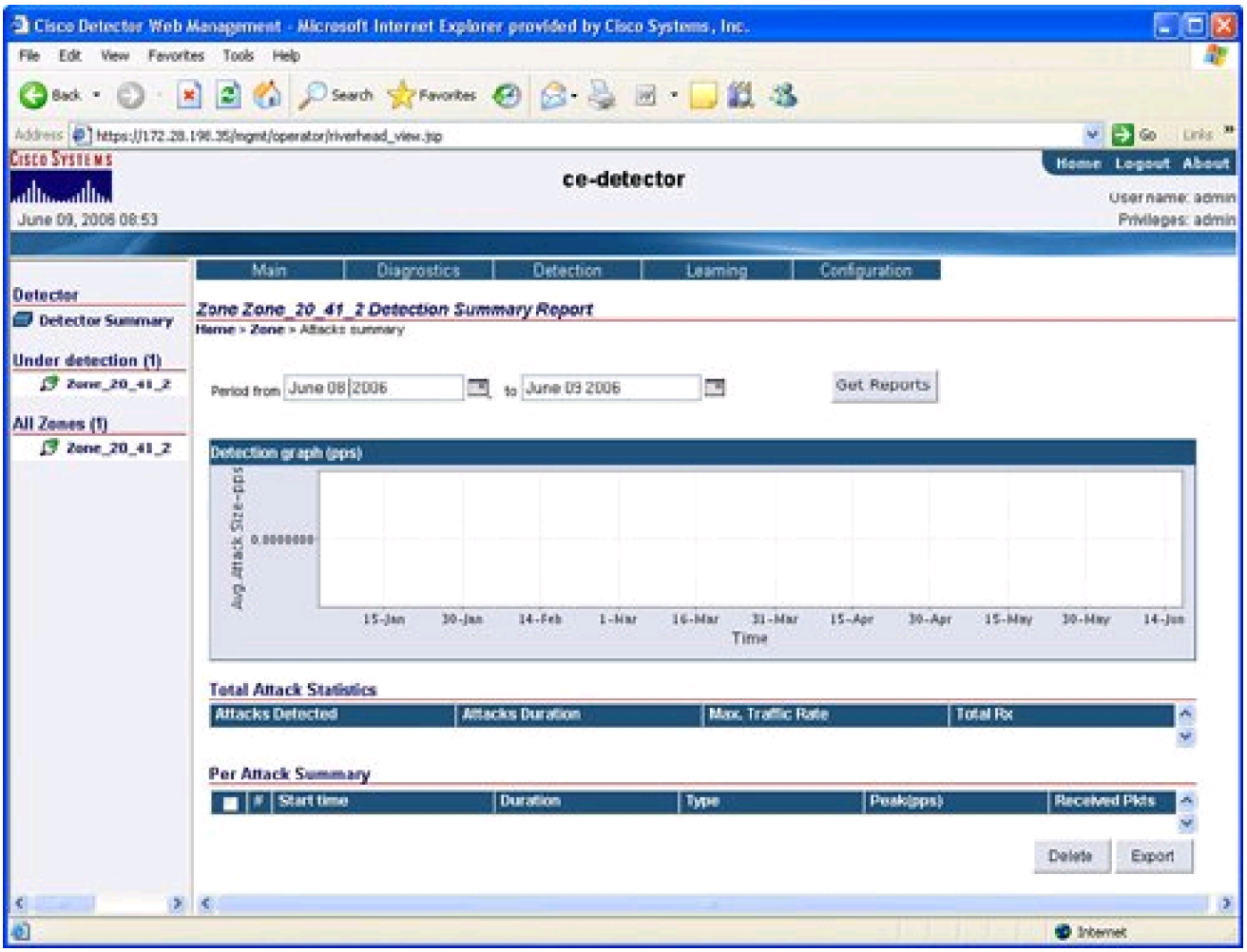
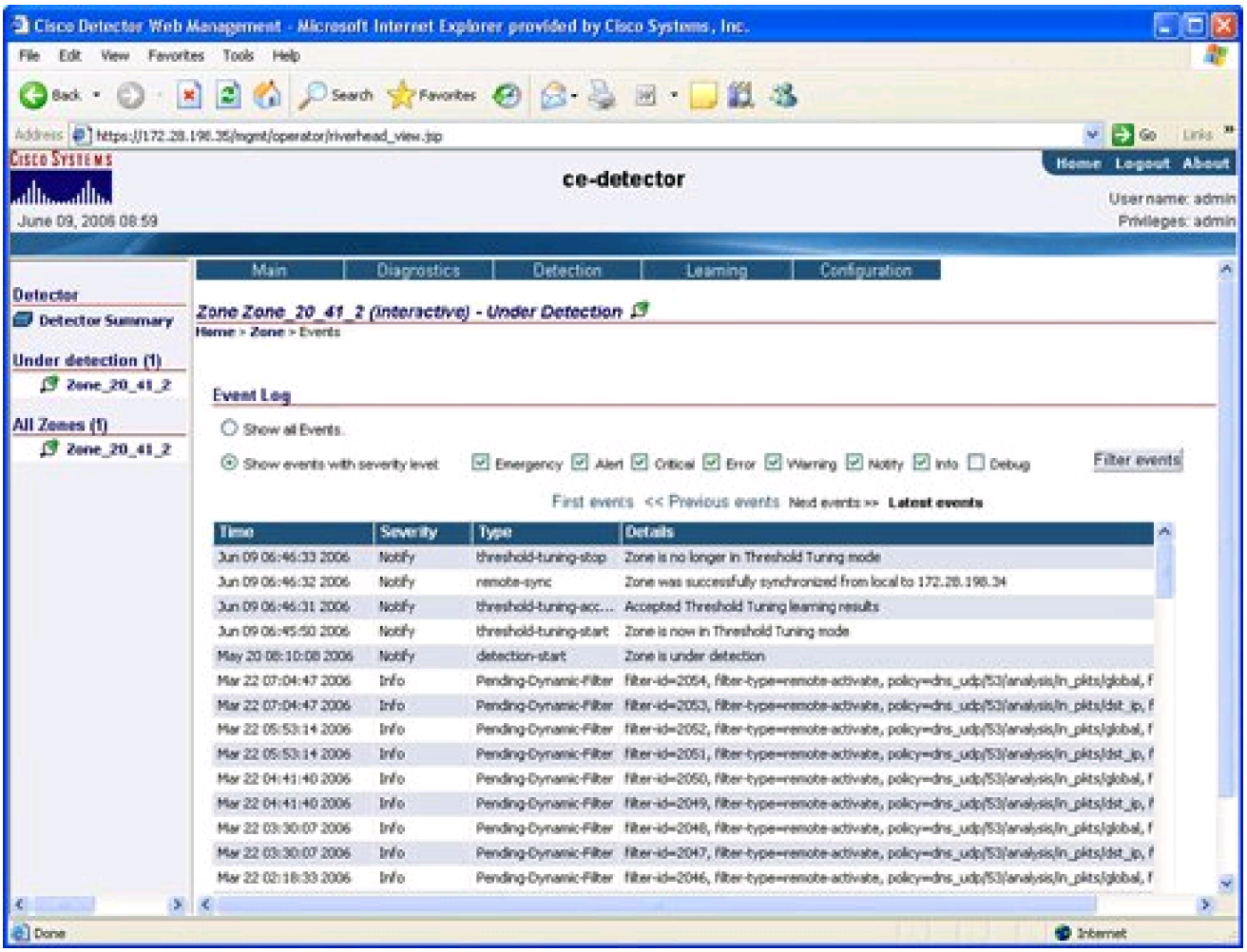


Figure 2-9 shows an example of the diagnostic event log with details on Traffic Anomaly Detector activity, warnings, and pending dynamic filters.

Figure 2-9. Event Logs

[View full size image]


Cisco Detector Web Management - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.28.198.35/mgmt/operator/riverhead_view.jsp
Go Links
Cisco Systems
ce-detector
Home Logout About
June 09, 2006 08:59
User name: admin
Privileges: admin
Main Diagnostics Detection Learning Configuration
Detector
Detector Summary
Under detection (1)
Zone_20_41_2
All Zones (1)
Zone_20_41_2
Zone Zone_20_41_2 (interactive) - Under Detection
Home > Zone > Events
Event Log
Show all Events
Show events with severity level Emergency Alert Critical Error Warning Notify Info Debug
Filter events
First events << Previous events Next events >> Latest events
Time Severity Type Details
Jun 09 06:46:33 2006 Notify threshold-tuning-stop Zone is no longer in Threshold Tuning mode
Jun 09 06:46:32 2006 Notify remote-sync Zone was successfully synchronized from local to 172.28.198.34
Jun 09 06:46:31 2006 Notify threshold-tuning-acc... Accepted Threshold Tuning learning results
Jun 09 06:45:50 2006 Notify threshold-tuning-start Zone is now in Threshold Tuning mode
May 20 08:10:08 2006 Notify detection-start Zone is under detection
Mar 22 07:04:47 2006 Info Pending-Dynamic-Filter filter-id=2054, filter-type=remote-activate, policy=dns_udp/53/analysis/in_pkts/global, f
Mar 22 07:04:47 2006 Info Pending-Dynamic-Filter filter-id=2053, filter-type=remote-activate, policy=dns_udp/53/analysis/in_pkts/dst_ip, f
Mar 22 05:53:14 2006 Info Pending-Dynamic-Filter filter-id=2052, filter-type=remote-activate, policy=dns_udp/53/analysis/in_pkts/global, f
Mar 22 05:53:14 2006 Info Pending-Dynamic-Filter filter-id=2051, filter-type=remote-activate, policy=dns_udp/53/analysis/in_pkts/dst_ip, f
Mar 22 04:41:40 2006 Info Pending-Dynamic-Filter filter-id=2050, filter-type=remote-activate, policy=dns_udp/53/analysis/in_pkts/global, f
Mar 22 04:41:40 2006 Info Pending-Dynamic-Filter filter-id=2049, filter-type=remote-activate, policy=dns_udp/53/analysis/in_pkts/dst_ip, f
Mar 22 03:30:07 2006 Info Pending-Dynamic-Filter filter-id=2048, filter-type=remote-activate, policy=dns_udp/53/analysis/in_pkts/global, f
Mar 22 03:30:07 2006 Info Pending-Dynamic-Filter filter-id=2047, filter-type=remote-activate, policy=dns_udp/53/analysis/in_pkts/dst_ip, f
Mar 22 02:18:33 2006 Info Pending-Dynamic-Filter filter-id=2046, filter-type=remote-activate, policy=dns_udp/53/analysis/in_pkts/global, f
Done
Internet

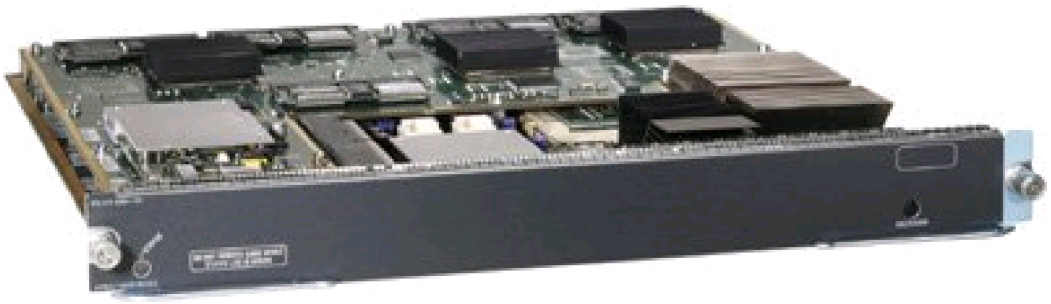
PREV NEXT

Configuring Cisco Guard

The Cisco Guard is the component of the DDoS mitigation solution that receives the network attack traffic for a zone from the Traffic Anomaly Detector. The Guard scrubs or removes the attack traffic and forwards or reinjects the good (nonattack) traffic back to the destination zone. The Guard is often deployed upstream at the ISP/backbone layer and can protect large network segments. A single Guard can protect more than one zone simultaneously as long as there are no overlapping IP addresses in multiple zones. A native self-protection mechanism is also contained in the Guard to protect the Guard itself from becoming the target of a DDoS attack.

The Guard is available as both an appliance and a Catalyst 6500/7600 service module. A picture of the Anomaly Guard service module is shown in Figure 2-10. The Anomaly Guard service module, unlike the appliance, contains no onboard interfaces. A single Catalyst chassis can house both the Anomaly Guard and Traffic Anomaly Detector service module.

Figure 2-10. Catalyst 6500/7600 Anomaly Guard Service Module



Source: Cisco Systems, Inc.

Like the Traffic Anomaly Detector, the Guard also features an easy-to-use WBM. The Guard's WBM is similar in philosophy to that of the Traffic Anomaly Detector's WBM in that the Guard WBM supports only a subset of the CLI that is implemented on the Guard. The Guard WBM features focus around the areas of zone configuration, status, and reports. Other Guard features, including zone traffic diversion, must be configured with the CLI since they are not supported in the Guard WBM.

Configuring and using the Guard includes the following:

- Bootstrapping
- Zones creation and synchronization
- Zone filters
- Zone traffic diversion
- Learning Phase
    - Policy construction
    - Threshold tuning

- Activating zone protection
- Attack reports

Bootstrapping

The process to bootstrap and initialize the Guard is similar to the process described previously for the Traffic Anomaly Detector in the Configuring the Traffic Anomaly Detector section. The Guard must have an interface configured, and the WBM service should be started and permitted with the Guard CLI in order to be managed by the Guard WBM.

Zone Creation and Synchronization

The zone that is to be protected must be either configured on the Guard or synchronized from the Traffic Anomaly Detector. Zones that are configured on the Guard can be configured in a manner similar to that described previously in the Zone Creation section for the Traffic Anomaly Detector. However, many users will instead want to synchronize the zones that were already created on the Traffic Anomaly Detector using the GUARD_zone template. This process to synchronize the zones from the Traffic Anomaly Detector must be performed with Guard CLI because the zone synchronization feature is not supported in the Guard WBM.

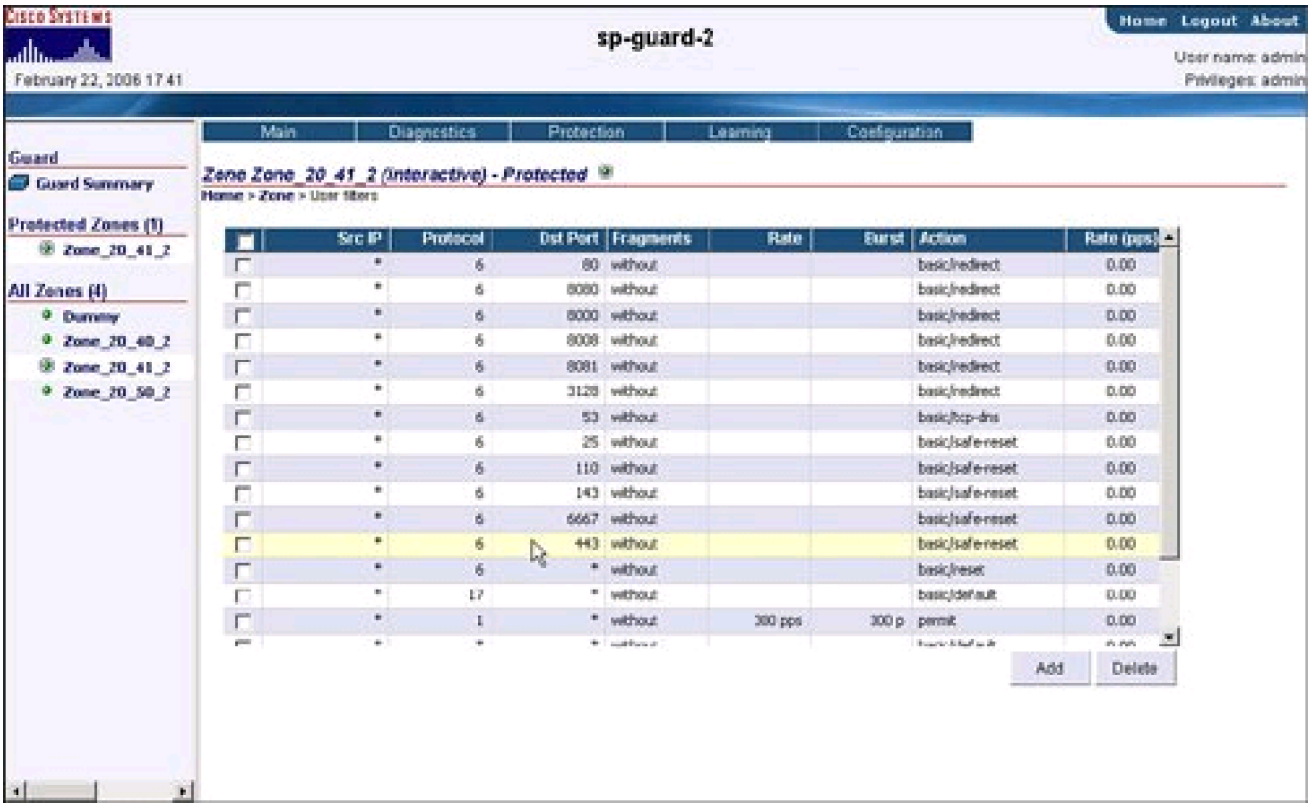
Cisco Guard Zone Filters

The Guard features user, bypass, flex, and dynamic filters. These filter types were described previously in this chapter in the section "Traffic Anomaly Detector Zone Filters" In the event of a suspected DDoS attack, the Guard generates dynamic filters. These dynamic filters are temporary and expire after the end of the DDoS attack. These dynamic filters instruct the Traffic Anomaly Detector on what action to perform on the suspected network attack traffic.

The Guard can also create a default set of user filters to provide a base of protection until additional dynamic filters are created after the analysis of network attack traffic. The user filters are displayed in Figure 2-11, which illustrates the user filters for a specific zone on the Guard.

Figure 2-11. Guard User Filter

[View full size image]

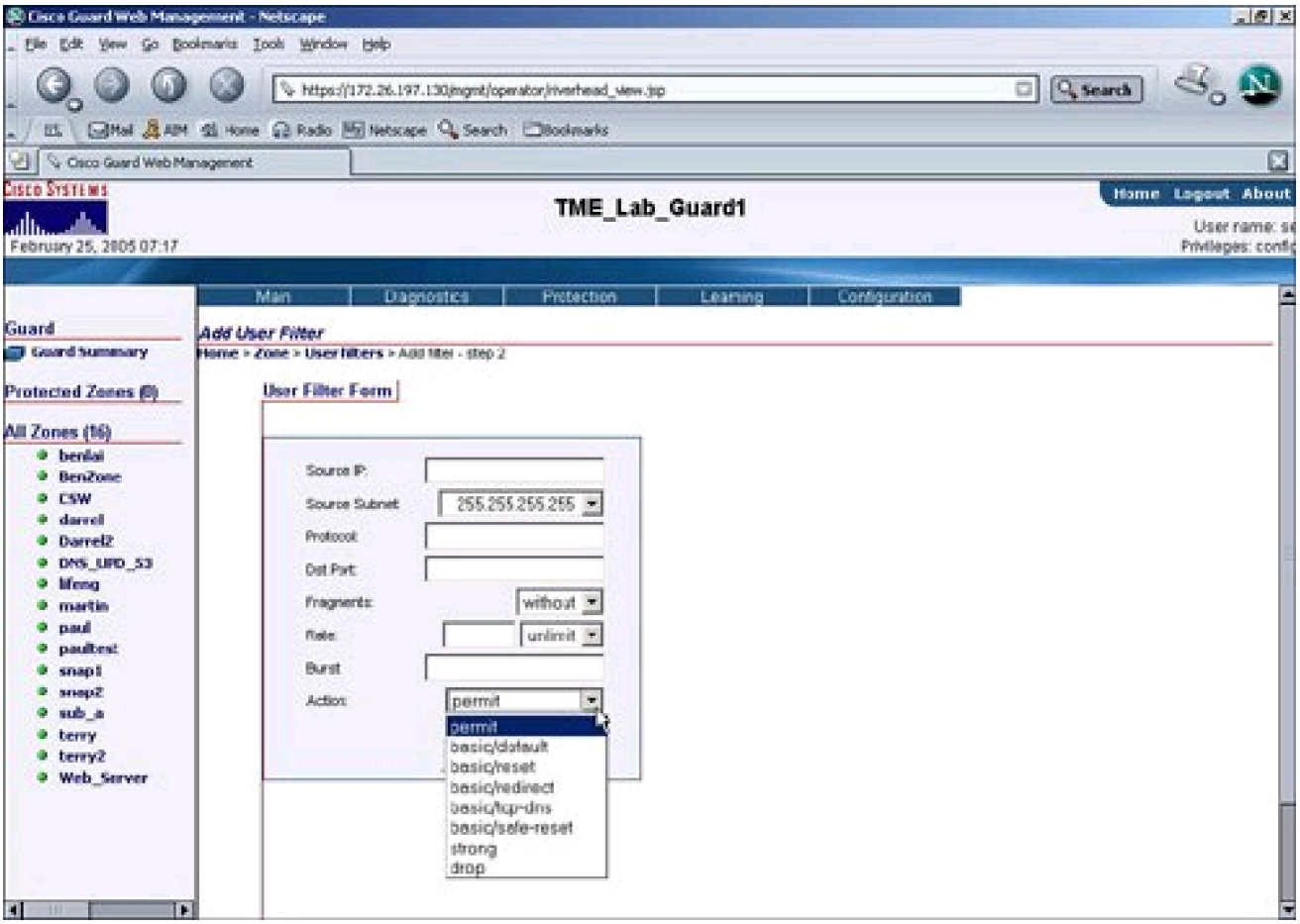


User filters can also be created manually on the Guard for a user to customize how the Guard should process a specific network traffic flow. Figure 2-12 provides an example of the options available when configuring a User Filter. The options for the User Filter include the following:

- **Source IP** Includes any wildcard (*)
- **Source Subnet** Select from drop-down
- **Protocol** Includes any wildcard (*)
- **Dst Port** Refers to the Destination Port (*)
- **Fragments** Includes With, Without, or *
- **Rate** Limits traffic to specified rate
- **Burst** Refers to the Burst traffic limit
- **Action** Includes parameters to permit traffic flow to avoid Guard antispoofing and antizombie protection, authenticate, and drop traffic

Figure 2-12. User Filter Creation

[View full size image]



Zone Traffic Diversion

Zone traffic diversion is composed of two phases:

- Divert potential DDoS traffic destined to the zone.
- Inject the scrubbed or good network traffic back from the Guard to the zone.

In the first phase, BGP routing updates are one of the most common mechanisms used to divert attack traffic from the router to the Guard for scrubbing. The Guard achieves this traffic diversion by sending a BGP update to the router to indicate that the next-hop for the zone is the Guard itself. This BGP announcement from the Guard contains a more specific prefix to ensure that the Guard is the best path for the next-hop to the zone. This BGP announcement from the Guard is often sent with a no export and no community string option to ensure that this BGP announcement is not propagated to other routes within the network.

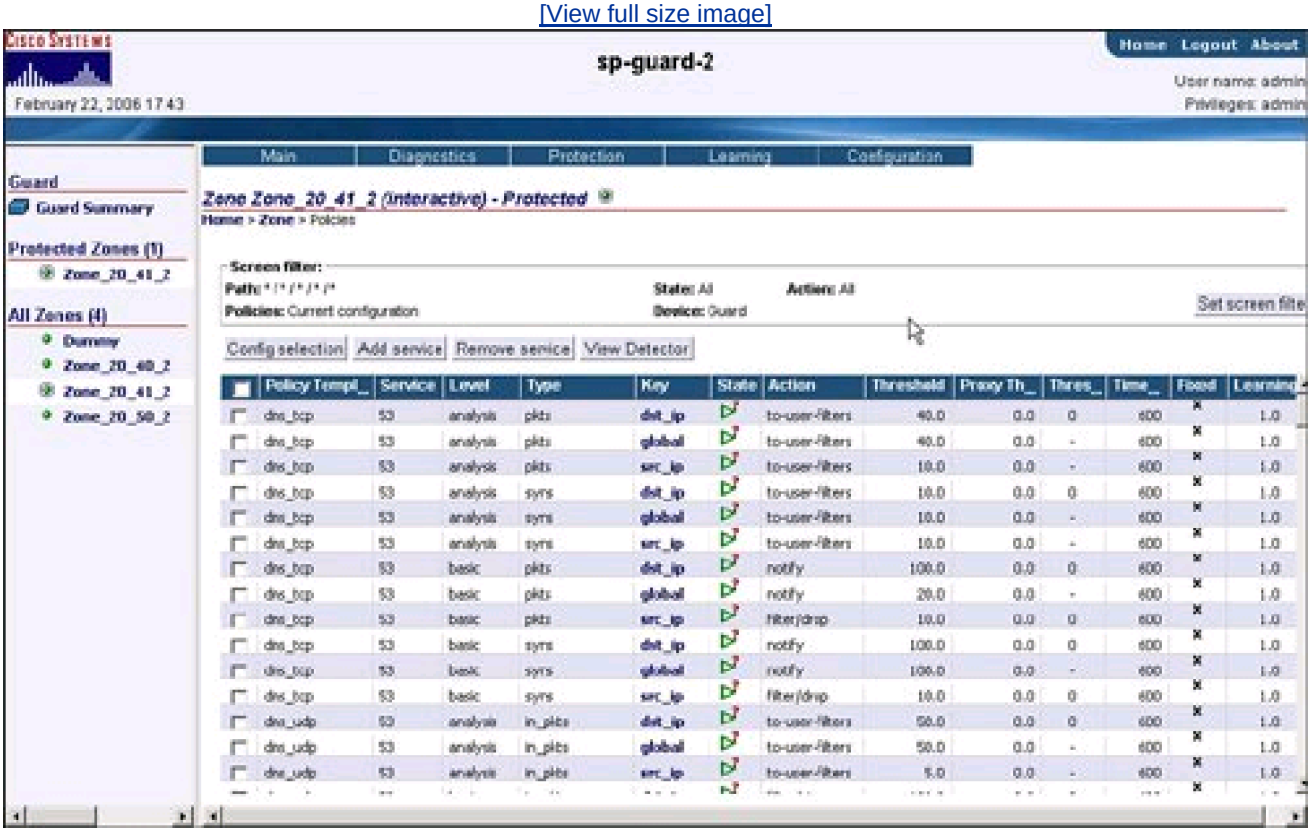
For the second phase of traffic diversion, several traffic forwarding mechanisms, including next-hop router discovery, policy-based routing, VPN routing and forwarding (VRF), VLANs and GRE/IPIP tunnels, can be used to inject the scrubbed traffic back to the destination zone. Both the process to divert the network attack traffic to the Guard and reinject the scrubbed traffic back to the zone must be configured with CLI as they are not supported by the Guard WBM. Zone traffic diversion must be configured with CLI prior to initiating the learning phase for policy creation and threshold tuning.

Learning Phase

The Guard undergoes a learning phase similar to the learning phase described previously for the Traffic Anomaly Detector. The learning phase is composed of a policy construction phase and a threshold-tuning phase. Figure 2-13 displays the policies for the dns_tcp and dns_udp services for a specific zone on the Guard WBM. Both the Traffic Anomaly Detector and the Guard WBM feature the ability to cross-launch the policy display in the Guard and Traffic Anomaly Detector WBM for additional comparison purposes.

Figure 2-13. Display of Policy for a Zone on the Guard

[View full size image]

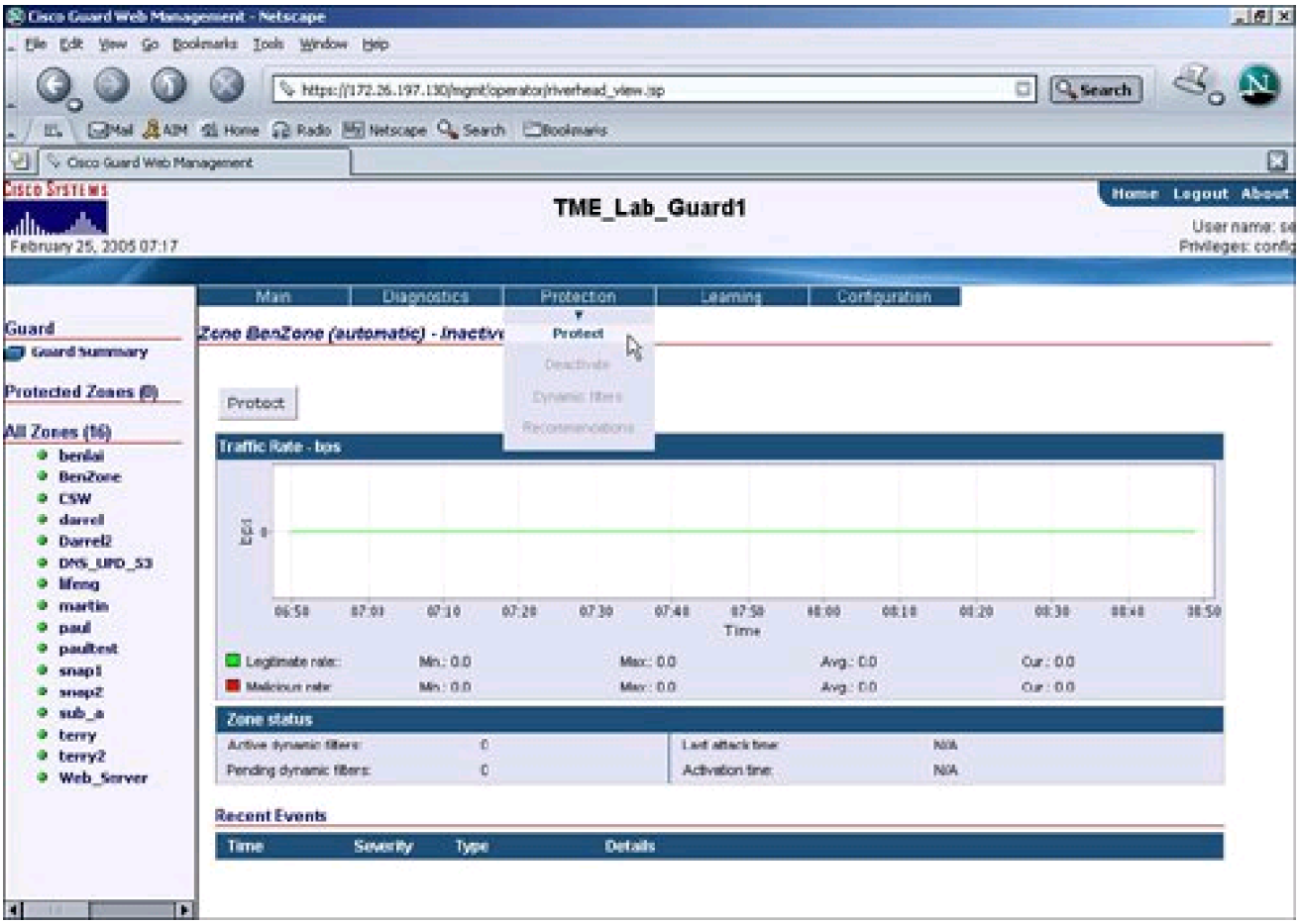


Activating Zone Protection

A zone must be placed into protect mode after the zone configuration, policy construction, threshold tuning, and traffic diversion configuration has been completed. A zone can be automatically placed into protect mode by a trigger from the Traffic Anomaly Detector during a DDoS attack. The trigger from the Traffic Anomaly Detector can indicate whether the entire zone should be placed into protect mode or if a specific IP address in a zone should be placed into protect mode by the creation of a subzone. You can also manually place a zone in protect mode through the Protection tab in the Guard WBM, as shown in Figure 2-14.

Figure 2-14. Placing a Zone in Protect Mode

[View full size image]

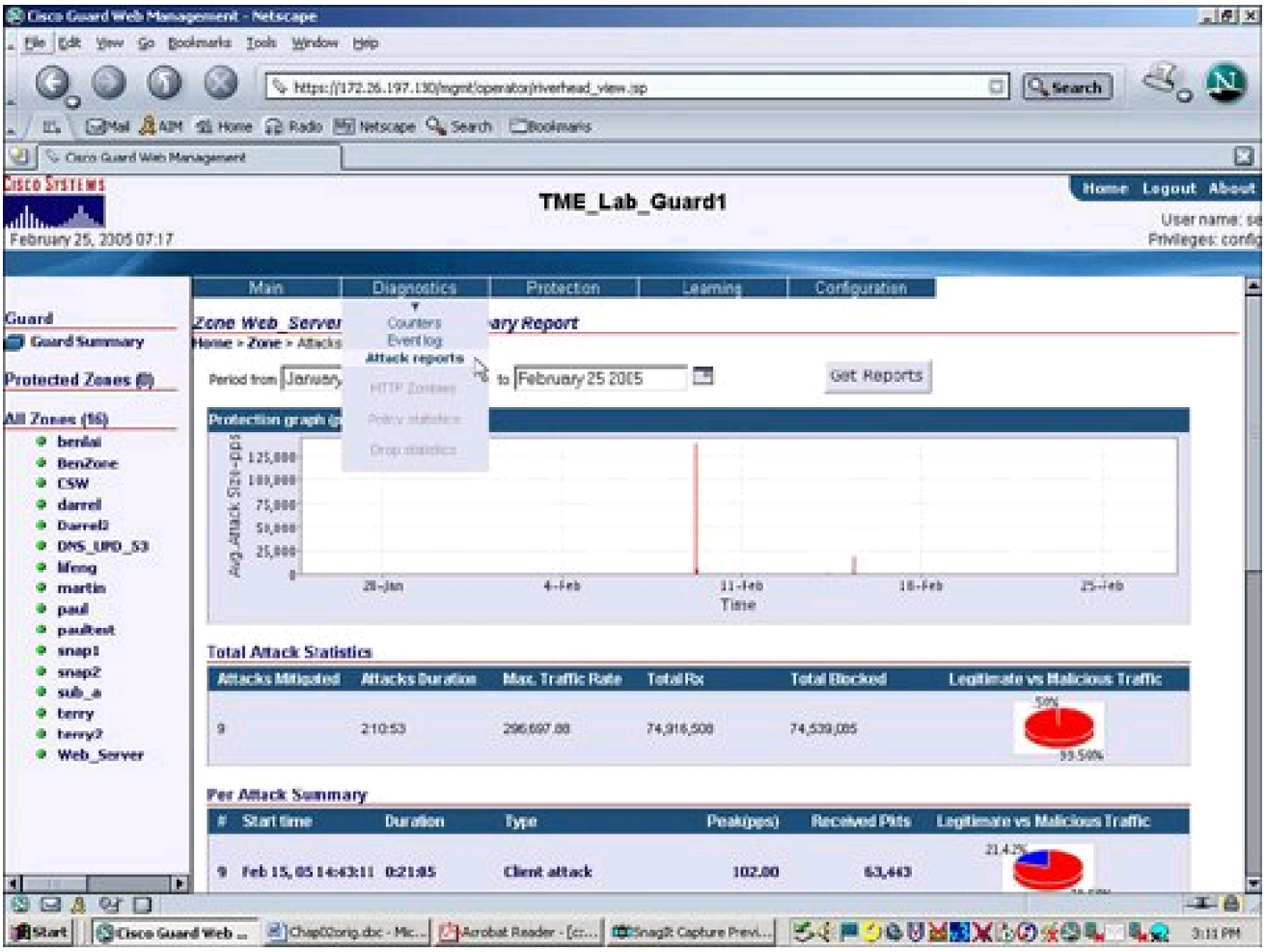


Generating Attack Reports

You can generate an extensive list of attack reports from the Guard WMB. These attack reports include metrics on the number of mitigated attacks and a per-attack summary with a breakdown of legitimate versus malicious network traffic. Figure 2-15 displays the beginning of an attack report with total attack statistics.

Figure 2-15. Total Attack Statistics

[View full size image]



Like the Traffic Anomaly Detector, these attack reports on the Guard are also exportable in both text and XML format.

PREV NEXT

Summary

DDoS attacks are an attempt to prevent valid users from using network resources by flooding the network. This flooding of the network is often performed by hundreds or thousands of compromised zombie computers. Cisco DDoS mitigation is composed of two key components: the Traffic Anomaly Detector and the Guard. Both the Traffic Anomaly Detector and the Guard have a subset of their CLI that is managed by a Traffic Anomaly Detector WBM and a Guard WBM.

The Traffic Anomaly Detector and Guard combine to form a comprehensive solution that protects a zone. A zone can be an IP address, subnet, network, or ISP. The Traffic Anomaly Detector and Guard participate in a learning phase that creates a baseline of valid network traffic for each zone. This learning phase is composed of a policy creation phase to create policies to protect the zone and a threshold-tuning phase. The threshold-tuning phase creates minimum threshold values for each configured protocol that are based on the sample network traffic observed during the learning phase. Once network traffic for a specific application exceeds the tuned threshold, the Guard can create a dynamic filter or leverage a user filter to attempt to protect the zone against the DDoS attack. The specific DDoS attack traffic for that zone is diverted to the Guard, often with a BGP routing update mechanism. This DDoS traffic is then scrubbed by the Guard and reinjected back to the zone, often with a tunneling or VLAN mechanism. Both the Traffic Anomaly Detector and the Guard WBM features a rich-set of status and attack reports to visualize the DDoS attack and mitigation process for the protected zone.

References

Cisco Systems, Inc. DDoS Attack Prevention.http://www.cisco.com/en/US/netsol/ns480/networking_solutions_sub_solution_home.html

Cisco Systems, Inc. Cisco Traffic Anomaly Detector User Guide.
http://cisco.com/application/pdf/en/us/guest/products/ps5887/c2001/ccmigration_09186a00803bd0d8.pdf

Cisco Systems, Inc. Cisco Traffic Anomaly Detector Web-Based Management User Guide.
http://cisco.com/application/pdf/en/us/guest/products/ps5887/c2001/ccmigration_09186a00802d7255.pdf

Cisco Systems, Inc. Cisco Traffic Anomaly Detector Web-Based Management User Guide (Software Version 5.0).
http://www.cisco.com/en/US/products/hw/modules/ps2706/products_module_configuration_guide_chapter09186a00804bef24.html

Cisco Systems, Inc. Cisco Guard Configuration Guide (Software Version 3.1(0)).
http://www.cisco.com/en/US/products/ps5888/products_configuration_guide_book09186a00803bed03.html

Cisco Systems, Inc. Cisco Guard Web-Based Management User Guide (Software Version 3.1(0)).
http://www.cisco.com/en/US/products/ps5888/products_configuration_guide_book09186a00802d1baf.html

Cisco Systems, Inc. Cisco Anomaly Guard Module Web-Based Management Configuration Guide, Glossary.
http://www.cisco.com/en/US/products/hw/modules/ps2706/products_module_configuration_guide_chapter09186a00803f3ee7.html

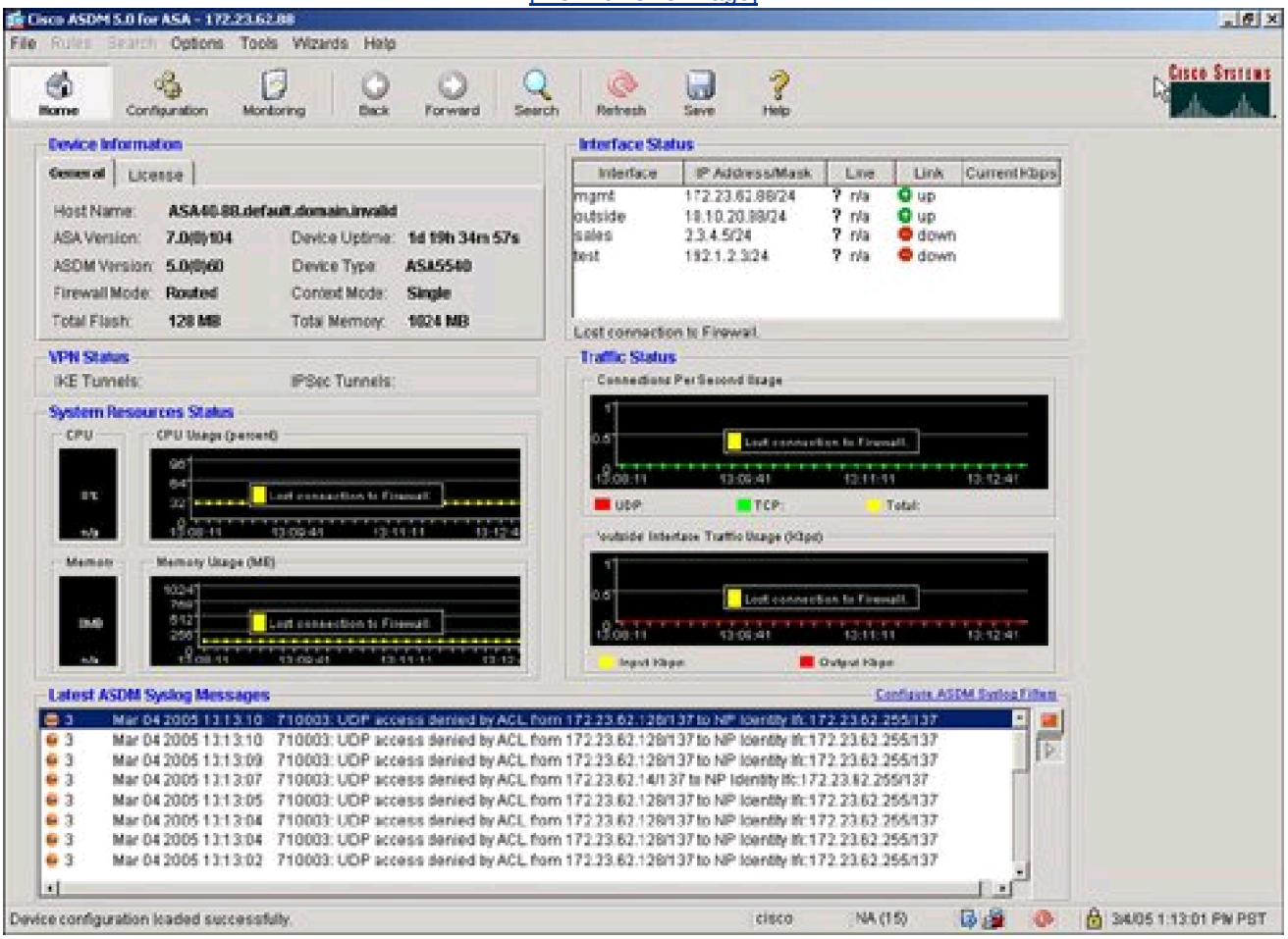
Chapter 3. Cisco Adaptive Security Appliance Overview

The Cisco Adaptive Security Appliance (ASA) line combines the functions of a firewall, Virtual Private Network (VPN), and intrusion prevention system (IPS) in a single appliance. This product line is adaptive, which means that it provides several mechanisms that enable the network to be self-defending. The ASA product line is also built to be extensible to add new self-defending capabilities like antivirus, antispam, antiphishing, and antispyware protection, which are supported in the Content Security and Control Security Services Module (CSC-SSM) on the ASA product line.

The ASA product line contains several models, including the Cisco ASA 5505, Cisco ASA 5510, Cisco ASA 5520, Cisco ASA 5540, and the Cisco ASA 5550. Each of these ASA models has a different capacity and price point. The ASA is managed by an easy-to-use Adaptive Security Device Manager (ASDM). ASDM is a follow-on release to the popular PIX Device Manager (PDM). ASDM features several enhancements over PDM, including a near real-time syslog viewer. Figure 3-1 shows the ASDM main screen.

Figure 3-1. ASDM Main Screen

[View full size image]



This chapter, which is similar in scope to the other chapters in this book, provides an overview of some of the self-defending components of the ASA product line, with an emphasis on how to manage the device using management products such as the device manager. This chapter is intended to be an overview and a pointer to more detailed or advanced publications, as provided in the References section. In this chapter, you will learn about the antispoofing, IPS, application or protocol inspection, antivirus, antispam, antiphishing, and antispyware protection on the ASA product line.

PREV NEXT

Antispoofing

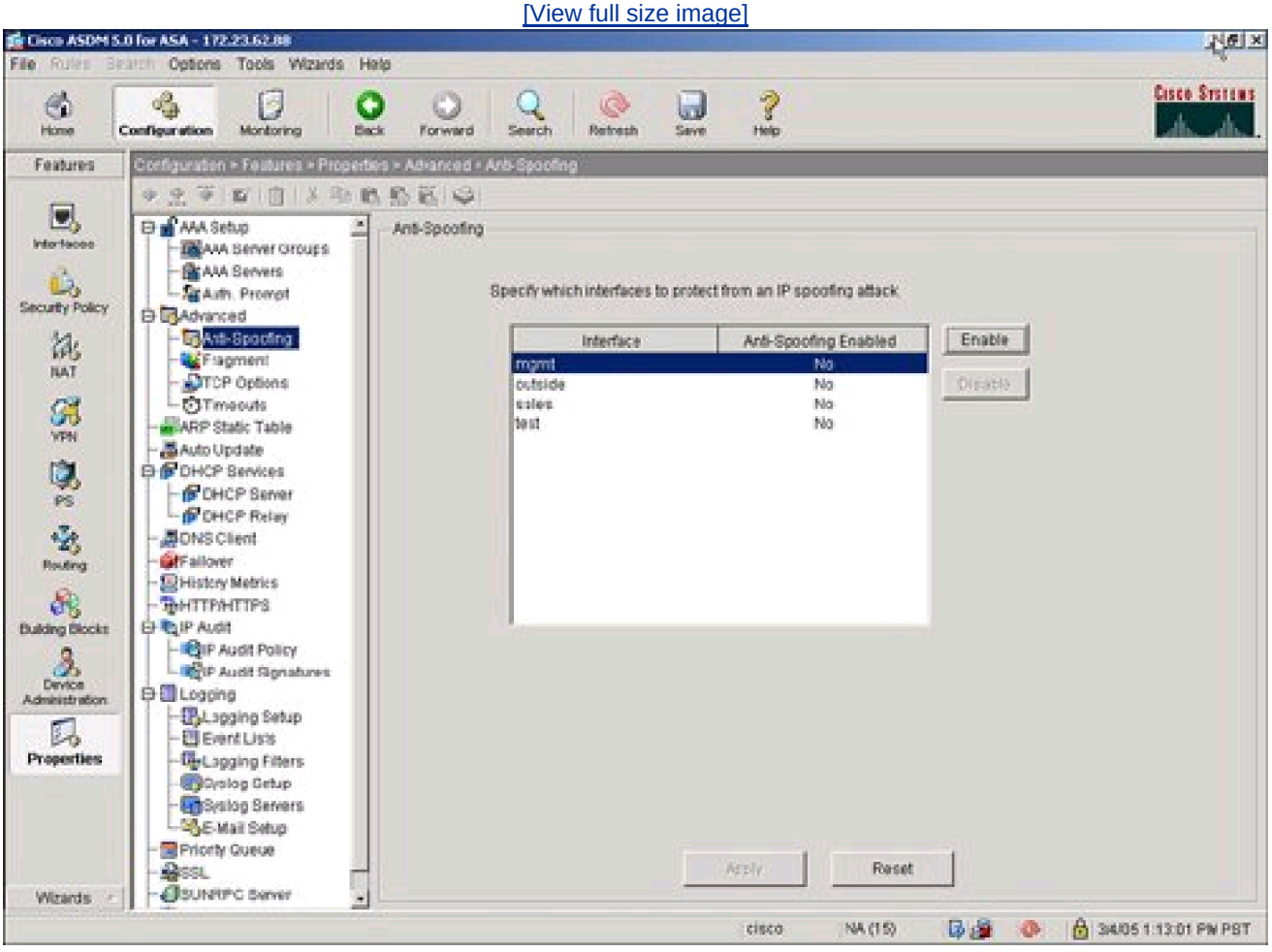
Cisco ASA contains several features to enhance the ability of the network to be self-defending. One example of these features is the ability for the ASA to implement an antispoofing function. Antispoofing helps to protect an interface of the ASA by verifying that the source of network traffic is valid.

The antispoofing feature protects an individual interface from IP address spoofing by creating filters to confirm both source address and route integrity. The antispoofing feature creates an **ip verify reverse-path** command-line interface (CLI) command. The antispoofing feature verifies route integrity by performing a route lookup on the source address of an incoming packet. This packet is dropped if a route does not exist back to the source address or if the route does not match the interface of the incoming packet. The inability to have a route back to the source address for an interface is considered to be suspect for a denial-of-service (DoS) attack because many attacks use IP spoofing to disguise the true source IP address of the attacker.

Figure 3-2 displays an example of where to enable antispoofing on an interface by selecting the interface and selecting the Enable button under Antispoofing in ASDM. This antispoofing feature is also called Unicast Reverse Path Forwarding (uRPF).

Figure 3-2. Antispoofing/uRPF Configuration

[View full size image]



Intrusion Prevention Service

Cisco ASA supports an inline Intrusion Prevention Security Service on the Advanced Inspection and Protection Security Services Module (AIP-SSM). The Intrusion Prevention module provides the ability to identify and drop the IP packets of an active network attack. The actual configuration of the IPS signatures is not shown in the base ASA configuration file, which can be displayed with telnet/SSH or ASDM. The existence of an AIPSSM module is indicated in the **show module** telnet/SSH CLI command as shown in Example 3-1.

Example 3-1. *The* show module *Command*

```
asdm-89/admin# show module

Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5520 Adaptive Security Appliance         ASA5520            P3000000192
  1 ASA 5500 Series Security Services Module-10  ASA-SSM-10         JAB0818067A

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 000b.fcf8.c623 to 000b.fcf8.c627  1.0          1.0(10)0     7.2(0)47
  1 000b.fcf8.0156 to 000b.fcf8.0156  1.0          1.0(10)0     6.0(0.51)S212.0

Mod SSM Application Name          Status          SSM Application Version
--- ------------------------------ --------------- ----------------------
  1 IPS                           Up              6.0(0.51)S212.0

Mod Status            Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  0 Up Sys            Not Applicable
  1 Up                Up
```

The process to configure IPS inspection of network traffic with the AIP-SSM with ASDM includes the following:

- Launch ASDM for IPS Configuration
- Configure service policy rules to specify a class of traffic for IPS inspection
- Define the IPS signature set for inspection of network traffic

Launch ASDM for IPS Configuration

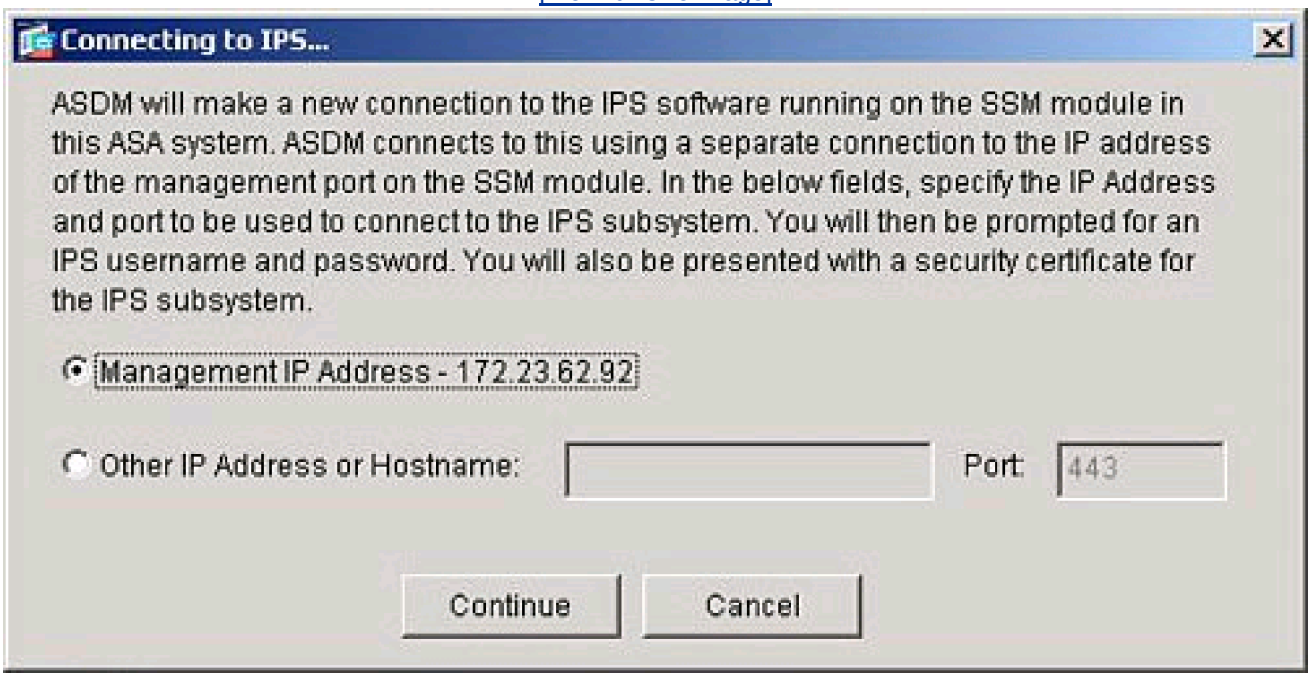
IPS Configuration is simple and intuitive with ASDM. You initiate IPS Configuration by selecting **Configuration** from the top panel and **IPS** from the left panel. The AIP-SSM module can be separately managed from the ASA chassis and has its own IP address. In addition to ASDM, you can also manage the AIP module by telnet/SSH directly to the IP address of the IPS module. You can also centrally manage the ASA AIP-SSM with the Cisco Security Manager.

Cisco Security Manager is Cisco's centralized security manager that you can use to manage or configure security components on ASA, IPS, and router devices. Cisco Security Manager is a very strategic element in the Cisco security portfolio. Cisco Security Manager is discussed in detail in Chapter 9, "Cisco Security Manager."

You can display or view the CLI file of the AIP-SSM, which can be created with ASDM, by issuing the **session module** *slot* command from the base ASA platform. ASDM will indicate the IP address of the AIP-SSM automatically after you select **Configure** and **IPS** from the main ASDM homepage. The AIP-SSM module also supports a separate username and password. Figure 3-3 shows an example of how to access the GUI display of the AIPSSM module configuration from ASDM.

Figure 3-3. Connecting to IPS Configuration in ASDM

[View full size image]

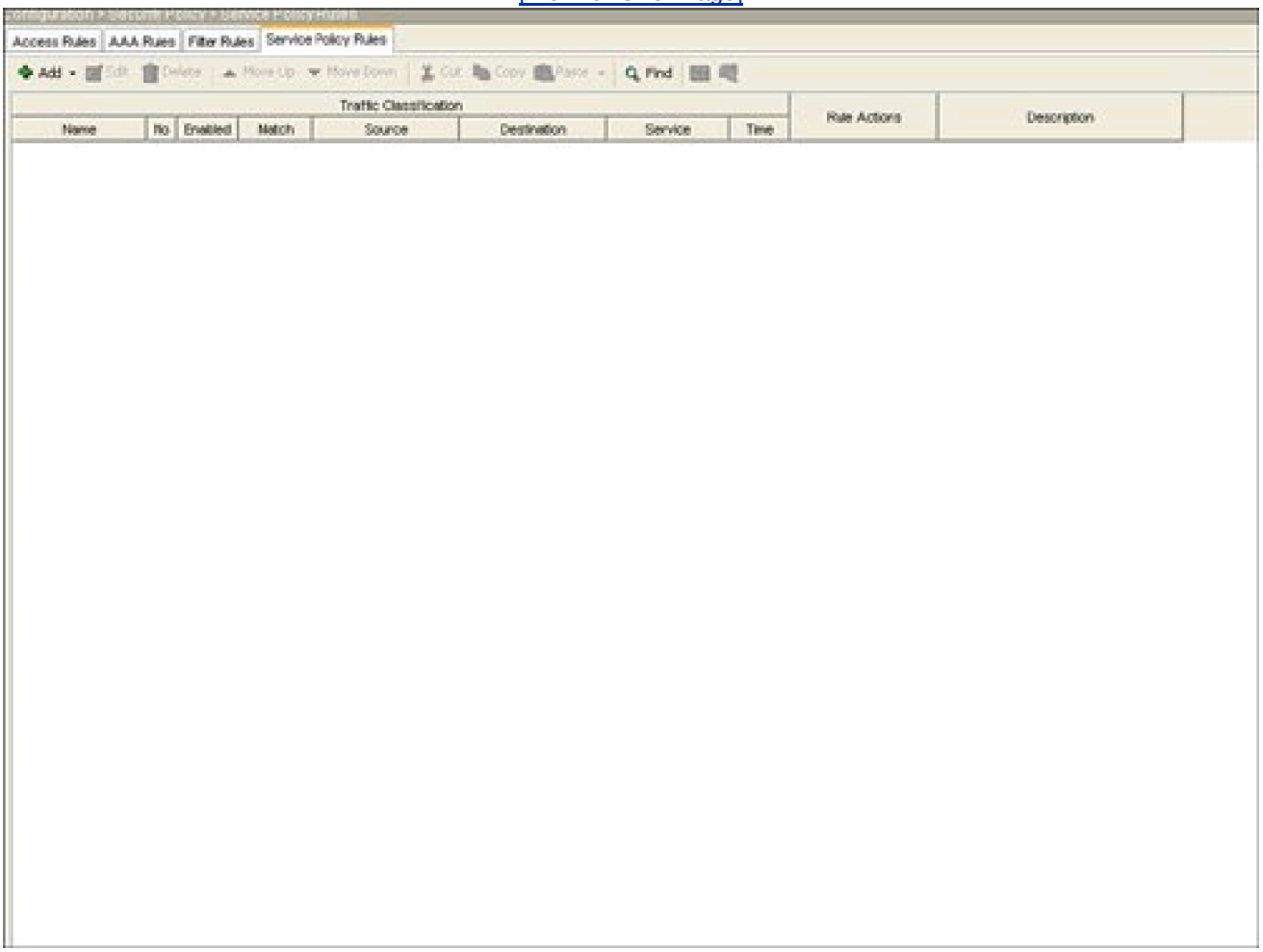


Configure Service Policy Rules

ASA also provides the ability to specify which subset of network traffic will be sent from the ASA chassis to the AIP-SSM module for IPS inspection. The definition of network traffic to send to the AIP-SSM module is configured under the Service Policy Rules section as shown in Figure 3-4.

Figure 3-4. Service Policy Rules

[View full size image]



The steps to configure a specific traffic flow in a service policy rule include the following:

Step 1. Select Service Policy Rule Table Configuration

Step 2. Configure a service policy

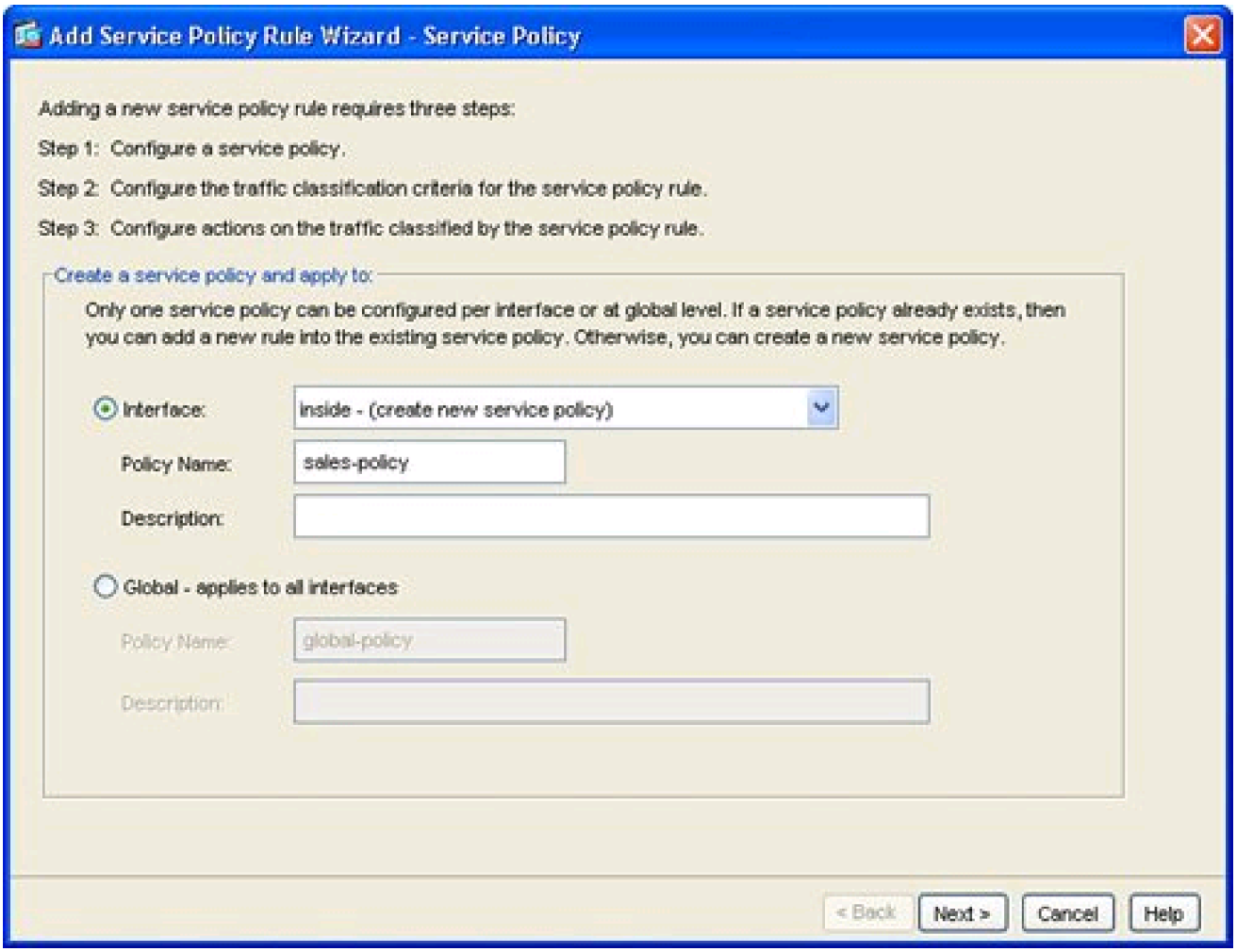
Step 3. Configure or select the traffic class that will be managed

Step 4. Configure the action, for example, send to AIP-SSM module for inspection, for the service policy rule

The next step, as indicated in Figure 3-5, is configuration of the individual interface or global list of interfaces for the service policy rule. There can be only one service policy rule that is applied to an interface.

Figure 3-5. Interface for Service Policy Rule

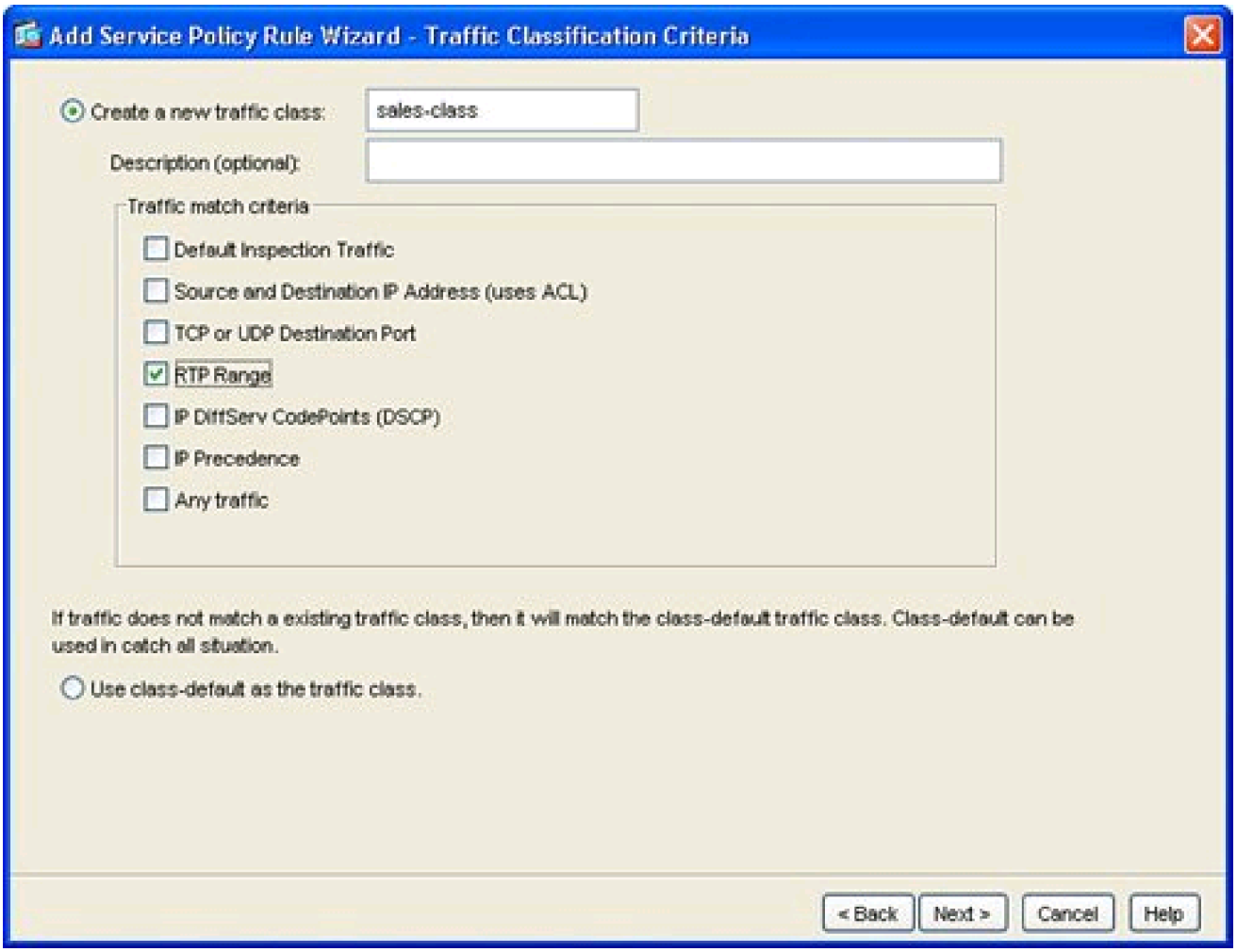
[View full size image]



Next, configure the traffic class name and network traffic to be matched in the service policy rule. Figure 3-6 shows the Traffic Classification Class window.

Figure 3-6. Create Traffic Class

[View full size image]



This example created a new traffic class in order to process or match network traffic for Real-Time Protocol (RTP) packets. RTP is used for voice and multimedia network traffic. Figure 3-7 displays how to define the RTP port range of 4000 to 5000 in the new traffic class for the interface.

Figure 3-7. Define Network Traffic for Traffic Class

[View full size image]

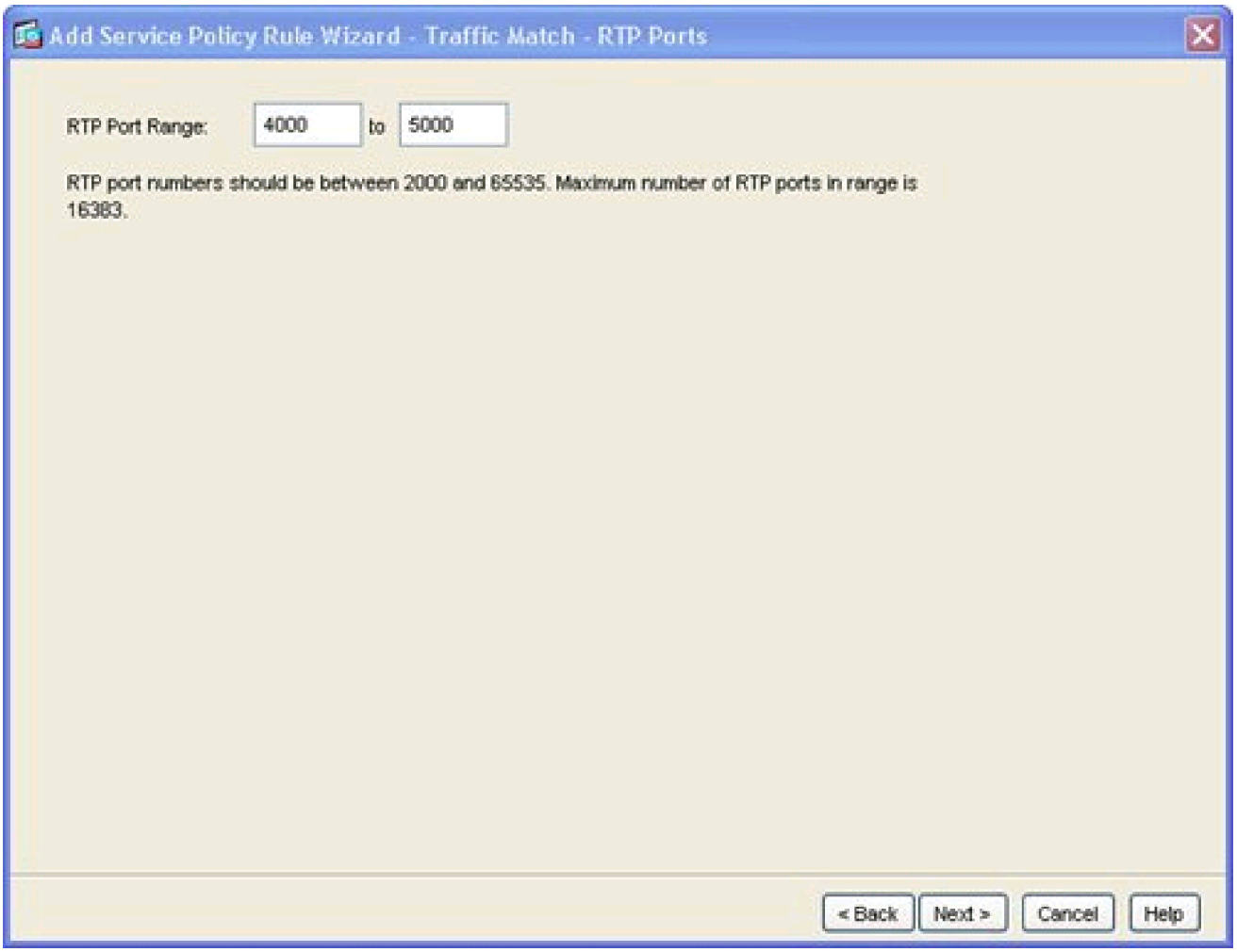


Figure 3-8 defines how to configure IPS inspection for this traffic flow. Configuring IPS prevention for this traffic flow in the service policy rule sends the matched traffic class from the ASA chassis to the AIP-SSM module for IPS inspection. This example defines IPS to be inline. Inline IPS means that this traffic can be dropped for a match of an IPS signature for packets that match the network traffic class. This example also defines IPS to fail-open, which means that, in the event of a failure of the AIP-SSM module, this traffic class for the specified interface will not be dropped and will continue to flow through the ASA.

Figure 3-8. Enable IPS for Traffic Flow

[View full size image]

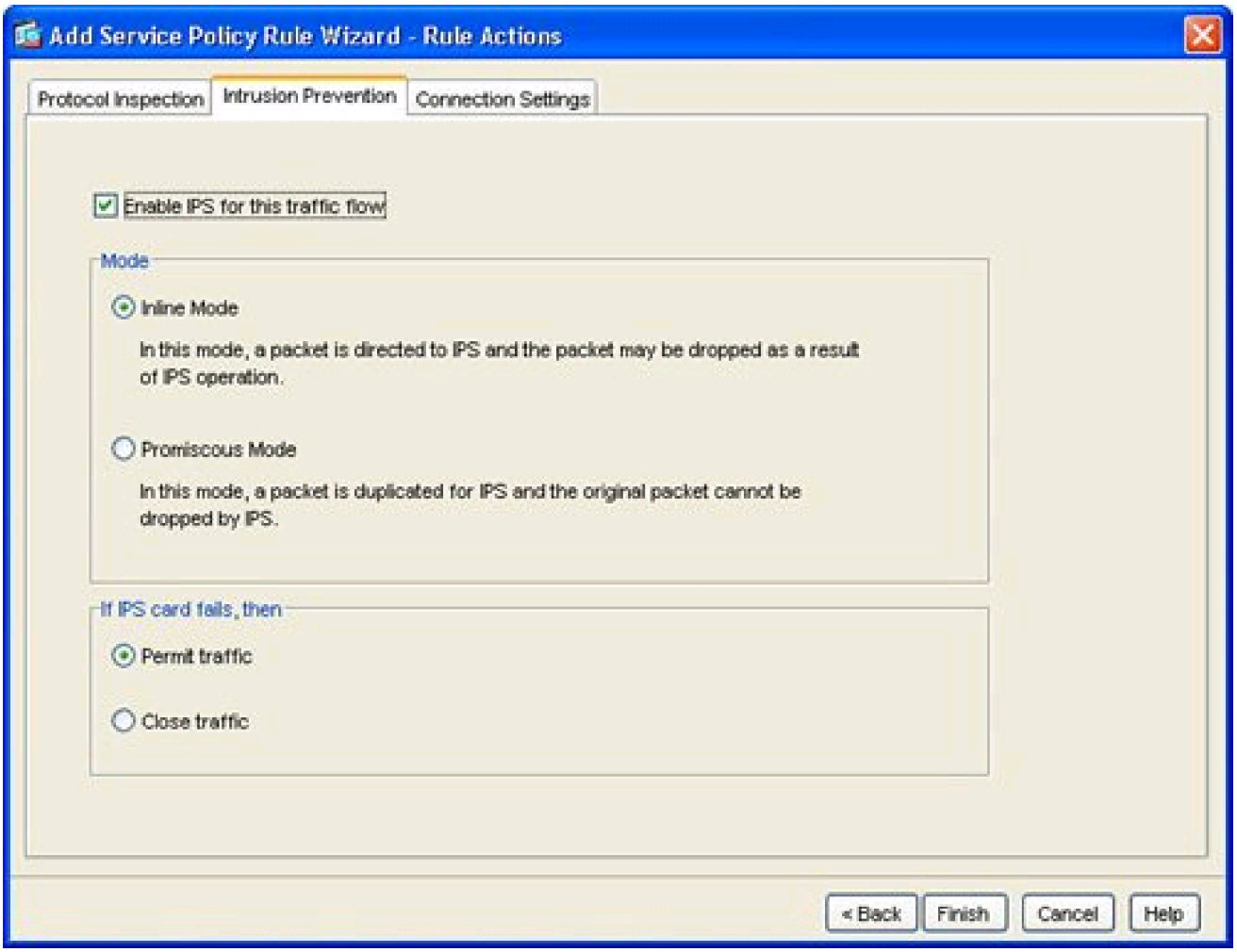
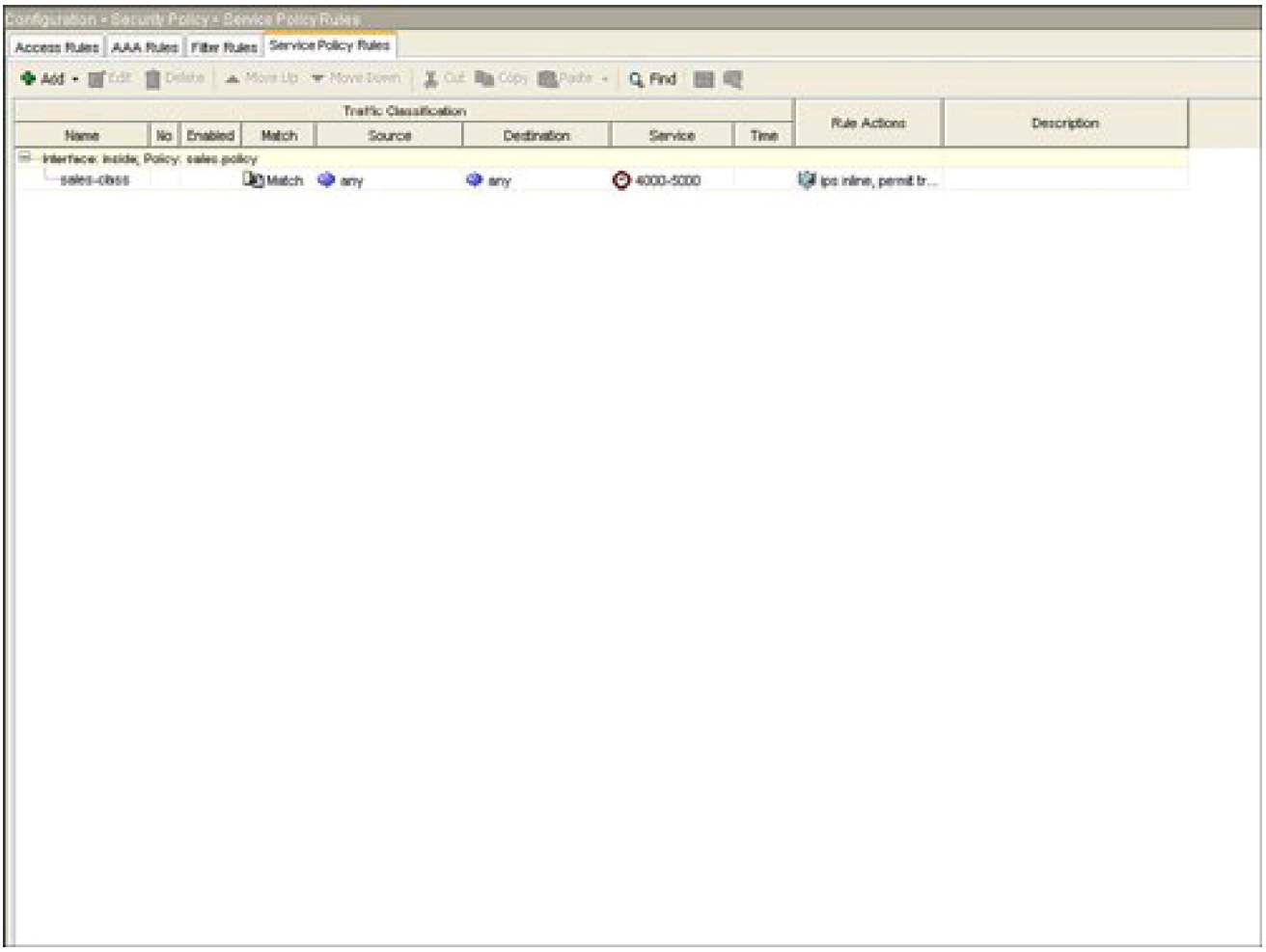


Figure 3-9 displays the resulting service policy rule in the service policy table for the new traffic class to send RTP packets from the inside interface to the AIP-SSM module for inline IPS inspection.

Figure 3-9. Service Policy Rule Table Entry

[View full size image]



Example 3-2 displays the resulting **class-map**, **policy-map,** and **service-policy** CLI commands on the base ASA platform.

Example 3-2. CLI for Service Policy Rule

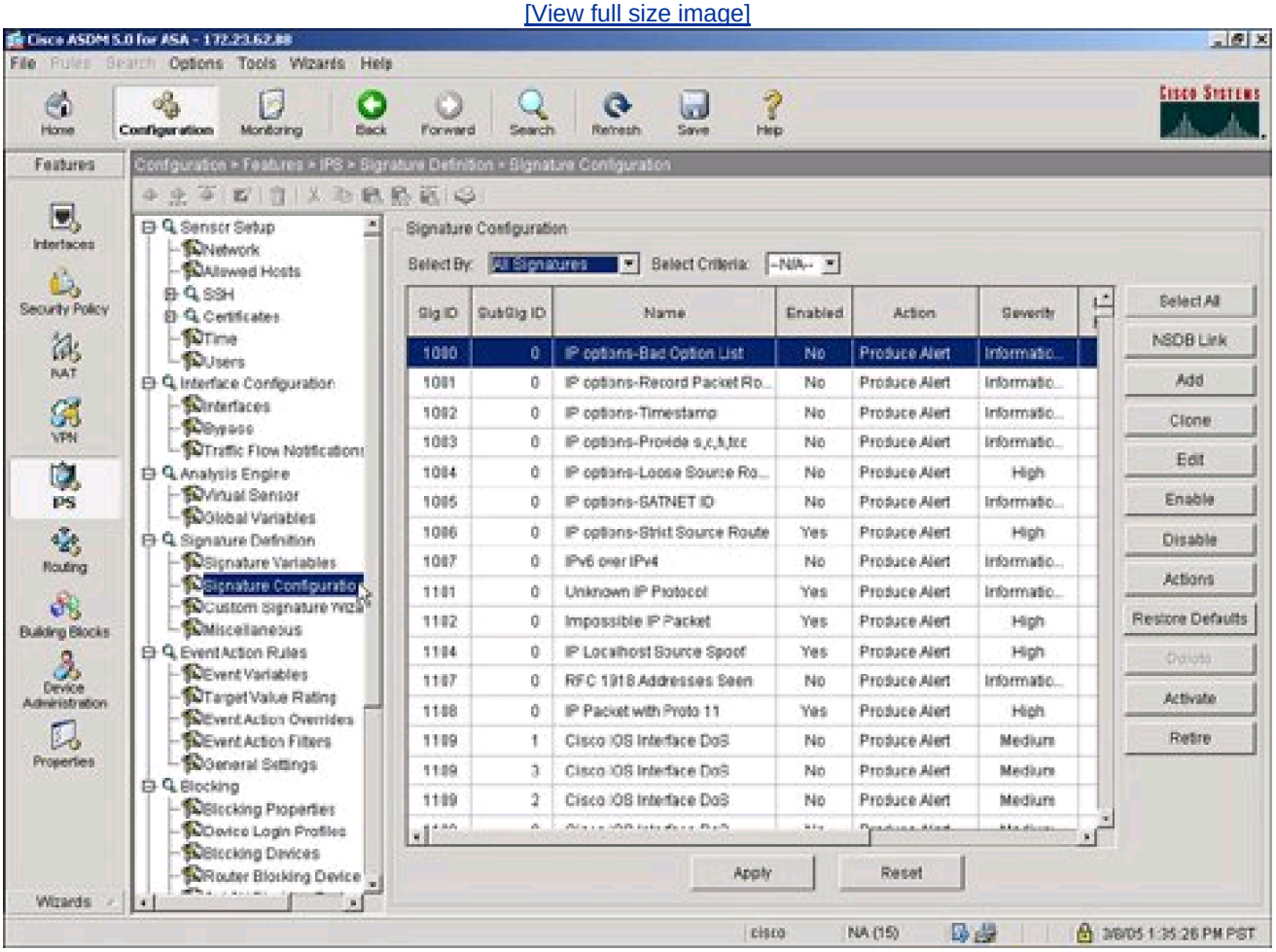
```
class-map sales-class
 match rtp 4000 1000
!
!
policy-map sales-policy
 class sales-class
  ips inline fail-open
!
service-policy sales-policy interface inside
```

Define IPS Signatures

After configuring any specific service policy rules, you next configure the specific IPS signatures that will be used to inspect the network traffic for a potential network attack. IPS can be inline, which means that the ASA product deals with the real network packet of a possible attack in real time, as opposed to a copy of the network traffic from a span port on a Catalyst LAN switch as typically implemented with an intrusion detection system (IDS) solution. IPS signature configuration is initiated by selecting the Signature Configuration option in ASDM as shown in Figure 3-10.

Figure 3-10. IPS Signature Configuration

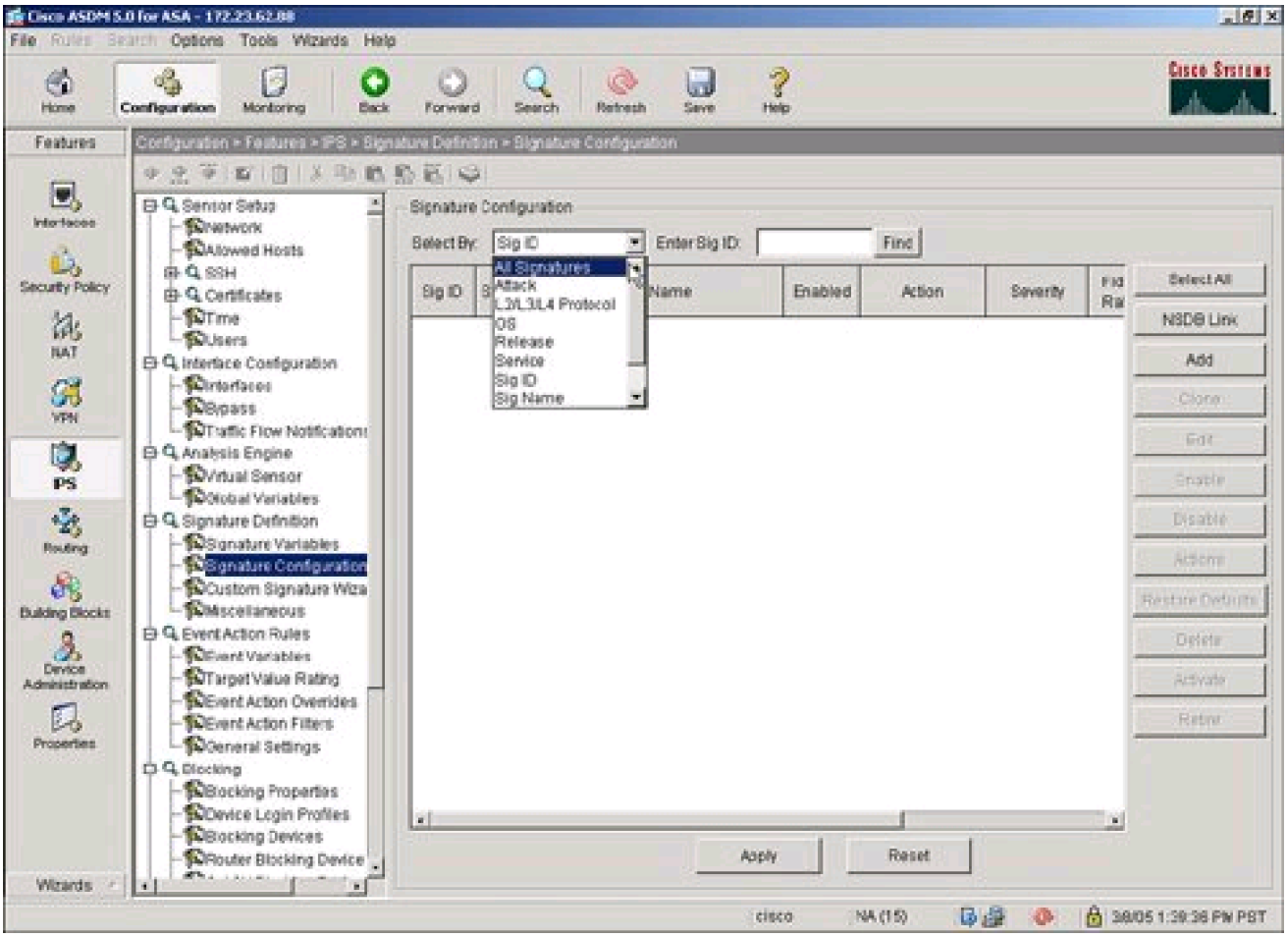
[View full size image]



IPS signatures are divided into several subcategories, including Layer 2/Layer 3/Layer 4 (L2/L3/L4) protocol, attack, and operating system (OS) platforms. Target OS platform signatures include Linux, Windows, MacOS, Netware, and Cisco IOS. Figure 3-11 displays the signatures subcategories.

Figure 3-11. IPS Signature Subcategories

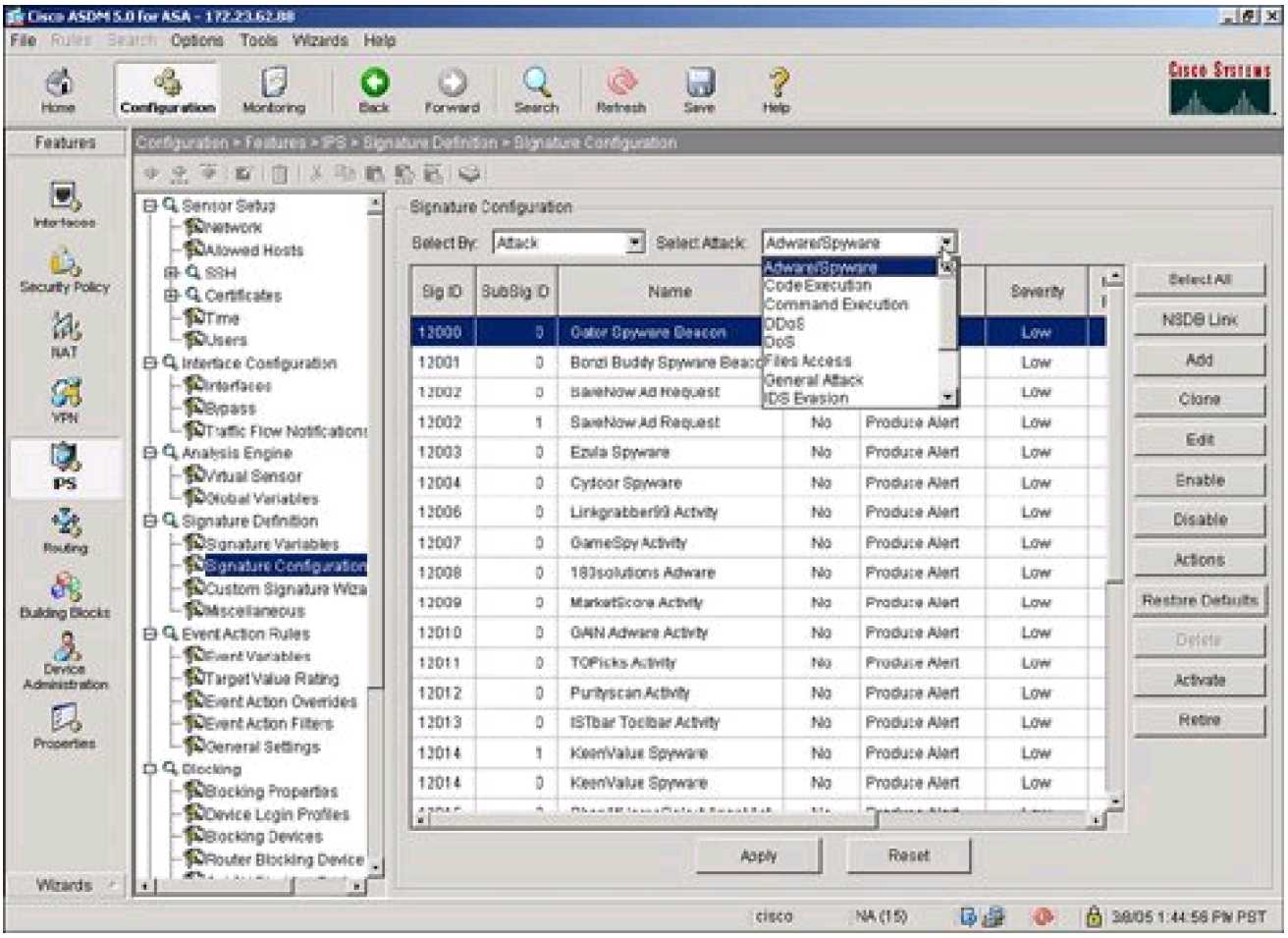
[View full size image]



The attack signatures are composed of several attack subcategories including adware/ spyware, distributed denial of service (DDoS), DoS, and file access. Figure 3-12 shows an example of these attack subcategories.

Figure 3-12. Attack Signature Subcategories

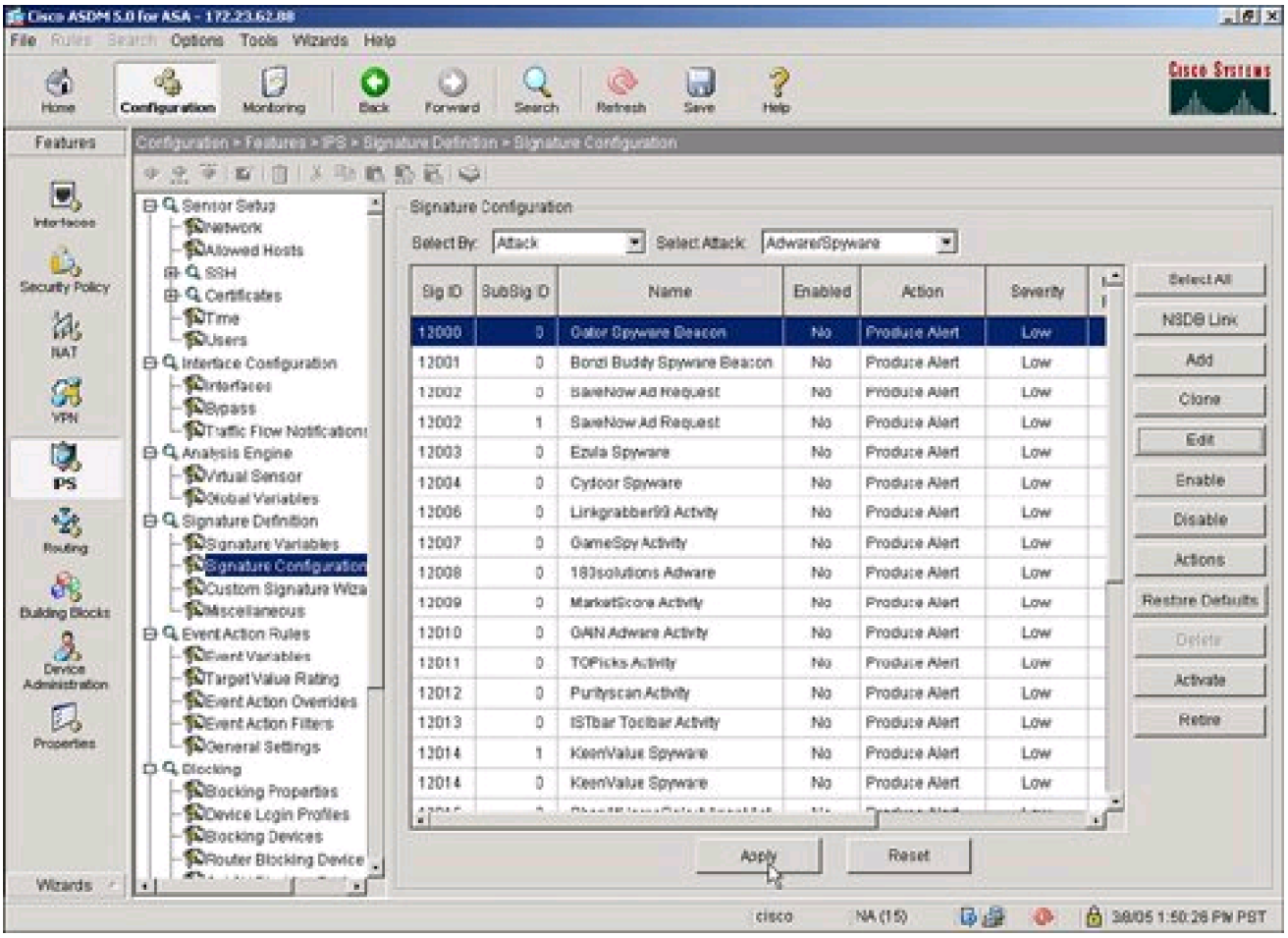
[View full size image]



Let's say that a user wants to deploy the attack signatures to detect spyware. The process to deploy the attack signature is as simple as selecting the spyware category, highlighting the spyware signature, and then selecting the Enable and Apply buttons. The location in ASDM to select a spyware signature and to select the Enable and Apply buttons in ASDM is shown in Figure 3-13.

Figure 3-13. Applying Spyware Detection Signatures

[View full size image]


Cisco ASDM 5.0 for ASA - 172.23.62.88
File Rules Search Options Tools Wizards Help
Home
Configuration
Monitoring
Back
Forward
Search
Refresh
Save
Help
Cisco Systems
Features
Configuration > Features > IPS > Signature Definition > Signature Configuration
Interfaces
Security Policy
NAT
VPN
IPS
Routing
Building Blocks
Device Administration
Properties
Wizards
Sensor Setup
Network
Allowed Hosts
SSH
Certificates
Time
Users
Interface Configuration
Interfaces
Bypass
Traffic Flow Notification
Analysis Engine
Virtual Sensor
Global Variables
Signature Definition
Signature Variables
Signature Configuration
Custom Signature Wiza
Miscellaneous
Event Action Rules
Event Variables
Target Value Rating
Event Action Overrides
Event Action Filters
General Settings
Blocking
Blocking Properties
Device Login Profiles
Blocking Devices
Router Blocking Device
Signature Configuration
Select By: Attack
Select Attack: Adware/Spyware
Sig ID
SubSig ID
Name
Enabled
Action
Severity
12000 0 Gator Spyware Beacon No Produce Alert Low
12001 0 Bonzi Buddy Spyware Beacon No Produce Alert Low
12002 0 SaveNow Ad Request No Produce Alert Low
12002 1 SaveNow Ad Request No Produce Alert Low
12003 0 Ezula Spyware No Produce Alert Low
12004 0 Cydoor Spyware No Produce Alert Low
12006 0 Linkgrabber99 Activity No Produce Alert Low
12007 0 GameSpy Activity No Produce Alert Low
12008 0 180solutions Adware No Produce Alert Low
12009 0 MarketScore Activity No Produce Alert Low
12010 0 GAIN Adware Activity No Produce Alert Low
12011 0 TOPicks Activity No Produce Alert Low
12012 0 Purityscan Activity No Produce Alert Low
12013 0 ISTbar Toolbar Activity No Produce Alert Low
12014 1 KeenValue Spyware No Produce Alert Low
12014 0 KeenValue Spyware No Produce Alert Low
Select All
N3DB Link
Add
Clone
Edit
Enable
Disable
Actions
Restore Defaults
Delete
Activate
Retire
Apply
Reset
cisco
NA (15)
3/8/05 1:50:28 PM PST

PREV NEXT

Protocol Inspection Services

Cisco ASA features the ability to perform application or protocol inspection on specific Layer 4Layer 7 protocols. Many network attacks attempt to exploit a vulnerability in the handling of a network protocol. The ability for the ASA to inspect the contents of network packets for certain protocols can enable the ASA to identify a potential attack and be self-defending. Protocol inspection can also verify dynamic port assignments and rewrite embedded network addresses within the protocol data packets. The protocols that are supported for protocol inspection in ASA include the following:

- **Computer Telephone Interface Quick Buffer Encoding (CTIQBE)** CTIQBE is used by Cisco IP SoftPhone and Cisco CallManager.
- **Domain Name System (DNS)** DNS translates a name to an IP address.
- **Enhanced Simple Mail Transport protocol (ESMTP)** ESMTP adds Extended Hello to SMTP.
- **File Transfer Protocol (FTP)** Use FTP to transfer files across a network using PUT and GET.
- **GPRS Tunneling Protocol (GTP)** GPRS is a 3G data service for GSM mobile phones. A separate license is required to enable GTP protocol inspection on ASA.
- **H.323 and H.225** H.323 are endpoints that participate in a Voice over IP (VoIP) call, and H.225 is the ITU call control signaling protocol.
- **H.323 Registration, Admission, and Status (RAS)** This is the H.323 gatekeeper discovery and registration protocol.
- **Hypertext Transfer Protocol (HTTP)** This protocol enables web browsing.
- **Internet Control Message Protocol (ICMP)** ICMP ping is used to determine if there is connectivity to an IP address across the network.
- **ICMP Error** Ping error codes.
- **Internet Locator Service (ILS)** ILS is used in Microsoft NetMeeting.
- **Media Gateway Control Protocol (MGCP)** MGCP controls media gateways from controllers and call agent.
- **Network Basic Input/Output System (NetBIOS)** NetBIOS is used for Windows print sharing.
- **Point-to-Point Tunneling Protocol (PPTP)** PPTP was the first VPN protocol supported by Microsoft dial-up networking.
- **Remote Shell (RSH)** RSH is the UNIX utility to remotely execute commands.
- **Real Time Streaming Protocol (RTSP)** RTSP is the IETF protocol for streaming media such as video on a network.
- **Session Initialization Protocol (SIP)** SIP is the IETF protocol for voice over IP (VoIP).
- **Skinny Call Control Protocol (SCCP)** SCCP is the voice communication protocol between Cisco CallManager and VoIP phones.
- **Simple Network Management Protocol (SNMP)** SNMP is used for network monitoring and management by reading and writing to Message Information Blocks (MIBs).
- **SQLNET** This is the SQL*NET protocol for Oracle database.
- **Sun Remote Procedure Call (SunRPC)** This is the Sun client/server protocol for distributed computing. Network File System (NFS) also uses this protocol.

- **Trivial File Transfer Protocol (TFTP)** TFTP is the protocol to transfer a file accross a network or boot a network device.
- **X Display Manager Control Protocol (XDMCP)** This is the protocol for communication between a display manager and X server.

PREV NEXT

HTTP Inspection Engine

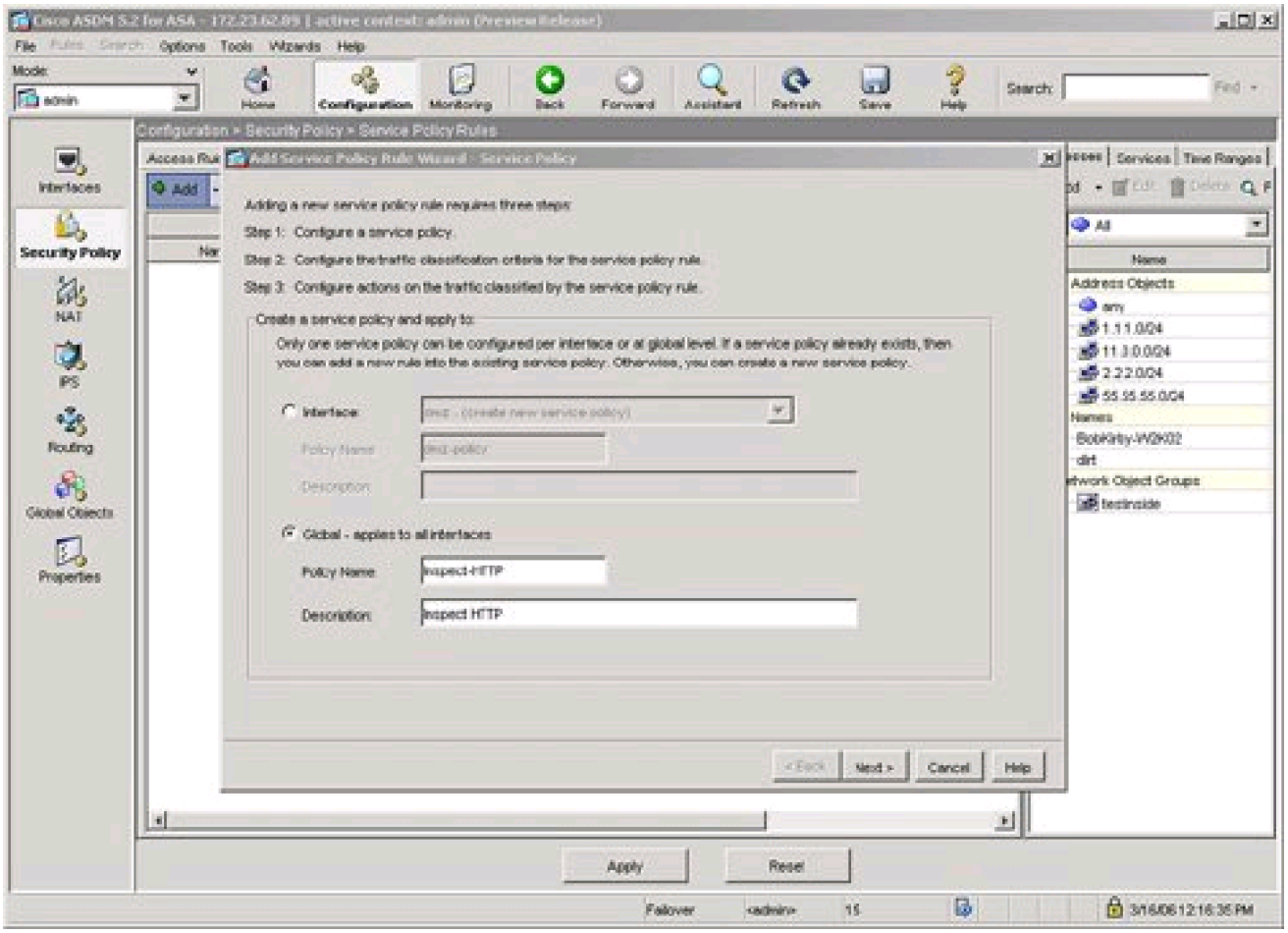
HTTP or web traffic is one of the most popular types of traffic on networks today. ASA includes the ability to inspect HTTP traffic flows to detect possible network attacks. You can initiate the process to configure the inspection of an HTTP traffic flow under the Service Policy Rules section. This process to initiate the creation of a traffic flow for HTTP inspection is similar to the process to define a traffic flow with Service Policy Rules for IPS inspection as described in the "Intrusion Prevention Service" section earlier in this chapter. The configuration to inspect a certain HTTP traffic flow results in a class-map and policymap statement, similar to the CLI output for the IPS Service Policy Rule configuration.

The HTTP inspection engine allows the ASA to mitigate potential network attacks that are tunneled over TCP port 80, the HTTP port. The HTTP inspection engine also verifies that the network traffic is RFC-compliant and not a series of malformed or handcrafted packets designed to potentially launch a network attack. URL length is also inspected to help detect any handcrafted large URLs that can be designed to create a network attack.

ASDM features an easy-to-use wizard to walk you through the Service Policy Rule definition process. You can configure HTTP inspection globally for all traffic through the ASA, or you can configure protocol inspection for a single interface. In the Add Service Policy Rule Wizard, as shown in Figure 3-14, you can configure a rule to be global, which applies to all interfaces on the ASA.

Figure 3-14. Global Rule to Inspect HTTP

[View full size image]



The next step is specification of what traffic or ports will be inspected.Figure 3-15 displays an example of how to select the inspection of TCP packets, and Figure 3-16 configures the HTTP/web service to inspect HTTP/WWW, or TCP port 80.

Figure 3-15. Inspect TCP

[View full size image]

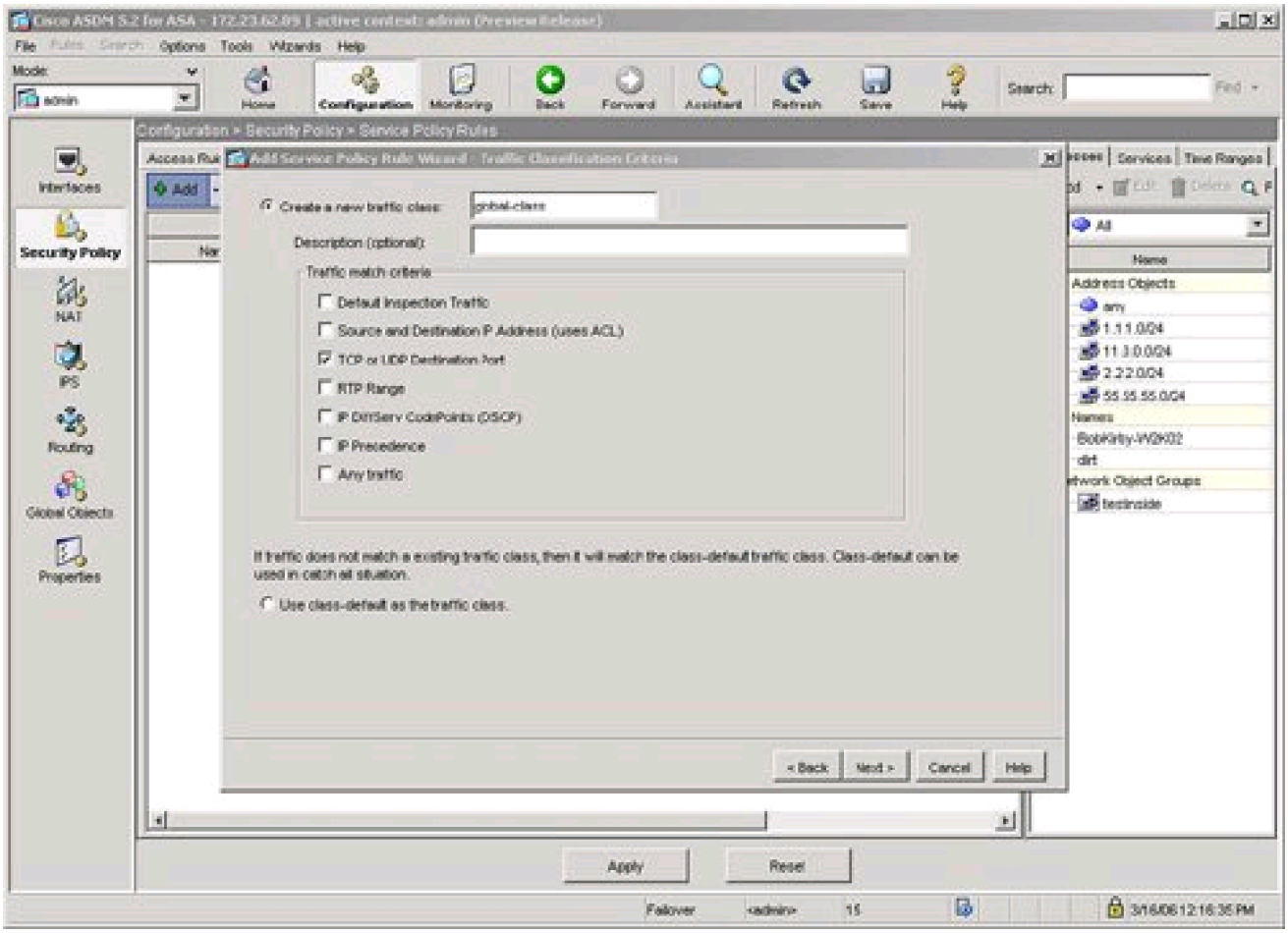
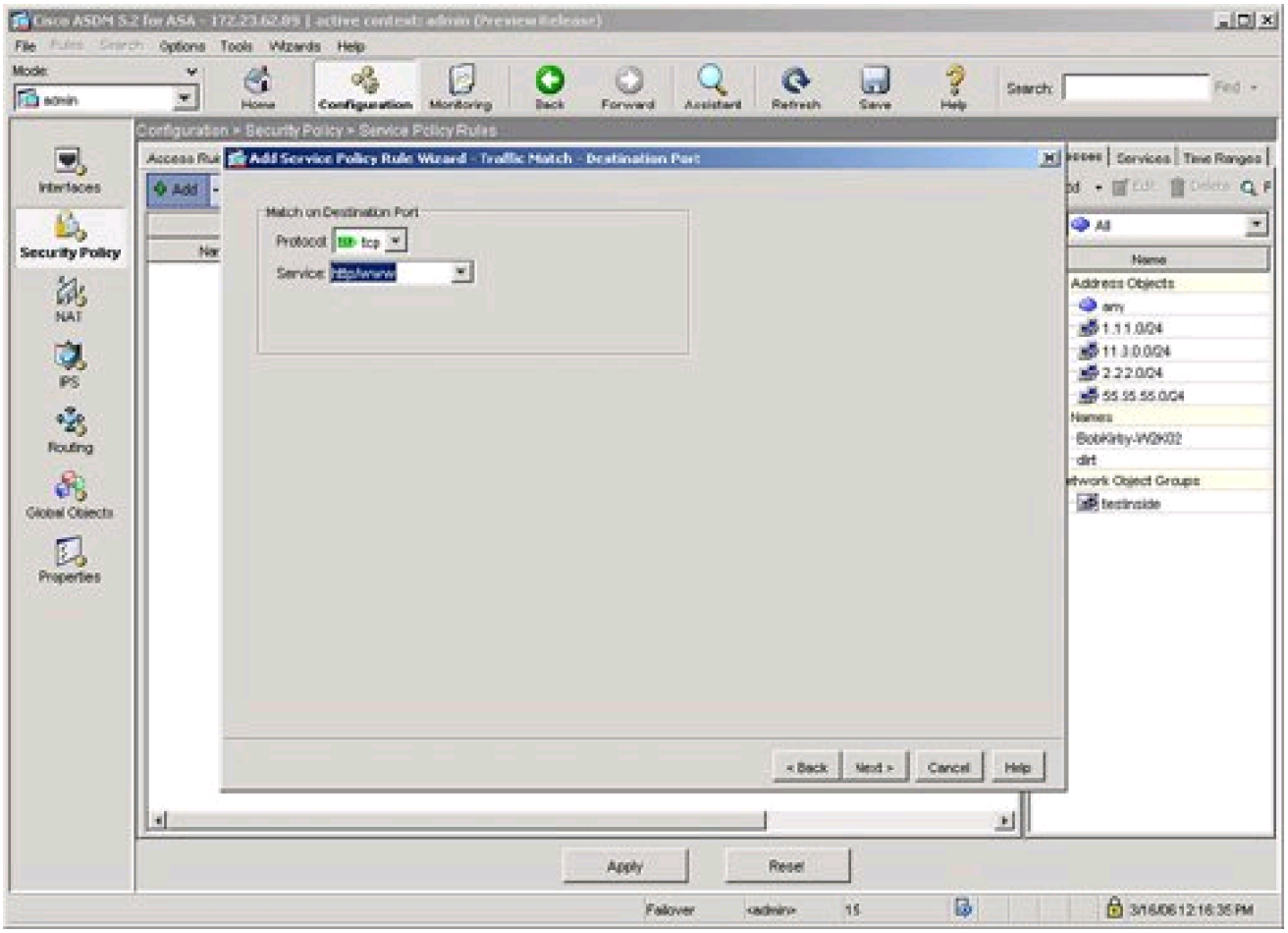


Figure 3-16. Inspect HTTP/Web Service

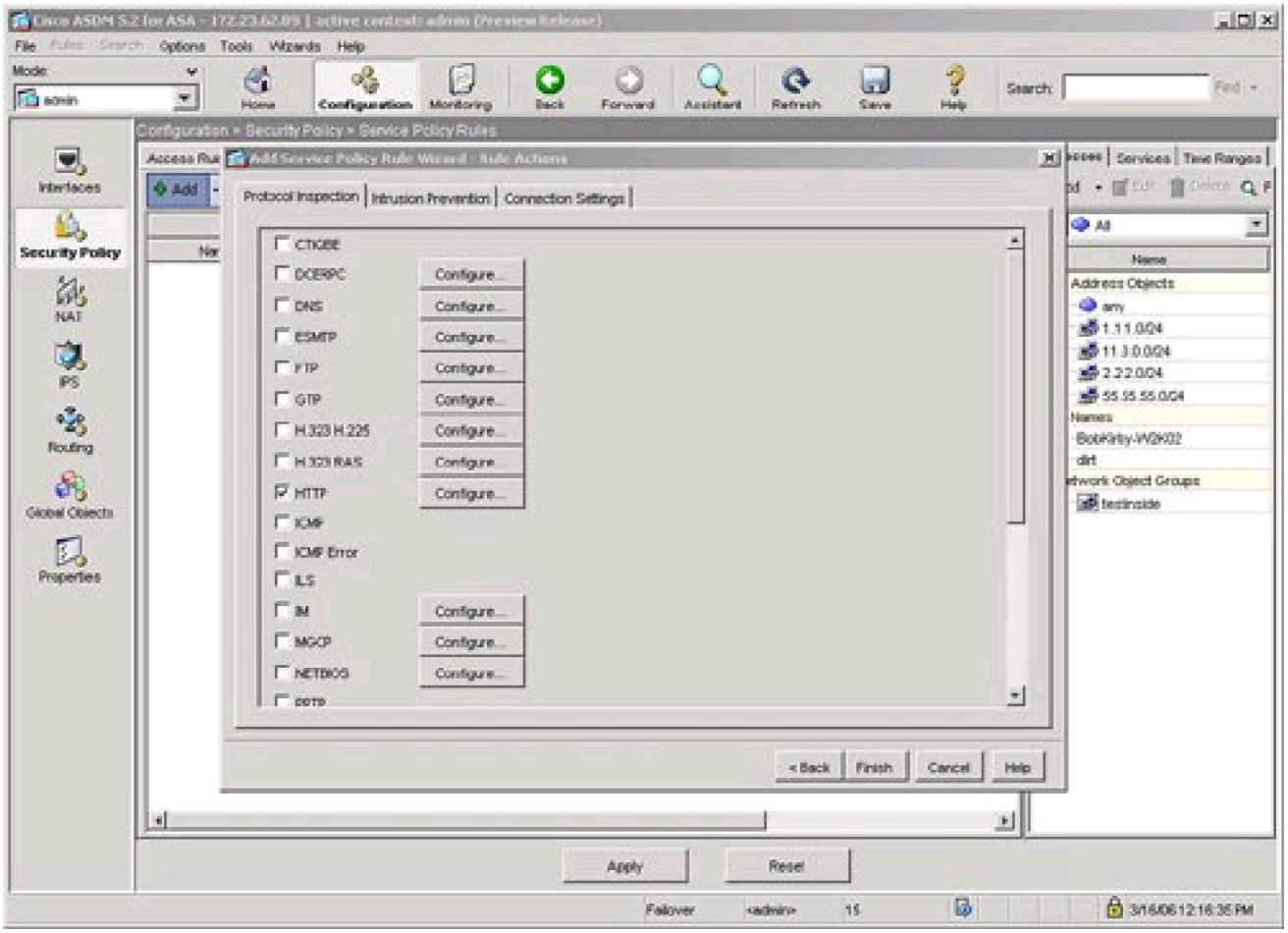
[View full size image]



The next step in the wizard enables you to configure protocol inspection. HTTP inspection can be selected for inspection, as shown in Figure 3-17.

Figure 3-17. Select HTTP for Protocol Inspection

[View full size image]



Several DDoS attacks send only part of the TCP handshake to initiate but never complete a TCP connection. This DDoS attack can result in a large TCP connection table that can consume resources that would otherwise go to servicing legitimate network traffic. The ASA supports the ability to configure a threshold for the maximum number of embryonic, or developing, connections that are allowed at one time by the appliance. Maximum connection parameters can provide protection against DDoS attacks on the ASA. The Maximum TCP and User Datagram Protocol (UDP) Connections field allows the ASA to configure a threshold of how many connections are active through the appliance at one time. The Maximum Embryonic Connections field controls the size of the internal state table for TCP connections.

The Randomize Sequence Number feature allows the ASA to create random, nonpredictable sequence numbers for TCP connections. The ability to randomize sequence numbers creates an additional layer of abstraction and protection against network attackers who endeavor to predict sequence numbers and masquerade as legitimate network connections. The Randomize Sequence Number feature is on by default.

As mentioned in the previous chapters, the DDoS Guard is typically deployed upstream close to the protected zone or servers. The ASA and DDoS Guard can provide a layered defense against DoS and DDoS attacks. Max Embryonic Connections and Randomize Sequence Number protection on the ASA can be the first line of defense, and the DDoS Guard can be second line of defense against the network attack.

A TCP Map is used to configure the customized inspection and protection for TCP connections. A TCP Map can be configured as part of the HTTP inspection to provide TCP and HTTP protection for web traffic. A TCP Map can also be configured separately and independent of HTTP inspection.

TCP Map

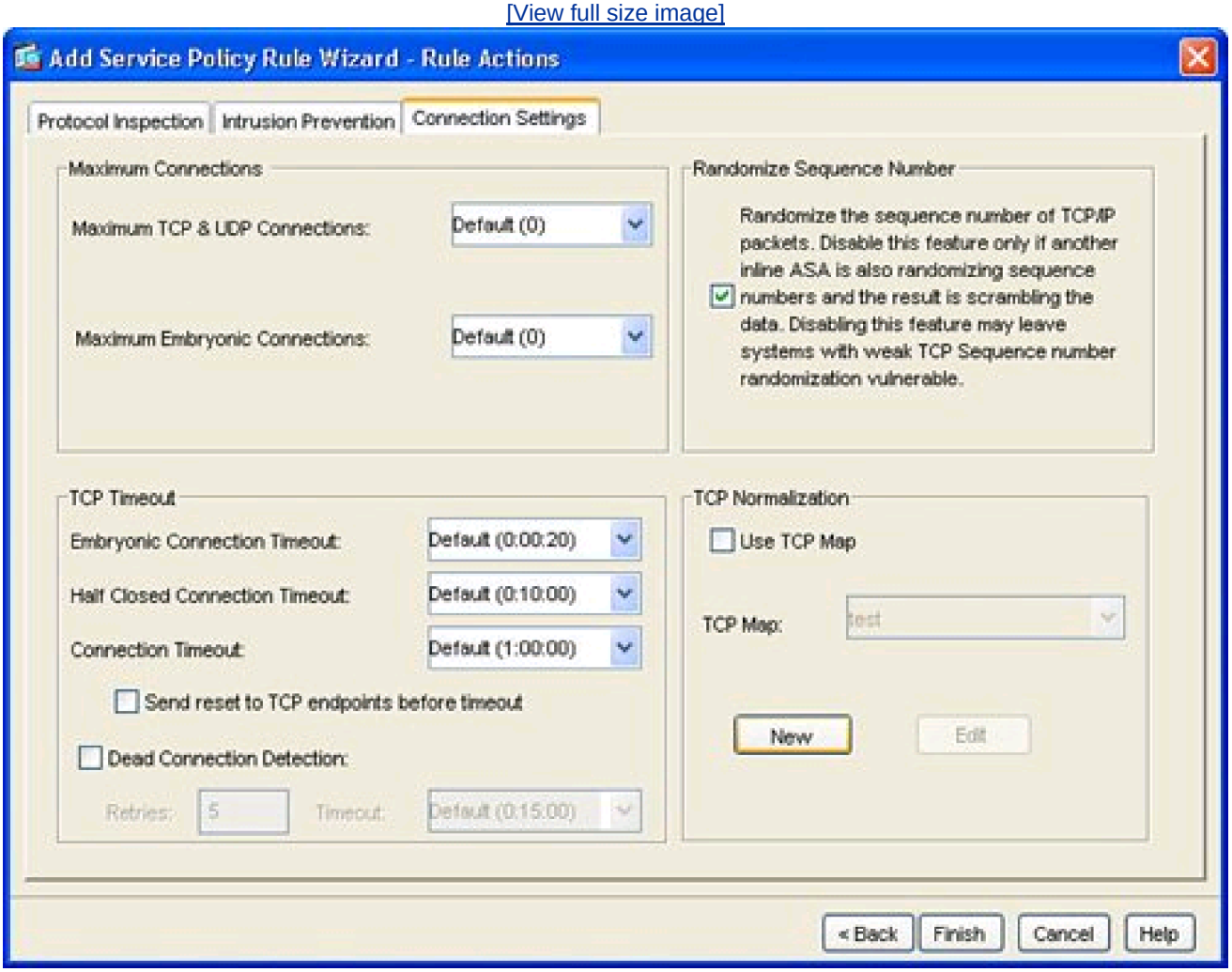
Cisco ASA features the ability to tailor how TCP connections should be policed and normalized. TCP maps dictate how TCP sessions

should be managed for a specific traffic flow. You can configure TCP maps as part of application protocol inspection, as evidenced by the ability to create a TCP map while defining protocol inspection for HTTP.

To create a new TCP map that can be used as part of HTTP protocol inspection, select the connection settings and the **Use TCP Map** option under TCP Normalization as shown in Figure 3-18. You can use TCP maps to police the behavior of a connection to reduce vulnerabilities and to minimize the chance of a network attack through the specified TCP connection.

Figure 3-18. Use TCP Map

[View full size image]

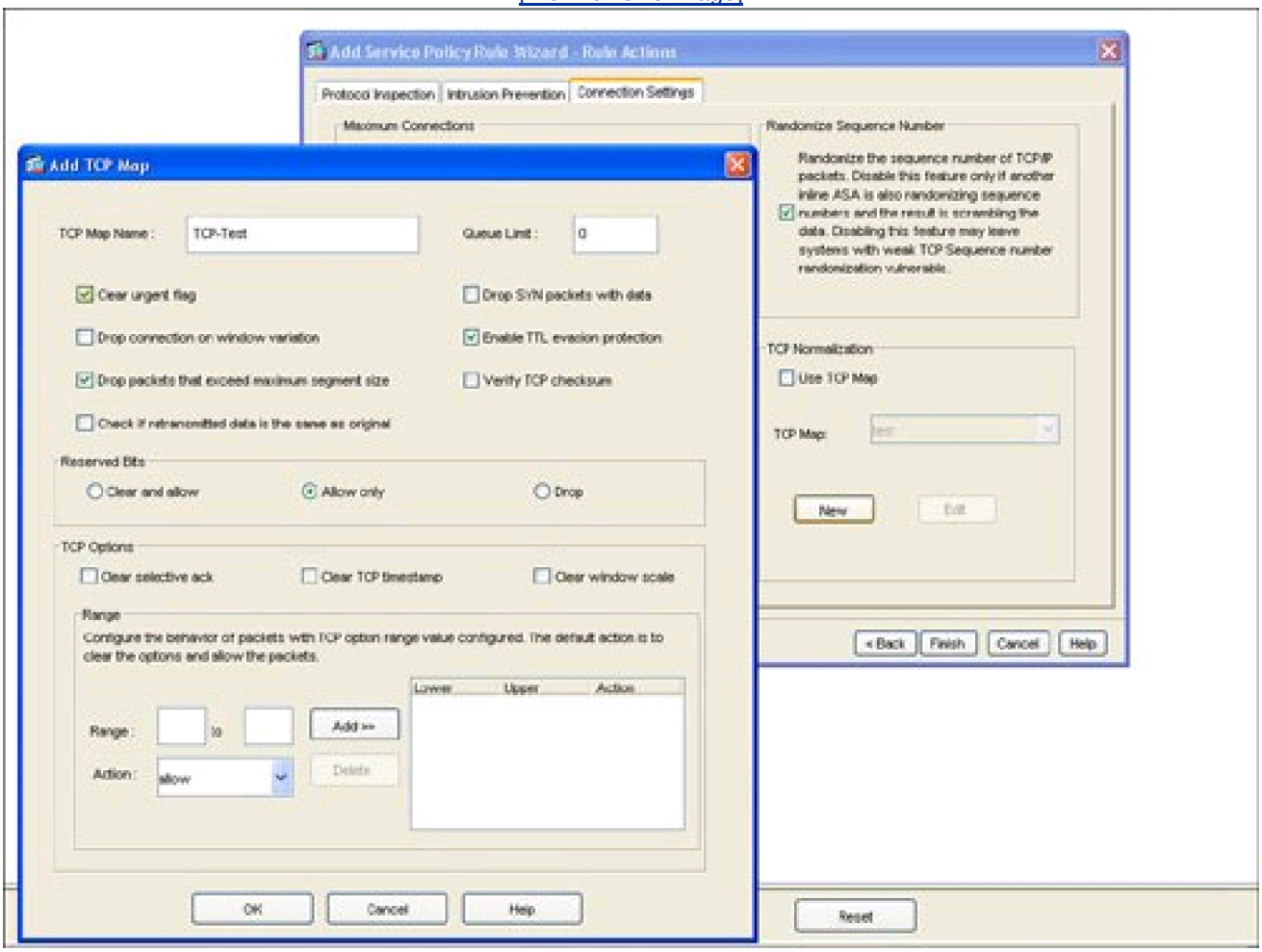


TCP normalization is the process of inspecting TCP flows for traffic that may not be normal and could possibly be used to implement a network attack. TCP maps determine what part of the TCP flow will be inspected to identify fields in TCP packets that may not be normal or standard.

Figure 3-19 displays an example of TCP Map configuration options.

Figure 3-19. TCP Map Options

[View full size image]

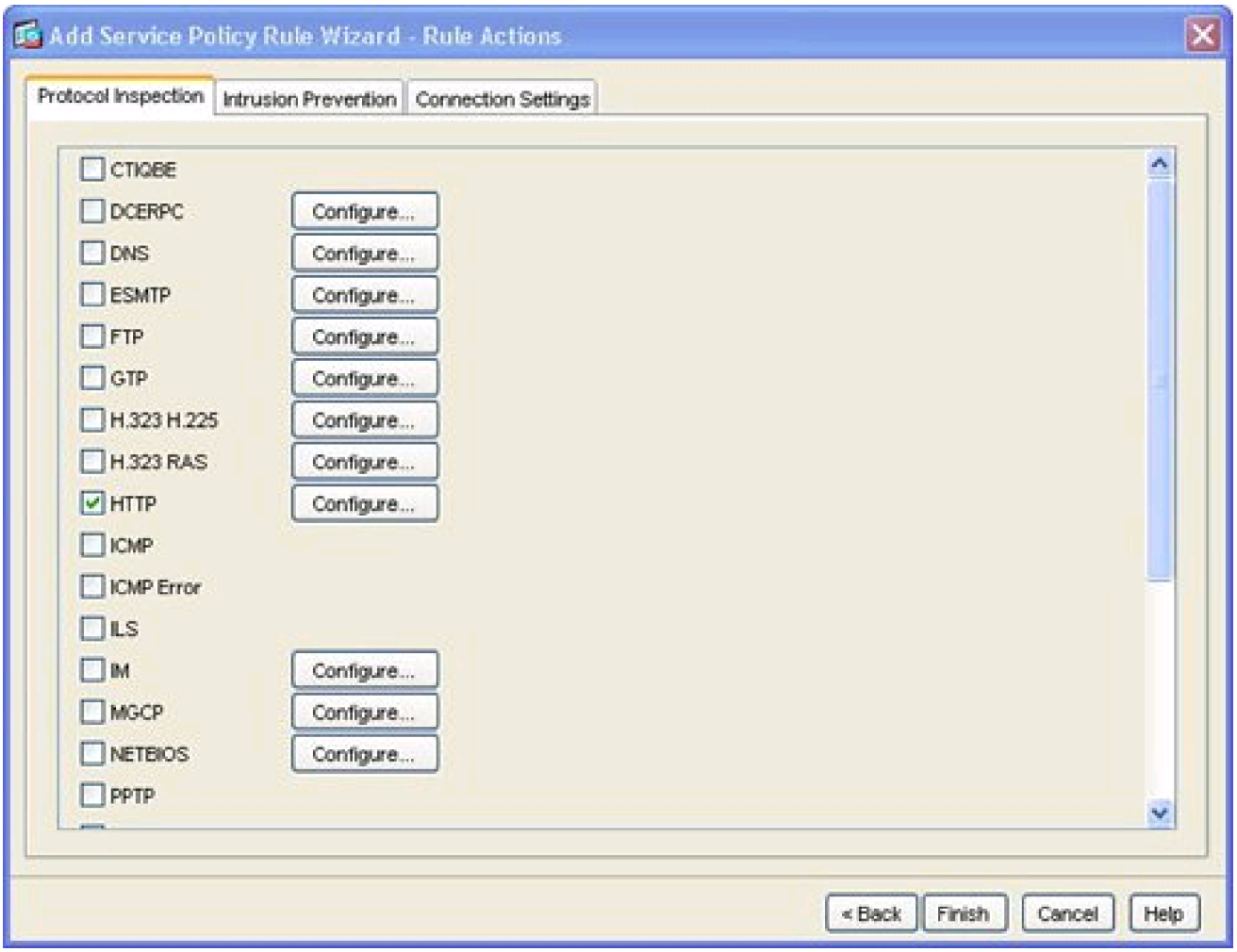


HTTP Map

Figure 3-20 displays an example of selecting protocol inspection for HTTP and the location to configure or select a customized HTTP map. An HTTP map is used to define the parameters of the inspection for HTTP. Multiple HTTP maps are allowed in order to have different HTTP normalization and enforcement rules for different traffic flows on different interfaces.

Figure 3-20. Configure HTTP Map

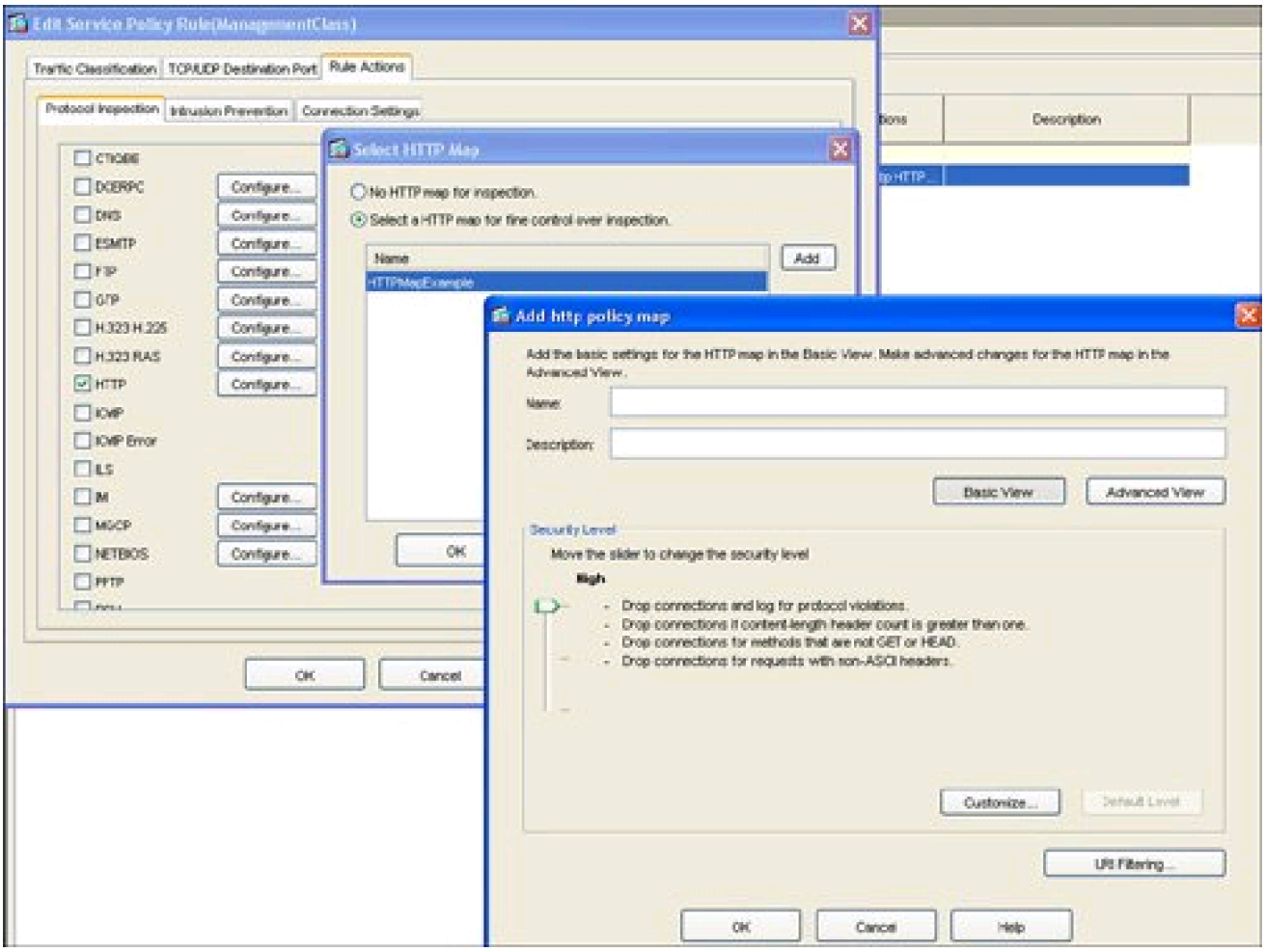
[View full size image]



An HTTP map can be configured to allow customized or specific processing for an HTTP protocol violation. Figure 3-21 displays an example of how to select an HTTP Map and the location of how to initiate the customization process for an HTTP map.

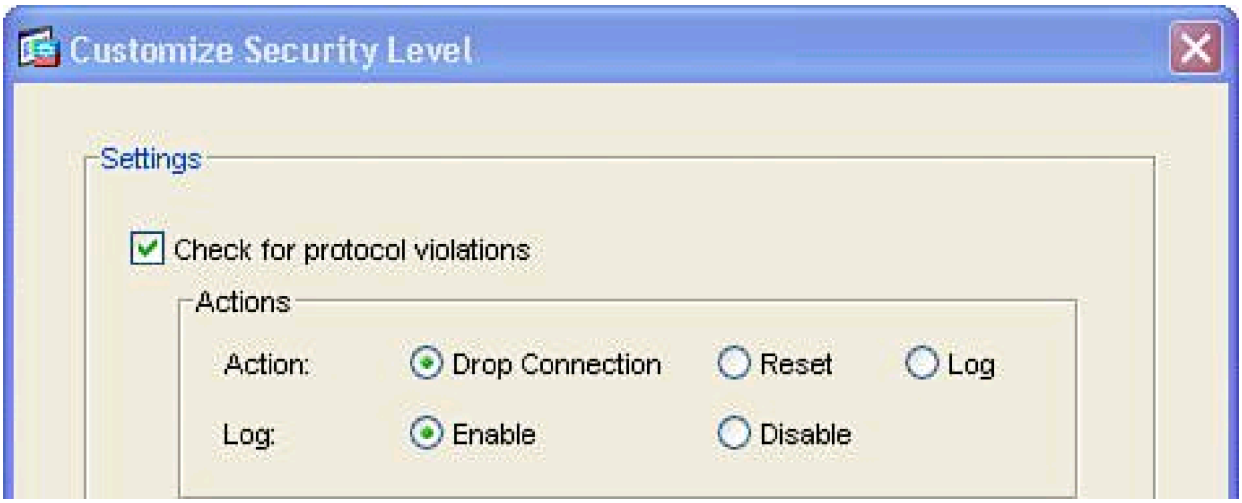
Figure 3-21. Select HTTP Map

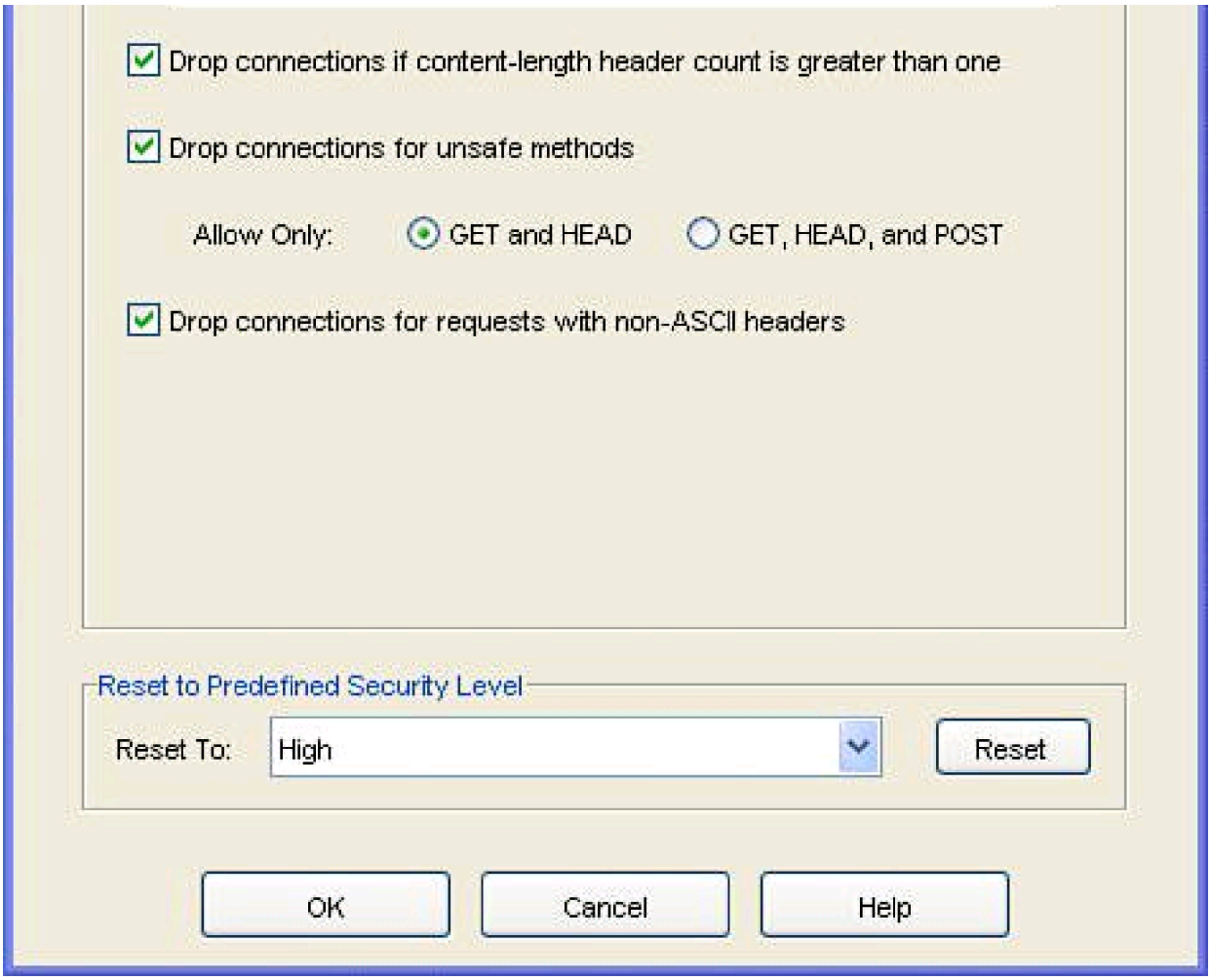
[View full size image]



An HTTP connection can be allowed, reset, or dropped, depending on conformance to the RFC standard. A syslog can also be generated for an HTTP connection that triggers the defined condition. ASDM can reset any HTTP connection that does not conform to the HTTP protocol. This stance to reset an HTTP connection in an HTTP Map enables the ASA to be self-defending by automatically resetting the nonconforming or suspect HTTP connection that could be used for a potential network attack. Figure 3-22 displays an example of the customizable options under the basic view of an HTTP Map and the basic protocol violation parameters in an HTTP map.

Figure 3-22. HTTP Map Protocol Violation Customization





The advanced view of an HTTP Map allows additional customization features, including the ability to restrict certain content or application types in an HTTP connection. For example, Figure 3-23 displays an example of how an HTTP Map can be customized to prevent or block MP3 download through an HTTP connection.

Figure 3-23. HTTP Content Type Inspection

[View full size image]

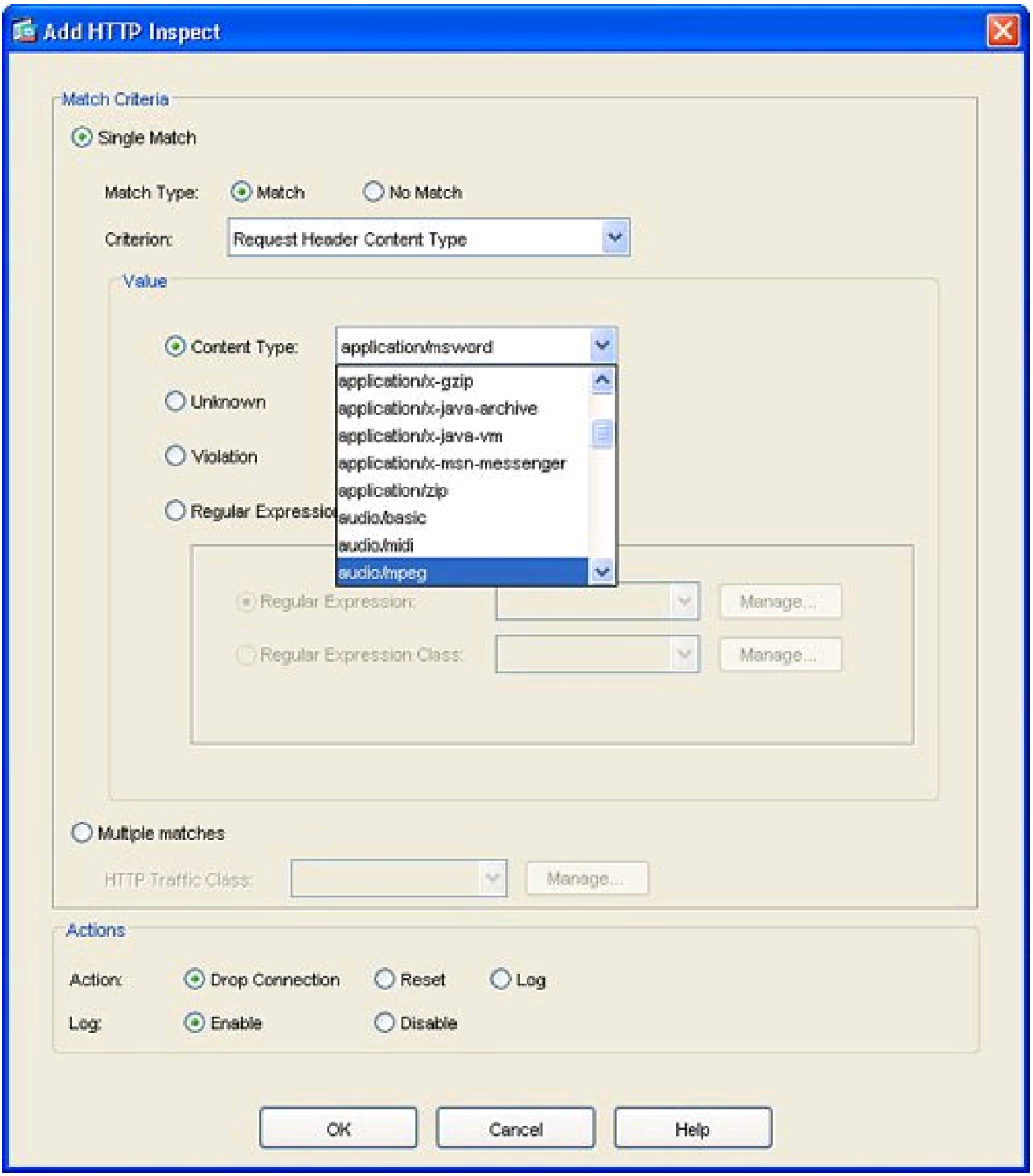
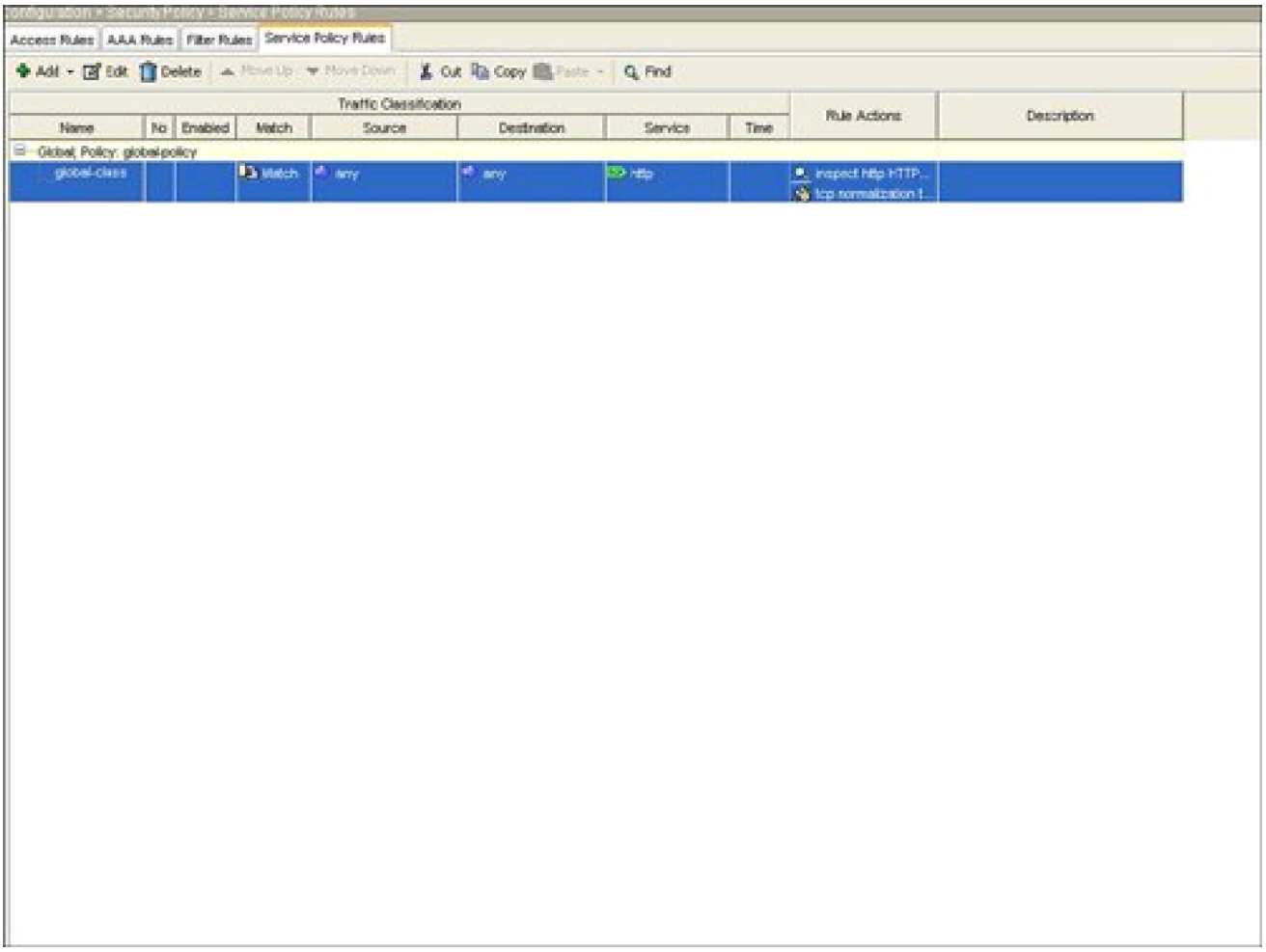


Figure 3-24 provides an example of a configured service policy rule to inspect TCP and HTTP traffic and references the corresponding TCP and HTTP maps.

Figure 3-24. Service Policy Rule for TCP and HTTP Protocol Inspection

[View full size image]


Access Rules
AAA Rules
Filter Rules
Service Policy Rules
Add
Edit
Delete
Move Up
Move Down
Cut
Copy
Paste
Find
Traffic Classification
Name
No
Enabled
Match
Source
Destination
Service
Time
Rule Actions
Description
Global Policy: globalpolicy
global-class
Match
any
any
http
Inspect http HTTP...
tcp-normalization t...

PREV

NEXT

Configuring Content Security and Control Security

The partnership between Cisco Systems and Trend Micro has enabled the creation of the Content Security and Control Security Module for the ASA product line. This Content Security and Control Security Service Module (CSC-SSM) implements many of the advanced virus, phishing, spam, and spyware control functions on the ASA platform. The functions that are implemented on the CSC-SSM Module include the following:

- Antivirus
- Antiphishing
- Antispam
- Antispyware
- URL filtering/blocking
- Content filtering
- File blocking

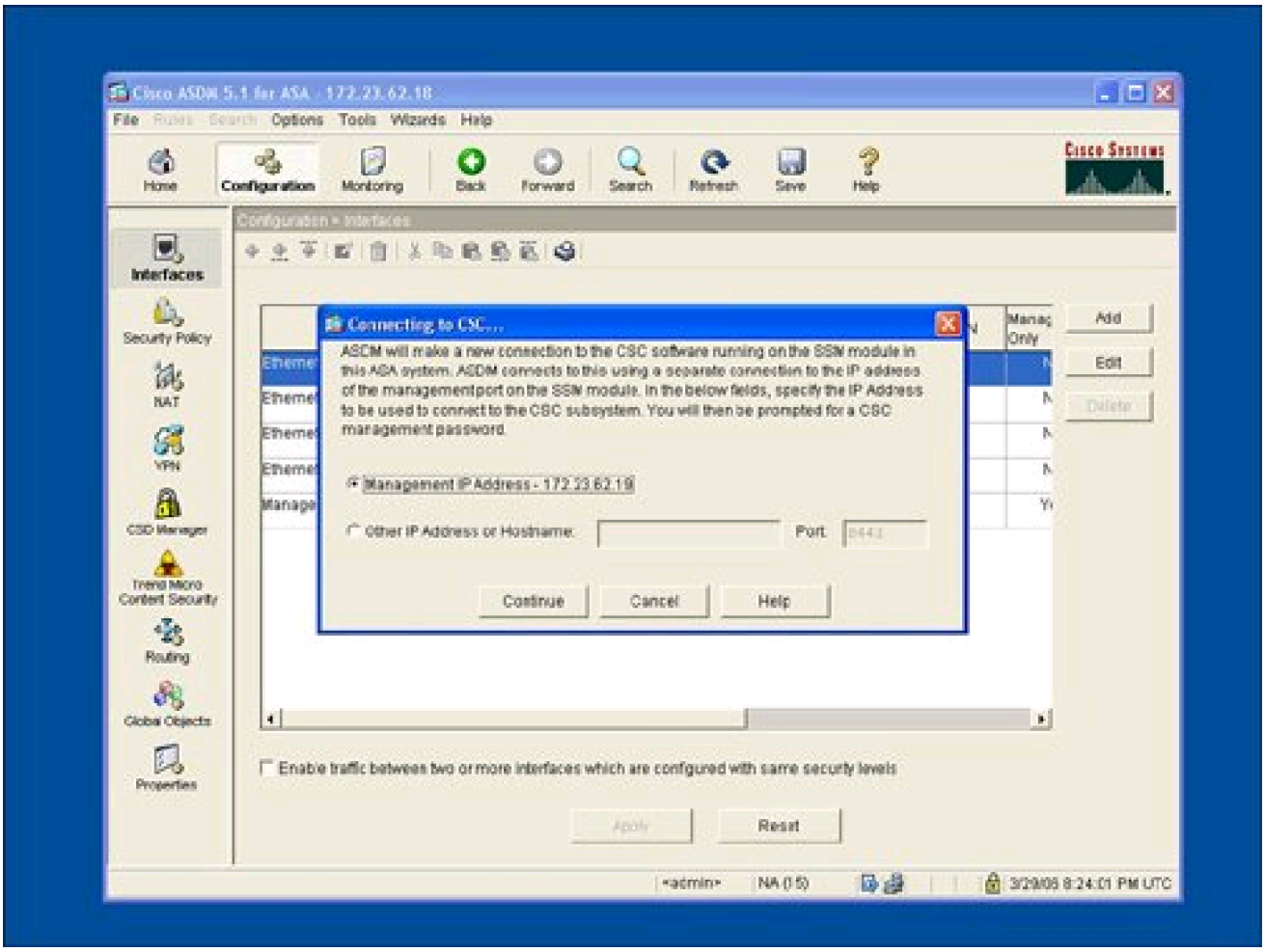
The base CSC-SSM license contains support for the antivirus, antispyware, and fileblocking features. An additional plus license is required to enable the antiphishing, antispam, URL filtering/blocking, and content filtering features. You can implement these base and plus functions on the following network protocol types that are supported by the CSC-SSM module:

- POP3
- SMTP
- HTTP
- FTP

The CSC-SSM module can be managed with ASDM. The CSC-SSM module management through ASDM uses the IP address, username, and password for the CSC-SSM module. Figure 3-25 displays the Trend Micro Content Security icon in ASDM and the initial logon to the Content Security SSM. In addition to ASDM management, the CSC-SSM modules can also be centrally managed by Trend Micro's Trend Micro Control Manager (TMCM) centralized management product.

Figure 3-25. Content Security Icon and CSC-SSM Logon in ASDM

[View full size image]



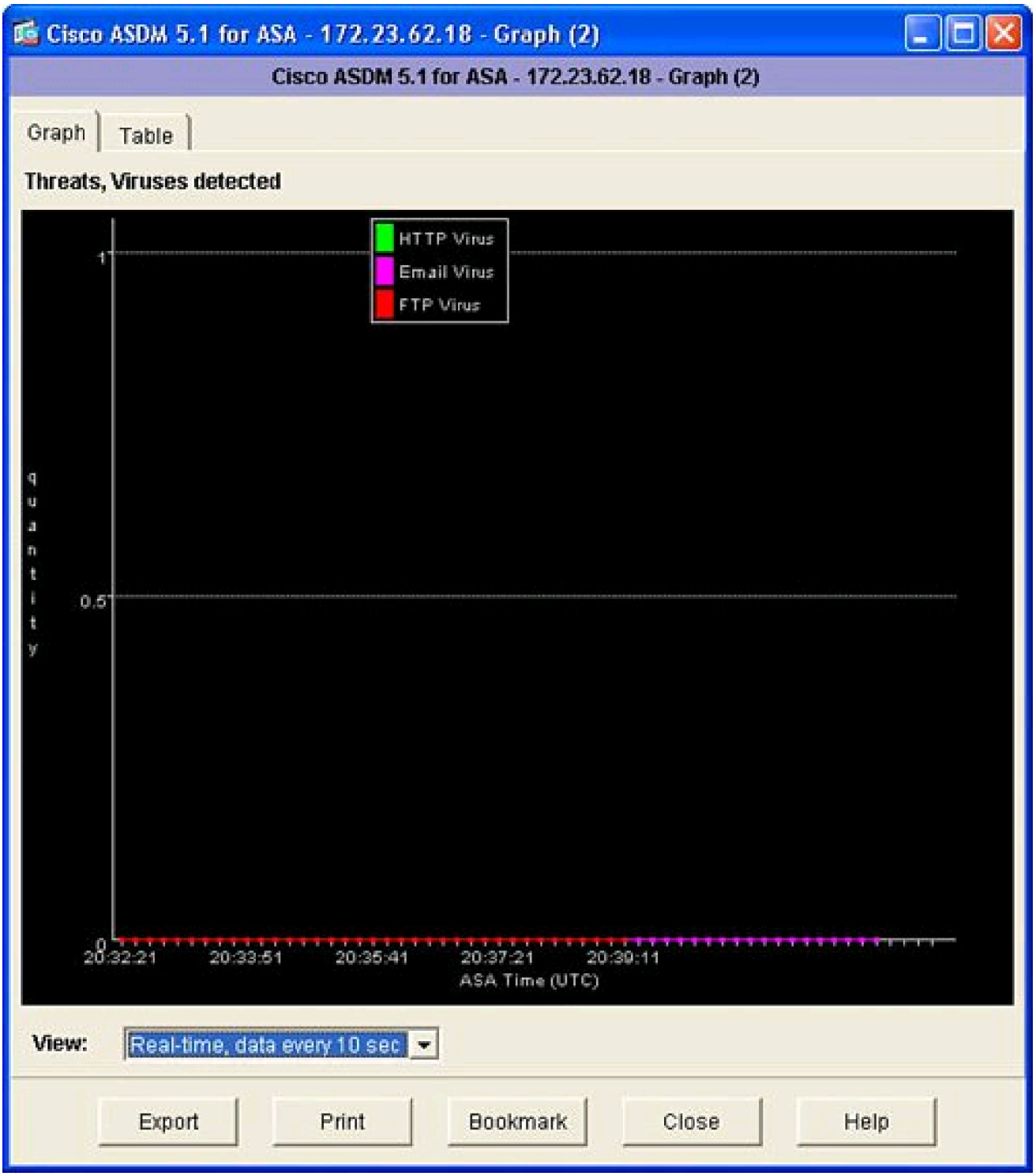
The main Content Security tab on the ASDM homepage features a near real-time update of the security threats that have been detected by the Content Security module. These security threats are divided into the following categories:

- Virus
- Spyware
- URL filtered/blocked
- Spam

Figure 3-26 displays the graphs in ASDM for virus detection. Similar threat graphs are also available for spyware detection, spam detection, and URL filtering/blocking protection. The threat graphs can be accessed from the Monitoring area in ASDM by selecting the Threat option under the Trend Micro Content Security icon.

Figure 3-26. Threat Graphs

[View full size image]



The CSC-SSM configuration process to send network traffic from the ASA chassis to the CSC-SSM is similar to that of other features in ASA, including the IPS-SSM module. CSCSSM, like IPS-SSM, uses the service policy rules described earlier in the "Intrusion Prevention Service" and "Protocol Inspection" sections of this chapter to specify what network traffic should be sent from the ASA chassis to the CSC-SSM module. The user can initiate configuration of the CSC-SSM module by selecting Configuration from the top of the ASDM GUI and then selecting the Trend Micro Content Security option from the left side of the ASDM GUI. Selecting the Configuration option for Trend Micro Content Security will result in the display of the items that can be configured on the CSC-SSM module including Content Security and Control Services Module (CSC-SSM) setup, web (URL filtering/blocking), mail (scanning, content filtering, antispam), file transfers (scanning, blocking), and updates.

Content Security and Control Services Module (CSC-SSM) Setup

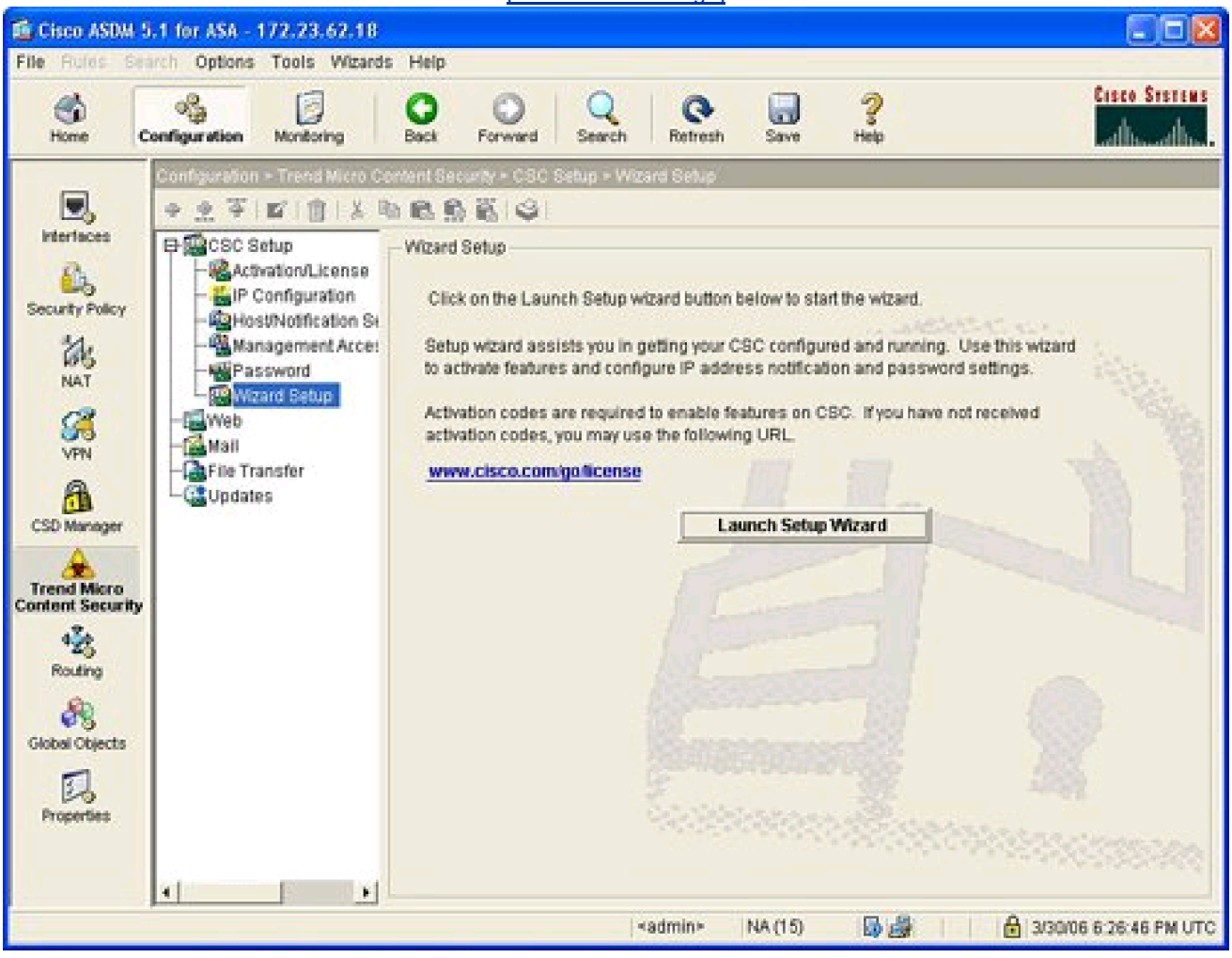
CSC Setup options include the following:

- Activation/license
- IP configuration
- Host/notification settings
- Management access host/networks
- Password
- Setup Wizard

The CSC-SSM Setup Wizard walks the user through each of the CSC-SSM setup steps. Figure 3-27 displays CSC Setup options in the GUI and the launch point for the Setup Wizard screen of the CSC-SSM Setup Wizard.

Figure 3-27. CSC-SSM Setup Wizard

[View full size image]



Web

The CSC-SSM module features the following web or HTTP functions:

- URL blocking (antiphishing and antispyware)
- URL filtering
- HTTP/web scanning
- File blocking

The configuration of these web features requires ASDM to launch the integrated Trend Micro InterScan for Cisco CSC-SSM management.

Trend Micro InterScan requires an additional password to be entered to log on. Figure 3-28 displays the web options in ASDM for CSC-SSM, and Figure 3-29 provides the resulting logon screen to Trend Micro InterScanFigure 3-30 displays the Summary page in Trend Micro InterScan, which can be displayed after logon to Trend Micro InterScan from ASDM.

Figure 3-28. Trend Micro Content Security Options

[View full size image]

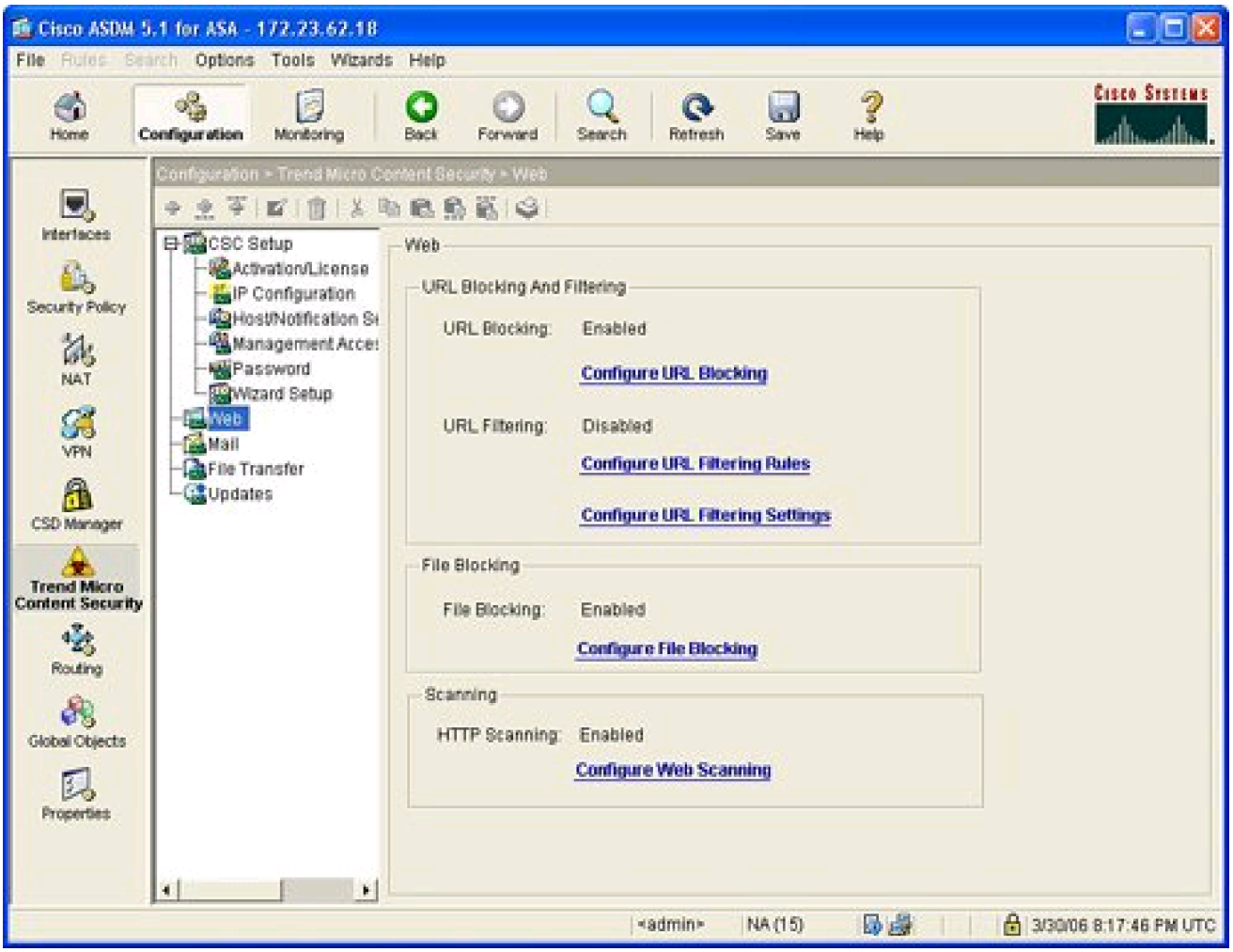
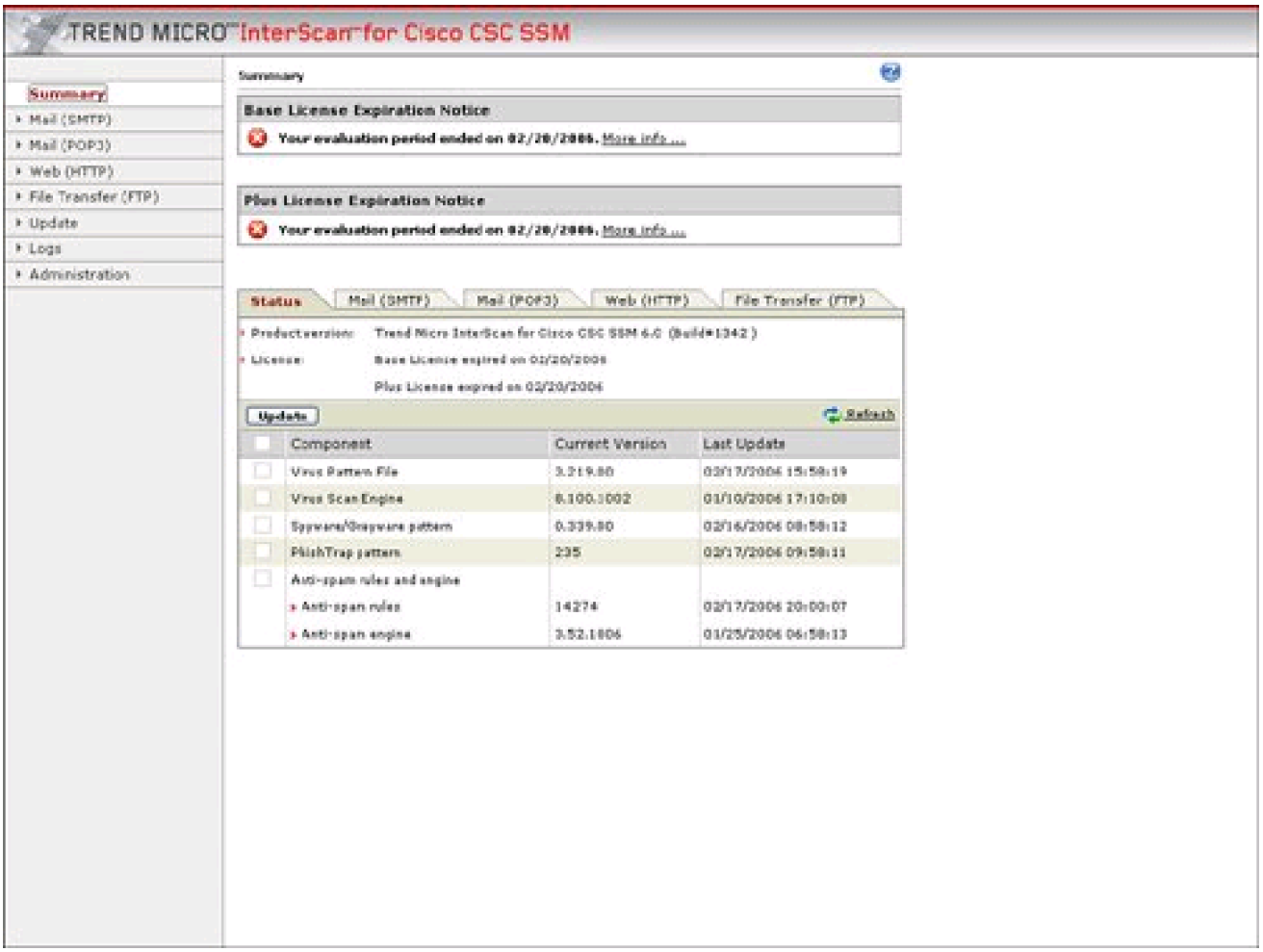


Figure 3-29. Log on to Trend Micro InterScan for Cisco CSC-SSM

[View full size image]

Figure 3-30. Trend Micro InterScan Summary

[View full size image]



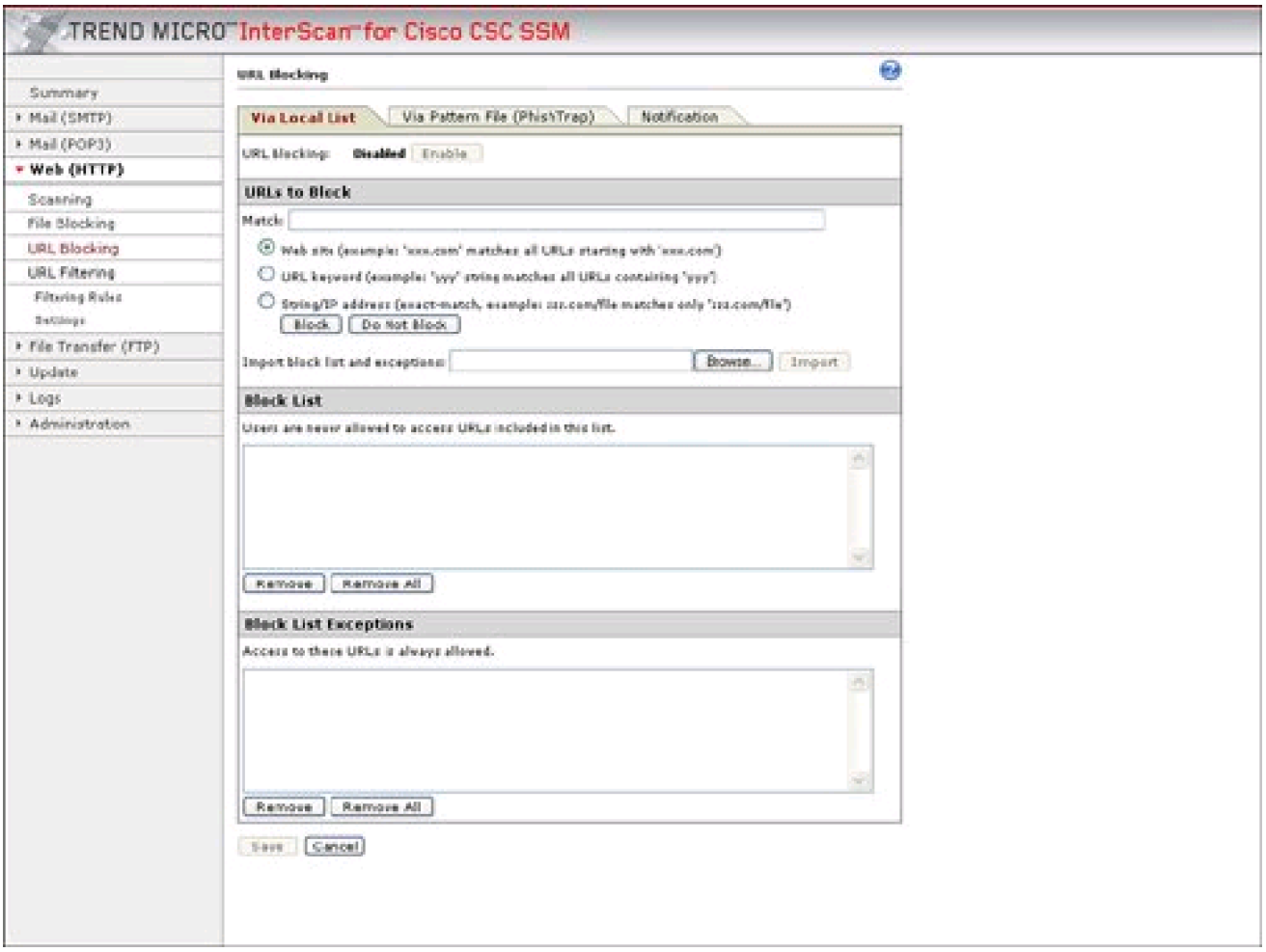
URL Blocking

URL Blocking allows a specific URL to be blocked, thus preventing a user from accessing a specific website or webpage. ASDM, through the launch of the integrated Trend Micro InterScan Device Manager, allows the URL blocking feature to be configured including blocking on wildcards and the ability to always allow a specific list of URLs.

Figure 3-31 displays the location to select web URL blocking configuration and the resulting configuration options that are displayed in Trend Micro InterScan.

Figure 3-31. URL Blocking in Trend Micro InterScan

[View full size image]



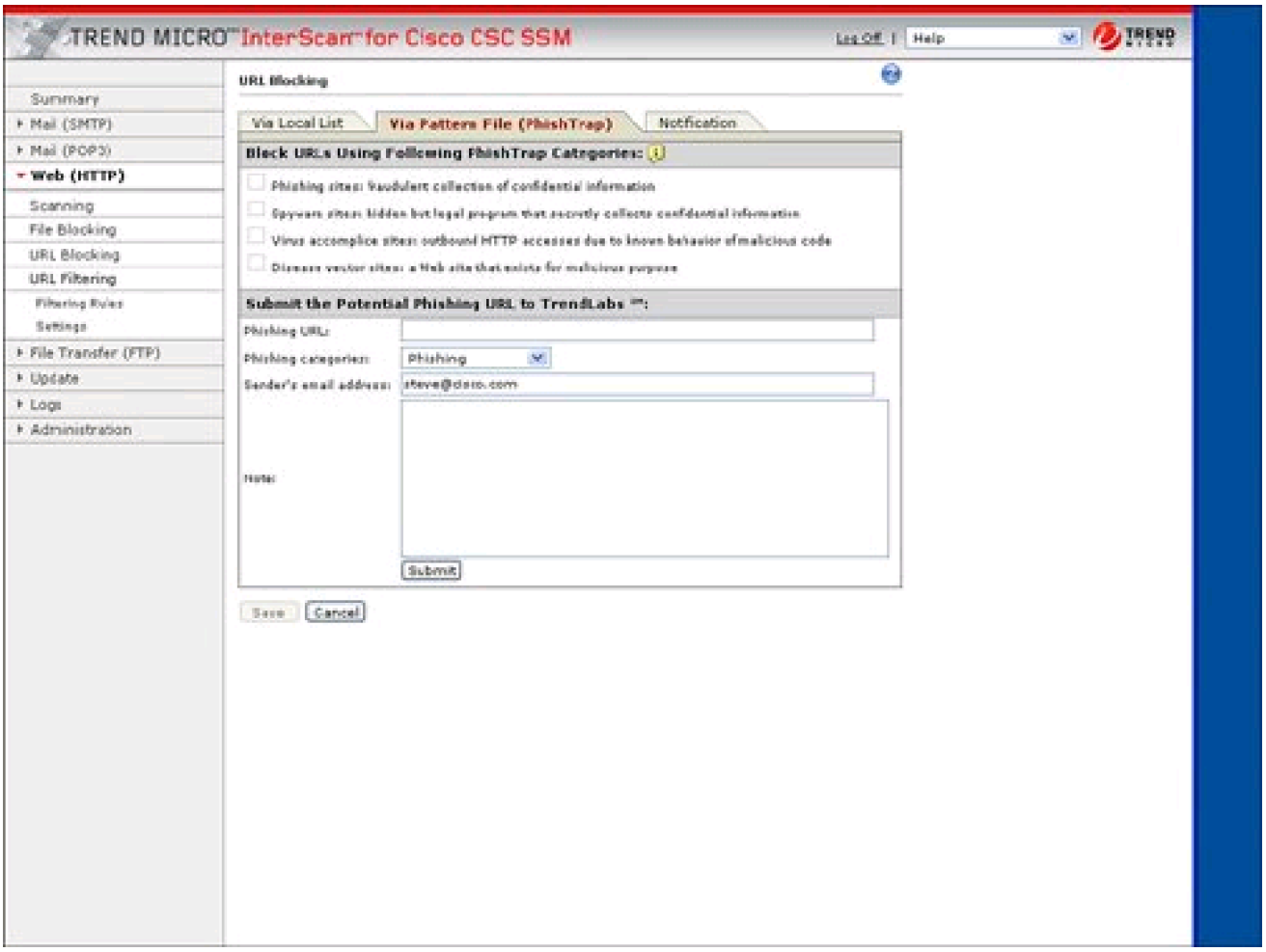
Phishing is a type of malware with which an e-mail is sent to an unsuspecting user with a link to a fake website. These phishing e-mails can attempt to trick the user to log on to what appears to be a valid banking or e-commerce site. However, what the user is really logging on to is a fake website, and the attacker's purpose is the gathering of the user's account information.

Trend Micro collects and maintains a list of these phishing or fake websites. The CSC-SSM module can block the HTTP connection and protect the user from accessing one of these known phishing websites. Trend Micro also collects a list of known websites that harbor spyware. Network attackers often plant spyware on more vulnerable websites and attempt to download spyware to unsuspecting users that frequent these websites. The CSC-SSM module also features the ability to block URL access to prevent users from accessing one of these known websites that are rife with spyware.

Figure 3-32 provides an example of how antiphishing and antispyware can be enabled for URL inspection through the ASA CSC-SSM. Figure 3-32 also displays how you can identify a specific phishing site and update Trend Micro's phishing sites list.

Figure 3-32. Antiphishing and Antispyware

[View full size image]



URL Filtering

CSC-SSM supports the use of predefined types of websites that can be filtered, including entertainment, gambling, job search, and so on. The websites within these categories are updated and maintained through Trend Micro. These categories of websites can also be filtered based upon the time of day to permit certain sites during leisure time but not during standard work hours.

Scanning

Scanning enables the CSC-SSM module to scan HTTP traffic, including that for web mail, and to detect and remove certain viruses or spyware that could be used to implement a network attack. CSC-SSM also features the ability to clean an infected file or to delete the infected file before it is transported to the user over the scanned HTTP or web connection.

File Blocking

File blocking enables certain file types or file extensions to be blocked so they are not transported over an HTTP or web download

connection. File types that can be blocked include MP3, JPG, EXE, java, and Microsoft Office applications.

Mail

CSC-SSM can provide protection for the POP3 and SMTP mail protocols. The CSC-SSM module supports the following mail security functions for incoming and outgoing POP3 and SMTP network traffic:

- Scanning
- Spam protection
- Content filtering

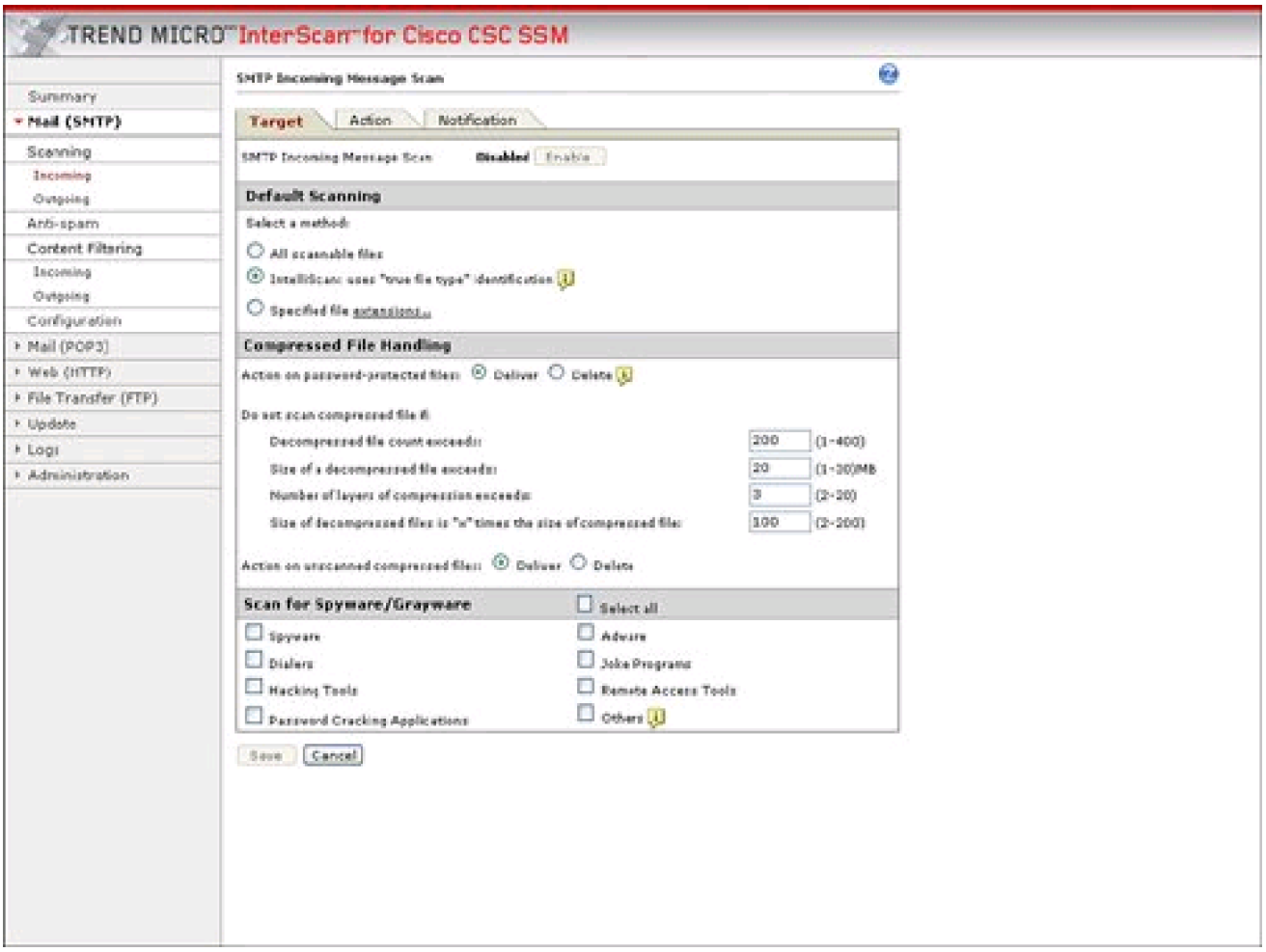
Scanning

Scanning allows incoming and outgoing e-mail to be scanned for viruses, spyware, and other malware. Infected attachments can be either cleaned or deleted before they are delivered to the user.

Figure 3-33 displays an example of configuring virus and other malware scanning for incoming SMTP mail.

Figure 3-33. Scanning Configuration for Incoming SMTP Mail

[View full size image]



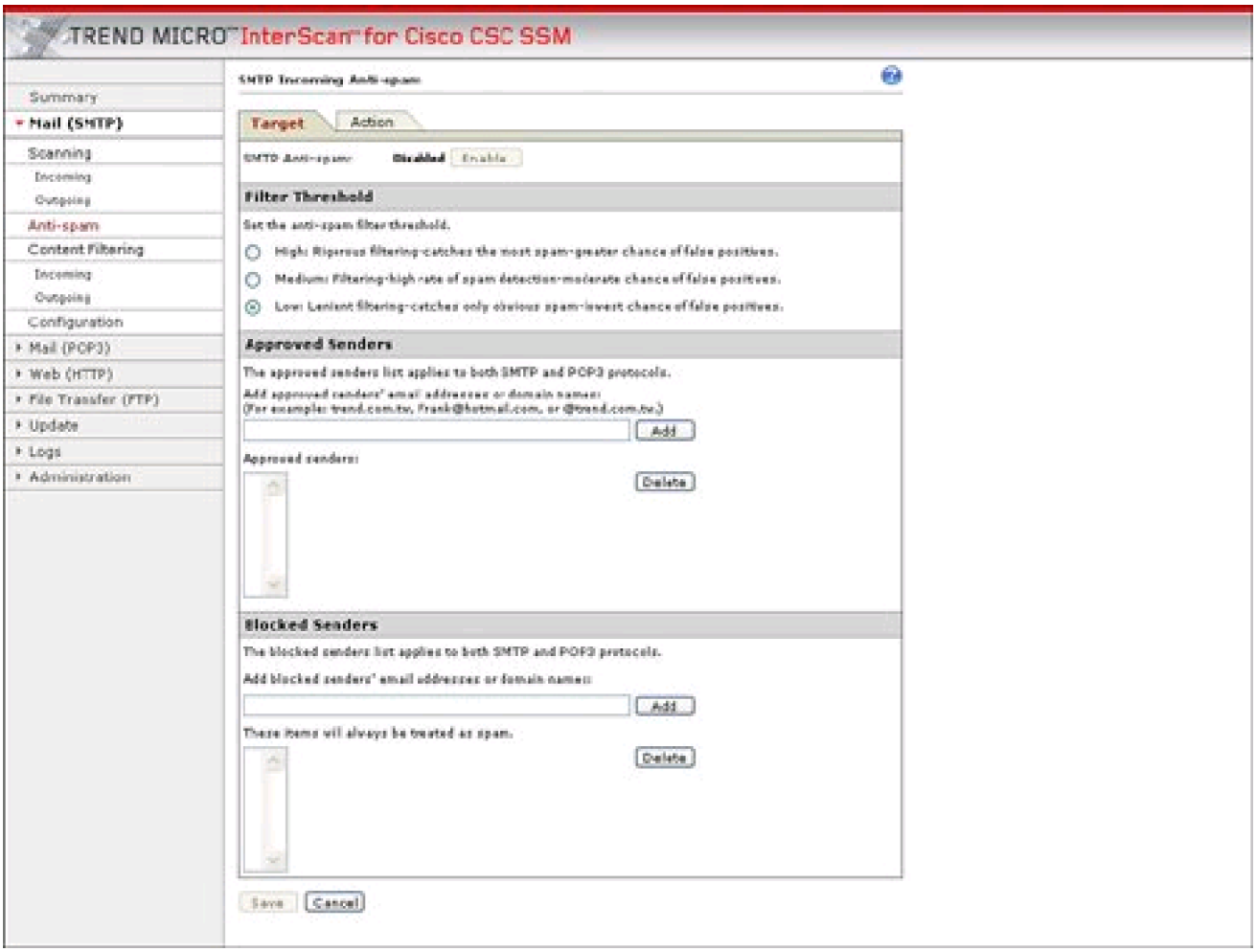
Antispam

The Mail configuration option in Trend Micro InterScan for CSC-SSM also contains the ability to protect e-mail users from spam. Spam messages can contain a potential network threat, in addition to being a nuisance. The antispam capability in ASA CSC-SSM can both reduce the exposure to spam-based network attacks and increase productivity by reducing spam to users of a network.

The antispam capability enables the administrator to define spam threshold buckets of high, medium, or low. The easy-to-use configuration of Antispam through the integration of ASDM and Trend Micro InterScan also enables the administrator to permit specific e-mail sources or block specific e-mail sources/spammers. Figure 3-34 displays the Antispam configuration options of ASA CSC-SSM.

Figure 3-34. Antispam Configuration

[View full size image]

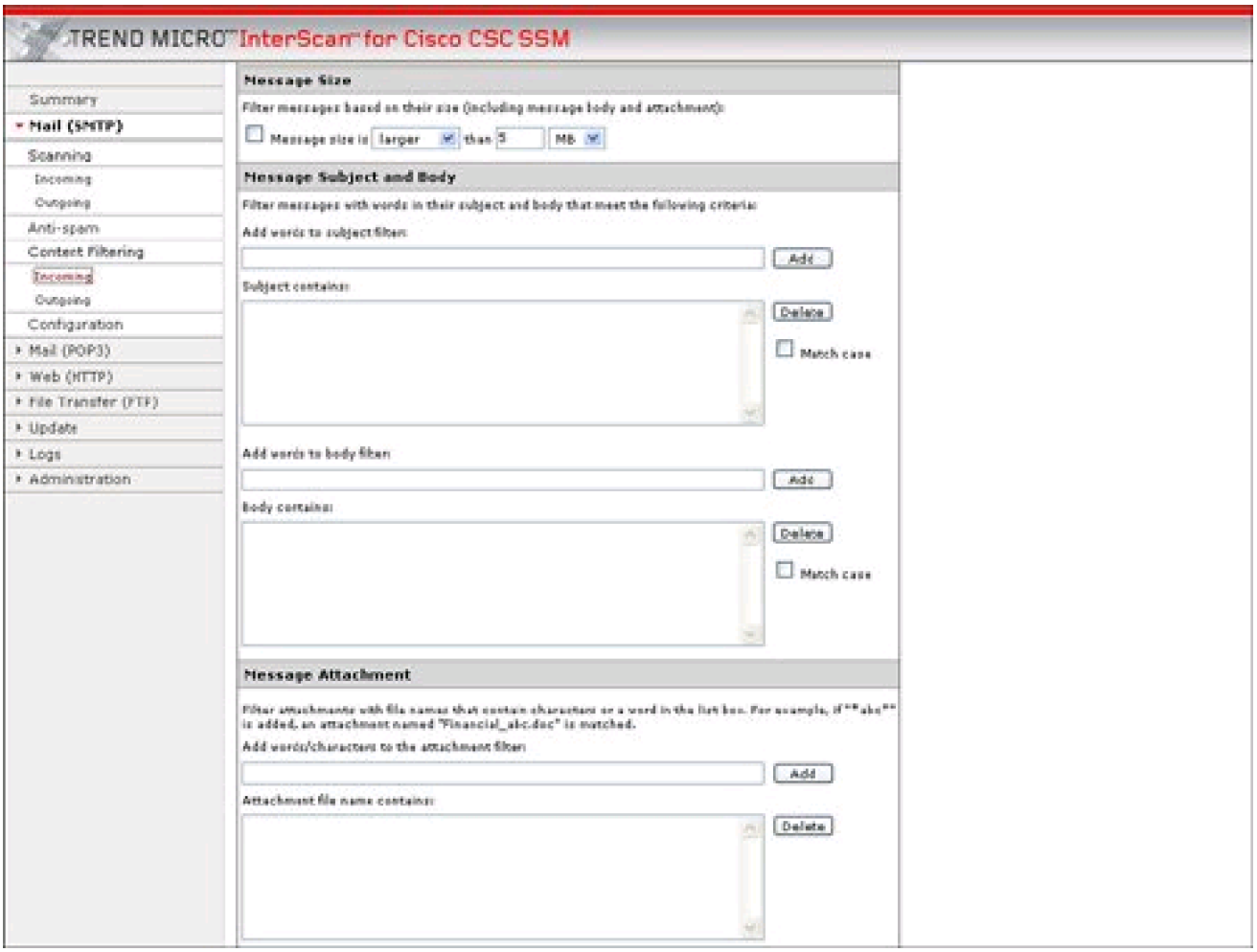


Content Filtering

The CSC-SSM module can filter mail based upon the type of content in the e-mail. For example, mail that exceeds a certain size can be filtered. Mail with a certain filename on an attachment or an attachment of a certain file type, like MP3, JPG, or EXE, can also be filtered or removed from an e-mail before delivery to the user. Figure 3-35 displays an example of the content filtering options.

Figure 3-35. Content Filtering Configuration

[View full size image]



File Transfer

CSC-SSM provides protection for file transfers using FTP. CSC-SSM allows both the scanning of FTP network traffic for viruses and other malware and the blocking of file transfers based upon file types. File types that can be blocked include MP3, JPG, EXE, Java, and Microsoft Office file extensions. The file transfer, or FTP, scanning, and blocking configuration options are very similar to the web scanning and file blocking features described in the "web" section for CSC-SSM in this chapter.

PREV NEXT

Summary

The Cisco ASA product line offers an extensive list of security features in a single appliance, including firewall, antispoofing, protocol inspection, VPN, IPS, content security, and control security. IPS, content security, and control security are implemented as a hardware security services module (AIP-SSM and CSC-SSM). The CSC-SSM module implements advanced security functions, including antivirus, antispam, antiphishing, URL filtering and blocking, and file transfer scanning and blocking. The extensible architecture of the ASA product line, combined with the partnership with Trend Micro on the Content Security and Control Security Service Module (CSC-SSM), enable the ASA product to be the platform for future security innovations.

The different footprint, capacity, and price points of the ASA product line enable the ASA to be used in both remote branches and the data center. ASA features an easy-to-use device manager, ASDM, that allows new users to get up-to-speed quickly on configuring the ASA. ASA is also centrally managed by the Cisco Security Manager, which enables hundreds of ASA appliances to be managed with thousands of routers for a single view of security configuration, integration, and enforcement between these two platforms. The Cisco Security Manager can also centrally manage the IPS signature configuration on the ASA AIP-SSM module along with other Cisco IPS devices.

References

Abelar, Greg . Securing Your Business with Cisco ASA and PIX Firewalls. Cisco Press, 2005.

Cisco Systems, Inc. Cisco Adaptive Security Appliance Command Line Configuration Guide, Version 7.0.
http://www.cisco.com/en/US/products/ps6120/products_configuration_guide_chapter09186a00804522f6.html

Cisco Systems, Inc. Cisco Security Appliance Command Reference, Version 7.0
http://cisco.com/application/pdf/en/us/guest/products/ps6120/c2001/ccmigration_09186a0080666332.pdf

Cisco Systems, Inc. Content Security and Control SSM Administrator Guide.
http://www.cisco.com/en/US/partner/products/ps6120/products_administration_guide_book09186a00805ac11d.html (Requires Cisco.com registration.)

Chapter 4. Cisco Incident Control Service

Cisco and Trend Micro have partnered to create several security components. One component of the partnership is the antivirus signatures in Cisco Intrusion Prevention System (IPS) products. Another component of the partnership is the Content Security and Control Security Services Module for the Adaptive Security Appliance (ASA) as discussed in Chapter 3, "Cisco Adaptive Security Appliance Overview." A third component of the partnership is the automatic download of access lists and new incident signatures for attacks such as worms and viruses from Trend Micro to Cisco router, ASA, and IPS devices. The download of access lists and signatures for new security incidents from Trend Micro helps to enable Cisco networks to be self-defending against new network attacks. Cisco Incident Control Service (Cisco ICS) manages the worm and virus access list and signature download service from Trend Micro.

Cisco ICS enables the automatic or manual download of access lists and IPS signatures to security devices. The download of access lists from Trend Micro can enable a new attack to be identified and stopped or slowed in less than one hour. Trend Micro maintains a database of new attacks, such as worms. Trend Micro, through the Cisco ICS and the service with Trend Micro, attempts to define an access list that will stop the new network worm within one hour of the discovery of the worm. This access list provides the broad protection against the worm, while Trend Micro creates a specific, custom signature to stop the worm. Trend Micro attempts to define a custom signature to stop the incident within several hours of identifying the incident or worm. This signature can also be either automatically or manually downloaded to the IPS device to stop the newly identified network incident.

Chapter 3 discusses the ASA appliance with support for IPS signatures, access lists, and antivirus protection. Cisco ICS, with the update service from Trend Micro, provides an extra layer of protection in the self-defending network by deploying or recommending access lists and IPS signatures when a new network outbreak such as a worm is identified. In addition to using TrendLabs to identify a new network attack, Cisco ICS also is a product in the self-defending network that focuses on worm mitigation.

Note

In this chapter, as with many other chapters in this book, some of the text and figures were created while the Cisco ICS product was being developed in order to get this book to you as soon as possible once the products are released. You may see some minor differences in the graphical user interface (GUI) and functionality between the figures in this chapter and the released products. GUIs also often change between different released versions of the product, so you may also see some differences between the text and figures in this book and products released after this book's publication date.

This chapter describes the role of Cisco ICS in controlling network incidents and explains the different options, including outbreak prevention access control lists (OPACLs), outbreak prevention signatures (OPSigs), outbreak prevention reports, and logs.

Implementing Outbreak Management with Cisco ICS

Cisco ICS is a centralized management product from Cisco that manages the automated IPS signature update service with Trend Micro for new security incidents. Cisco ICS can deploy a broad access control lists (ACLs) to stop the spread of a newly identified infection through the network. These ACLs are known as OPACLs.

After analysis of the new network incident by Trend Micro, Cisco ICS can also deploy a specific signature to mitigate a new network infection outbreak such as a worm. These signatures are known as OPSigs. OPSigs can be deployed to IOS routers with IPS signatures and other Cisco IPS systems.

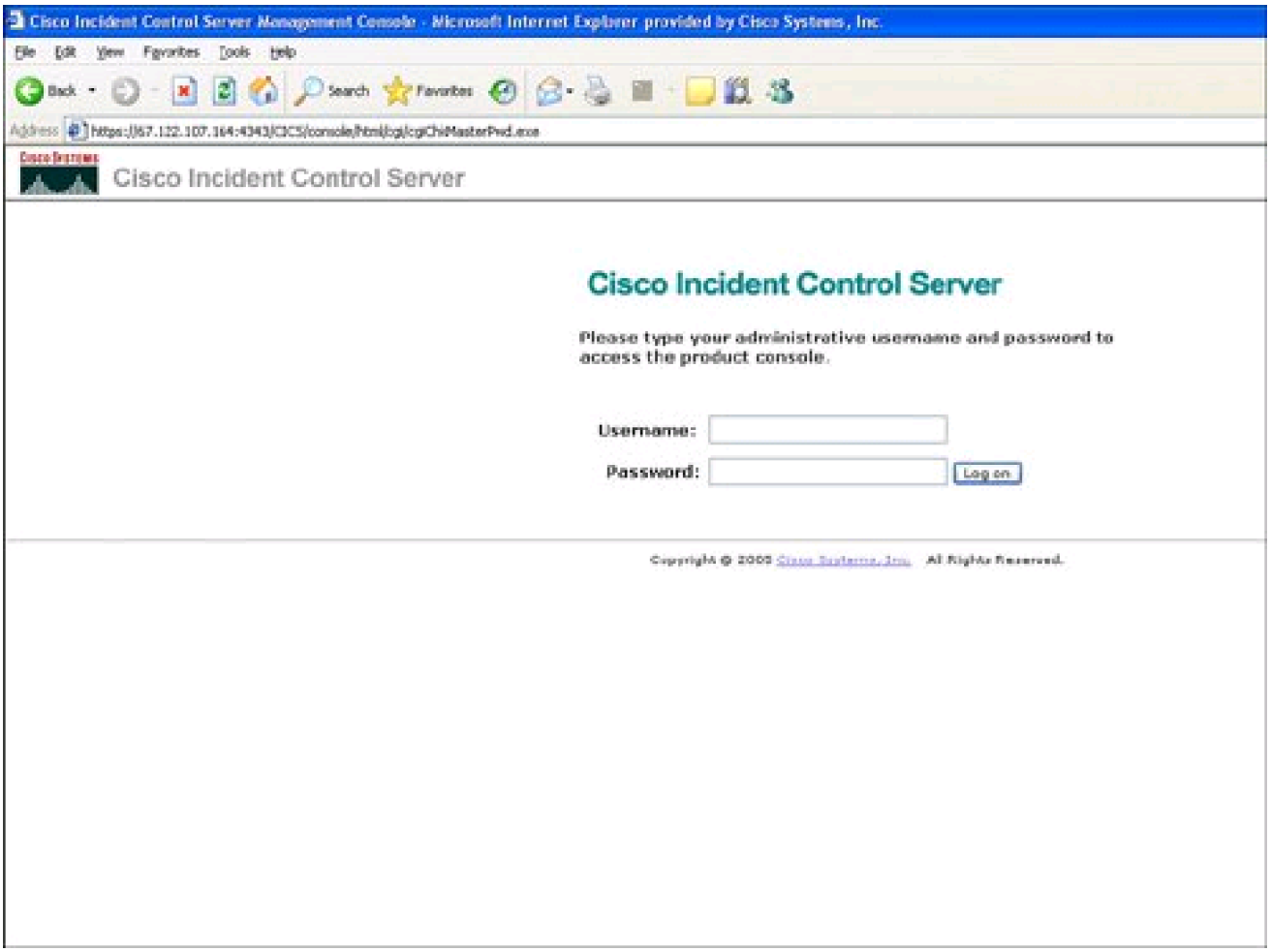
The first step in the ICS system is the identification of a new network threat. After a network threat is identified, Trend Micro will post on its website the information required to mitigate or reduce the impact of the network attack. The typical list of events that transpires to control the network incident includes the following items:

1. Trend Micro's TrendLabs identifies a new network threat or attack.
2. Trend Micro's TrendLabs creates an outbreak management task file. This outbreak management task file contains a broad OPACL that will prevent the outbreak from spreading throughout the network.
3. Cisco ICS can automatically download this outbreak management task file for the new network threat.
4. The OPACL in the task file can be either automatically deployed or manually deployed after human intervention. There is also an exception list that will prevent Cisco ICS from applying an ACL for a specific port for common network traffic, such as HTTP (TCP Port 80).
5. TrendLabs releases an OPSig to enable IPS devices to detect the new network threat. Typically the OPSig is released within a few hours of the release of the outbreak management task file with the OPACL.
6. Cisco ICS downloads the OPSig, either automatically or manually.
7. The original OPACL expires after the download of the OPSig.
8. Cisco ICS uses IPS events to determine if a host is sending network traffic that is considered to be a network threat and could possibly be infected. If a host is determined to be infected, the infected host is added to the watch list in Cisco ICS.

Cisco ICS is a Windows server application, and the client GUI is a web browser. Internet Explorer is required as the web browser since ActiveX is used as part of the client GUI. The logon screen for the Cisco ICS is displayed in Figure 4-1.

Figure 4-1. Cisco ICS Logon

[View full size image]



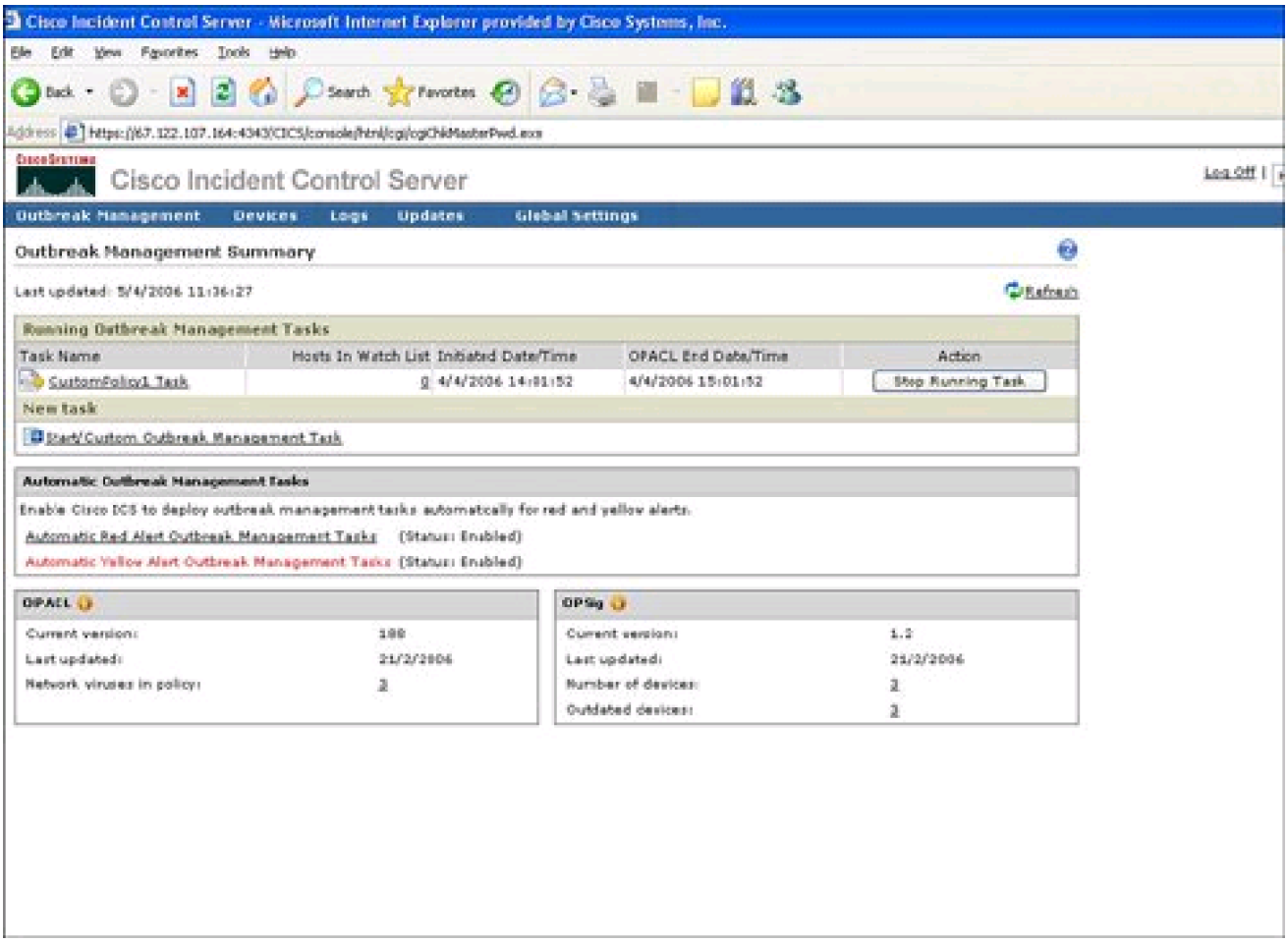
Outbreak Management Summary

The Cisco ICS summary page shown in Figure 4-2 provides a summary of the tasks to manage a network outbreak. The Outbreak Management Summary page is divided into the following areas:

- Active Outbreak Management Tasks
- Automatic Outbreak Management Tasks
- OPACL
- OPSigs

Figure 4-2. Cisco ICS Summary Page

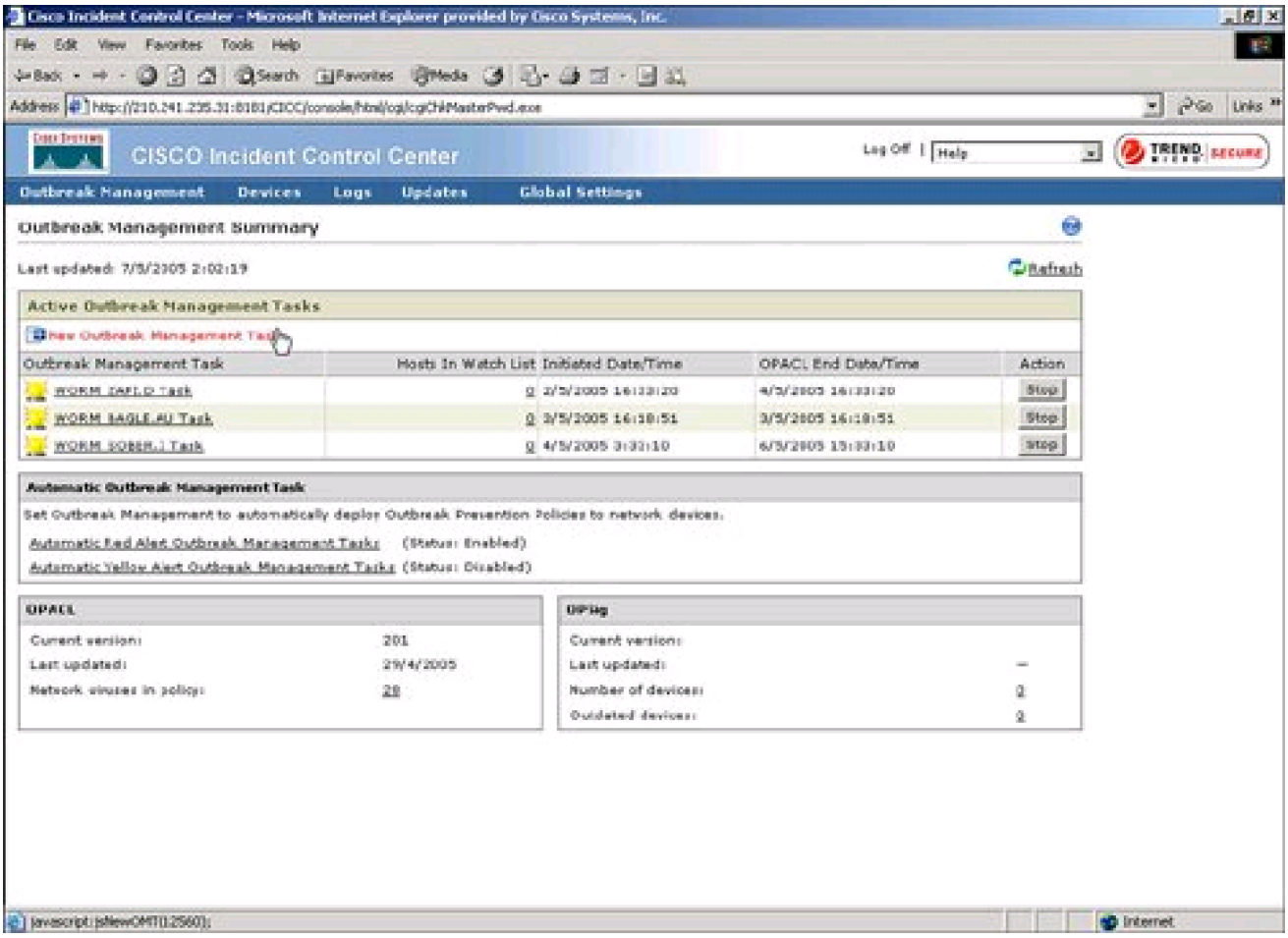
[View full size image]



Any new outbreak management tasks are highlighted at the top of the Active Outbreak Management Tasks. The location to select a new outbreak management task is displayed in Figure 4-3.

Figure 4-3. Selecting a New Outbreak Management Task

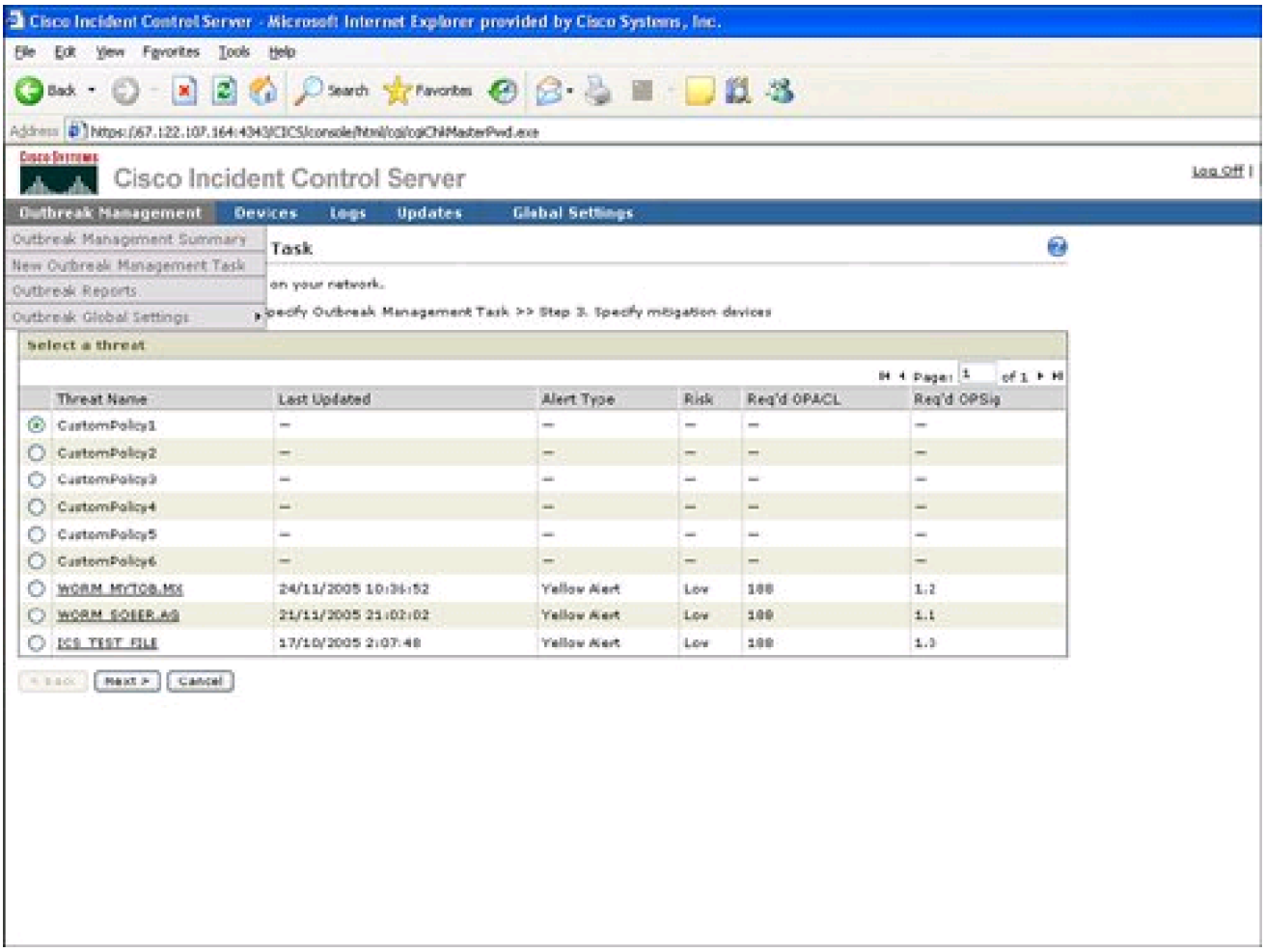
[View full size image]



Selecting a new outbreak management task results in the display of network threats with the new threat or corresponding outbreak management task selected, as shown in Figure 4-4.

Figure 4-4. Selecting Name of Threat

[View full size image]

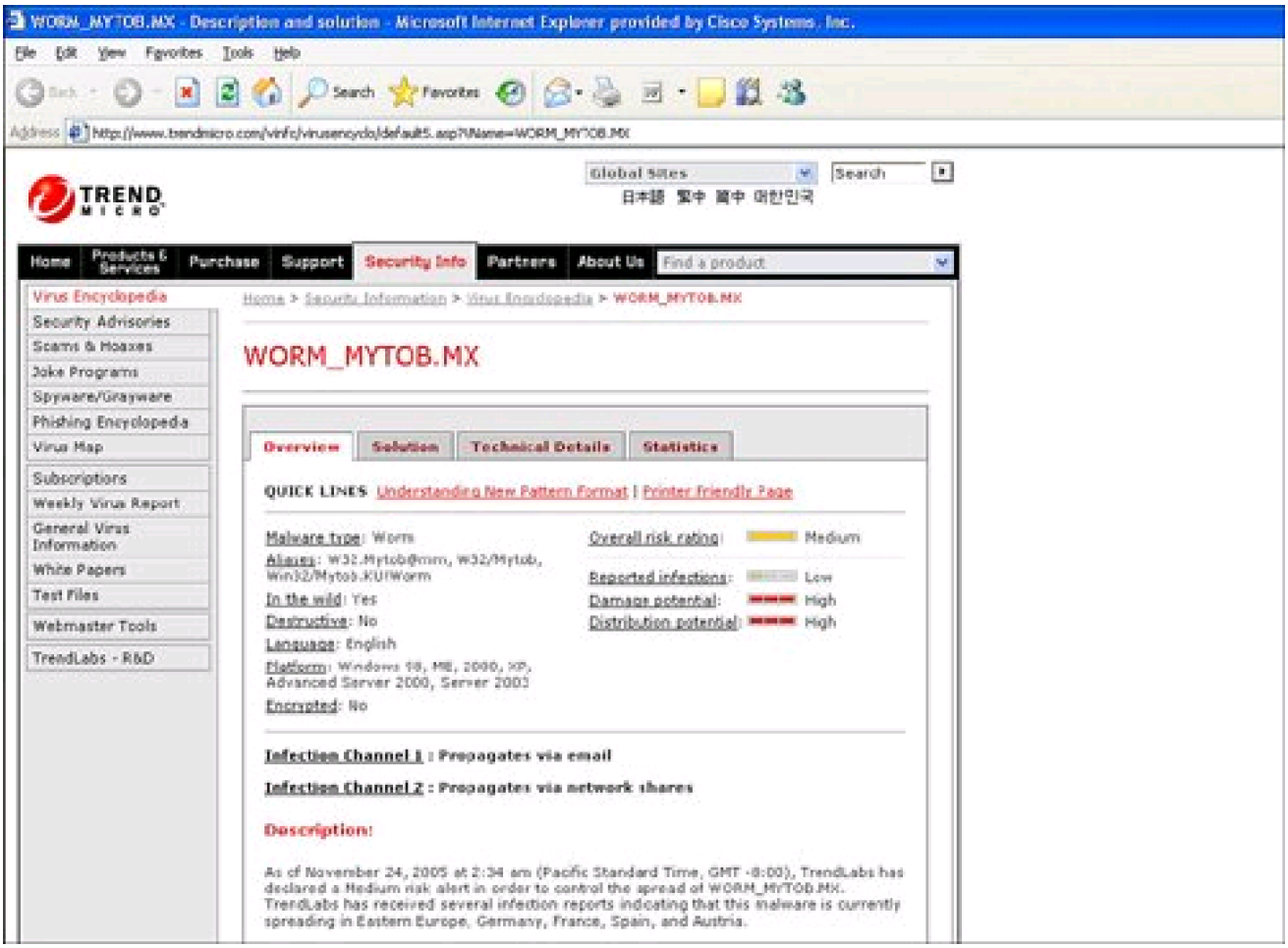


Information and Statistics on Network Threats from Trend Micro

Each threat name contains a link to information about that threat from Trend MicroFigure 4-5 provides an overview of the network threat from Trend Micro. The network threat information is displayed by selecting the name of the threat or incident.

Figure 4-5. Overview of Threat

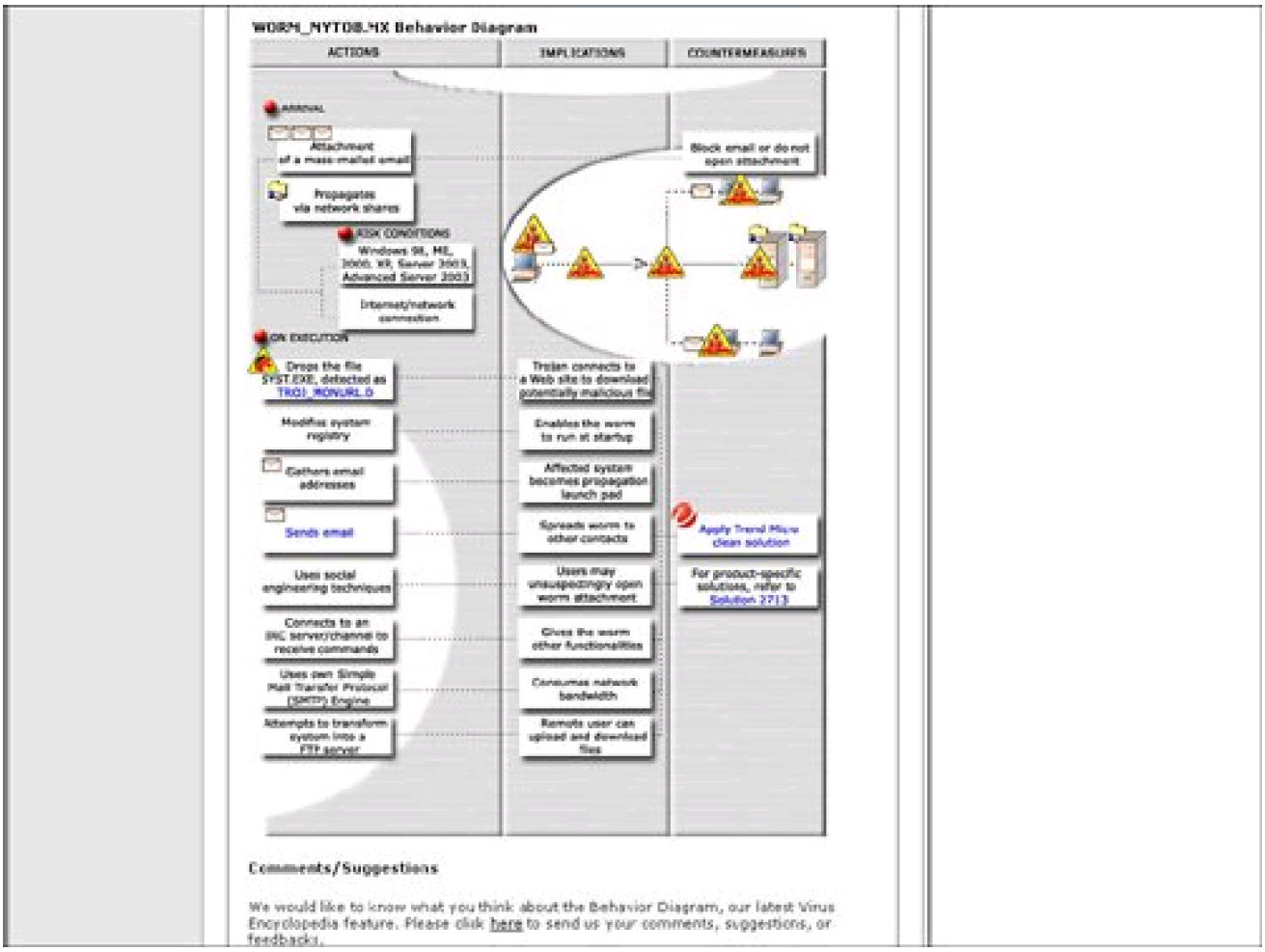
[View full size image]



The overview can also contain a behavior diagram of the network threat. A behavior diagram can contain actions, implications, and countermeasures for the network threat. Figure 4-6 provides an example of a behavior diagram from Trend Micro.

Figure 4-6. Behavior Diagram of Threat

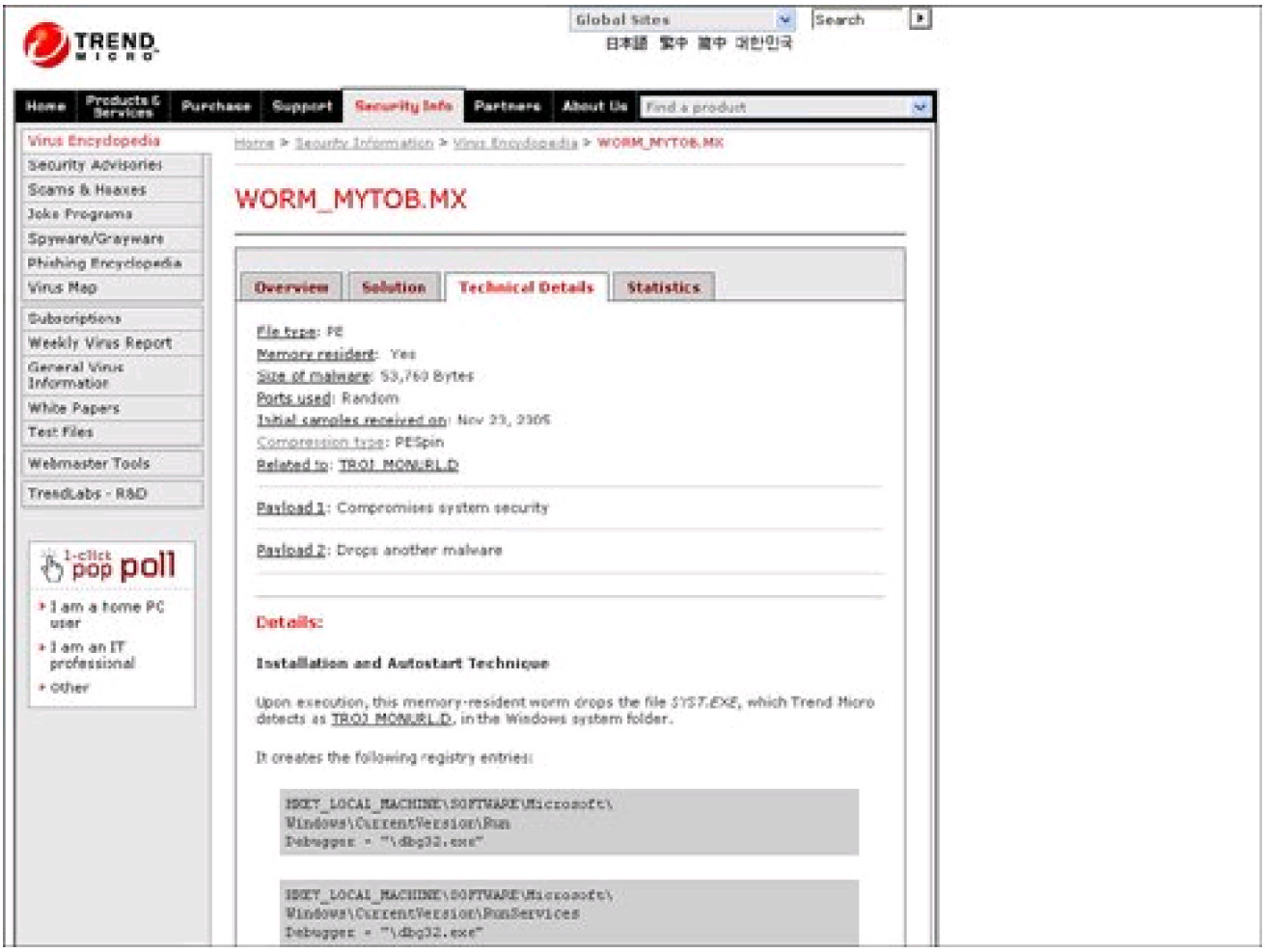
[View full size image]



The security information about the threat from Trend Micro can also contain technical details of the network threat. Figure 4-7 shows a technical details sample.

Figure 4-7. Technical Details of Threat

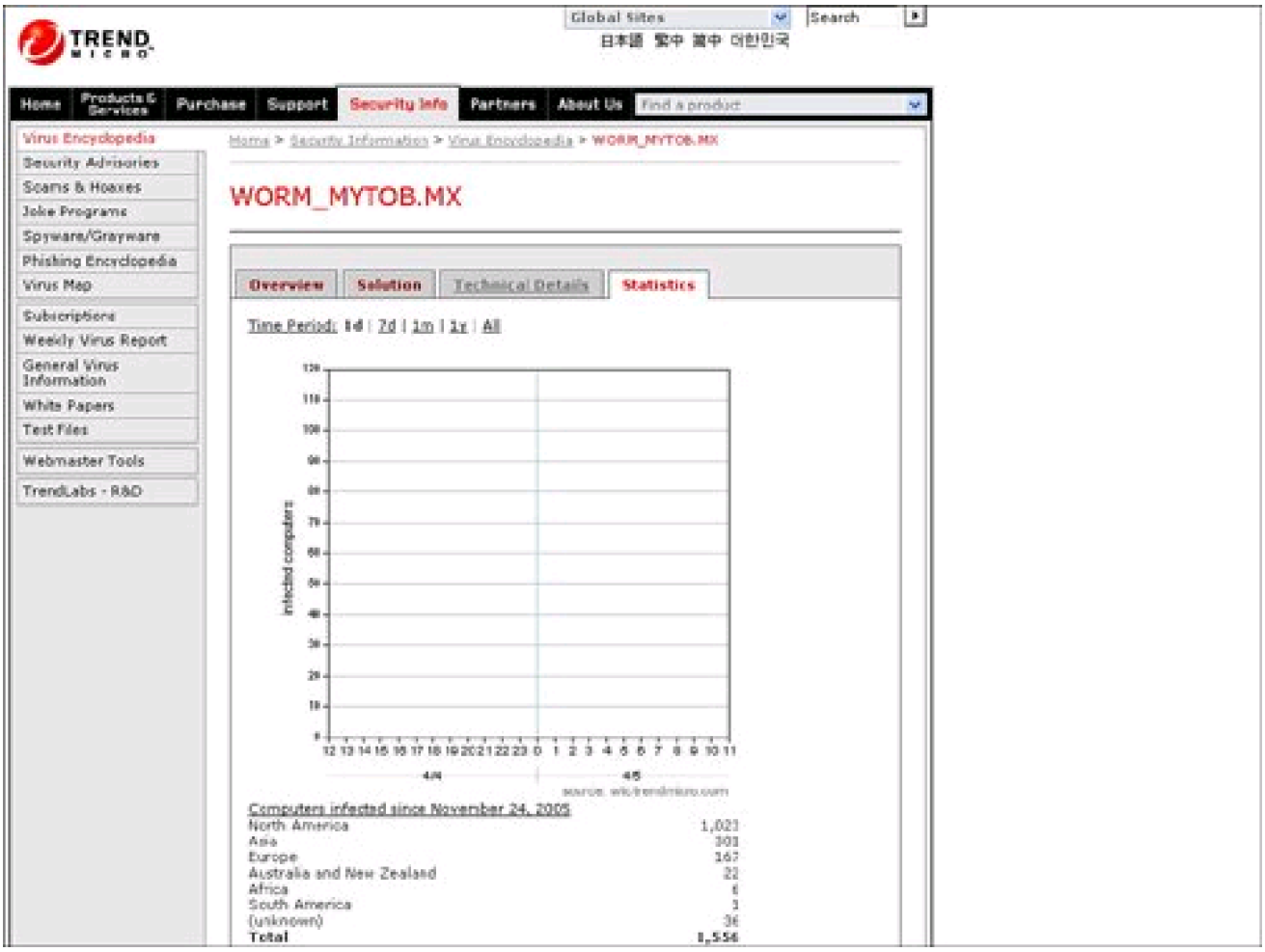
[View full size image]



Statistics of the threat are also provided in the security information from Trend Micro. Information like the number of computers infected by the network threat and a one-day trend of how many computers are infected by the threat can be provided in the Statistics option. These statistics tend to be global and based upon aggregate information from Trend Micro. Figure 4-8 displays an example of statistics on a network threat.

Figure 4-8. Statistics of Threat

[View full size image]

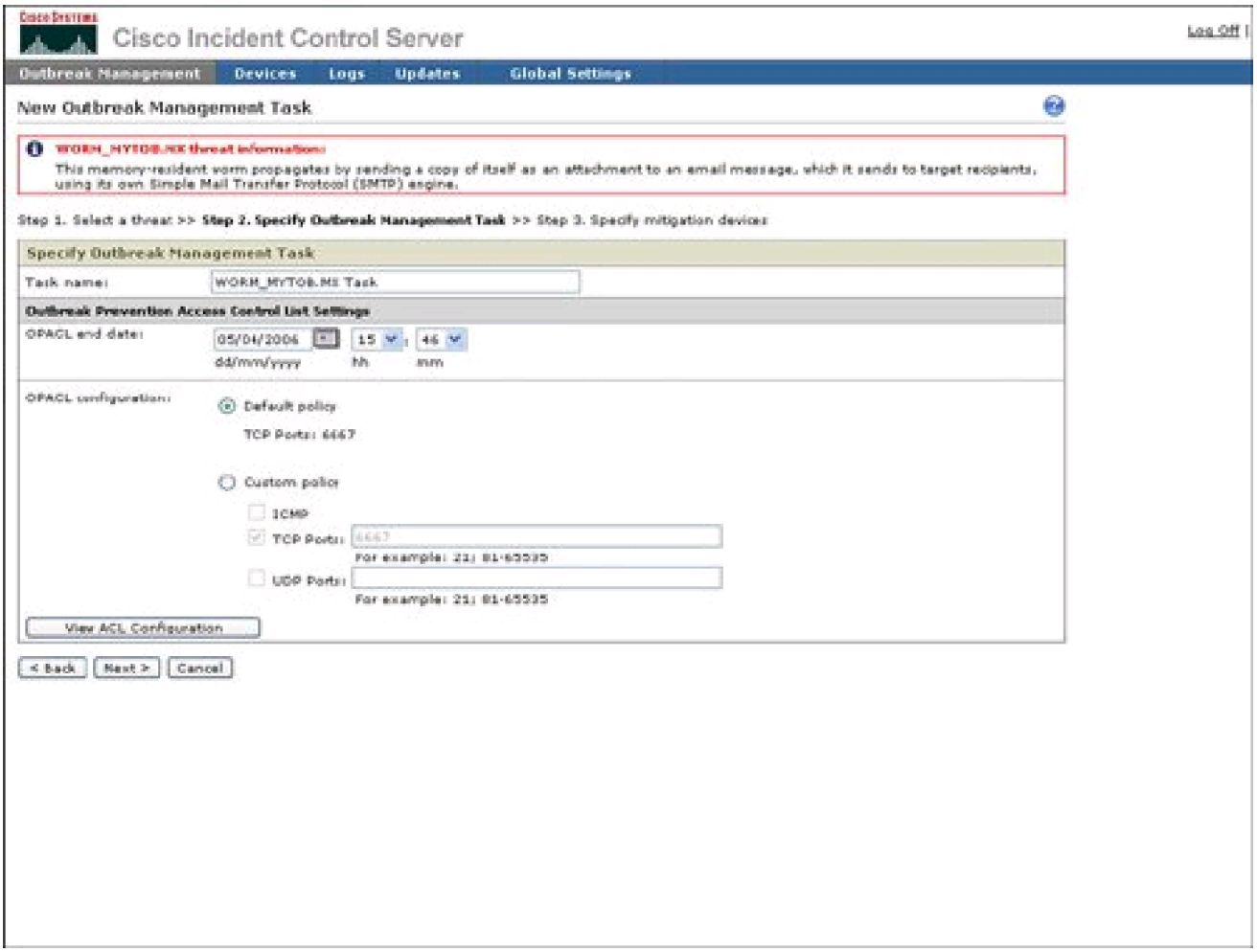


New Outbreak Management Task

Selecting Next from the New Outbreak Management Task list in Figure 4-4 displays information about the recommended OPACL deployment to stop the network attack. OPACL information includes the time or end date at which the OPACL should expire, the ability to configure a custom OPACL, and the ability to view the OPACL configuration. An example of a display of this OPACL information for a new outbreak management task is provided in Figure 4-9.

Figure 4-9. OPACL Information for Threat

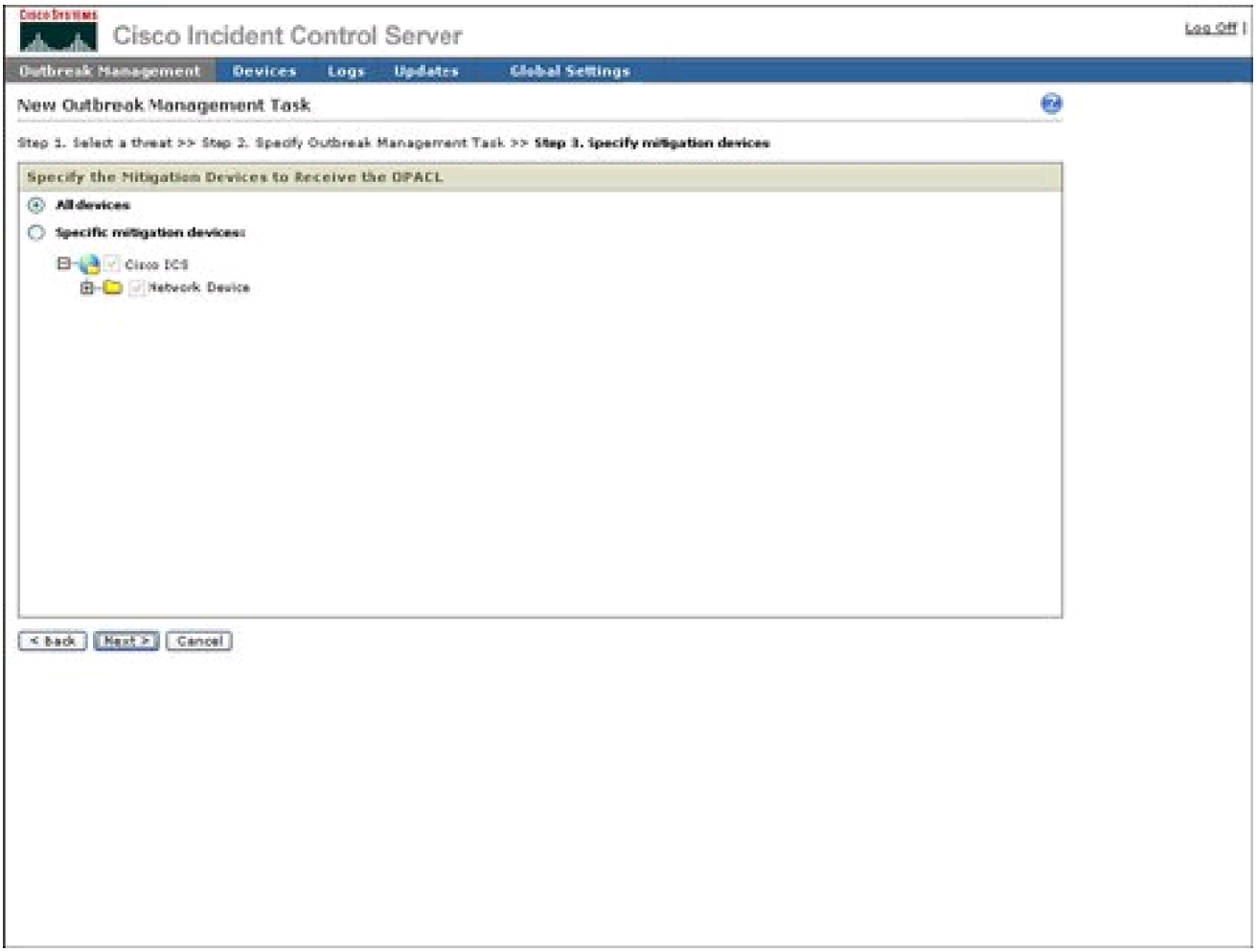
[View full size image]



The next step in setting up a new outbreak management task is defining the target devices that will receive the OPACL. The wizard, by default, will select a default set of devices with an option to change the set of target devices. An example of the target device configuration for the OPACL is provided in Figure 4-10.

Figure 4-10. Select Target Device for OPACL

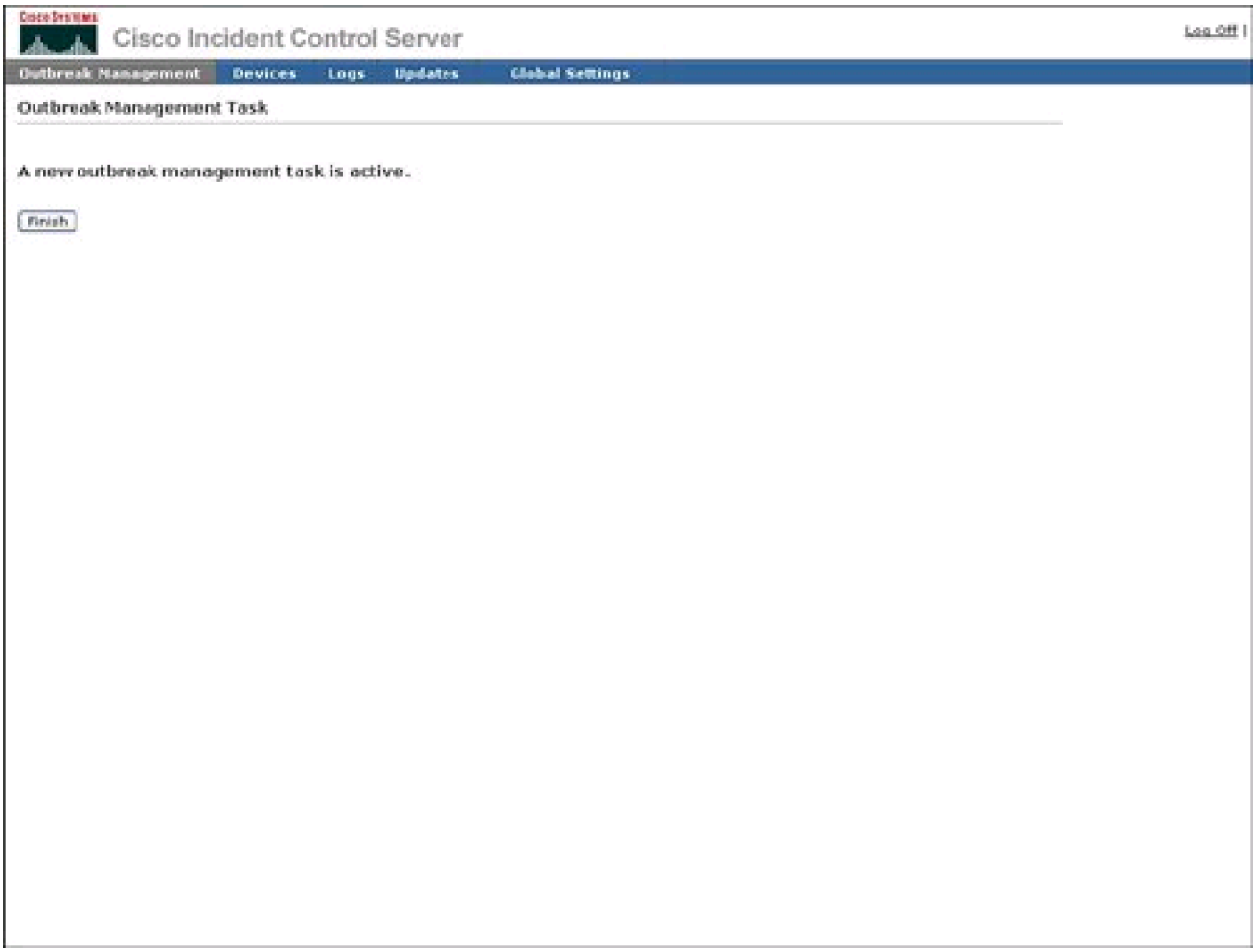
[View full size image]



Selecting the target devices and then clicking Finish will result in the running of a new outbreak management task. Figure 4-11 displays an example of a summary that indicates that a New Outbreak Management Task is now running.

Figure 4-11. New Outbreak Management Task Running

[View full size image]



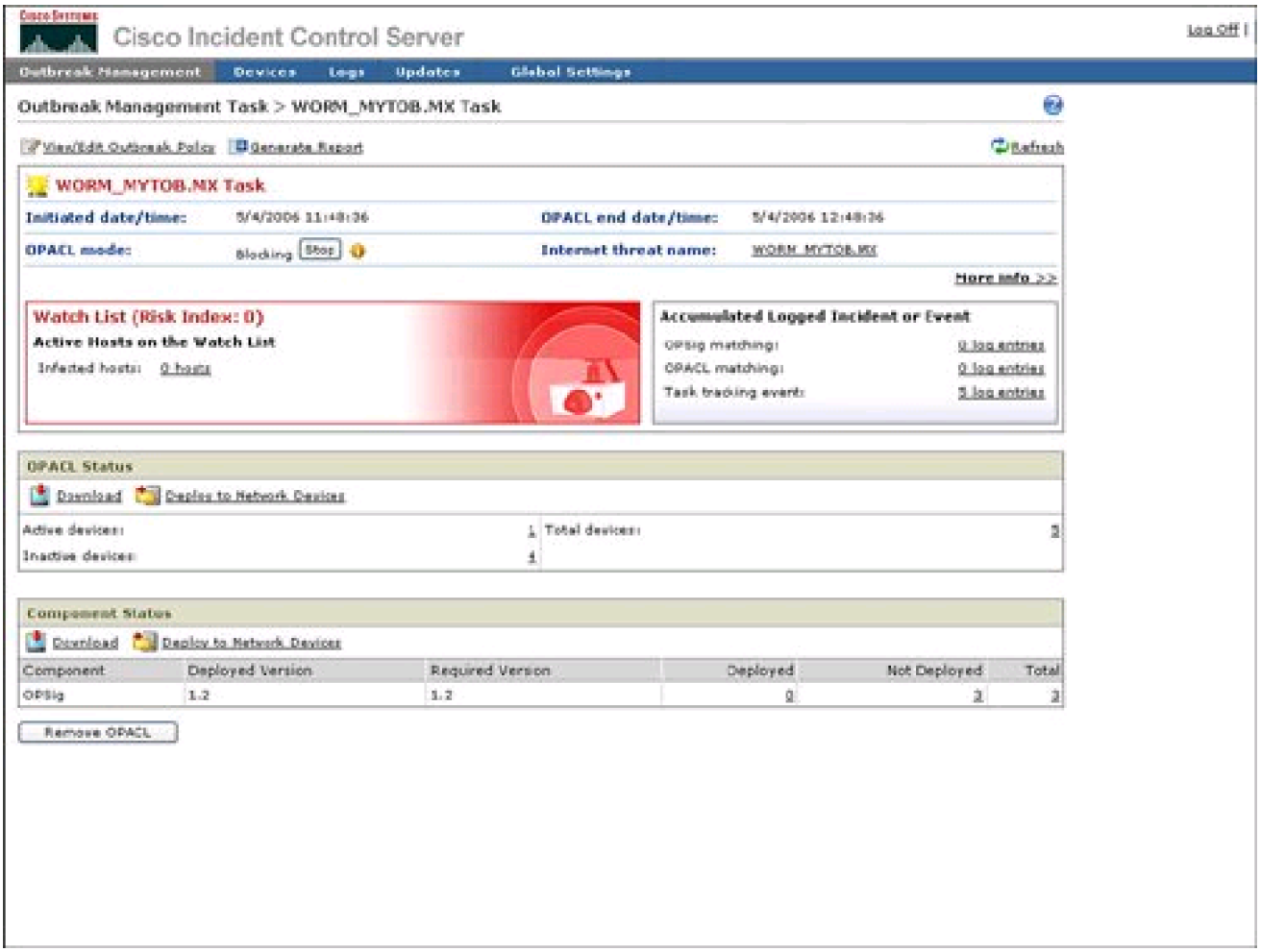
The network threat that was identified in the New Outbreak Management Task list should now be listed in the Outbreak Management Task List. Information for each network threat in the Outbreak Management Task List includes the following:

- Task name
- Hosts in watch list
- Initiated date/time
- OPACL end date/time
- Action to stop task

You can stop an outbreak management task by clicking the Stop button in the Action column, as shown in Figure 4-12.

Figure 4-12. Stop Management Task

[View full size image]

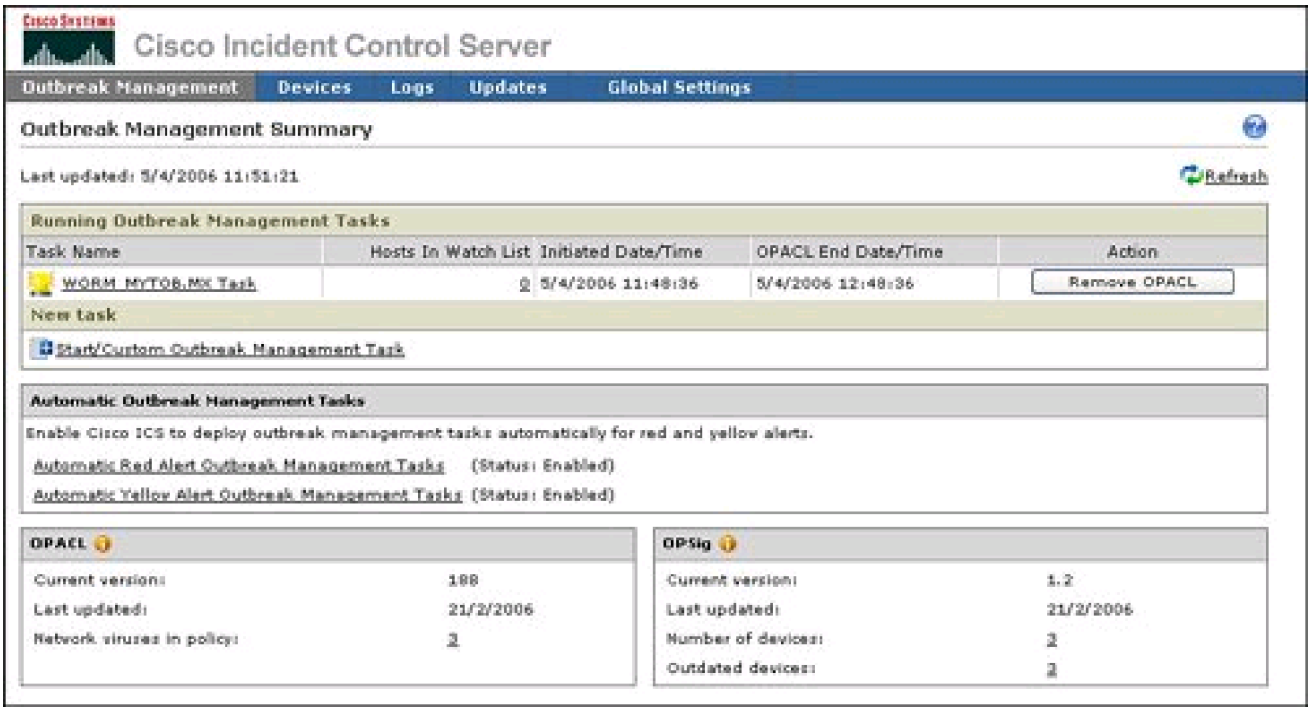


Cisco ICS features the ability to recommend an OPACL or to automatically deploy an OPACL in the event of a detected network threat. Cisco ICS enables the automatic deployment option to be configured by type of alert. These alerts can be divided into two classes: red and yellow. Red alerts are more mission-critical, whereas yellow alerts are less impactful.

Figure 4-13 displays how the task automation default status per red and yellow alert class is shown to the user.

Figure 4-13. Automated Outbreak Management Alert Level

[View full size image]



Outbreak Settings

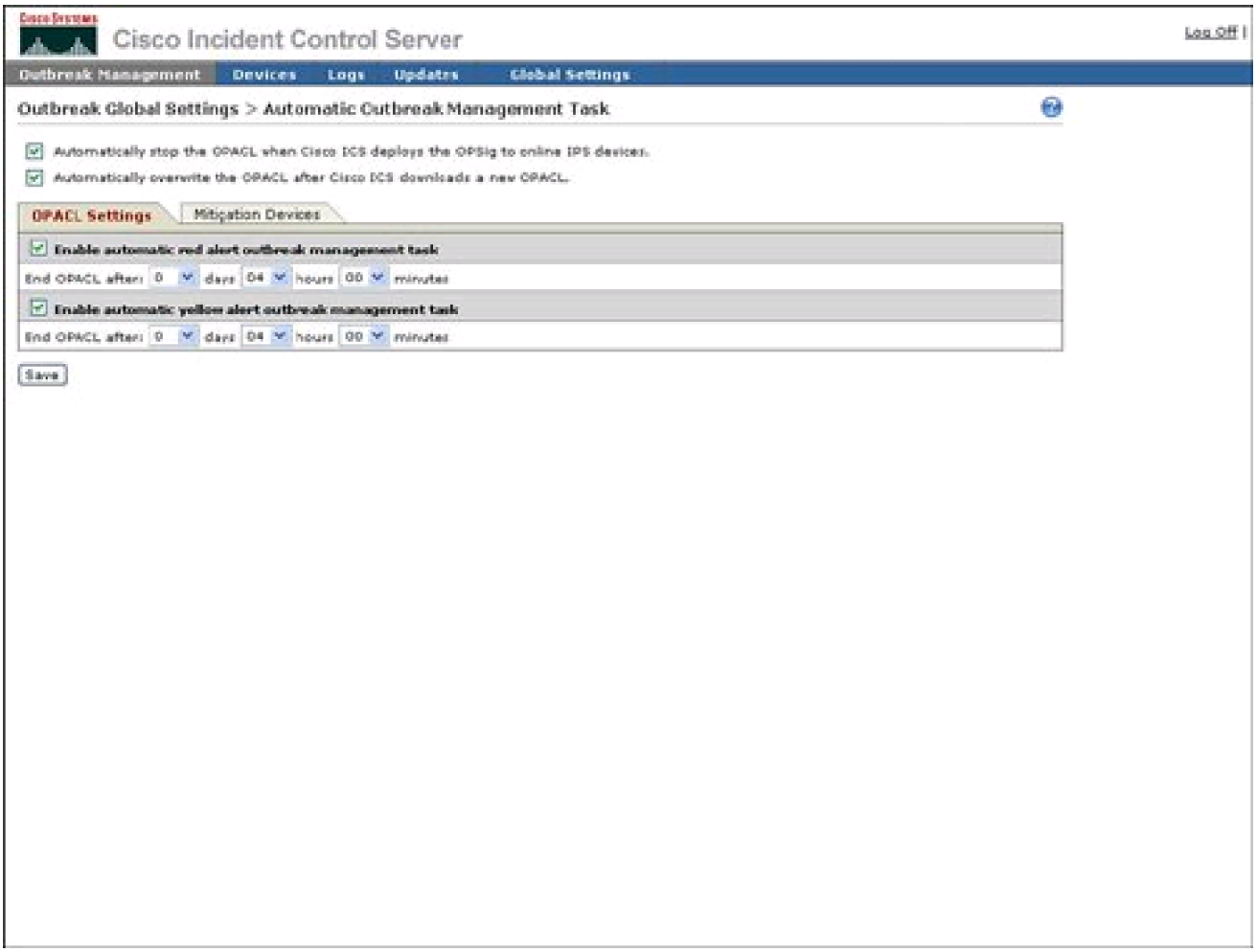
Specific parameters for outbreak settings include the following:

- Automatically stop OPACL when OPSig has been deployed
- Automatically overwrite OPACL settings for new OPACL
- Enable automated outbreak management task for red and yellow alerts
- End OPACL after a specific number of days
- Default target devices for OPACL deployment

Figure 4-14 provides an example of the configurable outbreak settings for automated task deployment.

Figure 4-14. Automatic Outbreak Management Tasks Outbreak Settings

[View full size image]


Cisco Incident Control Server
Log Off
Outbreak Management
Devices
Logs
Updates
Global Settings
Outbreak Global Settings > Automatic Outbreak Management Task
Automatically stop the OPACL when Cisco ICS deploys the OPSig to online IPS devices.
Automatically overwrite the OPACL after Cisco ICS downloads a new OPACL.
OPACL Settings
Mitigation Devices
Enable automatic red alert outbreak management task
End OPACL after: 0 days 04 hours 00 minutes
Enable automatic yellow alert outbreak management task
End OPACL after: 0 days 04 hours 00 minutes
Save

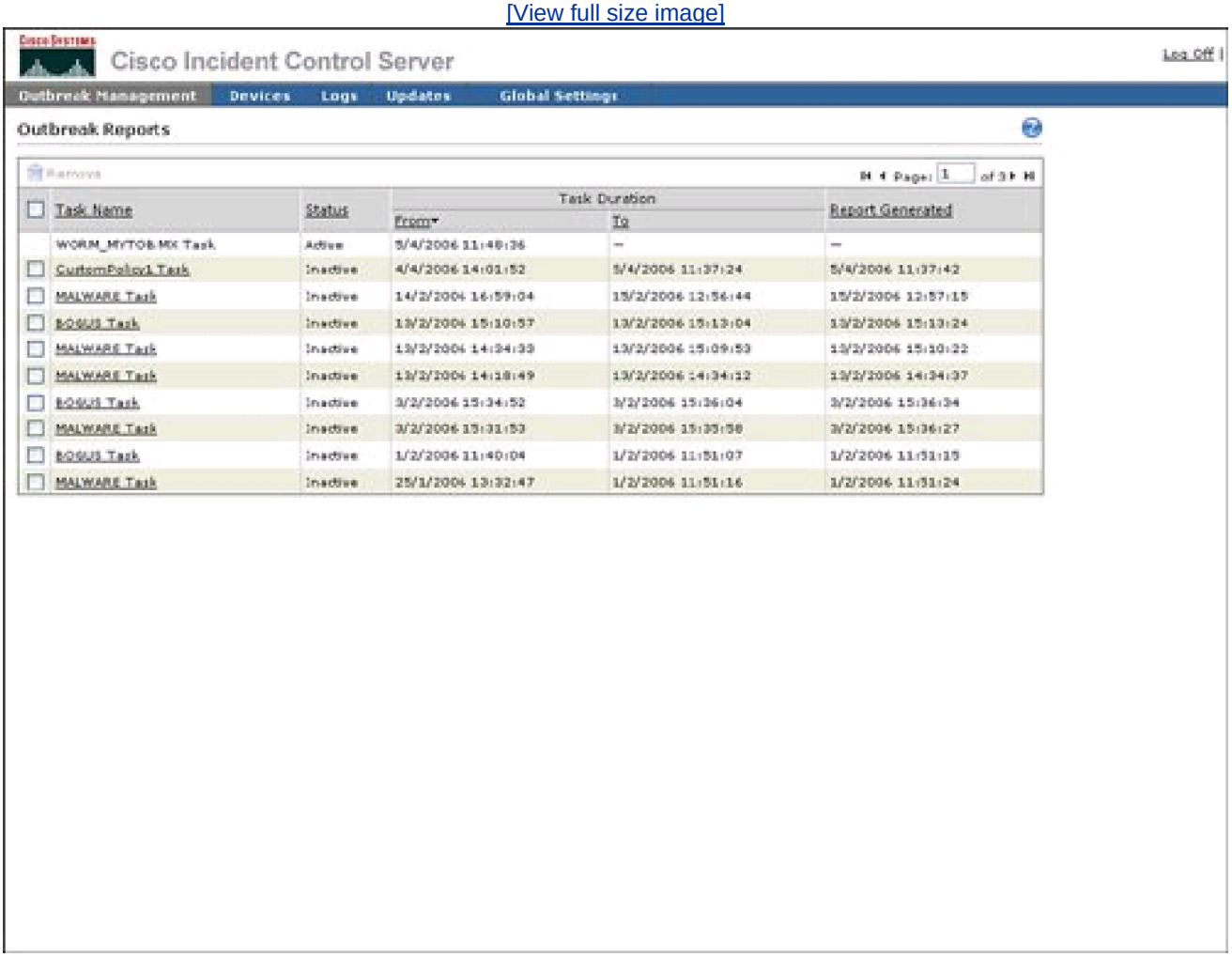
PREV NEXT

Displaying Outbreak Reports

The Outbreak Management tab provides a drop-down link to outbreak reports, as shown in Figure 4-15.

Figure 4-15. Select Outbreak Reports

[View full size image]



The selection of the incident or worm from the Outbreak Management Task from this list will display the outbreak report for that outbreak management task. Information in outbreak reports includes the following:

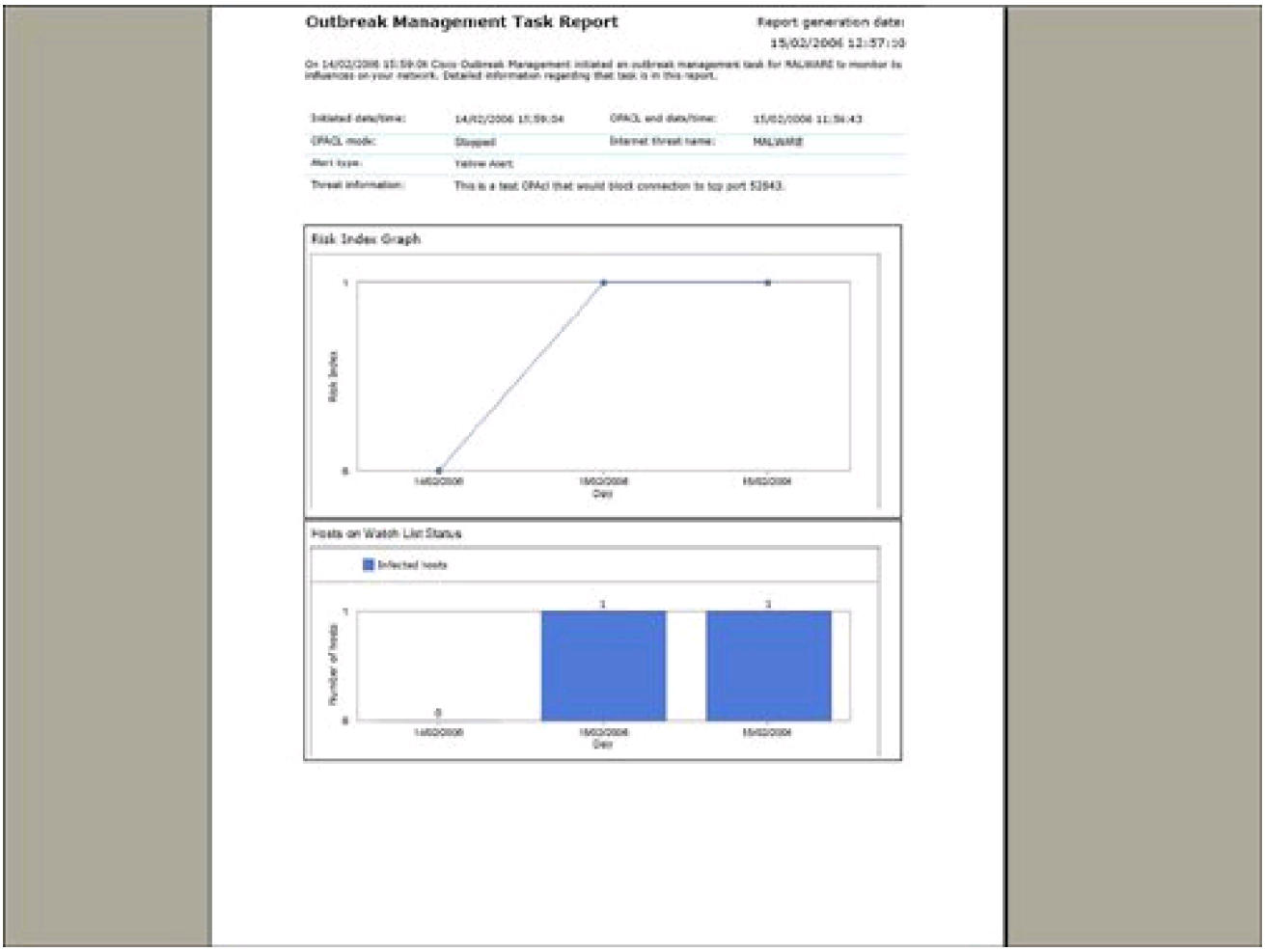
- Executive summary
- Initiated date and time

- OPACL end date and time
- OPACL mode
- Threat name
- Alert type
- Threat information
- Risk index graph
- Hosts on watch list
- Infected hosts
- IPS virus incident status
- OPACL matching status
- Accumulated log incident
- OPACL status
- Service component status

An example of the beginning of an outbreak report is provided in Figure 4-16.

Figure 4-16. Sample of Outbreak Report

[View full size image]

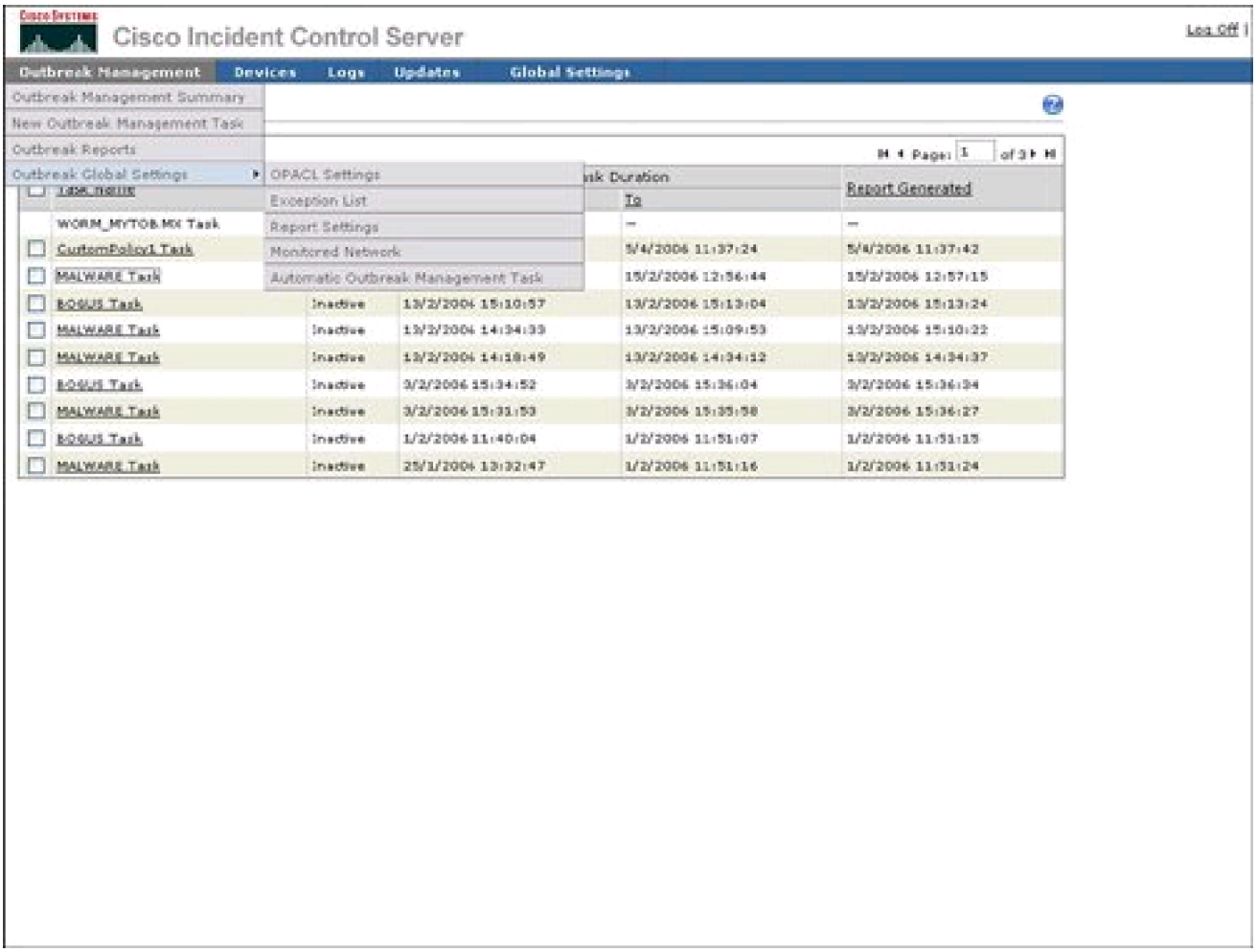


Cisco ICS includes configurable settings to manage the self-defending characteristics of the network to contain a network incident. To access the outbreak settings that are a part of Cisco ICS, select Outbreak Settings from the Outbreak Management list, as shown in Figure 4-17. Components of outbreak settings include the following:

- **OPACL Settings** Use for blocking or logging
- **Exception List** Define ports that will not receive OPACLs
- **Report Settings** Define how automatic reports are generated
- **Watch List Settings** Indicate which hosts or networks will be watched for attack
- **Automatic Outbreak Management Task** Define whether OPACLs and OPSigs will be automatically deployed for alert classes

Figure 4-17. Outbreak Global Settings

[View full size image]



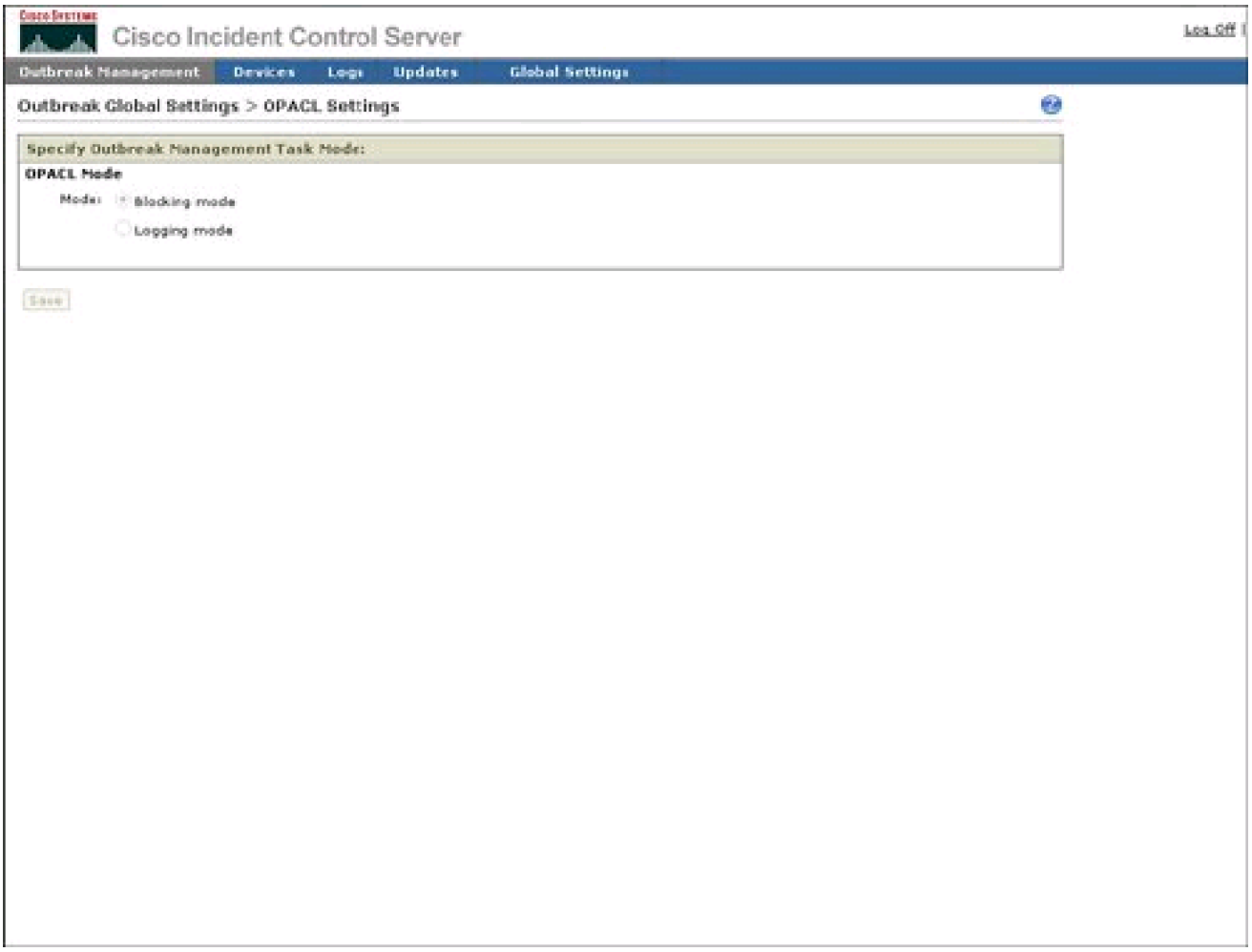
The following sections describe the outbreak settings in more detail.

OPACL Settings

The primary purpose of OPACL Settings is configuration of Cisco ICS in blocking or logging mode for OPACLs. Blocking mode will enable Cisco ICS to deploy the OPACL to the network device in order to automatically block the spread of the infection through the network. Logging mode will notify the operator of what OPACL should be applied, but will leave the actual configuration and deployment of that OPACL to the network operator. An example of how to configure OPACL for blocking or logging is provided in Figure 4-18.

Figure 4-18. OPACL Settings

[View full size image]

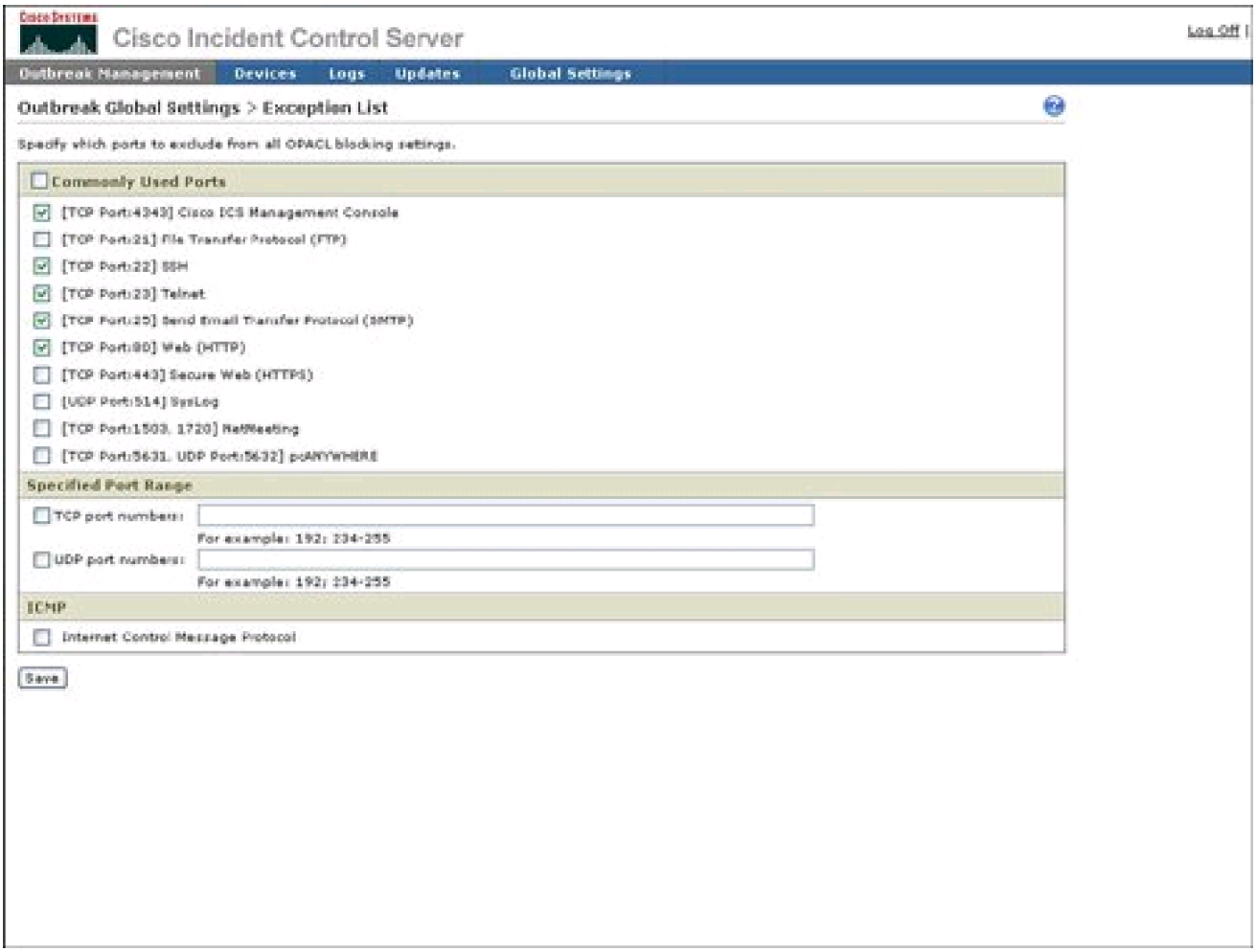


Exception List

The Exception List provides a mechanism to exclude service fields or ports from OPACL deployment. Cisco ICS provides a default list of commonly used ports, for example HTTP (80), to be excluded from OPACL deployment. Cisco ICS also provides a way to exclude a port range or both TCP and User Datagram Protocol (UDP) parts. The ability to exclude Internet Control Message Protocol (ICMP), or ping, is also provided. An example of how to exclude ports from OPACL deployment is provided in Figure 4-19.

Figure 4-19. Exception List

[View full size image]

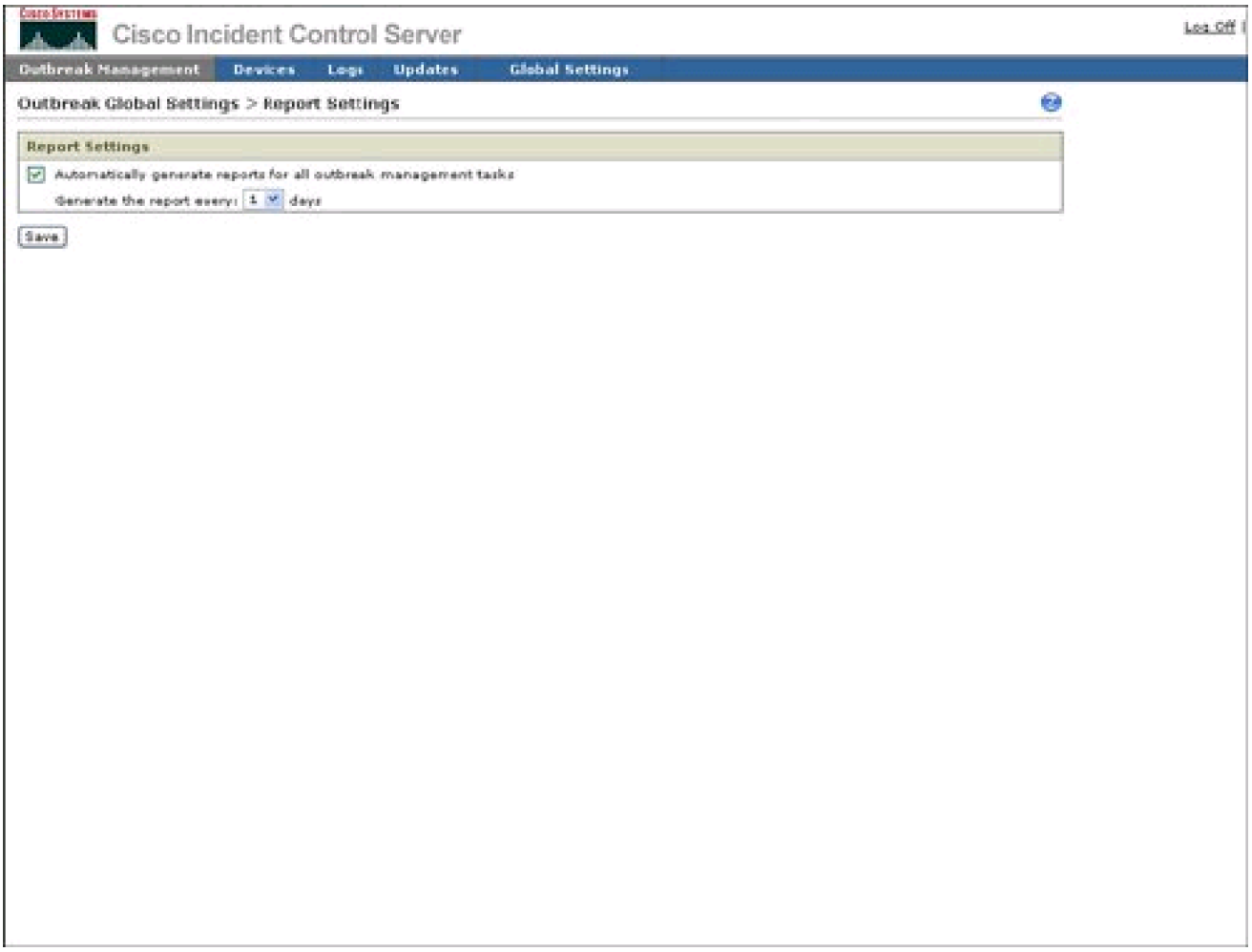


Report Settings

As indicated in Figure 4-20, Report Settings provides a mechanism to configure the automatic generation or reports and the frequency of report generation.

Figure 4-20. Report Settings

[View full size image]

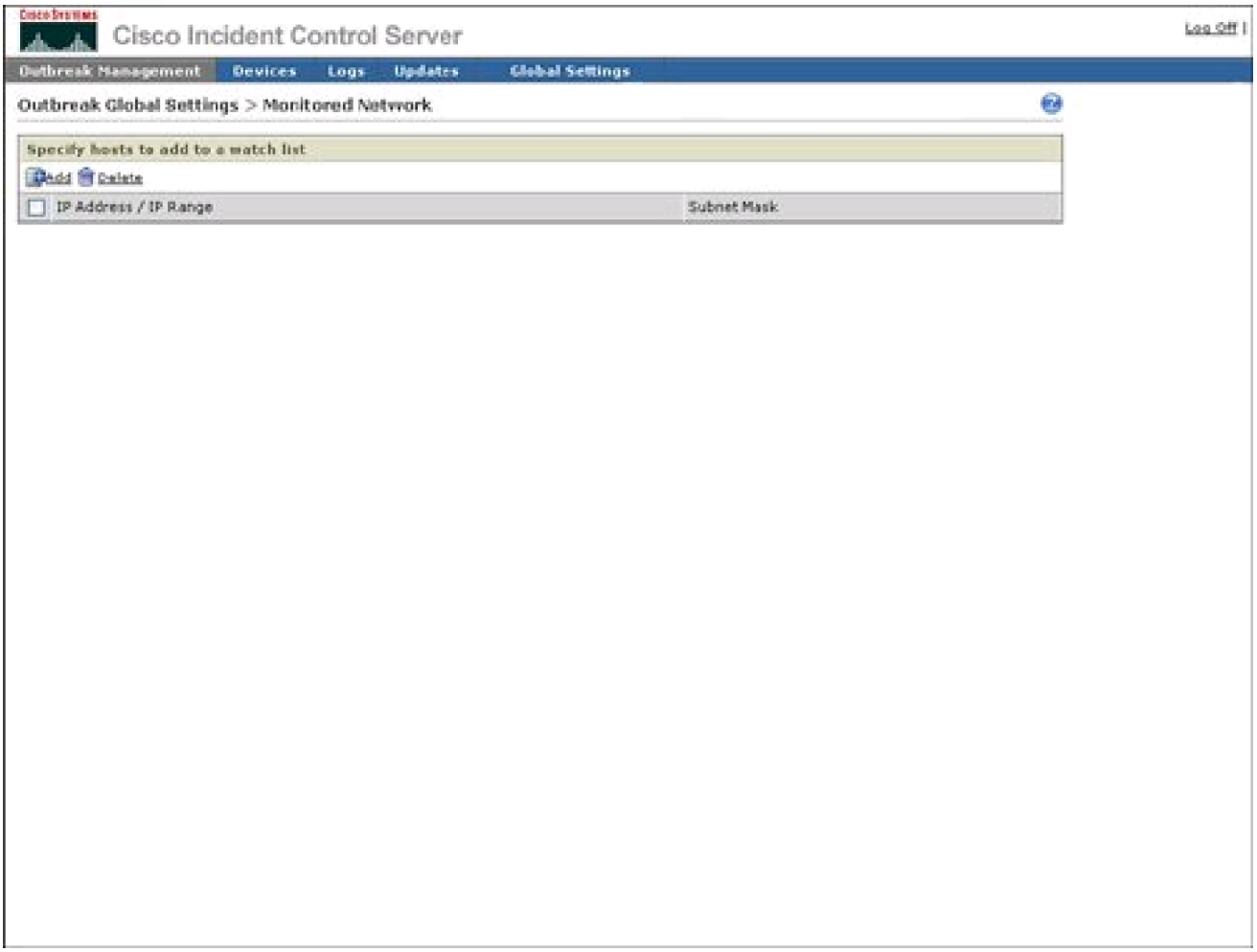


Watch List Settings

The watch list is intended to indicate which hosts in the network may have been infected by a network attack. Figure 4-21 shows that you can configure the watch list for an IP address or a range of IP addresses. Cisco ICS will use the IPS signatures to determine if a host is sending network traffic that could be due to an infection and will add this host to the watch list.

Figure 4-21. Watch List

[View full size image]



Automatic Outbreak Management Task

The Outbreak Settings link under Outbreak Management provides a way to access the Automatic Outbreak Management Task configuration. This Automatic Outbreak Management Task configuration specifies whether yellow and red alerts can receive automatic OPACL and OPSig deployment by Cisco ICS or if an operations person must manually review and deploy the OPACLs and OPSigs. The Automatic Outbreak Management Task configuration is identical to Automatic Outbreak Management Task configuration that was displayed earlier in Figure 4-13.

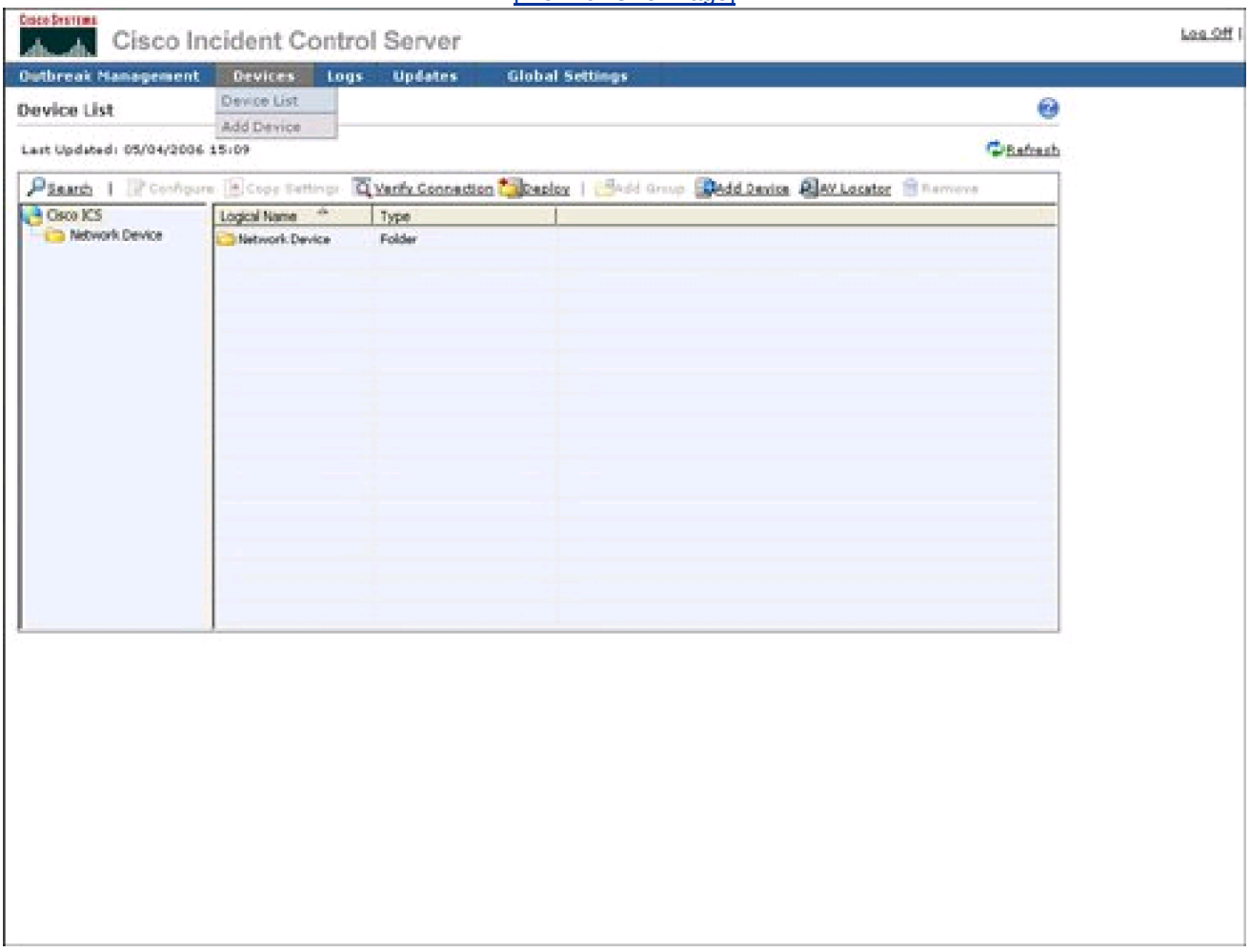
PREV NEXT

Displaying Devices

The Devices drop-down list provides a way to display the list of devices that are managed by the Cisco ICS. The Devices drop-down list also provides a mechanism to add a device to the list of devices under management. Figure 4-22 displays the Devices drop-down list to view the device list and to add a device.

Figure 4-22. Devices

[View full size image]



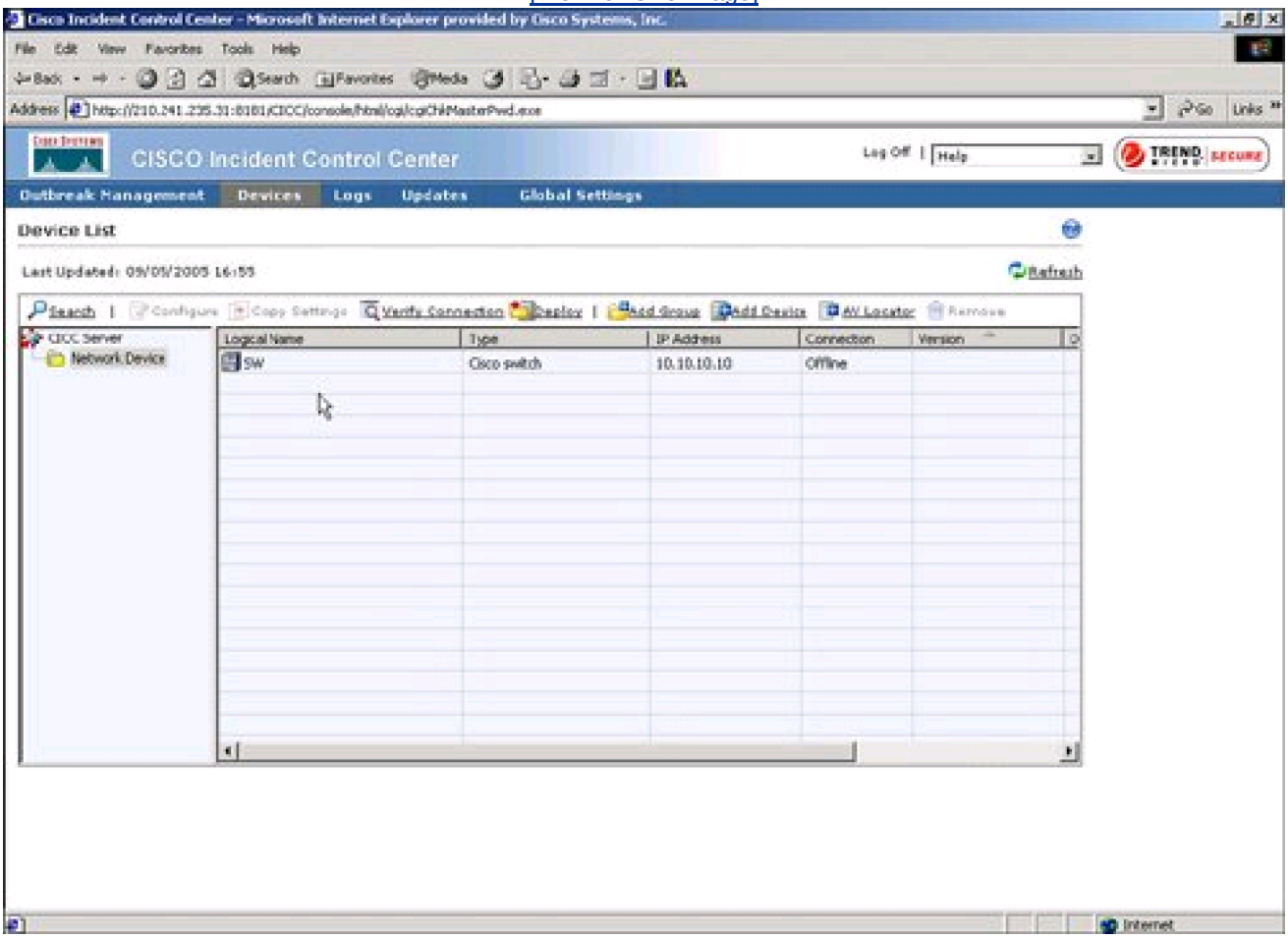
The following sections describe the Device List and Add Device options.

Device List

The Device List contains a list of devices that will be managed by Cisco ICS. These devices in the list can receive OPACLs and OPSigs and can be self-defending against a network incident. An example of a Device List is shown in Figure 4-23.

Figure 4-23. Device List

[View full size image]

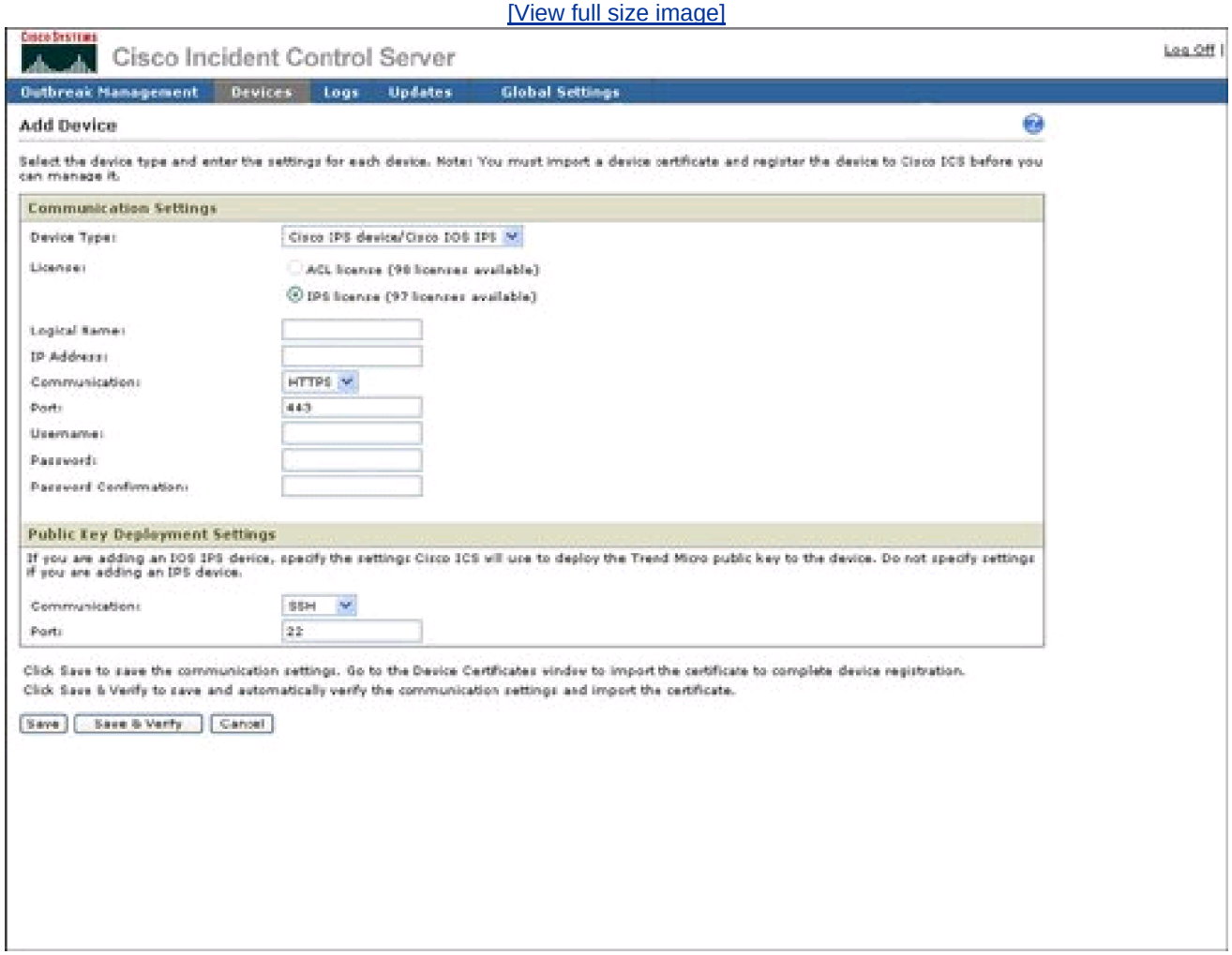


Add Device

The Add Device function enables a Cisco IPS, router, or switch to be added to the Cisco ICS server. There is also an Add Device link from the Device List in addition to the link from the main Device tab. Figure 4-24 displays the parameters related to how to add a device to the Cisco ICS server.

Figure 4-24. Add Device

[View full size image]



PREV NEXT

Viewing Logs

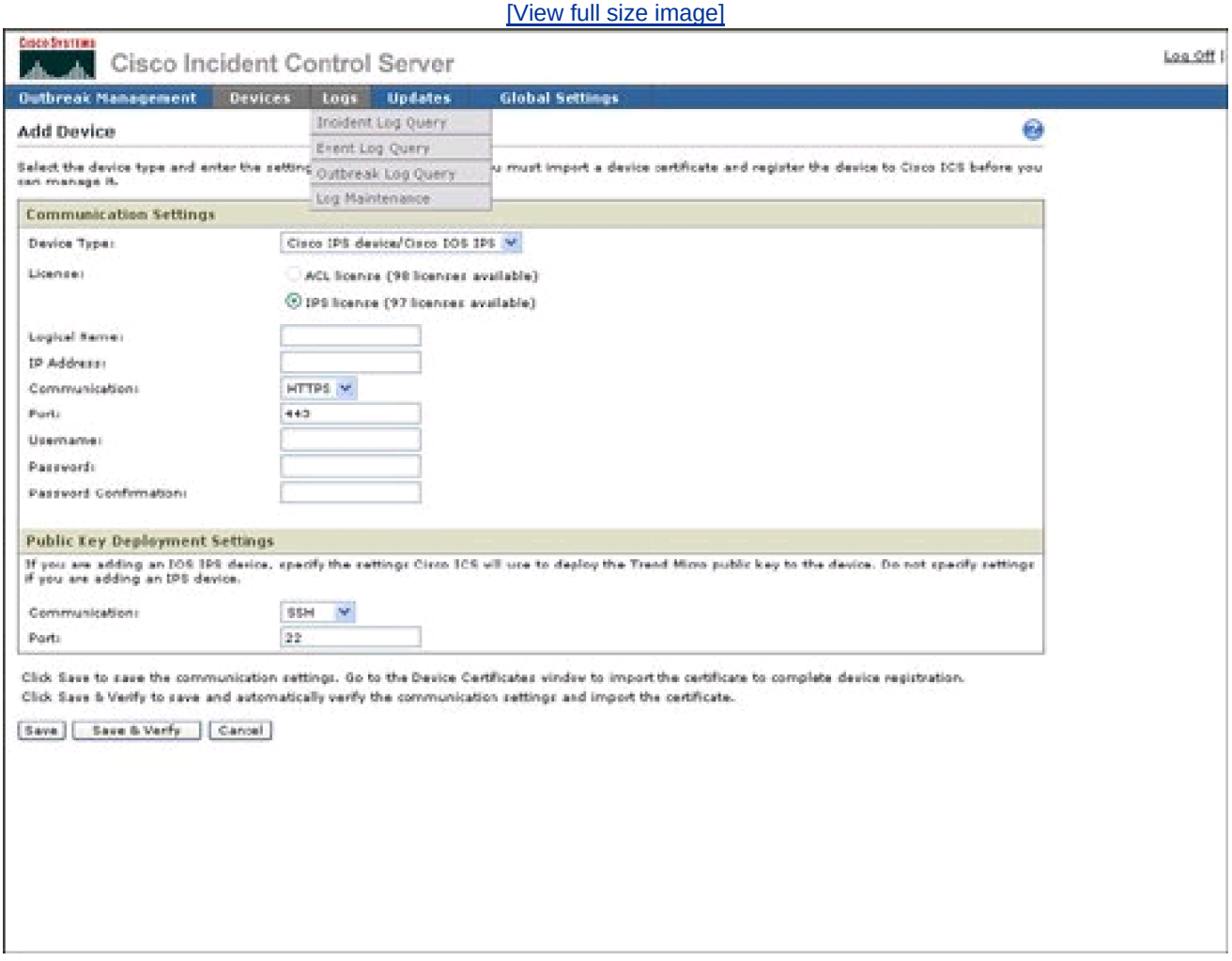
Cisco ICS provides a variety of log functions including the following:

- Incident Log Query
- Event Log Query
- Outbreak Log Query
- Log Maintenance

An example of the log functions from the Logs drop-down list is provided in Figure 4-25.

Figure 4-25. Logs

[View full size image]



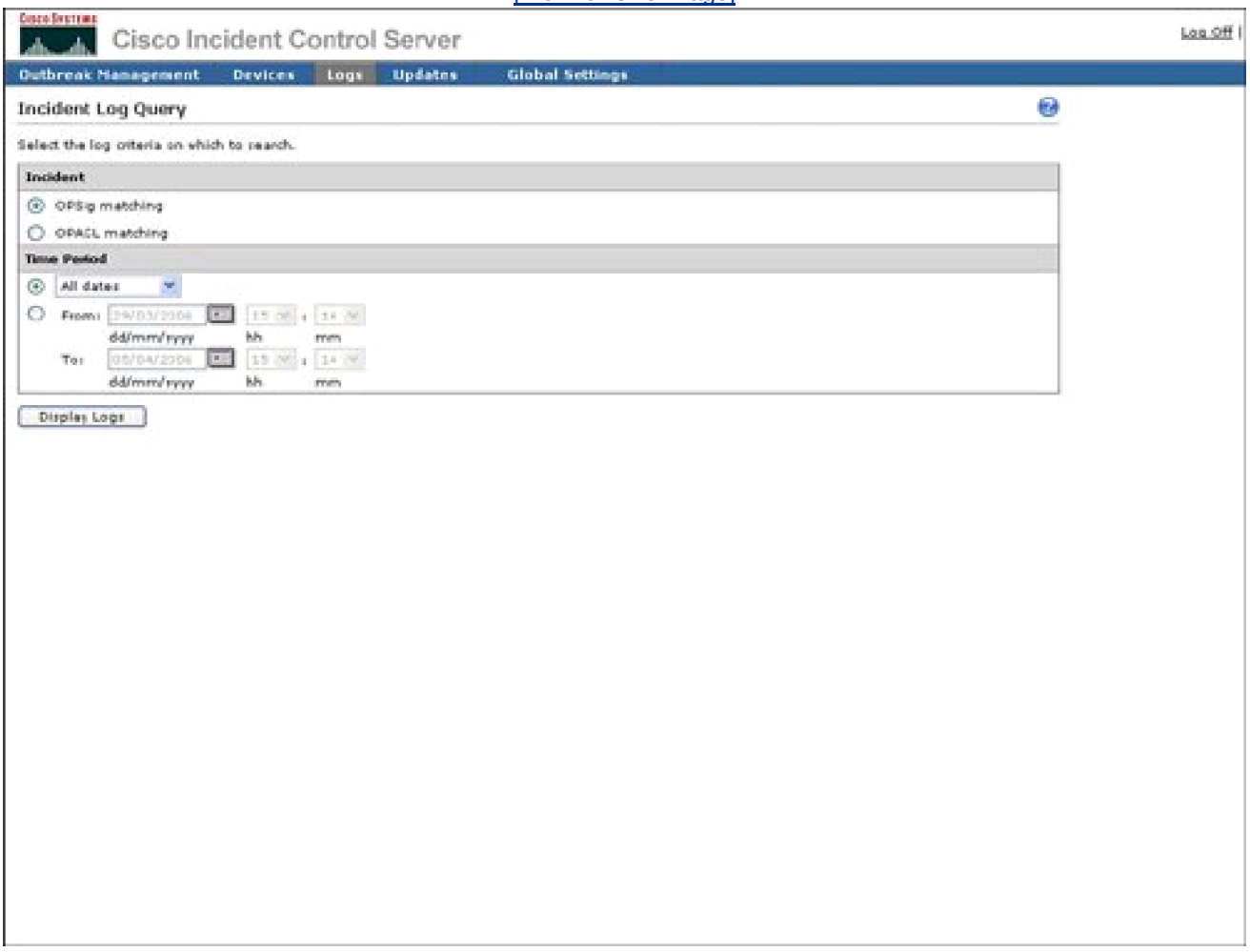
The following sections describe each log function in more detail.

Incident Log Query

The Incident Log Query function provides a way to display the logs from IPS Virus Detection or an OPACL Matching during a specific range of dates. Figure 4-26 displays an example of the configuration parameters for an Incident Log Query.

Figure 4-26. Incident Log Query

[View full size image]



Event Log Query

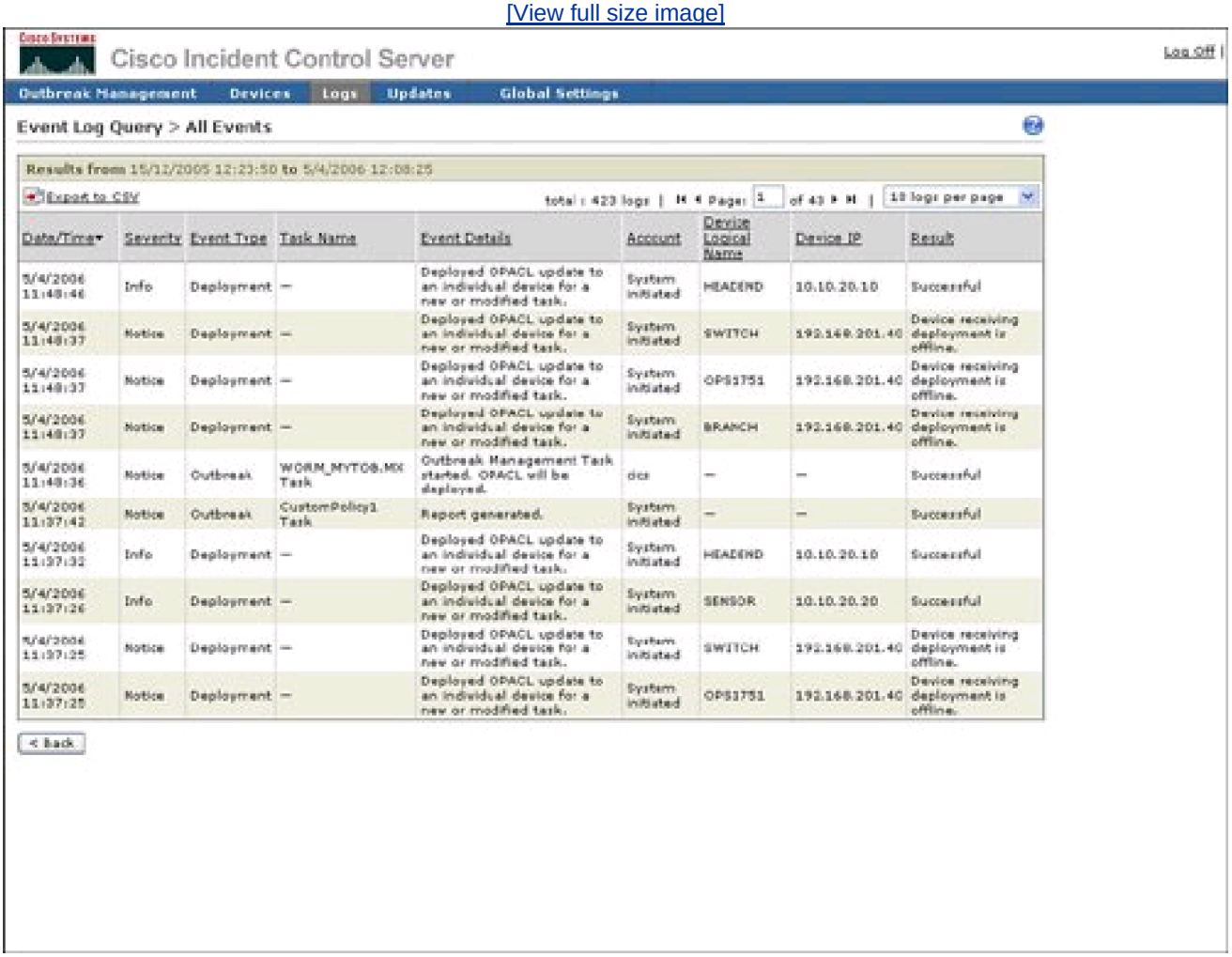
The logs in Cisco ICS can be queried based upon event type and date range. An example of the types of event logs includes the following:

- System Events
- Outbreak Events
- Server Update Events
- Deployment Events
- Connection Status Event
- Host Event

Figure 4-27 provides a sample of the result from an Event Log Query.

Figure 4-27. Event Logs

[View full size image]

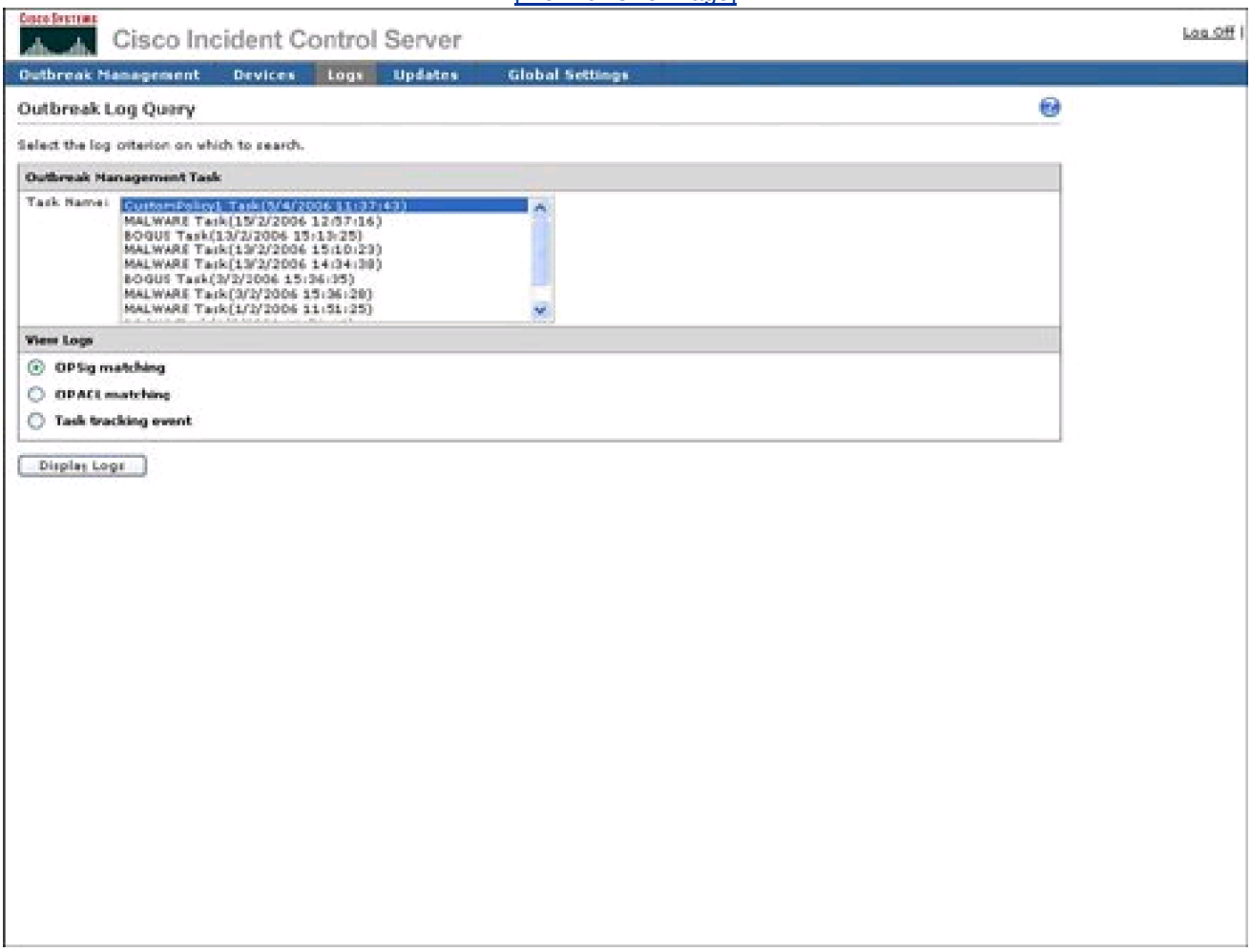


Outbreak Log Query

The Outbreak Log Query provides a way to display all logs that relate to a certain outbreak management task, as shown in Figure 4-28. Outbreak log query can be considered a subset of the event log query.

Figure 4-28. Outbreak Log Query

[View full size image]

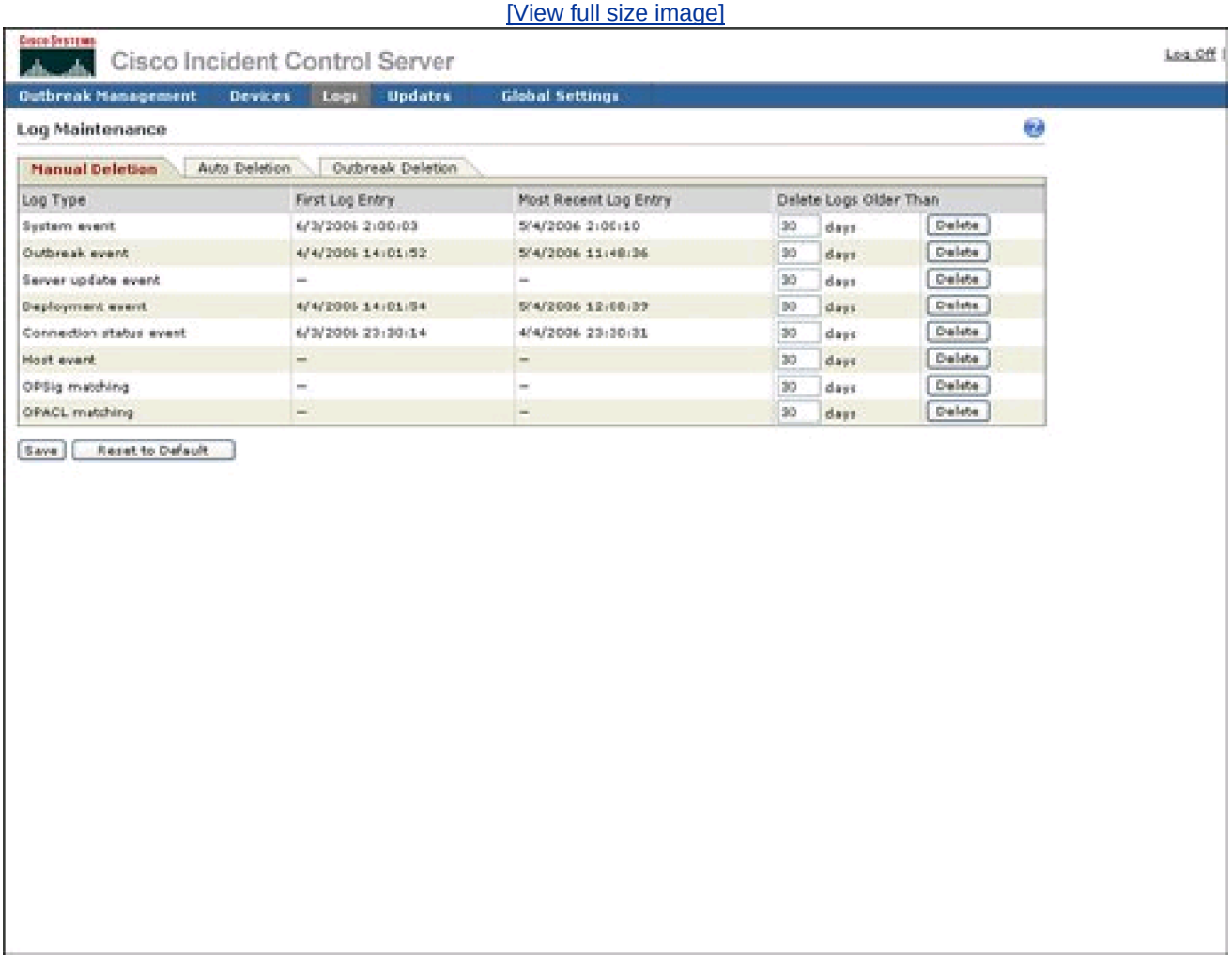


Log Maintenance

Log Maintenance provides a way to manually purge logs of certain types or to define time periods to automatically purge logs from Cisco ICS. Logs can also be exported in commaseparated value (CSV) format. Figure 4-29 displays some of the options to purge logs under Log Maintenance.

Figure 4-29. Log Maintenance

[View full size image]



Note

Cisco ICS also features Update and Global Setting tabs in the main GUI. This chapter does not focus on the update global setting feature because this tends to be more generic and related to product maintenance and less specific to the self-defending characteristics of the Cisco ICS product.

PREV NEXT

Summary

The Cisco ICS is created by the partnership between Cisco and Trend Micro. Cisco ICS provides an additional layer of self-defense that can contain network incidents with a focus on preventing networkwide virus and worm outbreaks. Cisco ICS works in concert with a subscription service from Trend Micro where Trend Micro monitors and identifies new network threats. Trend Micro first creates a broad access list, or OPACL, to stop the network outbreak. Trend Micro further investigates the new network threat and then creates an IPS signature, or OPSig, as a very specific mechanism to stop the outbreak or worm.

Cisco ICS can deploy OPACLs and OPSigs either automatically, without user intervention, or manually, with user approval. OPACLs and OPSigs can also be applied automatically or manually, based upon classes of events, as designated by the red and yellow alert levels. Cisco ICS complements the base level of access lists and IPS protection as described in Chapter 3. In addition to the ASA platform, Cisco ICS can also apply OPACLs to routers and switches and OPSigs to IPS devices, including routers, appliances, and Catalyst 6500/7600 IPS service modules.

References

Cisco Systems, Inc. Administrator Guide for Cisco Incident Control Service.
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/ics/ics10/admin/index.htm

Chapter 5. Demystifying 802.1x

802.1x is a public standard that defines port-based user authentication. 802.1x is also a mechanism for user identity and authentication over both wired and wireless network infrastructures. 802.1x is considered by many to be fairly complex, with several Extensible Authorization Protocol (EAP) types that define how authentication is implemented on the network. This chapter attempts to demystify 802.1x, provide an overview of Cisco Identity-Based Networking Services (IBNS) and machine authentication, and discuss how 802.1x can complement Network Admission Control (NAC). In this chapter, you also learn the basics of some of the most popular EAP types and how 802.1x can participate in an EzVPN network for telecommuting and remote branch offices.

Fundamentals of 802.1x

The IEEE 802.1x standard is designed to provide port-based user authentication onto a network. Prior to the 802.1x standard, many mechanisms existed to determine if a user was authorized to join the network. However, these mechanisms were often proprietary and typically were often independent of the port or entrance point in to the network. The ability to define port or link-layer authentication to the network allows the ability to assign a user or group of users network access policy attributes including virtual LAN (VLAN) and access control lists (ACLs) when the user authenticates and logs on to the network. IEEE 802.1x provides a standard mechanism for port or link-level user authentication and works in concert with traditional port-level security.

An example of traditional port-level security is the ability to specify what MAC addresses, or layer 2 addresses, are allowed through a particular Catalyst LAN switch port. In addition to user-based authentication, IEEE 802.1x can also support device-based authentication to authenticate a device name to a certificate authority or to a Windows Active Directory system prior to user authentication. The IEEE 802.1x standard was designed to provide an open, secure, and scalable mechanism for port-based or link-layer user authentication.

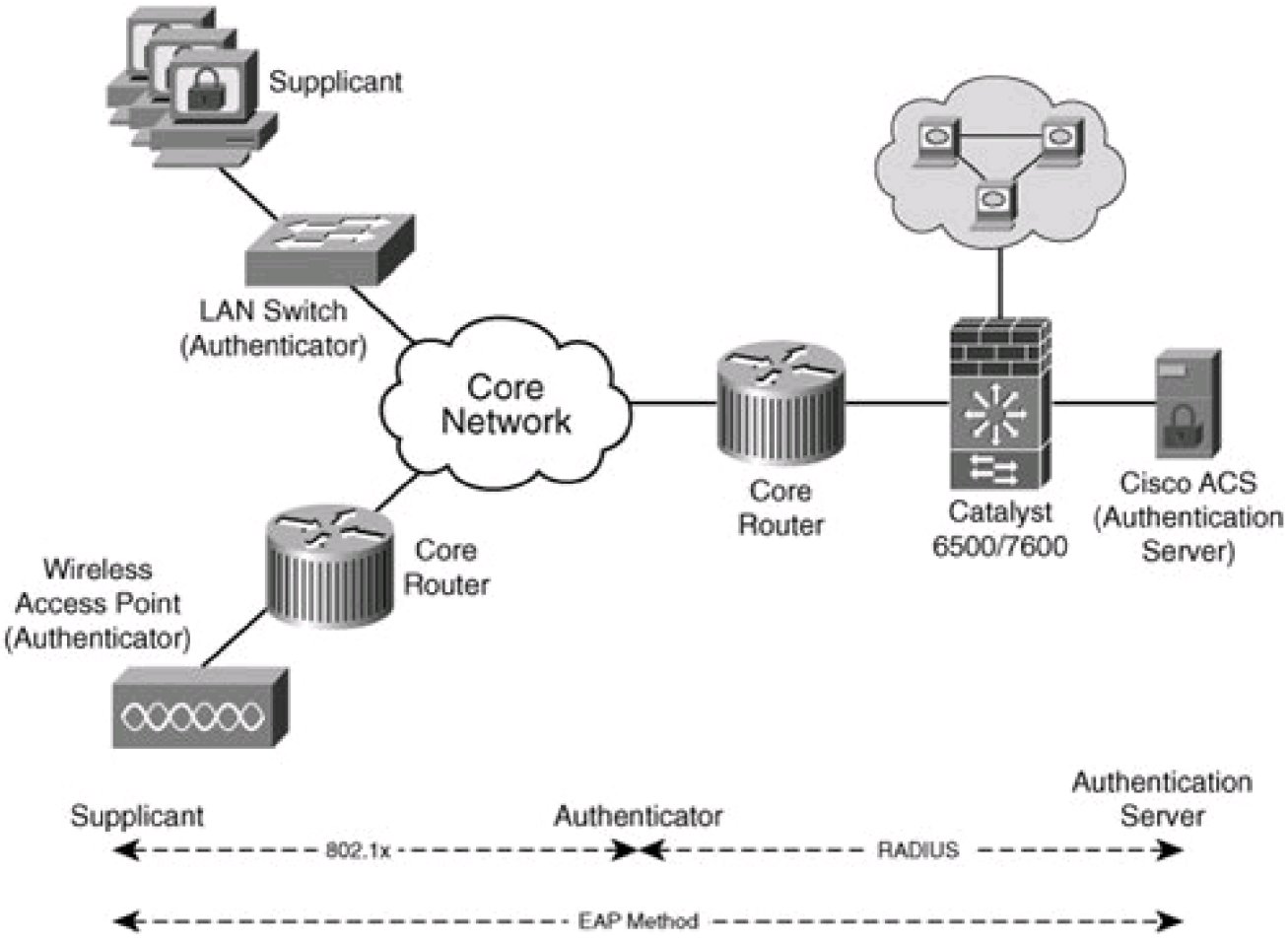
802.1x comprises the following three major components:

- **Authentication server** The authentication server is an 802.1x server and often contains other user authentication services like Remote Authentication Dial-In User Service (RADIUS). The authentication server often provides user authentication services for both 802.1x and other access methods like remote access IPSec VPNs. Cisco Secure Access Control Server (ACS) is an example of an authentication server.
- **Authenticator** The authentication client, or authenticator, is the network component that receives the initial request for port-based user authentication. The authenticator is typically a switch or wireless access-point.
- **Supplicant** The supplicant resides on the end-device, like a laptop, desktop computer, or PDA. Some end-device platforms, including the pervasive Microsoft XP, contain a native 802.1x supplicant. Full-featured 802.1x supplicants can also be purchased from third parties for Windows and other platforms, including Linux and MacOS.

IEEE 802.1x defines a PPP connection between the end-device supplicant (for example, PC) and authenticator (for example, Catalyst LAN switch). IEEE 802.1x allows EAP messages to be transported between the supplicant and the authentication server. Communication between the authenticator and authentication server (for example, Cisco Access Control Server [ACS]) is performed with the RADIUS protocol. Figure 5-1 displays an example of the 802.1x components in a network.

Figure 5-1. 802.1x Network

[View full size image]


Supplicant
LAN Switch
(Authenticator)
Core
Network
Core
Router
Catalyst
6500/7600
Cisco ACS
(Authentication
Server)
Wireless
Access Point
(Authenticator)
Core
Router
Supplicant
Authenticator
Authentication
Server
802.1x
RADIUS
EAP Method

PREV NEXT

Introducing Cisco Identity-Based Networking Services

Cisco Identity-Based Networking Services (IBNS) is the product suite that implements 802.1x identity-based networking on Cisco networks. Cisco IBNS implements the capabilities defined in the IEEE 802.1x standard, which acts as a foundation for identity-based networking. For example, a Cisco switch can be an authenticator, and a Cisco ACS can be an authentication server in an IBNS/802.1x Cisco network.

IBNS also adds a layer of additional functionality that is not contained in the IEEE 802.1x standard. Cisco IBNS networks allow a user to be placed in a specific VLAN and apply specific ACLs after 802.1x port-based user authentication. Cisco IBNS also implements the advanced functionality including the Wake-on-LAN (WoL), Guest VLAN, and MAC authentication bypass features. WoL enables a remote server within the trusted network to reboot or initiate a connection to a remote 802.1x client that is not currently connected to the LAN in order to remotely install software updates. Guest VLAN allows unknown users to be placed into a Guest VLAN with restricted network permissions. MAC authentication bypass features allow devices that do not have an 802.1x supplicant (for example printers) to be granted or denied network access based upon MAC address.

Prior to IBNS with 802.1x, Cisco offered a proprietary identity management solution. This proprietary solution leveraged VLAN Management Policy Server (VMPS) as a VLAN distribution and assignment mechanism with the User Registration Tool (URT) for management. The introduction of the open 802.1x standard has enabled Cisco to implement an identity network solution, or IBNS, on the open 802.1x and RADIUS standards.

Machine Authentication

802.1x features the ability to authenticate a machine during the system boot of that machine. This machine authentication happens prior to dynamic IP address assignment and prior to port-based user authentication. Machine-based authentication supports only Windows machines because the machine name is authenticated against an Active Directory server. Microsoft's support for specific EAP types enables 802.1x to support machine authentication for multiple EAP types. An overview and details about the variety of EAP types that are supported in Cisco 802.1x are provided later in this chapter in the "EAP" section.

802.1. x and NAC

802.1x can use information including the machine name, client-side digital certificate, and username and password to identify and authenticate a user onto a port in the network. The authentication process can include any of the identity credentials or even a combination of these credentials. For instance, digital certificates can be used for device authentication, and username and password can be used for user authentication.

Network Admission Control (NAC) is also a form of authentication and can be considered a superset of the authentication of 802.1x. NAC can use 802.1x as a base for identity authentication. NAC then extends the authentication process to check the security posture or other posture credentials to ensure that the device has the latest operating system (OS) service pack (SP), hot-fix, and antivirus updates. The additional security checks that are performed by NAC are often referred to as a security posture or posture credential check of the endpoint or device.

NAC also offers the ability to quarantine a machine for remediation. Remediation involves the process of allowing the machine to join a quarantined part of the network, such as a specific VLAN or quarantine VLAN. NAC can also enable the display of instructions of how to download the required OS SP and antivirus updates to join the network safely and be removed from the guest or quarantine VLAN. Chapter 6, "Implementing Network Admission Control," provides a detailed overview of the NAC framework that is implemented with routers, switches, and Cisco ACS. The integration between 802.1x and NAC enables the identity and posture credential check to occur in a single 802.1x transaction. NAC can use 802.1x as a base for identify authentication, but then extend the authentication process to include other posture credentials such as OS patches and antivirus updates.

Using EAP Types

EAP is a component of an 802.1x network. EAP is designed to create a mechanism to provide authentication types that leverage existing authentication, authorization, and accounting (AAA) solutions. EAP messages can be transferred from the 802.1x supplicant to the authenticator or authentication server. The communication between the authenticator to the authentication server, such as Cisco ACS, is performed with RADIUS messages. These RADIUS messages are often transported over User Datagram Protocol (UDP). EAP is defined in RFC 2284, "PPP Extensible Authentication Protocol (EAP)." Examples of EAP types include the following:

- **EAP MD5** EAP MD5 supports one-way authentication, similar to Challenge Handshake Authentication Protocol (CHAP). CHAP is defined in RFC 1994 and uses a shared secret for authentication. The authenticator can receive an MD5 hash derived from the shared secret in order to verify the validity of the authentication request.
- **EAP Transport Layer Security (TLS)** EAP TLS uses digital certificates
- **LEAP** Wireless EAP supports mutual authentication
- **Protected EAP (PEAP)** PEAP was coauthored by Microsoft and Cisco. Microsoft Windows also includes a native PEAP supplicant. PEAP can also be used for Layer 3 NAC, or NAC with the authentication client on an IOS router. PEAP also supports both MSCHAPv2 and Generic Token Card (GTC). MSCHAPv2 is Microsoft CHAP version 2 and implements addition support for changing passwords. Microsoft's Active Directory is an example of a directory that supports the MSCHAPv2 protocol for authentication. GTC allows authentication to be based upon one-time passwords and logon passwords and does not require a directory to support MSCHAPv2.
- **EAP FAST** EAP FAST is the EAP type for Layer 2 NAC (authentication client on a Catalyst LAN switch) with 802.1x (NAC-L2-802.1x). EAP FAST is also good on wireless networks since EAP FAST is tunneled LEAP.

The following sections describe each type of EAP in more detail.

EAP MD5

EAP MD5 is one of the simplest authentication mechanisms. EAP MD5 uses one-way authentication, which means that only the supplicant has to provide authentication to the authenticator. In other words, the supplicant is not protected from a rogue authenticator. EAP MD5 is not the best choice for wireless LANs because it is a one-way authentication protocol. EAP MD5 uses the MD5 hash that was originally defined in 1992. Microsoft Windows XP contains a native EAP MD5 802.1x supplicant and uses a password on the end-user workstation.

EAP TLS

EAP Transport Layer Security (TLS) uses digital certificates for user authentication and key generation. TLS uses both the certificate of the client and authentication server to implement mutual authentication. EAP TLS verifies that the user possesses an RSA key pair that is signed in the certificate. EAP TLS generates a unique key per session for each user. EAP TLS is defined in RFC 2716, "PPP EAP TLS Authentication Protocol."

LEAP

LEAP is an EAP type designed to authenticate users attempting gain access to a wireless network. LEAP can use Cisco ACS as the authentication server. LEAP provides a secure wireless connection and promotes a unique session key for encryption for each user. The Cisco Aironet Client contains a LEAP supplicant for 802.1x wireless networks.

PEAP

PEAP was designed to provide a more secure or protected form of EAP as an alternative to EAP MD5. PEAP is supported by Microsoft and provides a protected EAP for authentication on both wireless networks and LANs. PEAP uses digital certificates on the server-side to provide secure and encrypted authentication. PEAP can use EAP GTC to provide two-factor user authentication with one-time passwords. PEAP can also use MSCHAPv2 to provide a unique session key without the overhead of a client-side digital certificate solution.

PEAP is a popular EAP type on 802.1x networks today because it enables a Microsoft machine with an 802.1x supplicant to authenticate on both wireless and wired (Ethernet LAN) networks. The popularity of PEAP can also be attributed to the fact that Microsoft XP contains a native PEAP 802.1x supplicant. PEAP MSCHAPv2 in addition to EAP TLS described earlier are two EAP types that support Windows machine authentication.

EAP FAST

EAP FAST is a technology that can use Cisco ACS as the authentication server. EAP FAST allows the EAP protocol to be transmitted over a secure, encrypted TLS tunnel. EAP FAST is also highly secure through the use of strong secrets, or Protected Access Credentials (PAC). Cisco ACS uses a master key to generate these credentials. PACs can be provisioned both in-band and out-of-band for the authentication process.

In addition to being a strong security solution, EAP FAST can be a higher-performing solution than some of the other EAP protocols because EAP FAST can use shared secrets rather than more resource-intensive mechanisms, like digital certificates or public key infrastructure (PKI). EAP FAST can be an attractive candidate for embedded devices with low processor power since it does not have to process digital certificates. EAP FAST can be used in Layer 2 or LAN switch NAC deployment. EAP FAST can also be used for 802.1x authentication to both wired and wireless networks.

PREV NEXT

VPN and 802.1x

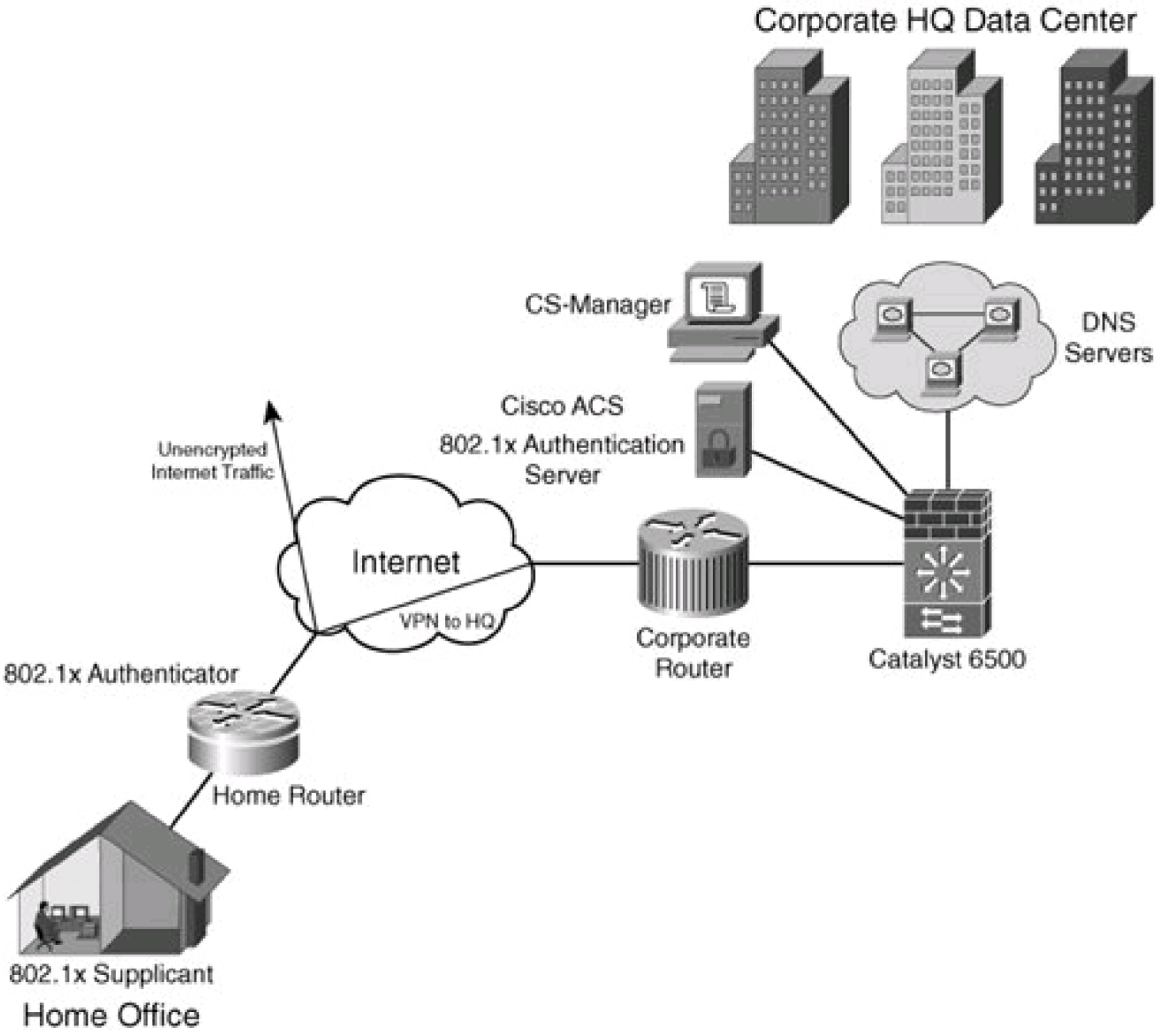
Port-based user authentication is very useful in a remote-access or teleworker environment. The ability for people to work at home after hours or on weekends can provide a major boost in productivity. However, the ability for people to work from home also has risks because the home network is typically not controlled by the IT staff of the employer. Due to security risks, the IT staff of the employer would like only the employee to access the corporate network, and not the PCs or PDA of that employee's spouse or kids. For example, the employee's daughter takes her laptop to college and downloads MP3s. Unfortunately, in this process she also downloads the latest virus in addition to the latest tune from her favorite band. She goes home for the weekend to get her laundry done and uses the wireless network at home to IM with her college friends. In this process, she inadvertently places the virus on the employer's network through the tunneled connection from the employee's house that first goes through the employer's corporate network prior to the Internet.

802.1x authentication can be used to allow only the employee's laptop to join the VPN connection to the corporate network, while allowing the college student at home to use the Internet through the home network. An 802.1x authenticator is embedded or included in the home router as an IOS feature. In this example, the home router receives information from the 802.1x supplicant on the laptop. The home router, or 802.1x authenticator, sends the authentication request to the authentication server at the corporate network. The authentication server in many Cisco self-defending networks is the Cisco Secure ACS.

Figure 5-2 shows an example of a teleworker network with a VPN to the corporate network using 802.1x authentication. InFigure 5-2, the at-home college student can access the Internet through the same home network router that the employee uses to access the corporate network. She does not risk infection to the corporate network because her network traffic goes directly to the Internet rather than going first to the corporate network and then to the Internet.

Figure 5-2. Teleworker VPN with 802.1x

[View full size image]



This teleworker network supports the ability for the VPN tunnel to remain active between the home network router and the access router at the corporate network. The IT staff at the employer's network can define an IP pool for valid employee devices that need to connect to the corporate network and a separate IP pool for nonemployee machines. The dual IP pool solution has the advantage that the employee machines can use the corporate DNS server and the nonemployee machines can use the ISP DNS server.

PREV NEXT

Summary

802.1x is an IEEE standard that defines how to identify a user and grant a user access to a network. 802.1x is a link layer, or Layer 2, authorization protocol that defines how a user is granted port-based access to a network. 802.1x is composed of three major components: supplicant, authenticator, and authentication server. The supplicant resides on the enddevice to identify the user. The authenticator can exist in a Catalyst LAN switch, wireless access point, or router and forwards authentication requests from the supplicant device to the authentication server. The authentication server contains knowledge of the authorized users and the network privileges that should be granted to a user for network access. The Cisco ACS server is an example of an authentication server.

802.1x communication occurs between the supplicant and the authenticator. Communication between the authenticator and authenticator server is in the form of RADIUS records. EAP types are used to communicate between the supplicant and the authentication server. Many EAP types exist for different network scenarios, including oneway authentication (supplicant authenticates to authenticator), two-way authentication (protects supplicant devices against rouge authenticators), support for both wired (Ethernet) and wireless (WiFi) networks, and support for either passwords or digital certificates.

802.1x is a good base for user authentication. Other functionality can complement 802.1x user authentication. 802.1x also supports device or machine authentication. Machine authentication uses Microsoft's Active Directory, so machine authentication is only supported for Microsoft Windows PCs. Cisco IBNS layers additional functionality on to an 802.1x network, including the ability to bypass authentication based upon MAC address and the WoL feature to activate and reboot an idle computer in order to remotely install software applications, patches, and updates. NAC can also leverage an 802.1x network to provide additional checks of the security posture on the authenticating device to ensure that the device has the proper antivirus, service packs, and hotfix updates to safely join the network. 802.1x is also supported in Cisco's IOS routers and can implement additional security for remote employees and teleworkers by using 802.1x to allow the employee to safely access the corporate network while allowing other users on the home network to access the Internet without connecting through the corporate network.

References

Cisco Systems, Inc. User Guide for Cisco Secure ACS for Windows Server 3.3.
http://cisco.com/en/US/products/sw/secursw/ps2086/products_user_guide_book09186a00802335e2.html

Aboba, B., and D. Simon. RFC 2716, PPP EAP TLS Authentication Protocol. 1999.

Cisco Systems, Inc. Cisco IOS Easy VPN Remote with 802.1x Authentication.
http://cisco.com/en/US/tech/tk583/tk372/technologies_white_paper09186a00801fdef9.shtml

Cisco Systems, Inc. Layered Security in a VPN Deployment.
http://www.cisco.com/en/US/products/ps6660/products_white_paper0900aecd8046cbc4.shtml

Cisco Systems, Inc. FAQ: How Does 802.1x Work with Cisco IBNS?
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns75/c685/ccmigration_09186a0080259020.pdf

Cisco Systems, Inc. FAQ: Using Cisco Secure ACS with Cisco IBNS.
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns75/c685/ccmigration_09186a0080259063.pdf

Cisco Systems, Inc. FAQ: Overview of 802.1x and Cisco IBNS Technology.
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns75/c685/ccmigration_09186a0080258e2f.pdf

Cisco Systems, Inc. FAQ: VLAN Assignment with Cisco IBNS.
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns75/c685/ccmigration_09186a0080259047.pdf

Cisco Systems, Inc. Cisco LEAP.
http://www.cisco.com/en/US/products/hw/wireless/ps430/products_qanda_item0900aecd801764f1.shtml

Chapter 6. Implementing Network Admission Control

This chapter covers the following topics:

- Network admission control overview
- NAC Framework benefits
- NAC Framework components
- Operational overview
- Deployment models

Network Admission Control (NAC) is a technology initiative led by Cisco Systems working in collaboration with many leading security vendors, including antivirus and desktop management. Their focus is the creation of solutions that limit security threats, such as worms and viruses.

This technology provides a framework using existing Cisco infrastructure to enforce network admission policies on NAC-enabled endpoint devices, guaranteeing software compliance before network access is granted. If an endpoint device is determined noncompliant, a variety of admission actions are available to administrators, and how the actions are implemented is at the discretion of the network administrator. For example, a noncompliant endpoint may be placed in a quarantine area of the network and redirected to a remediation server to load the necessary software or patches. A notification is displayed to the user warning that their device is not compliant or, in the worse case, that they are denied network access entirely.

This chapter describes the Cisco NAC Framework, identifies benefits, describes the solution components and how they interoperate, and describes common deployment models.

Network Admission Control Overview

Worms and viruses continue to be disruptive, even though many businesses have significantly invested in antivirus and traditional security solutions. Not all users stay up to date with the many needed software security patches of antivirus files. Noncompliant endpoints are frequent and the reasons vary; for example:

- A user might choose to wait and install a new update later because they don't have the time
- A contractor, partner, or guest needs network access; however, the business may not control the endpoint
- The endpoints are not managed
- The business lacks the capability to monitor the endpoints and determine whether they are updated to conform to the business's security policy

When infected endpoints connect to the network, they unsuspectingly spread their infections to other improperly protected devices. This has caused businesses to examine how they should implement endpoint compliance enforcement besides user authentication before granting access to their networks.

Cisco Systems provides two network admission control solution choices:

- NAC Appliance
- NAC Framework

Chapter 7, "Cisco Clean Access," describes NAC Appliance, which was originally marketed as Cisco Clean Access (CCA). NAC Appliance is a turnkey self-sufficient package that does not rely on third-party products for determining and enforcing software compliance. This chapter focuses on NAC Framework.

NAC Framework is an integrated solution that enables businesses to leverage many of their existing Cisco network products, along with many third-party vendor products such as antivirus, security, and identity-based software. Vendor products must be NAC-enabled in order to communicate with the NAC-enabled network access devices. NAC Framework is extremely flexible because it can enforce more features available from other vendors' products. A comparison of customer preferences for choosing the NAC Appliance and NAC Framework is shown in Table 6-1.

Table 6-1. *NAC Customer Profile*

NAC Framework	NAC Appliance
Uses an integrated framework approach, leveraging existing security solutions from other vendors	Prefers bundled, out-of-the-box functionality with preinstalled support for antivirus and Microsoft updates
Complex network environment, leveraging many types of Cisco network access products	Heterogeneous network infrastructure
Longer, phased-in deployment model	Rapid deployment model
Can integrate with 802.1x	Independent of 802.1x

Source: Cisco Systems, Inc.[1]

NAC Framework Benefits

Following are some benefits that can be recognized by businesses that have implemented NAC Framework:

- **Protects corporate assets** Enforces the corporate security software compliance policy for endpoints.
- **Provides comprehensive span of control** All the access methods that endpoints use to connect to the network are covered, including campus switching, wireless, router WAN links, IP Security (IPSec), and remote access.
- **Controls endpoint admission** Validates all endpoints regardless of their operating system, and it doesn't matter which agents are running. Also provides the ability to exempt certain endpoints from having to be authenticated or checked.
- **Offers a multivendor solution** NAC is the result of a multivendor collaboration between leading security vendors, including antivirus, desktop management, and other market leaders. NAC supports multiple security and patch software vendors through APIs.
- **Leverages existing technologies and standards** NAC extends the use of existing communications protocols and security technologies, such as Extensible Authentication Protocol (EAP), 802.1x, and RADIUS services.
- **Leverages existing network and antivirus investments** NAC combines existing investments in network infrastructure and security technology to provide a secure admission control solution.

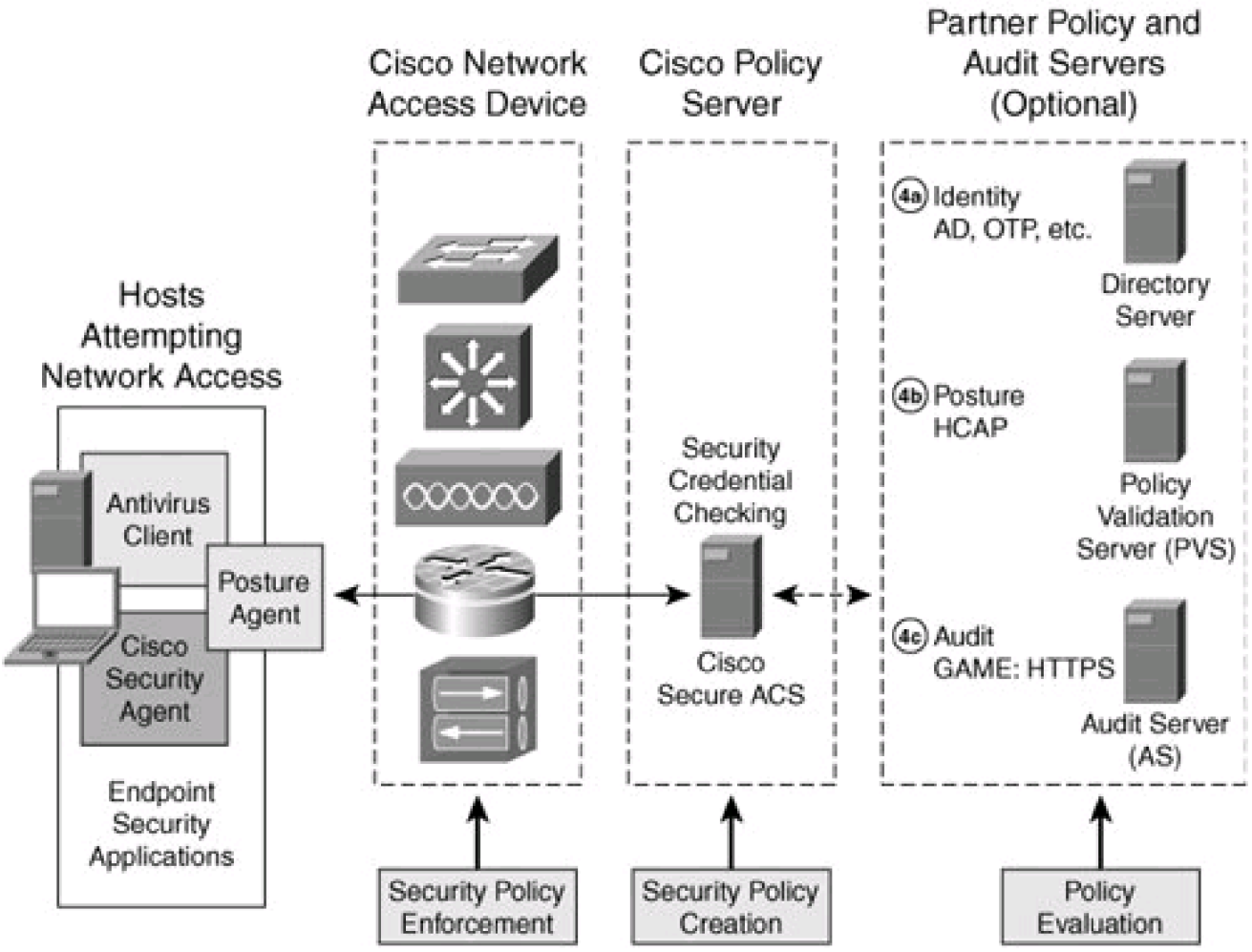
NAC Framework Components

The initial release of the Cisco NAC Framework became available in June 2004 and continues to evolve in phases. The functions of the solution architecture remain consistent; however, as each phase is introduced, more capabilities and deeper integration are added to the NAC Framework architecture. To stay up to date with NAC and partner products, refer to the URL www.cisco.com/go/nac.

NAC Framework includes the following main components, as shown in Figure 6-1:

Figure 6-1. NAC Framework Components

[View full size image]



- Endpoint security application
- Posture agent

- Network access devices
- Cisco Policy server
- Optional servers that operate as policy server decision points and audit servers
- Optional management and reporting tools are highly recommended (not shown)

The next sections describe the main components in more detail.

Endpoint Security Application

An endpoint security application is security software that resides on a host computer. Depending on the application, it can provide host-based intrusion prevention system (HIPS), antivirus scanning, personal firewall, and other host security functions. Cisco Security Agent is a HIPS example.

NAC partners provide NAC-enabled security applications that use a posture plug-in that communicates their credentials and state with a posture agent, both residing on the same endpoint. Many endpoint security applications provide antivirus capabilities, and some provide additional identity-based services. For a list of NAC partners, refer to www.cisco.com and search for "Network Admission Control Current Participants."

Posture Agent

A posture agent is middleware or broker software that collects security state information from multiple NAC-enabled endpoint security applications, such as antivirus clients. It communicates the endpoint device's compliance condition. This condition is referred to as the *posture* of an endpoint. The posture information is sent to Cisco Secure Access Control Server (ACS) by way of the Cisco network access device.

The *Cisco Trust Agent* is Cisco's implementation of the posture agent. Cisco has licensed the trust-agent technology to its NAC partners so that it can be integrated with their security software client products. The trust agent is free and is also integrated with the Cisco Security Agent. Cisco Trust Agent can work with Layer 3 Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP), and Cisco Trust Agent (CTA) version 2 can also work with Layer 2 with Extensible Authentication Protocol over 802.1x (EAPo802.1x) or Extensible Authentication Protocol over LAN (EAPoLAN).

Network Access Devices

Network access devices that enforce admission control policy include Cisco routers, switches, wireless access points, and security appliances. These devices demand endpoint security credentials and relay this information to policy servers, where network admission control decisions are made. Based on customer-defined policy, the network will enforce the appropriate admission control decisionpermit, deny, quarantine, or restrict. Another term for this device is security policy enforcement point (PEP).

Policy Server

A policy server evaluates the endpoint security information relayed from network access devices (NADs) and determines the appropriate

admission policy for enforcement. The Cisco Secure ACS, an authentication, authorization, and accounting (AAA) RADIUS server, is the foundation of the policy server system and is a requirement for NAC. Cisco Secure ACS is where the admission security policy is created and evaluated to determine the endpoint device's compliance condition or posture.

Optionally, Cisco Secure ACS may work in concert with other policy and audit servers to provide the following additional admission validations:

- **Identity** User authentication can be validated with an external directory server and the result is communicated to Cisco Secure ACS. Examples include Microsoft Active Directory and one-time password (OTP) servers.
- **Posture** Third-party, vendor-specific credentials such as antivirus and spyware can be forwarded using the Host Credential Authorization Protocol (HCAP) to NACenabled Policy Validation Servers (PVS) for further evaluation. This enables businesses to leverage existing policies maintained in their PVS to validate and forward the software compliance result to Cisco Secure ACS, ensuring that a consistent policy is applied across the entire organization.
- **Audit** Determines the posture for a NAC Agentless Host (NAH), which is a host without the presence of a posture agent such as Cisco Trust Agent. The Audit server works out of band and performs several functions:

  - Collects posture information from an endpoint.

  - Acts as a posture validation server to determine compliance of an endpoint and determine the appropriate compliance result in the form of a posture.

  - Communicates the result to Cisco Secure ACS using Generic Authorization Message Exchange (GAME) over an HTTPS session. GAME uses an extension of Security Assertion Markup Language (SAML), a vendorneutral language enabling Web services to exchange authentication and authorization information.

The optional validation policy servers communicate the user authentication status or compliance status or both to Cisco Secure ACS, which makes the final determination as to the admission policy for the endpoint. *Policy decision point* is a term used to describe the function Cisco Secure ACS performs.

Management and Reporting Tools

In addition to the required NAC components, a management system is recommended to manage and monitor the various devices. Reporting tools are available to operation personnel to identify which endpoints are compliant and, most importantly, which endpoints are not compliant. Examples include Cisco Security MARS and CiscoWorks Security Information Manager Solution (SIMS).

PREV NEXT

Operational Overview

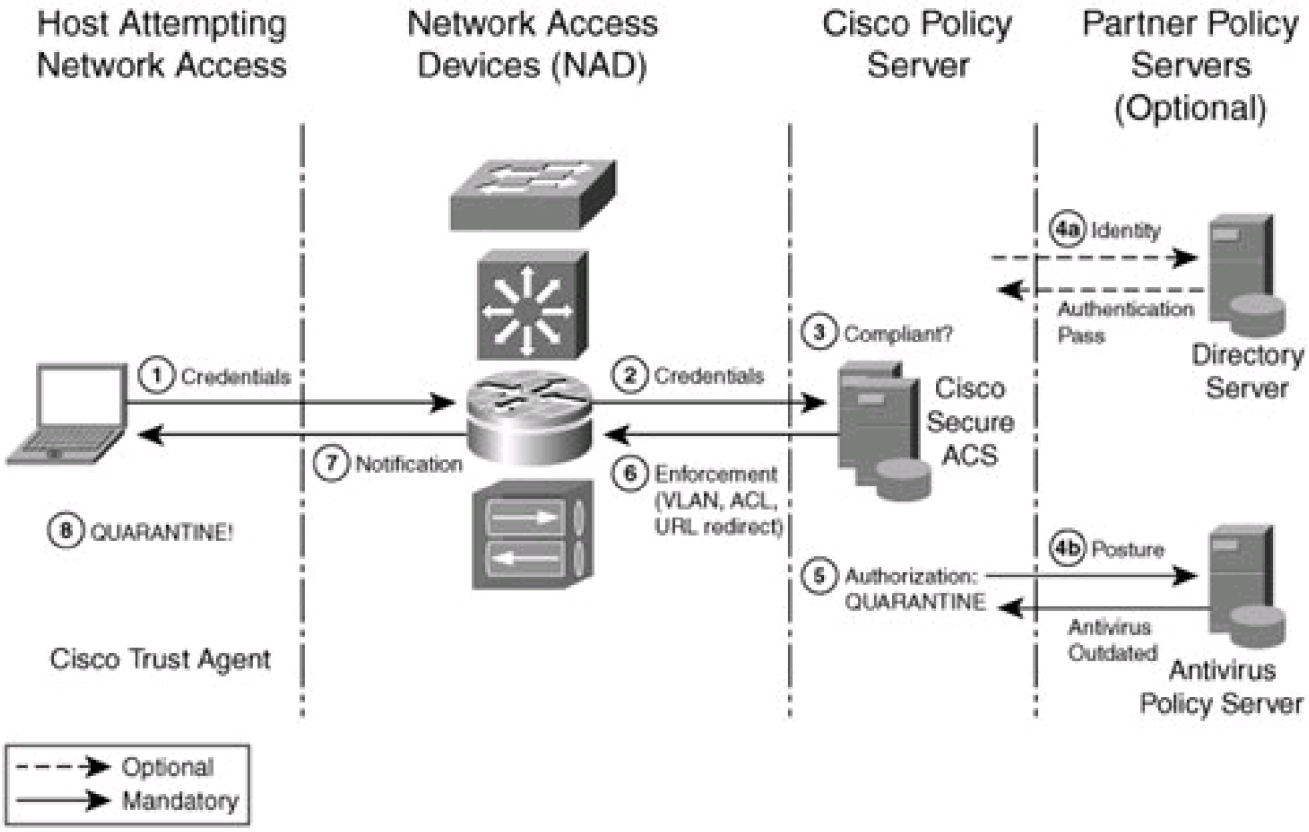
This section describes how NAC determines admission compliance and how it then uses the network to enforce the policy to endpoints.

Network Admission for NAC-enabled Endpoints

This section describes the process in which a noncompliant endpoint device is discovered and is denied full access until it is compliant with the admission policy. This scenario is shown in Figure 6-2.

Figure 6-2. Admission Process for Noncompliant Endpoint

[View full size image]



The following list is a summary of the admission process for a noncompliant endpoint shown in Figure 6-2:

1. An endpoint attempts to access the network.
2. The NAD notifies the policy server (Cisco Secure ACS) that an endpoint is requesting network access.
3. Cisco Secure ACS checks the NAC policy to determine whether the endpoint is compliant.
4. Cisco Secure ACS forwards specific information to other partner policy servers.
    a. Identity information is sent to a directory server for authentication validation.
    b. Host credentials are sent to an antivirus policy server for posture determination.
5. Cisco Secure Access uses information from the all-policy servers and decides the endpoints authorization. In this example, the endpoint is not compliant and is assigned a quarantine posture.
6. Quarantine enforcement actions are sent from Cisco Secure ACS to the NAD servicing the endpoint.
7. NAD enforces admission actions and communicates posture to Posture Agent.
8. Posture Agent notifies the user that the endpoint is quarantined.

The following sections explain each step in more detail.

Endpoint Attempts to Access the Network

In step 1, the admissions process begins when an endpoint attempts to access the network. What triggers the process is dependent upon the NAD's capabilities and configuration. The NAD initiates posture validation with Cisco Trust Agent using one of the following protocols:

- EAPoUDP
- EAPo802.1x

The protocol used is dependent upon the NAD to which the endpoint connects. Both of these protocols serve as a communication method between the endpoints using Cisco Trust Agent and the NAD. Cisco Trust Agent gathers credentials from NAC-enabled security applications such as antivirus.

NAD Notifies Policy Server

In step 2, the NAD notifies the policy server (Cisco Secure ACS) that an endpoint is requesting network access. A protected tunnel is set up between the policy server and the endpoints posture agent. Once communication is established, the credentials from each of the posture plug-ins are sent to Cisco Secure ACS.

Cisco Secure ACS Compares Endpoint to NAC Policy

In step 3, Cisco Secure ACS looks at the admission control policy and compares the endpoint credentials to the policy to determine whether it is compliant. It determines which of the following posture states to assign to the endpoint:

- **Healthy** Endpoint is compliant; no network access restrictions.
- **Checkup** Endpoint is within policy, but an update is available. This state is typically used to proactively remediate a host to the Healthy state or to notify a user that a more recent update is available and recommend remediation.
- **Transition** This state became available in NAC phase 2. The endpoint posturing is in process; provide an interim access, pending full posture validation. This state is applicable during an endpoint boot in which all services may not be running or audit results are not yet available.
- **Quarantine** Endpoint is out of compliance; restrict network access to a quarantine network for remediation. The endpoint is not an active threat but is vulnerable to a known attack or infection.
- **Infected** Endpoint is an active threat to other endpoint devices; network access should be severely restricted or totally denied all network access.
- **Unknown** Endpoint posture cannot be determined. Quarantine the host and audit or remediate until a definitive posture can be determined.

Cisco Secure ACS Forwards Information to Partner Policy Servers

In step 4, Cisco Secure ACS can optionally send user login (4a) and credentials (4b) to other policy decision servers. When this is done, Cisco Secure ACS expects to receive authentication status and a posture state from each of the policy decision servers.

In step 4a when NAC L2-802.1x is used, Cisco Secure ACS can send identity information to an authentication server. It confirms that the username and password are valid and returns a passed authentication message to Cisco Secure ACS. If identity authentication fails, no posture is checked and the endpoint fails authentication, resulting in no network access.

In step 4b in this example, an antivirus policy server determines that the device is out of compliance and returns a quarantine posture token to Cisco Secure ACS.

Keep in mind that NAC partner policy servers vary and offer a variety of compliance checks besides antivirus. For example, some vendors offer checking for spyware and patch management.

Cisco Secure ACS Makes a Decision

In step 5, Cisco Secure ACS compares all the posture states and determines which posture is the worst; infected is the worst and healthy is the best. It always assigns the worst state and takes the action for that posture. In this example, the user has passed authentication but the endpoint has been assigned a quarantine posture.

Cisco Secure ACS Sends Enforcement Actions

Cisco Secure ACS takes the actions assigned to a quarantine state. In this quarantine example, they can include the following:

- Enforce quarantine access; this varies based on the NAD.

- For NADs using NAC-L3-IP, the enforcement actions include a quarantine Access Control List (ACL) being applied to the endpoint.

- For NADs using NAC-L2-IP, the enforcement actions include a quarantine ACL being applied to the endpoint.

- For NADs using NAC-L2-802.1x, the enforcement action includes a quarantine virtual LAN (VLAN) being applied to the endpoint device.

- Optionally, the endpoint device may be assigned a URL redirect to the remediation server.
- Optionally, a notification message can be sent to the user, indicating that their device is not compliant and is being redirected for remediation.

NAD Enforces Actions

In step 7, the NAD receives the quarantine policy enforcement from Cisco Secure ACS and responds accordingly. In this example, such a response would be to quarantine the endpoint, enforce an endpoint URL redirect to the remediation server, and send a quarantine message to the posture agent.

Posture Agent Actions

In step 8, the posture agent displays the quarantine message, and the user is redirected to the remediation server.

Actions available vary by NAC partner products. Cisco Secure ACS is capable of sending different application actions from HCAP-compliant policy servers to their specific application plug-ins. This can trigger actions such as the following:

- Force an auto-remediation to a designated remediation server
- Force an auto-patch by instructing the host to download and apply a patch automatically
- Restart a stopped application service

In this example, the endpoint is now quarantined, and the user has been notified by a message. The user can elect to do nothing and remain quarantined, or comply and allow their computer to be updated.

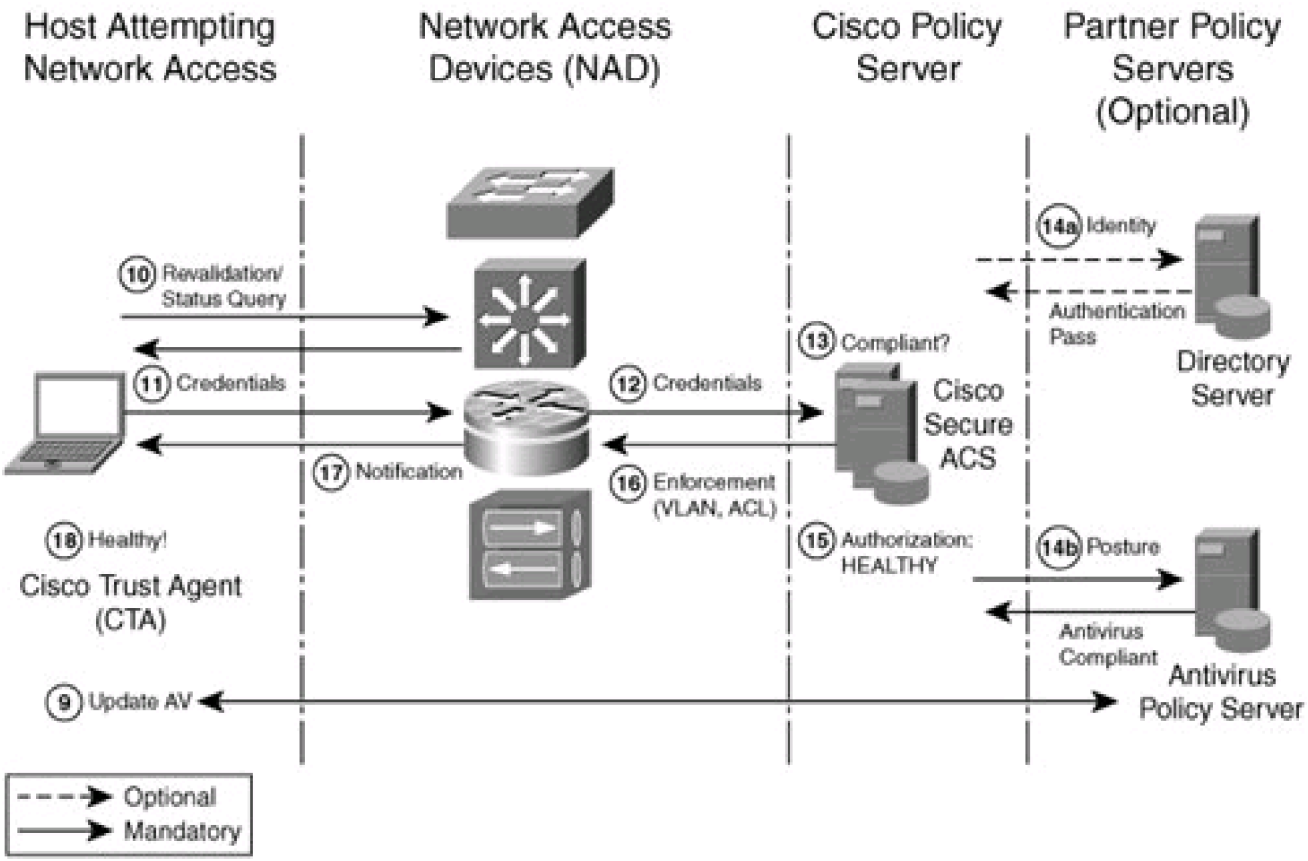
The admission control process can take very little time, as little as milliseconds. The time varies and is based on many factors, including:

- Where the endpoint is located in relation to the policy server and optional partner policy servers
- Where the remediation server is located
- NADs performance capability
- Network bandwidth
- How busy the policy servers are

As shown in Figure 6-3, an endpoint is changing from quarantine to healthy posture state.

Figure 6-3. Admission Process for Endpoint Changing from Quarantine to Healthy State

[View full size image]



The following list explains the process shown in Figure 6-3:

9. Endpoint remediated.

10. Endpoint polled for change of compliance.

11. Host credentials gathered from endpoint.

12. Host credentials passed to Cisco Secure ACS.

13. Cisco Secure ACS rechecks the NAC policy to determine whether the endpoint is compliant.

14. Cisco Secure ACS forwards specific information to other partner policy servers.

- **a.** Identity information is sent to a directory server for authentication validation.
- **b.** Host credentials are sent to an antivirus policy server for posture determination.

15. Cisco Secure Access uses information from all policy servers and decides the endpoints authorization. In this example, the endpoint is compliant and is assigned a healthy posture.

16. Healthy enforcement actions are sent from Cisco Secure ACS to the NAD servicing the endpoint.

17. NAD enforces admission actions and communicates healthy posture to Posture Agent.

18. Posture Agent can notify the user that the endpoint is healthy. Many businesses prefer that a healthy posture be transparent to the user with no message notification displayed.

Endpoint Polled for Change of Compliance

Once an endpoint has been assigned a posture, it stays in effect and is not checked again until a NAC timer has expired or a posture agent trigger occurs.

The following are configurable timers for NAC:

- **Status Query** Ensures that an endpoint remains compliant with the admission policy. The timer begins at policy enforcement for the endpoint; compliance is rechecked after the timer expires. Different Status Query timers can exist for different posture states. A shorter amount of time is beneficial for noncompliant states such as quarantine; the device can be rechecked sooner than a healthy device, in order to regain full network access.
- **Revalidation** A time in which the posture remains valid. It can be set lower when an outbreak occurs, to force all endpoints to go through the admission policy process again. This enables endpoints to timeout at different intervals depending on where their timers are, versus forcing all endpoints to go through the validation process at the same time.

  In phase 2 with NAC-L2-802.1x, there is no capability to send a status query from the NAD by way of 802.1x. To overcome this, beginning with version 2 of Cisco Trust Agent, an asynchronous status query capability exists. Cisco Trust Agent can send an Extensible Authentication Protocol Over Lan (EAPOL)-Start to the NAD, or CTA can frequently poll all registered NAC application posture plug-ins looking for a change in credentials. If a change exists, it will trigger an EAPOL-Start signaling for a new posture validation.

  In step 10 of Figure 6-3, the quarantine status query timer has expired.

The NAD is aware that the timer has expired for the endpoint, so it begins rechecking for compliance. The posture agent gathers credentials from the posture plug-ins of NACenabled security applications such as antivirus.

Revalidation Process

From step 11 through step 18, the process is the same as the example described in Figure 6-2. The NAD notifies the policy server (Cisco Secure ACS) that an endpoint requests network access. This time, the Cisco Secure ACS determines that the posture is healthy for all admission checks and that the user login is valid. Authentication is successful, and Cisco Secure ACS assigns the healthy policy.

The NAD receives the healthy policy enforcement from Cisco Secure ACS and responds accordingly by allowing full network access. The timers begin for the healthy state.

The NAD informs the posture agent of the healthy status, but no message is sent to the user this time. The user can now resume normal network activity.

Network Admission for NAC Agentless Hosts

The previous example described the admission process for a NAC-enabled endpoint running a posture agent, such as Cisco Trust Agent. This section describes the process for endpoints that do not have a posture agent.

NAC agentless hosts (NAH) can be accommodated by several methods, as shown in Table 6-2. A NAH exception list and whitelist can be

created to identify known endpoints that do not have a posture agent installed and running. The option chosen is dependent upon the NAC Framework component and the NAD enforcement method used.

Table 6-2. NAC Agentless Host Exceptions and Whitelisting

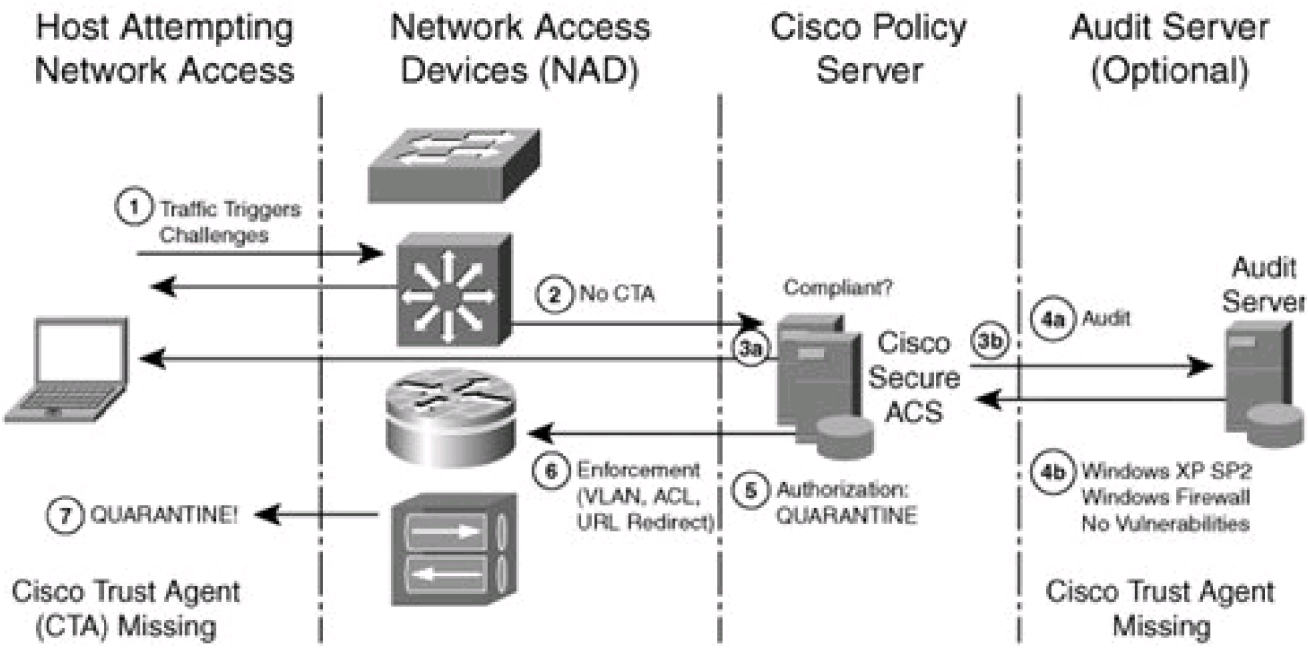
Component	Administration Model	NAC-L2 IP	NAC-L3 IP	NAC-L2 802.1x
NAD	• Distributed, managed at the device level • Does not scale	Device Type, IP, or MAC Enforcement by intercept ACL (IP/MAC)	Device Type, IP, or MAC Enforcement by intercept ACL (IP)	MAC-Auth-Bypass (identity + posture)
Cisco Secure ACS whitelist	• Centralized • Scales	MAC(posture only)	MAC(posture only)	MAC-Auth-Bypass (identity + posture)
Audit	• Centralized • Scales	Active network scan, remote login, browser object, hardware/software inventory	Active network scan, remote login, browser object, hardware/software inventory	Not supported at the time of this writing

Source: Cisco Systems, Inc.[2]

The audit server can be used for NAH in all enforcement methods and is a single centrally managed server. As shown in Figure 6-4, an audit server can be included as a decision policy server for NAH. The audit server can determine the posture credentials of an endpoint without relying on the presence of a posture agent.

Figure 6-4. Admission Control for NAC Agentless Host

[View full size image]



The following list explains the process shown in Figure 6-4:

1. An endpoint attempts to access the network. The trigger mechanism is dependent upon the NAD's capabilities and configuration. The NAD attempts to initiate posture validation with the posture agent, but no posture agent (Cisco Trust Agent) exists.

2. The NAD notifies the policy server (Cisco Secure ACS) that an endpoint is requesting network access with no Cisco Trust Agent (CTA) present.

3. Cisco Secure ACS cannot determine whether the NAH is compliant because no posture agent exists. Cisco Secure ACS performs the following:

    a. Assign a transition posture to grant a temporary, limited network access to the agentless host while the audit server is determining the full posture validation. The NAD enforces the transition admission policy.

    b. Notify the external audit server that the NAH is requesting admission.

4. Cisco Secure ACS cannot determine whether the NAH is compliant, so it notifies the audit server using GAME to conduct a scan on the endpoint.

    a. The audit server scans the endpoint. It evaluates the endpoint's software information against the audit server's compliance policy. It determines that the operating system patch level is compliant or healthy, but the posture agent is missing, so it is considered noncompliant.

    b. Quarantine is the application posture token (APT) assigned by the audit server for this NAH and is communicated to Cisco Secure ACS.

5. Cisco Secure ACS uses quarantine as the final posture, which is referred to as the system posture token (SPT), and takes the actions assigned to a quarantine state. The actions can include the following:

    - **Enforce quarantine access** This varies based on the NAD. For NAC-L3-IP, the enforcement actions include a quarantine ACL being applied to the endpoint.

For NADs using NAC-L2-IP, the enforcement actions include a quarantine ACL being applied to the endpoint.

For NADs using NAC-L2-802.1x, the enforcement action includes a quarantine VLAN.

- **Enforce Redirection (optional)** In this example, the endpoint device is assigned a URL redirect to the remediation server.

6. The NAD receives the quarantine policy enforcement from Cisco Secure ACS. It quarantines the endpoint and sends the endpoint a redirect URL to go to the remediation server.

7. The endpoint is now quarantined and redirected to a remediation server. With NAH, the URL redirect is the only way to provide feedback to the user because there is no posture agent present. At this point, the user can elect to do nothing and remain quarantined, or comply and allow their host to remediate by installing Cisco Trust Agent.

From this point, the NAC Framework process is the same as the example in which the endpoint state changed from quarantine to healthy as shown in Figure 6-3.

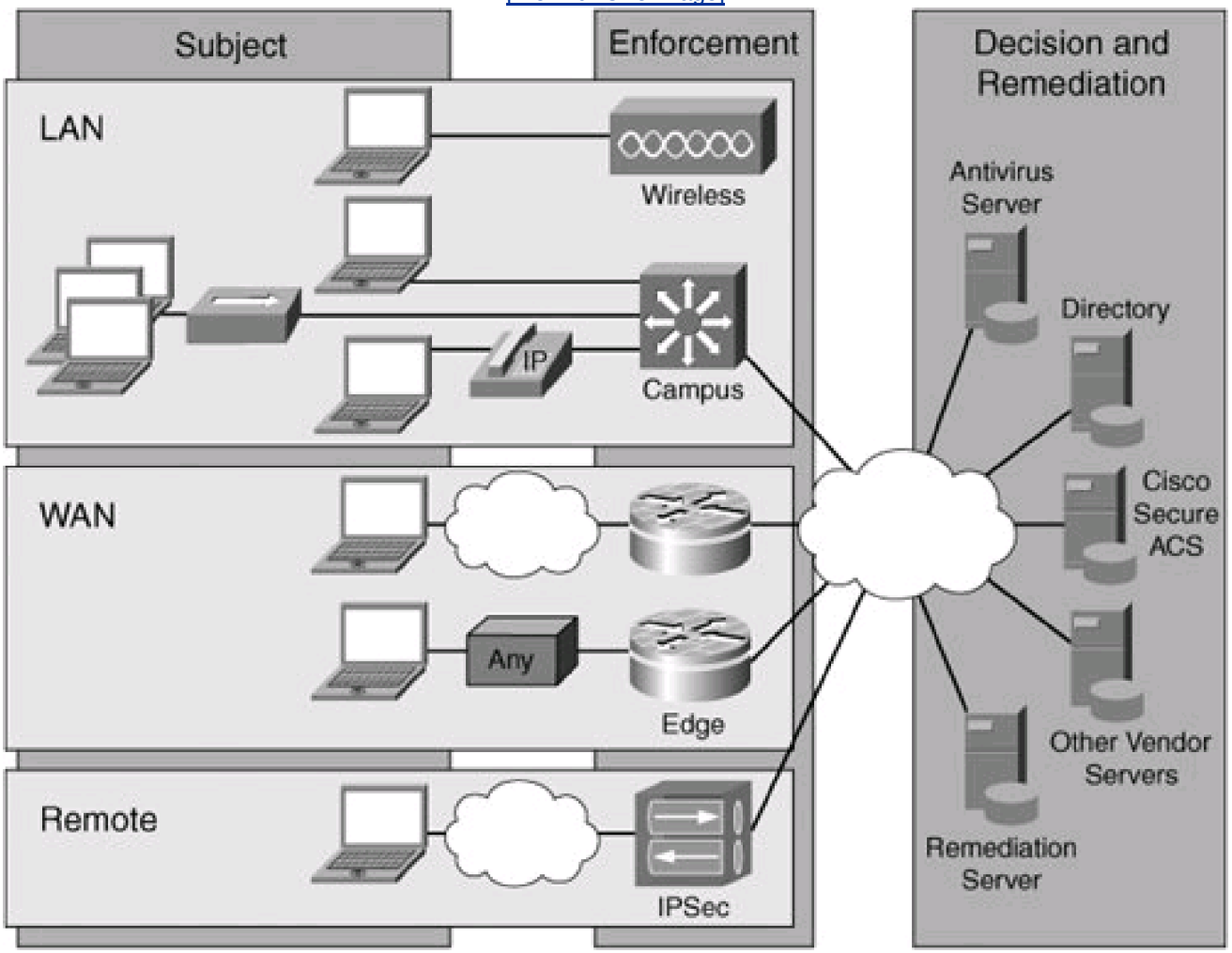
PREV NEXT

Deployment Models

Cisco NAC Framework is a flexible solution providing protection to connected endpoints regardless of network connectivity. As shown in Figure 6-5, it operates across all access methods including campus switching, wired and wireless, WAN and LAN links, IP Security (IPSec) connections, and remote access links.

Figure 6-5. NAC Deployment Scenarios

[View full size image]



Source: Cisco Systems, Inc.[3]

The first NAC Framework deployment rule of thumb is to use the NAC-enabled NAD closest to the endpoints for checking compliance, helping enforce a least-privilege principle. The second rule is that compliance checking for an endpoint should occur at one NAD (closest

to the endpoint), not throughout the network. The NAD might not be capable of performing compliance checks or enforcing the admission policy. Examples include non-Cisco devices or an older NAD that does not support NAC. As a result, NAC deployments will vary.

The following sections describe common NAC deployment scenarios.

LAN Access Compliance

NAC monitors desktops and servers within the office, helping to ensure that these endpoints comply with corporate antivirus and operating system patch policies before granting them LAN access. This reduces the risk of worm and virus infections spreading within an organization by expanding admission control to Layer 2 switches.

NAC Framework can also check wireless hosts connecting to the network to ensure that they are properly patched. The 802.1x protocol can be used in combination with device and user authentication to perform this validation using the NAC-L2-802.1x method. Some businesses might not want to use the 802.1x supplicant, so instead they may choose to use the NAC-L2-IP method using either IP or MAC.

NAC can be used to check the compliance of every endpoint trying to obtain network access, not just those managed by IT. Managed and unmanaged endpoints, including contractor and partner systems, may be checked for compliance with antivirus and operating system policy. If the posture agent is not present on the interrogated endpoint, a default access policy can be enforced limiting the endpoint to a specific subnet, thus limiting its ability to infect other devices on the entire network.

WAN Access Compliance

NAC Framework can be deployed at branch or home offices to ensure that endpoints comply with the latest antivirus and operating system patches before allowing them access to WAN or Internet connections to the corporate network. Alternatively, compliance checks can be performed at the main office before access is granted to the main corporate network.

Remote Access Compliance

NAC Framework helps to ensure that remote and mobile worker endpoints have the latest antivirus and operating system patches before allowing them to access company resources through IP Security (IPsec) and other virtual private network (VPN) connections.

PREV NEXT

Summary

The Cisco Network Admission Control is a framework comprising Cisco networking infrastructure along with a variety of partner products to enforce network admission policies on NAC-enabled endpoint devices, guaranteeing software compliance before granting network access.

The Cisco NAC Framework consists of the following components:

- NAC-enabled security applications such as antivirus and host intrusion protection systems such as Cisco Security Agent
- Posture agents such as Cisco Trust Agent
- Network access devices such as routers, switches, and wireless access points
- Cisco Secure ACS, which is the Cisco Policy Server
- Optional third-party validation policy servers
- Optional management and reporting tools

NAC allows the appropriate level of network access only to compliant and trusted endpoint devices such as PCs, servers, and PDAs. NAC can also identify noncompliant endpoints, deny them access, and place them in a quarantined area or give them restricted access to computing resources.

NAC agentless hosts can be identified by exception lists, whitelisting, or audit servers and can be evaluated before granting network access.

NAC Framework operates across all network access methods including campus switching, wired and wireless, router WAN and LAN links, IPSec connections, remote access, and dial-up links.

References

1 Cisco Systems, Inc. NAC Customer Profile Reference by Russell Rice. Network Admission Control (NAC) Cisco Security SEVT Update. April 6, 2005.

2 Cisco Systems, Inc. NAC Agentless Host Exceptions and Whitelisting. 2005.

3 Cisco Systems, Inc. Network Admission Control (NAC). 2005.

Chapter 7. Network Admission Control Appliance

In Chapter 6 you learned about the Network Admission Control (NAC) framework that is implemented with Cisco IOS routers and Catalyst LAN switches. Because NAC Framework is implemented with routers and switches, it leverages the existing network infrastructure.

This chapter describes the NAC appliance, which is also marketed as Cisco Clean Access (CCA). The NAC appliance offers a dedicated NAC deployment option that provides admission control functions including authentication, posture validation, and remediation. The NAC appliance is composed of a server and manager component. The NAC appliance server implements the admission control features, whereas the NAC appliance manager configures the policies on the NAC appliance servers. The NAC appliance also features an optional client agent for the Windows end stations within the network. The client agent provides additional security posture validation options, including Windows registry value, file, service, and application checks. The client agent can also assist the remediation process to help the end station download the necessary software updates to authenticate and safely join the network.

There are several deployment options for the NAC appliance. The NAC appliance server can be deployed in-band or out-of-band. An in-band deployment ensures that all data from the authenticated client flows through the NAC appliance server. An out-of-band deployment allows the NAC appliance server to be removed from data flow from the client after a successful authentication and subsequent network scans for posture validation.

NAC Appliance Features

NAC appliance is a dedicated, or turnkey, NAC deployment option that is implemented with dedicated server and management appliances. The option of a dedicated NAC appliance provides the ability to have a turnkey NAC deployment that does not use resources from existing network components like routers or switches. NAC appliance may also be considered to be a simpler NAC deployment option as a dedicated, self-contained appliance suite. For example, NAC appliance does not use a router or switch as the authentication client. NAC appliance also does not require 802.1x as a port-based user authentication mechanism and does not require an 802.1x authentication server. NAC appliance also does not require the customer to purchase third party vendor servers for policy validation, audit, and remediation.

NAC appliance offers several features, including the following:

- Authenticates device attributes and users for network admission.
- Provides an all-in-one NAC deployment option with a dedicated server appliance, manager appliance, and optional appliance agent for Windows PCs and laptops.
- Scans PCs, servers, and laptops on the network to identify infected or vulnerable hosts.
- Identifies vulnerabilities and views registry key values with an optional client agent. At the time of this writing, the client agent is offered at no additional cost.
- Quarantines vulnerable machines and facilitates remediation.
- Provides DHCP, DHCP Relay, and Network Address Translation (NAT) services to users on untrusted networks.
- Supports floating devices like public kiosks that require each new user to authenticate after the logoff of the previous user.
- Terminates VLANs between trusted and untrusted networks.
- Supports "bump-in-the-wire" and acts like an Ethernet bridge in addition to IP gateway scenarios. *Bump-in-the-wire* means that the NAC appliance server acts in a pass-through mode and does not require IP readdressing. IP gateway provides a routed option for the NAC appliance deployment.
- Allows IP Security (IPSec), Layer 2 Transport Protocol (L2TP), and Point-to-Point Tunneling Protocol (PPTP) encryption from PCs and laptops to be terminated on NAC appliance server between untrusted and trusted networks. The IPSec/L2TP/PPTP functionality requires specific software on the client system.
- Provides exemption or filters so that certain devices (based upon Layer 2 MAC address) and users do not have to be authenticated.
- Denies a specific device (MAC address), user, IP address or subnet from authenticating to the network.
- Allows the enforcement of bandwidth restriction for certain user classes.
- Incorporates a native high availability (HA) solution between two servers.
- Provides NAC Message Information Block (MIB) to integrate with Hewlett-Packard Open View (HP OV) SNMP systems.
- Offers a subscription service for automatic Microsoft OS, antivirus, and antispyware updates.
- Allows single sign-on with remote-access VPN.

NAC Appliance Manager

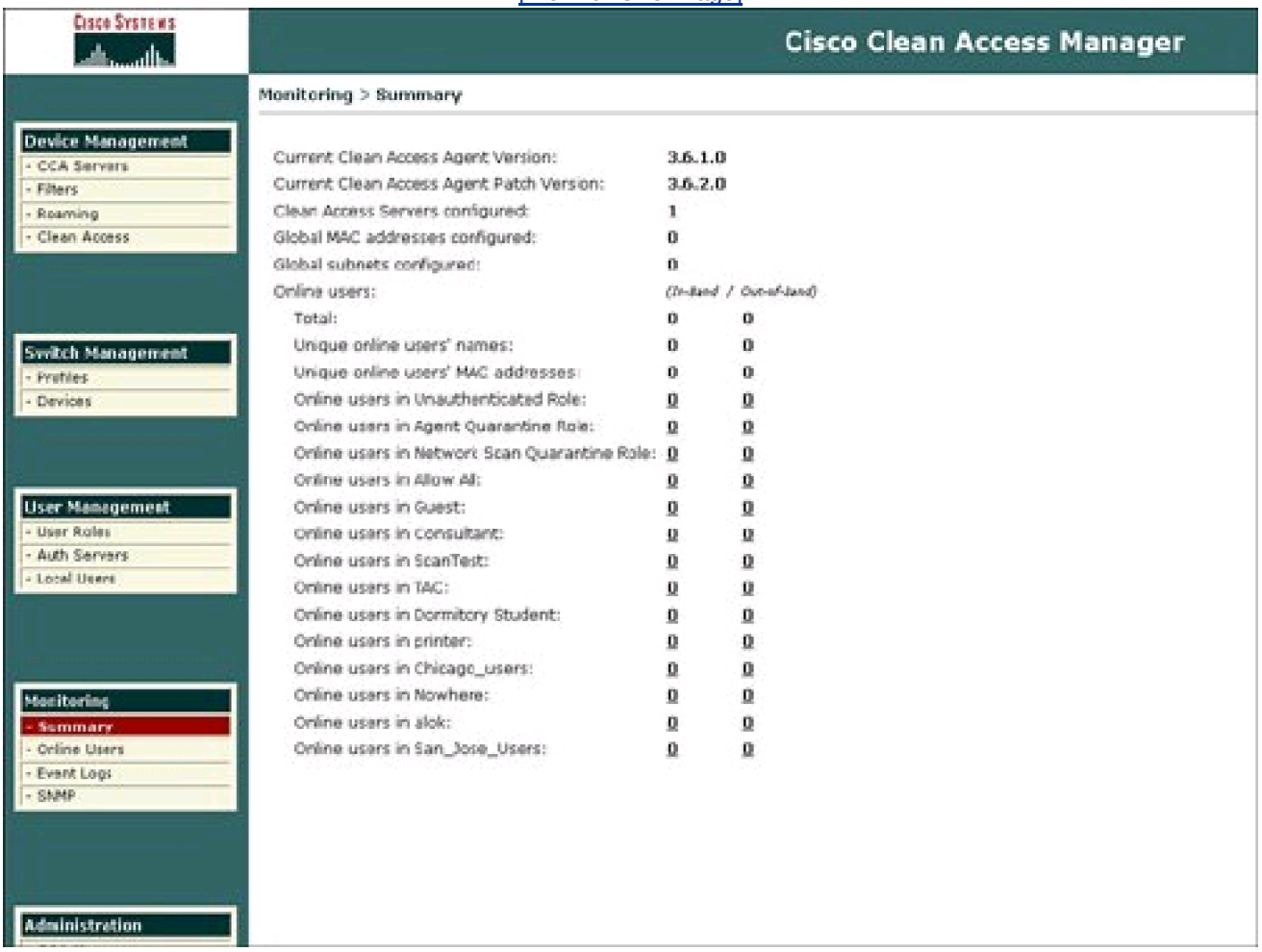
The NAC appliance servers are managed by the NAC appliance manager. NAC appliance also offers optional subscription services for automatic OS, antivirus, and antispyware updates.

A web browser is used as the client GUI to the NAC appliance manager. Configuration from the web GUI client is secured by using HTTPS between the client web browser and the NAC appliance manager. Users must provide a username and password to log on to the NAC appliance manager. Usernames and passwords can be stored in an external LDAP database or can be stored locally on the NAC appliance manager server. In addition to LDAP, Kerberos is also supported as an external administrator authentication method.

The NAC appliance manager can be ordered as an appliance or as standalone Linux software. The NAC Appliance (CCA) Manager contains a monitoring summary page that contains information about product version and online users. This monitoring summary is displayed in Figure 7-1.

Figure 7-1. NAC Appliance Manager Monitoring Summary

[View full size image]



The main functional areas of the manager homepage are organized under the five categories, as follows:

- Device Management
    - Configure network and local settings for each server
    - Configure filters for device names, MAC addresses, IP addresses, and subnets
    - Configure agent scanning parameter
- Switch Management
    - Is enabled for out-of-band (OOB) deployments only
    - Profile to add OOB LAN switches including Simple Network Management Protocol (SNMP) configuration
    - Receive SNMP traps from the OOB switches when configured to do so
    - Include list of OOB switches
    - Include discovered clients behind the OOB switches
- User Management
    - Define types of user roles, including quarantined and temporary users
    - Define authentication parameters for user groups
    - Specify external authentication servers including Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial-In User Service (RADIUS), Windows NT LAN Manager (NTLM), Kerberos, and transparent 802.1x
    - Associate assigned VLANs with user groups
    - Configure RADIUS accounting
    - Define local users for authenticating directly on NAC appliance server
- Monitoring
    - View summary of recent policy deployment and quarantines
    - View status of user categories and specific users
    - Display event notification and warning logs
- Administration
    - Configure manager settings, failover, digital certificates, and license key
    - Define the logon page that is presented to user groups during authentication
    - Specify admin privilege roles for managing the manager
    - Back up the manager database

Device Management

Device Management is the first item displayed in the manager. Device Management features are configured in the following categories:

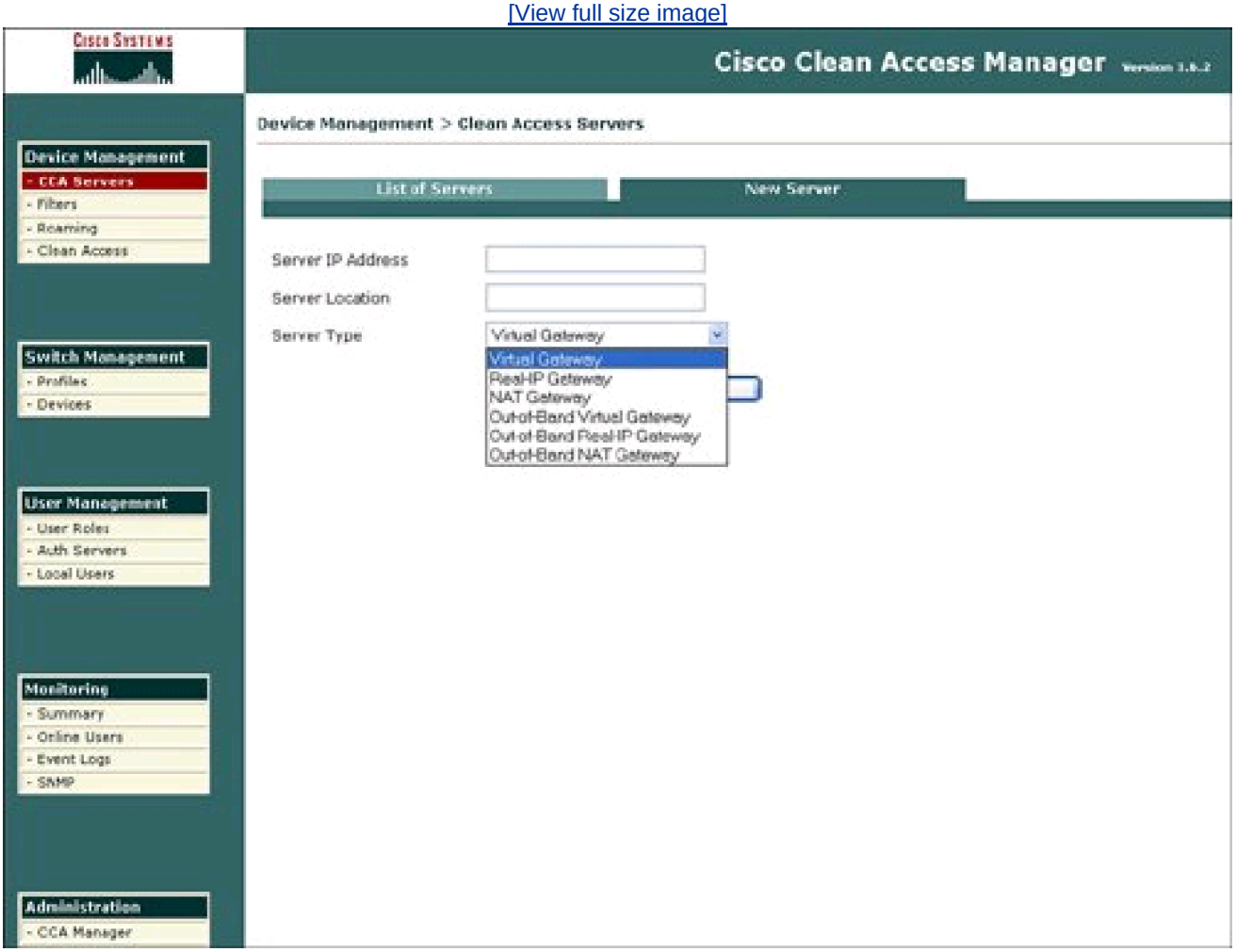
- CCA Servers
- Filters
- Clean Access

CCA Servers

The CCA Servers option displays a list of managed servers and also allows the ability to define a new server to be managed. The process to add a new server and select the server mode is displayed in Figure 7-2.

Figure 7-2. Add New CCA Server with Server Type

[View full size image]



The Cisco Clean Access Server can be configured in the following modes:

- Real IP Gateway (in-band_)
- Virtual IP Gateway (in-band)
- NAT Gateway (in-band)demo only
- Out-of-band (OOB) Real IP Gateway
- OOB Virtual IP Gateway
- OOB IP NAT Gatewaydemo only

The next sections describe each mode in detail.

Real IP Gateway

In the Real IP Gateway mode, the server sits between an untrusted subnet and a trusted subnet. The IP addresses for the server interfaces must be configured. Static routes must be configured since the server is not a router and does not broadcast routes. Both DHCP server and DHCP relay functions are supported in this mode. The server can either assign authenticated users an IP address from a DHCP pool or allow the DHCP-assigned process to relay through the server from the internal DHCP server on the trusted network to the end point on the untrusted network. Architecturally, this is similar to the functionality of a router.

Virtual IP Gateway

The Virtual IP Gateway mode is essentially a bump-in-the-wire deployment. In this mode, the server is inserted inline into an existing network segment. No readdressing of subnets or IP addresses is required for the Virtual IP Gateway, or bump-in-the-wire, deployment. In this mode, both interfaces on the server can share the same IP address. Only DHCP relay is supported because the Virtual IP Gateway does not allow a native DHCP server. VLAN termination also is not supported in Virtual mode. The manager must reside on a different subnet from the server, even in Virtual IP Gateway mode.

NAT Gateway

The NAT Gateway includes a NAT function that enables the user IP address on the untrusted network to be translated to a new IP address on the trusted network. If you select NAT Gateway, you will be presented with a pop-up window that indicates that NAT Gateway is recommended only for testing/demo purposes. The CCA (NAC Appliance) 3.6 documentation takes this idea a step further and indicates that NAT Gateway mode is not supported for production network deployment.

OOB Real IP Gateway, OOB Virtual IP Gateway, and OOB NAT Gateway

Cisco introduced support for out-of-band (OOB) deployments with the CCA 3.5 release. Prior to OOB support, the server was always inline with all user traffic from the client. This user traffic includes the initial authentication traffic and all of the actual data traffic from the client. OOB support allows the server to participate only in the authentication, scanning, and remediation flows for the user client and not the data traffic from the client for web browsing, e-mail, and so on. OOB support enables the implementation of a NAC deployment with fewer

servers and can result in a more scalable solution, as all data traffic does not have to travel through a server after authentication. The OOB solution requires a separate license key. A server can be deployed in OOB Real IP Gateway, or OOB Virtual IP Gateway modes.

An OOB deployment can remove the bottleneck of the processing power of the server for data traffic. OOB deployment enables greater than 1 Gbps, because all data traffic does not have to flow through the server after successful authentication. In an OOB deployment, only network traffic for authentication, security posture validation, and any required remediation flow through the NAC appliance server. OOB is an option only for wired (LAN) networks because OOB is not supported on wireless networks. It is also not recommended to enable 802.1x on a LAN switch interface that will participate in an OOB NAC appliance deployment due to potential conflicts with VLAN assignments.

The OOB deployment modes work in concert with the supported line of Layer 2 LAN switches. The manager defines which VLAN on the LAN switch will be assigned to the authenticating device. The manager uses SNMP v2c and v3 to obtain MAC address table information and to assign VLANs to authentication devices. The out-of-band modes also support VLAN quarantine because the server performs device remediation and can reside on the quarantine VLAN. Supported Catalyst LAN switches for OOB deployments include the following device models:

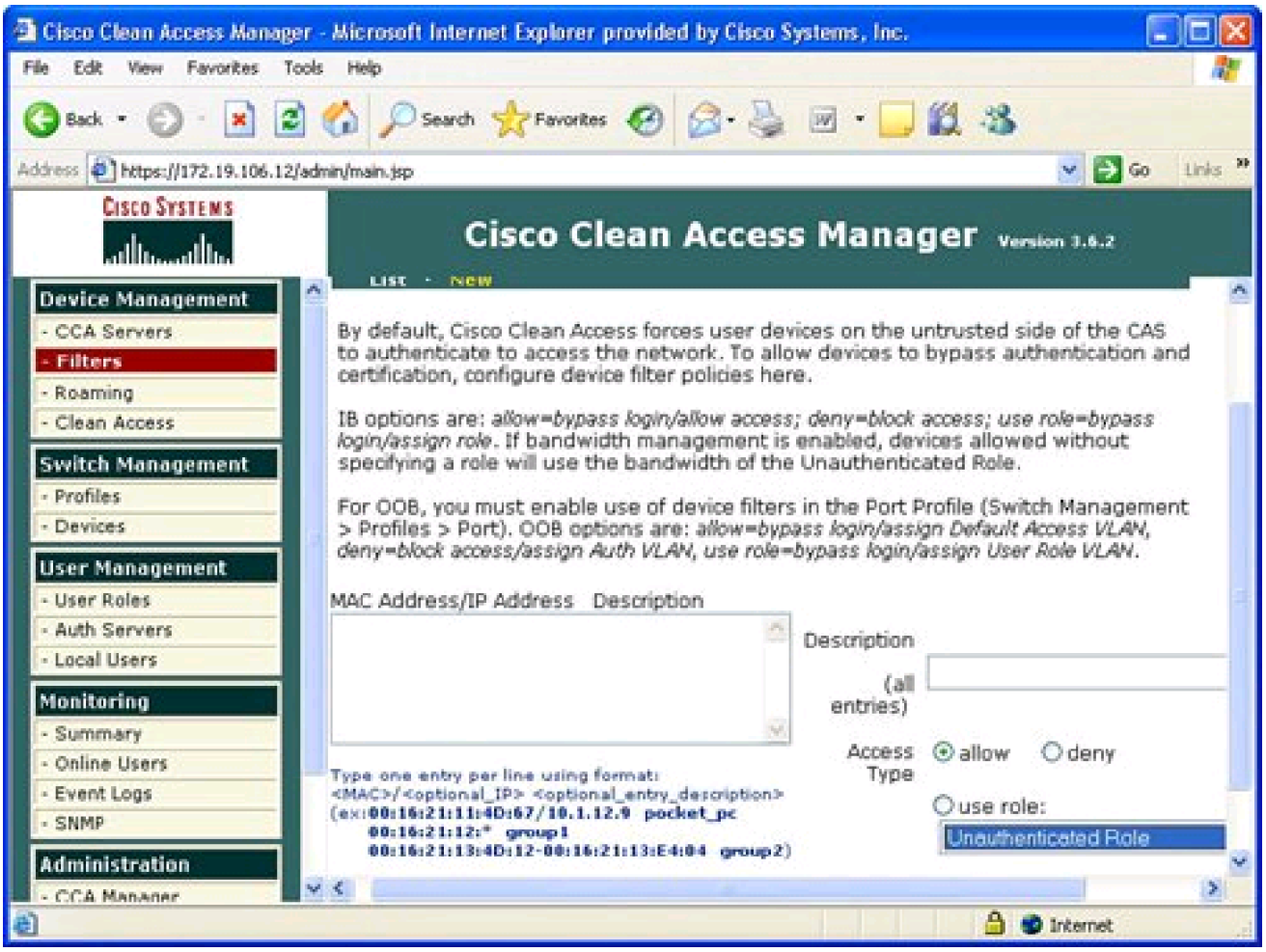
- Cisco Catalyst Express Series 500 (3.6.1+ only)
- Cisco Catalyst 2900 XL (3.5.4+ only)
- Cisco Catalyst 2940 (3.5.4+ only)
- Cisco Catalyst 2950
- Cisco Catalyst 2950 LRE
- Cisco Catalyst 2960 (3.5.7+ only)
- Cisco Catalyst 3500 XL (3.5.4+ only)
- Cisco Catalyst 3550
- Cisco Catalyst 3560 (3.5.1+ only)
- Cisco Catalyst 3750
- Cisco Catalyst 4000 (3.5.8+ only)
- Cisco Catalyst 4500
- Cisco Catalyst 6500

Filters

Filters provide the ability to exclude devices or subnets from the authentication process. Many security operators will want to provide filters to nonPC devices like printers and IP phones in order to ensure easy access to the network without going through the authentication process. Filters can be configured based upon device MAC address. A filter enables the ability to automatically allow or deny a device on to the network. Device filters also enable the ability to put a machine into a specific user role, such as employee or consultant, based upon MAC address. Figure 7-3 provides an example of device filters.

Figure 7-3. Device Filters

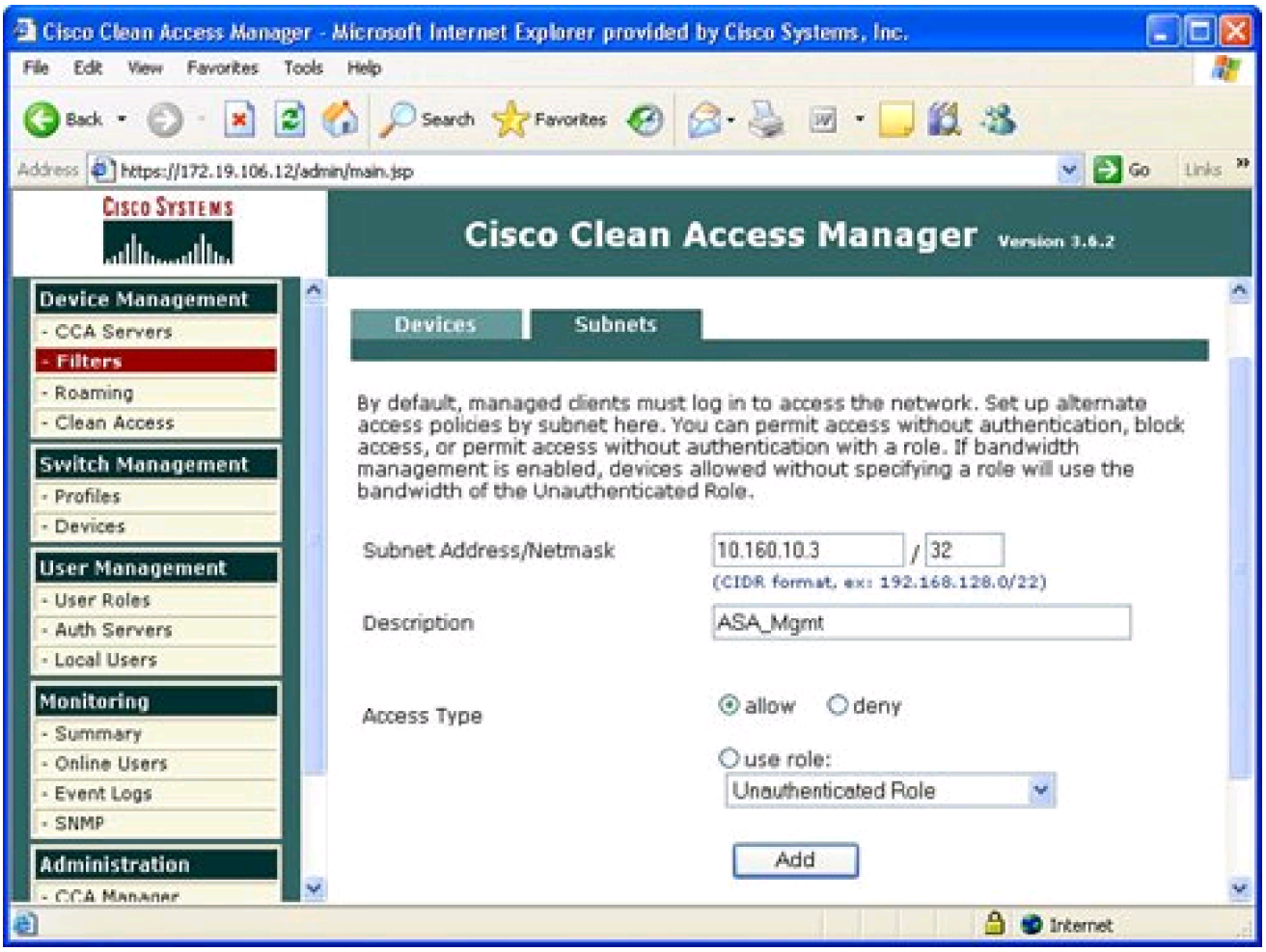
[View full size image]



In addition to MAC address device filters, the manager also supports the configuration of filters based upon subnet or IP address. The Device Management area of the manager allows the configuration of a user to bypass authentication based upon the user's IP address. This subnet filter capability also supports the mechanism to permit or deny a user access to the network based upon IP address. Similar to device filters, a user can also be assigned a user role such as employee or consultant based upon the source IP address. An example of how to configure a subnet filter is provided in Figure 7-4.

Figure 7-4. Subnet Filters

[View full size image]



Note

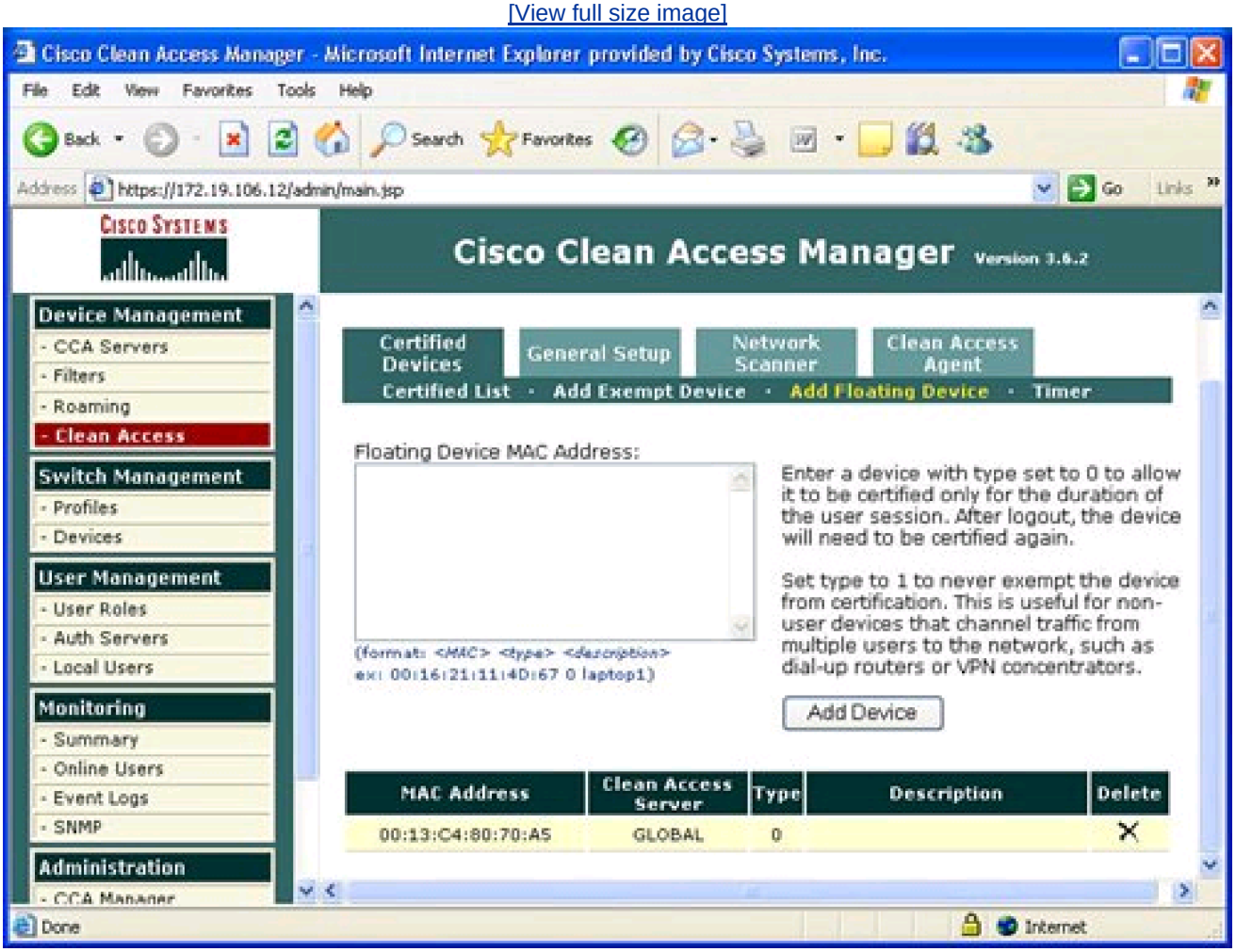
Previous versions of the NAC appliance managed wireless access points and allowed mobile users to roam between different access points and maintain an authenticated connection. Roaming and wireless access point management is now performed by the wireless LAN controller (WLC) management product and is no longer configured by the NAC appliance manager.

Clean Access

The Clean Access area under Device Management in the manager allows the display and configuration of exempt devices, floating device, general setup, network scanning, and agent configuration. Exempt devices are devices that are exempt based upon MAC address as discussed earlier in this chapter. Floating devices are designed for public places like online kiosks. Floating devices are authenticated during the user session. Once the user logs off, the next user on that deviceeven if it is the same usermust be reauthenticated. Floating devices are defined by their L2 MAC address. An example of the location to configure a floating device by adding its MAC address is displayed in Figure 7-5.

Figure 7-5. Floating Device

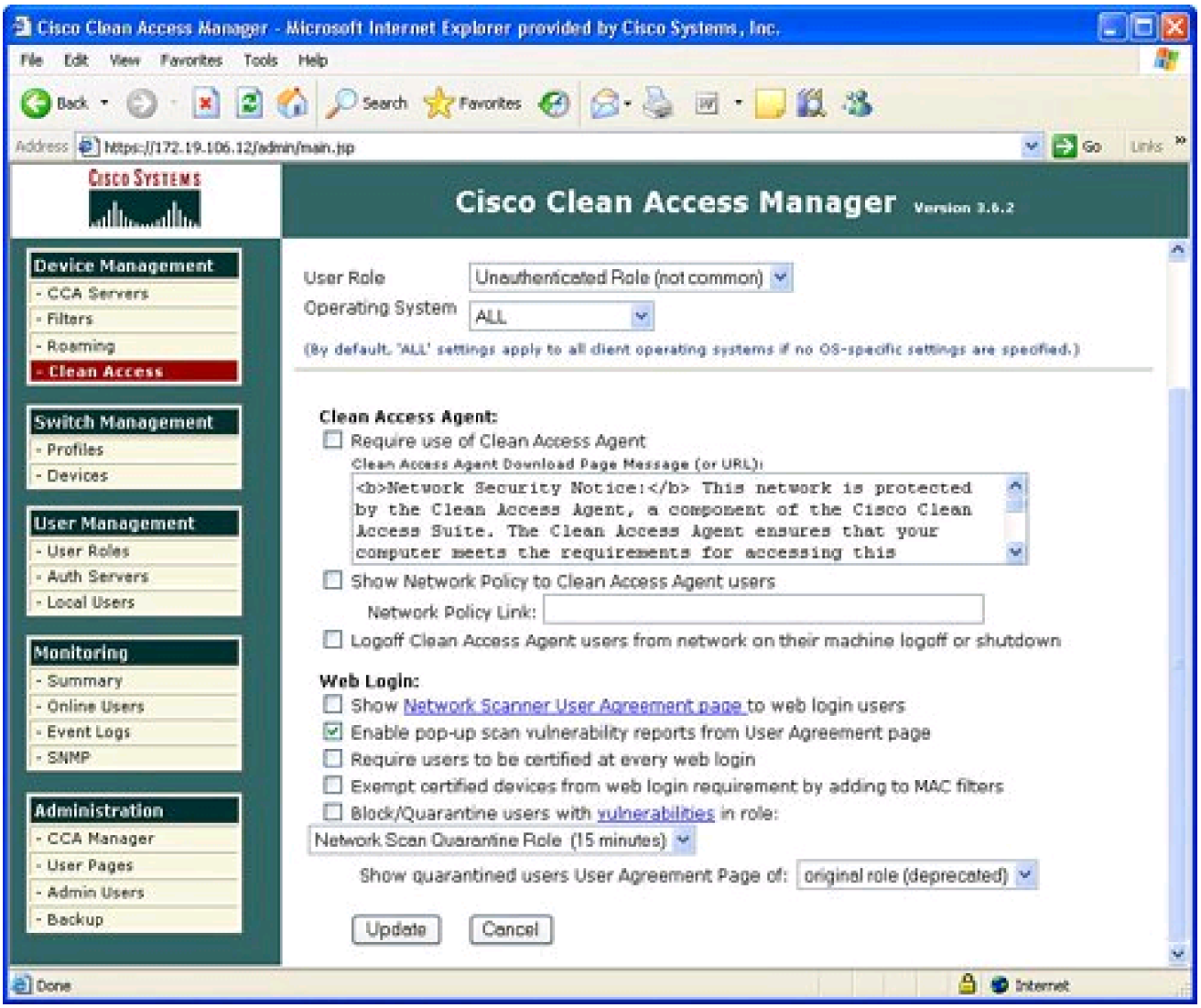
[View full size image]



General setup involves configuring the logon or restriction information that is displayed for the users in the various user roles. General setup also specifies whether the agent is required for a specific user role. Figure 7-6 displays an example of the General setup configuration parameters for a particular user role.

Figure 7-6. General Setup

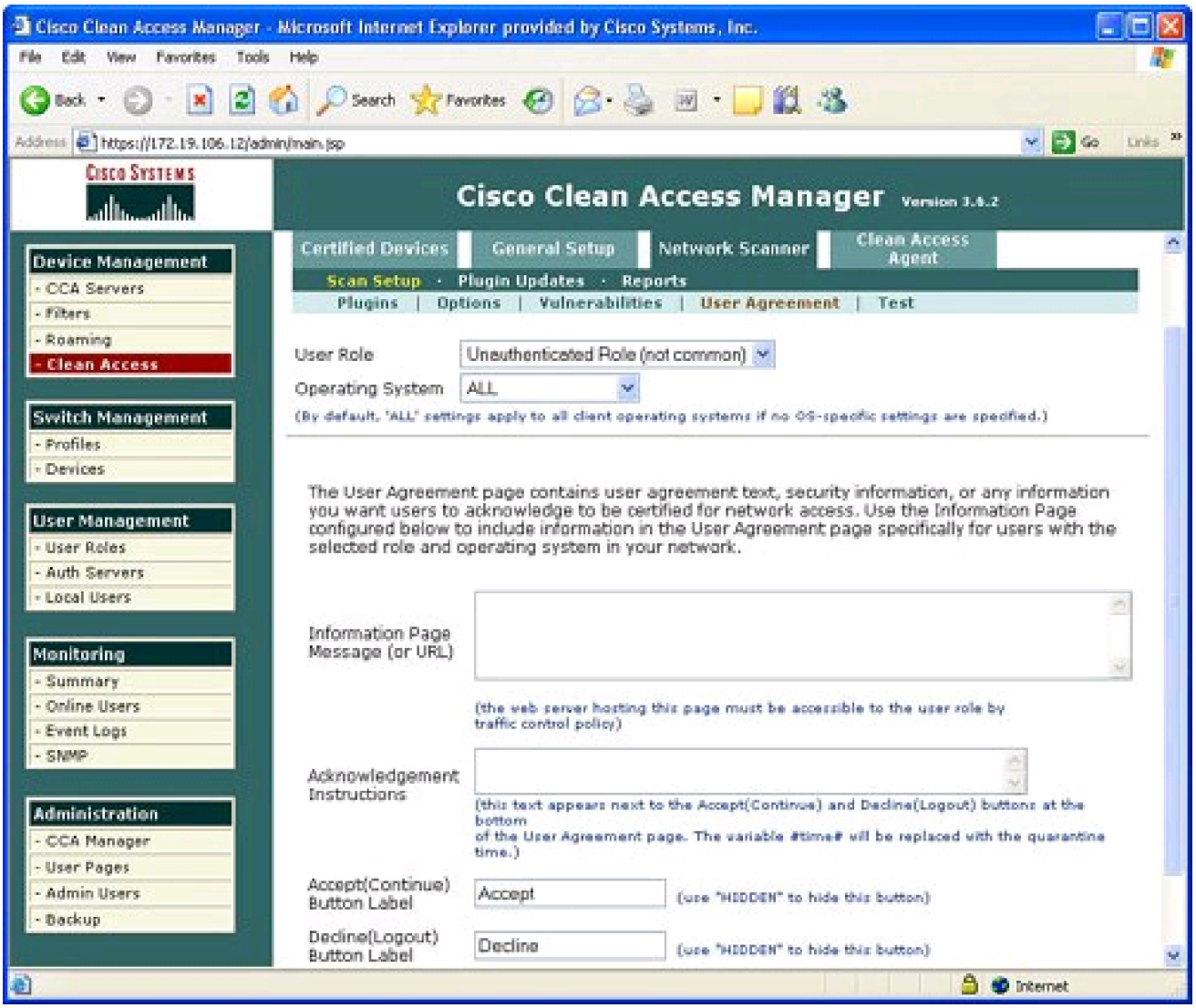
[View full size image]



The NAC appliance contains an embedded Nessus network scanner. The NAC appliance server supports Nessus plug-ins and provides a mechanism for users to download new Nessus plug-ins. Figure 7-7 provides the configuration options for the user-agreement that is displayed to the user to access a network, based upon a network scan.

Figure 7-7. User Agreement

[View full size image]



The optional agent provides an extra dimension of scanning and authentication to Windows clients. The agents can be distributed to Windows clients directly from the server. Agents allow registry checks to determine if OS hotfixes are applied. These registry checks can also be used to determine the existence of a specific software application and the inspection for a potential worm or virus infection.

In addition to registry checks, rules can also be defined in the manager to check if an end station with the agent has a specific file on the machine, or if a specific service or application is active on the Windows end station. Figure 7-8 displays some of the rules check list to determine if specific Windows hotfixes have been applied to a client with the agent. Figure 7-9 shows the parameters used to create a rule to inspect a client for a specific registry key. Figure 7-10 displays rules for checking the presence of specific antispyware products on clients with the agent installed.

Figure 7-8. Rules Check List

[View full size image]

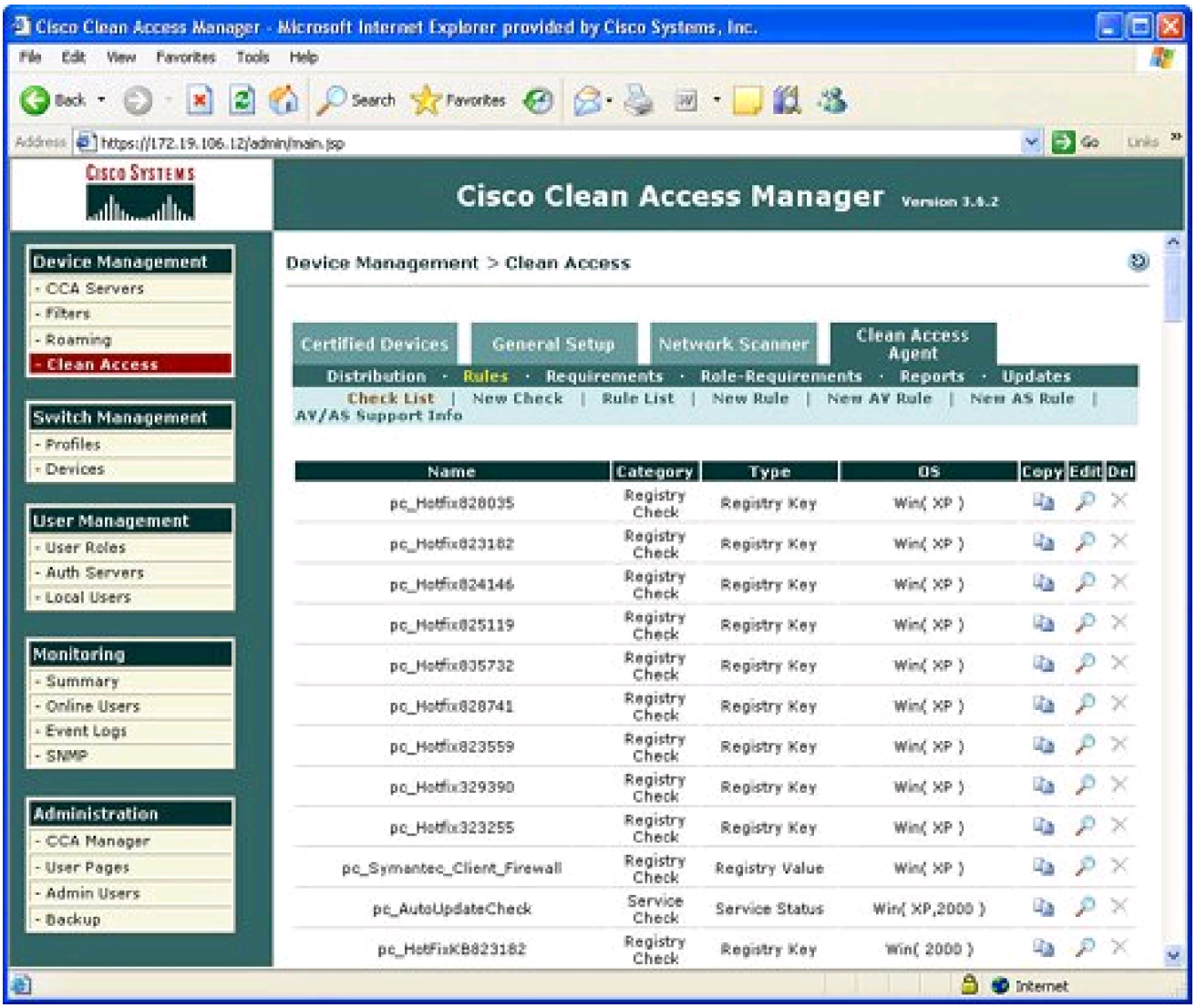


Figure 7-9. Registry Check

[View full size image]

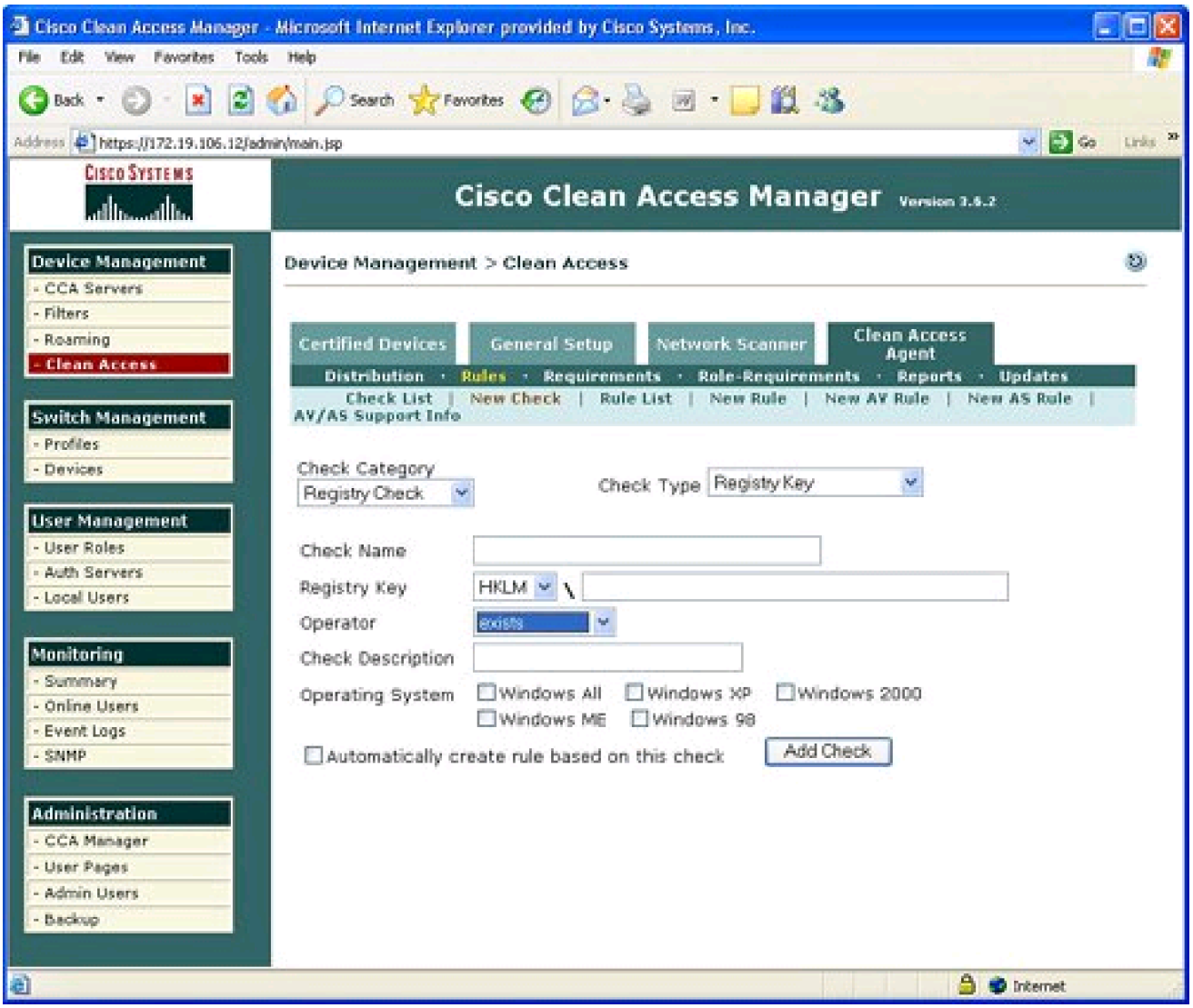
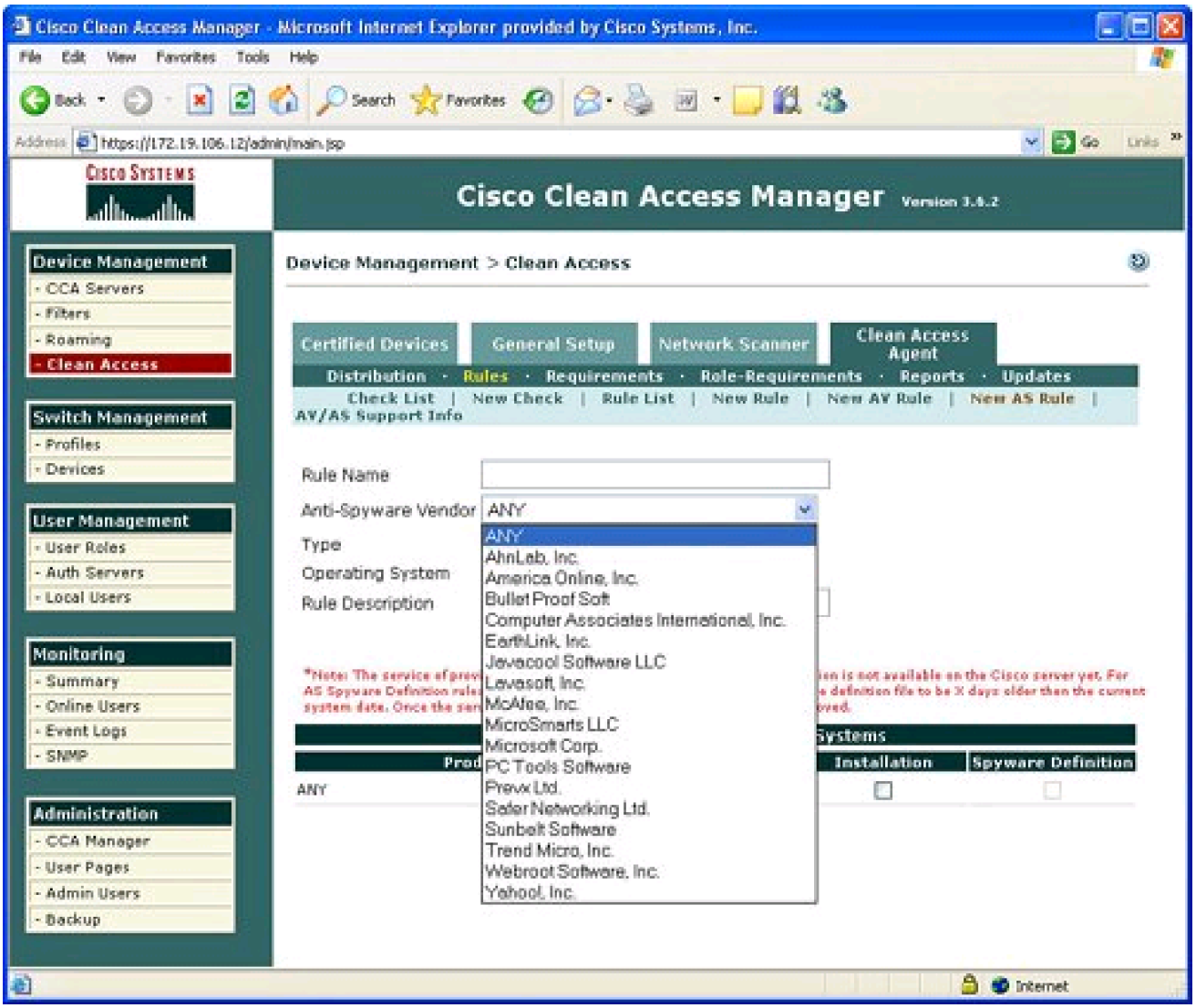


Figure 7-10. Antispyware Check

[View full size image]

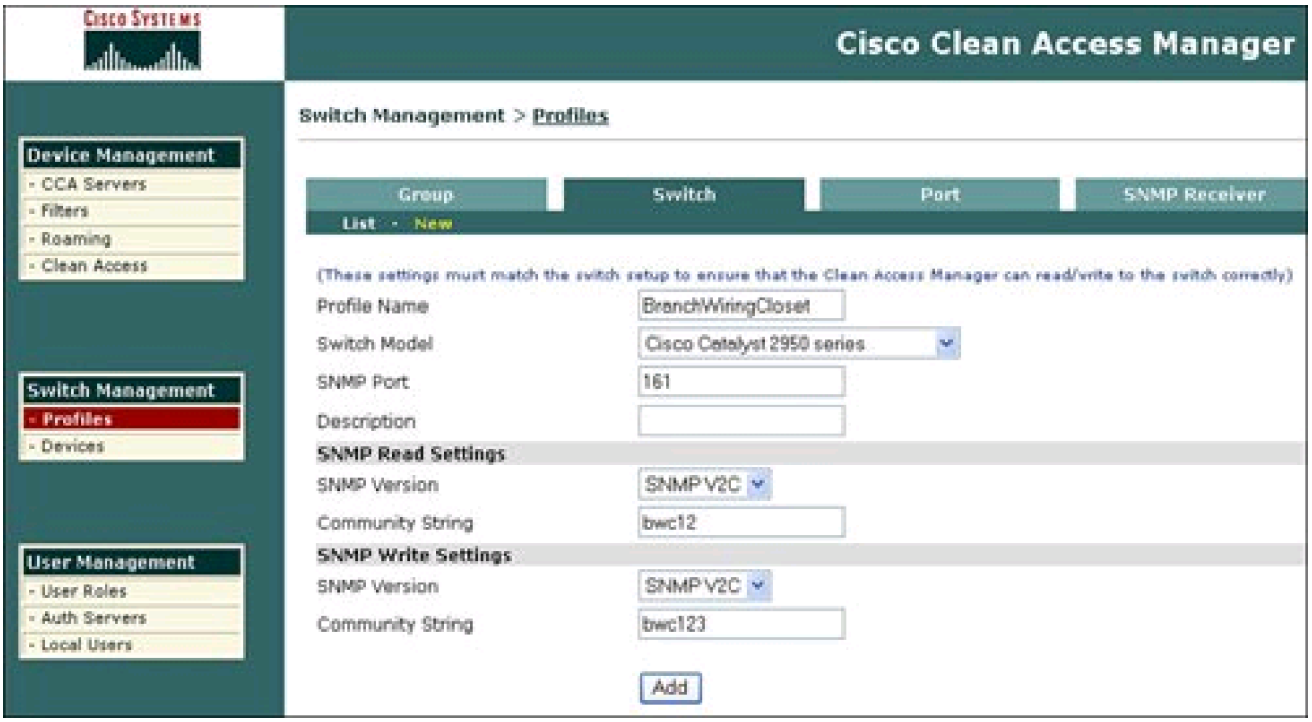


Switch Management

The switch management function is designed to configure LAN switches that will be used in an OOB NAC appliance deployment. The NAC appliance manager uses SNMP to manage the OOB LAN switches. Switch management is composed of the profiles and devices categories. A profile defines the type of LAN switch and the SNMP parameters that are used to manage the LAN switch. Figure 7-11 displays an example of the location and settings to configure a LAN switch profile.

Figure 7-11. Profile

[View full size image]



The device option under switch management enables the user to define or discover LAN switches that can be used for an OOB deployment. The IP address of a LAN switch can be defined, or the user can enter a range of IP addresses to search and discover LAN switches that can be used for OOB. The device option also displays the discovered clients or end stations of the OOB LAN switch. The clients are discovered based upon SNMP MAC notification updates or Link-up/Link-down SNMP traps from the LAN switch to the NAC appliance manager.

User Management

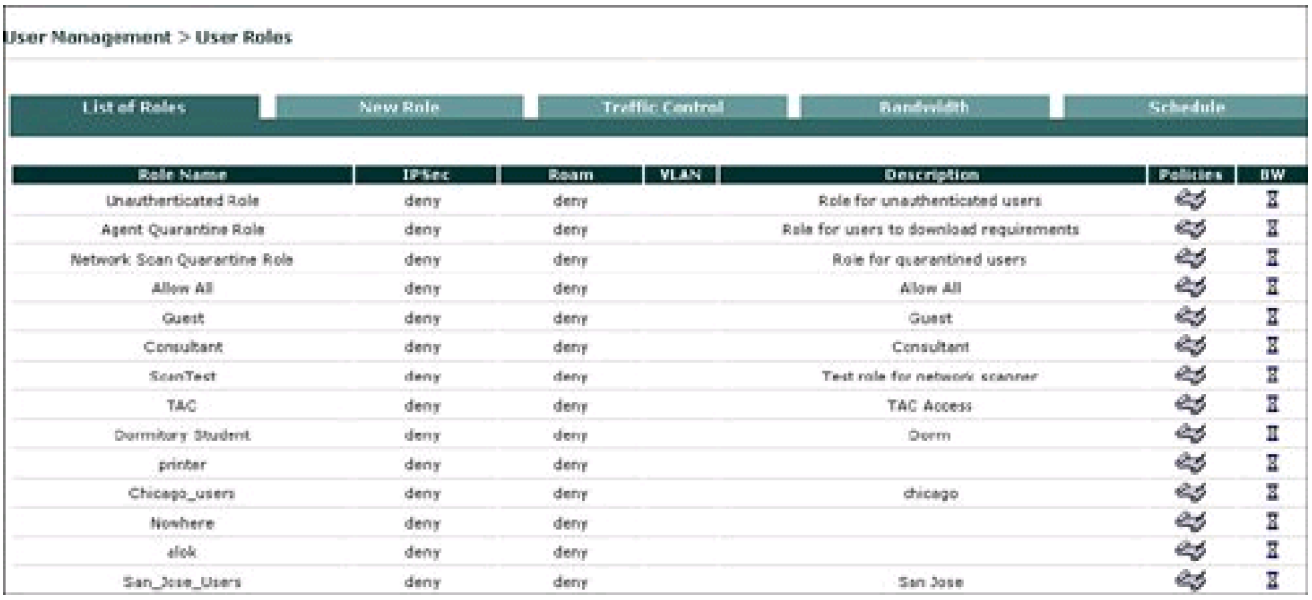
Each user is classified to participate in a specific user role. User roles are both predefined and customized. User roles are used to determine what an authenticated user can do on a network. Some of the parameters associated with user roles include the following:

- VLAN ID
- allowed networks and ports
- bandwidth permission
- session timeout
- host registry key restrictions

By default all user traffic is denied unless explicitly permitted by a global or local policy for authenticated users. Figure 7-12 displays a sample list of user roles.

Figure 7-12. List of Roles

[View full size image]



NAC appliance has a quarantine role for Windows users with the agent and a quarantine role for users with a vulnerability that was discovered during a network scan by the NAC appliance. The vulnerable user is placed in the quarantine role until they update their device to remove the identified vulnerability. Users will be moved from the quarantine role after remediation and a successful logon. One of the main drivers behind the different user roles is the definition of what a specific type of user is allowed to do on the network. The quarantine role allows users to access only a part of the network in order to download the required software updates to address the identified vulnerability in order to be remediated and be removed from the quarantine role.

Figure 7-13 displays an example of how the quarantine role is allowed permission to access only the remediation server. Users who are placed in the quarantine role must be remediated before they can join one of the other user roles that are designed for successful authentication and certification.

Figure 7-13. Traffic Control of Agent Quarantine Role

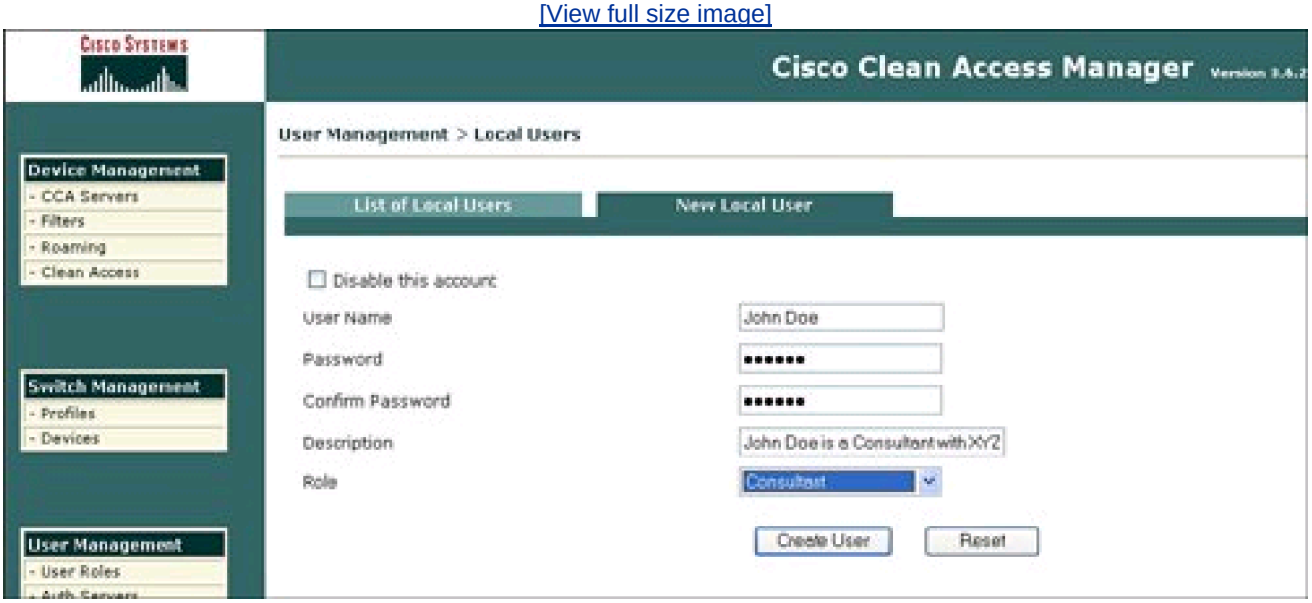
[View full size image]

Several mechanisms can associate, or map, a user to a user role during the authentication process. One example is the ability to map a user to a role based upon their VLAN ID.

The NAC appliance can authenticate users who are locally defined on the NAC appliance or leverage an external LDAP, RADIUS, or NTLM (Windows NT LAN Manager) database for user authentication. The NAC appliance manager allows the ability to define a local user, a user's logon password, and mapping to a specific user role that will define what the user can do once authenticated into the network. Figure 7-14 displays an example of defining a new user on the local user database and mapping that user to the consultant user role.

Figure 7-14. Create a Local User and Map to User Role

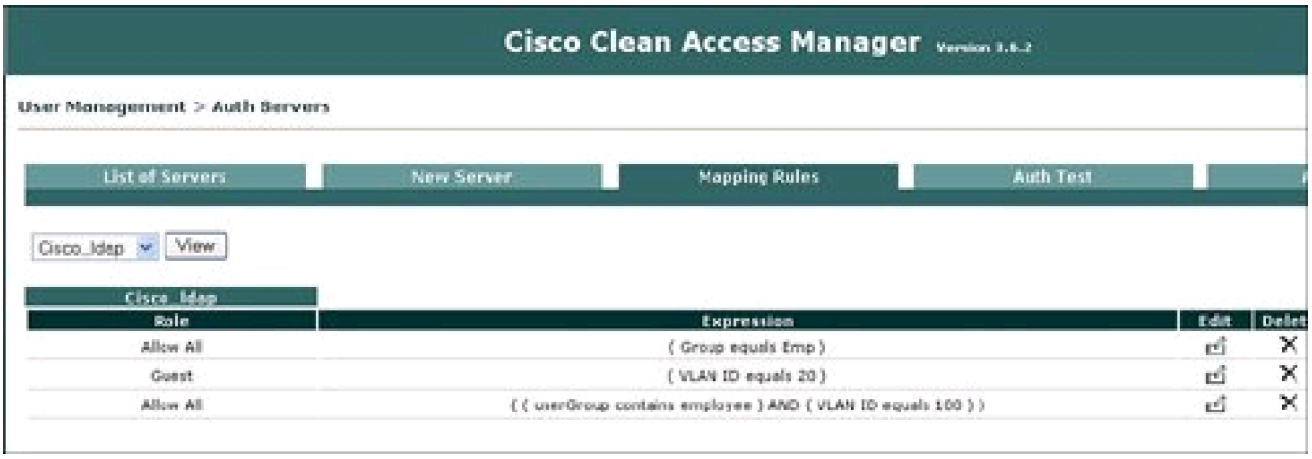
[View full size image]



Leveraging of an external authentication server offers several advantages over using the local user database on the NAC appliance. The benefits of the external authentication server include scalability and the ability to deploy the NAC appliance without having to manually redefine each user. The NAC appliance manager allows mapping rules to be defined to determine which role a user is assigned to after authentication and certification by the NAC appliance. Figure 7-15 displays how you can use an external LDAP database for authentication and mapping rules of user roles, based upon VLAN ID and group name.

Figure 7-15. Mapping Rules with External User Authentication Server

[View full size image]



Monitoring

The NAC appliance manager provides excellent monitoring capabilities that can be used to identify what is going on in the network. With the Monitoring feature of the manager, you can display all online users with specific details, including the following:

- user's IP address
- MAC address
- VLAN
- logon time
- user role

Figure 7-16 displays a summary of the monitoring statistics, andFigure 7-17 shows the specific user characteristics or parameters that can be displayed for each online user.

Figure 7-16. Monitoring Summary

[View full size image]

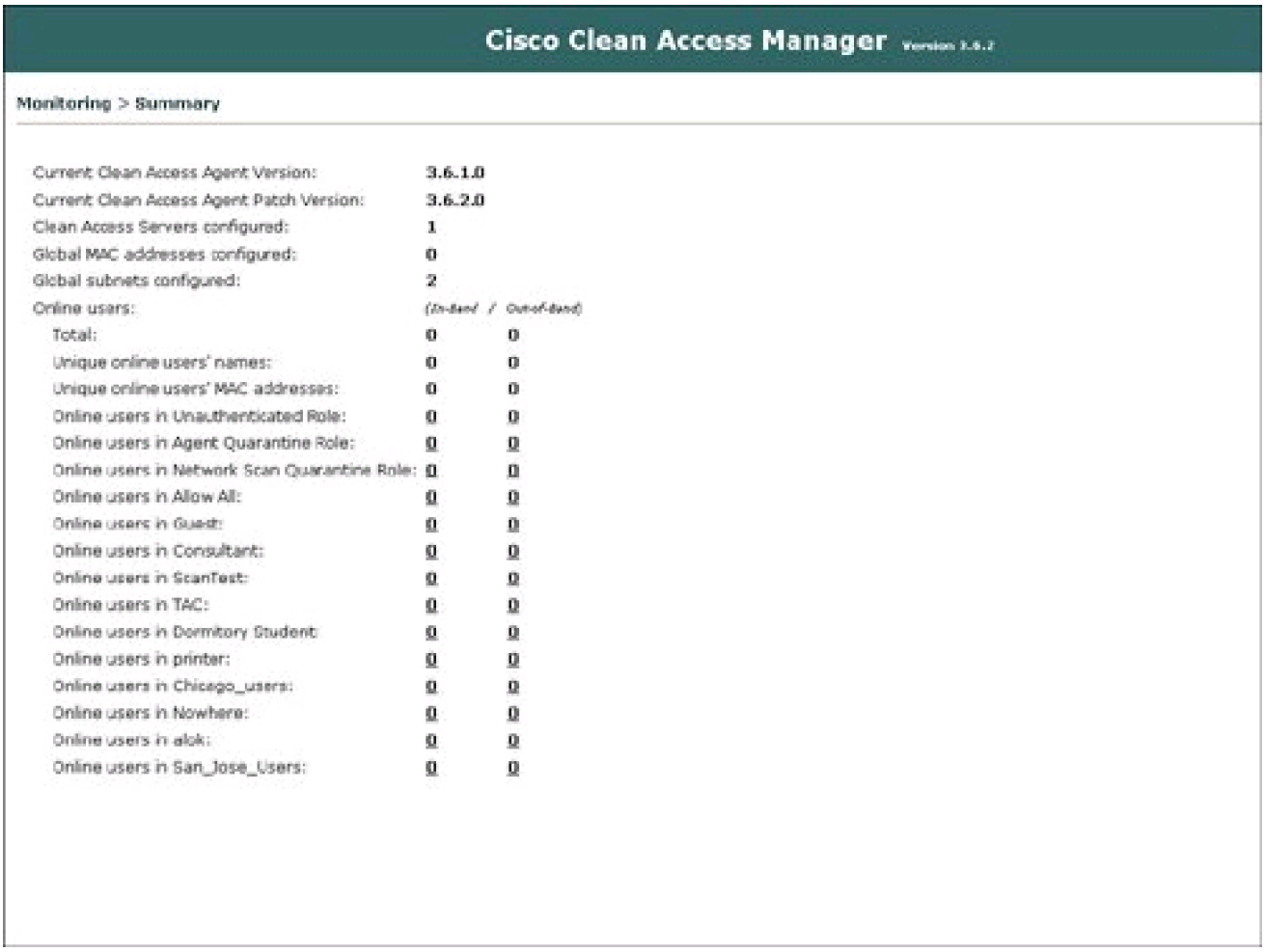
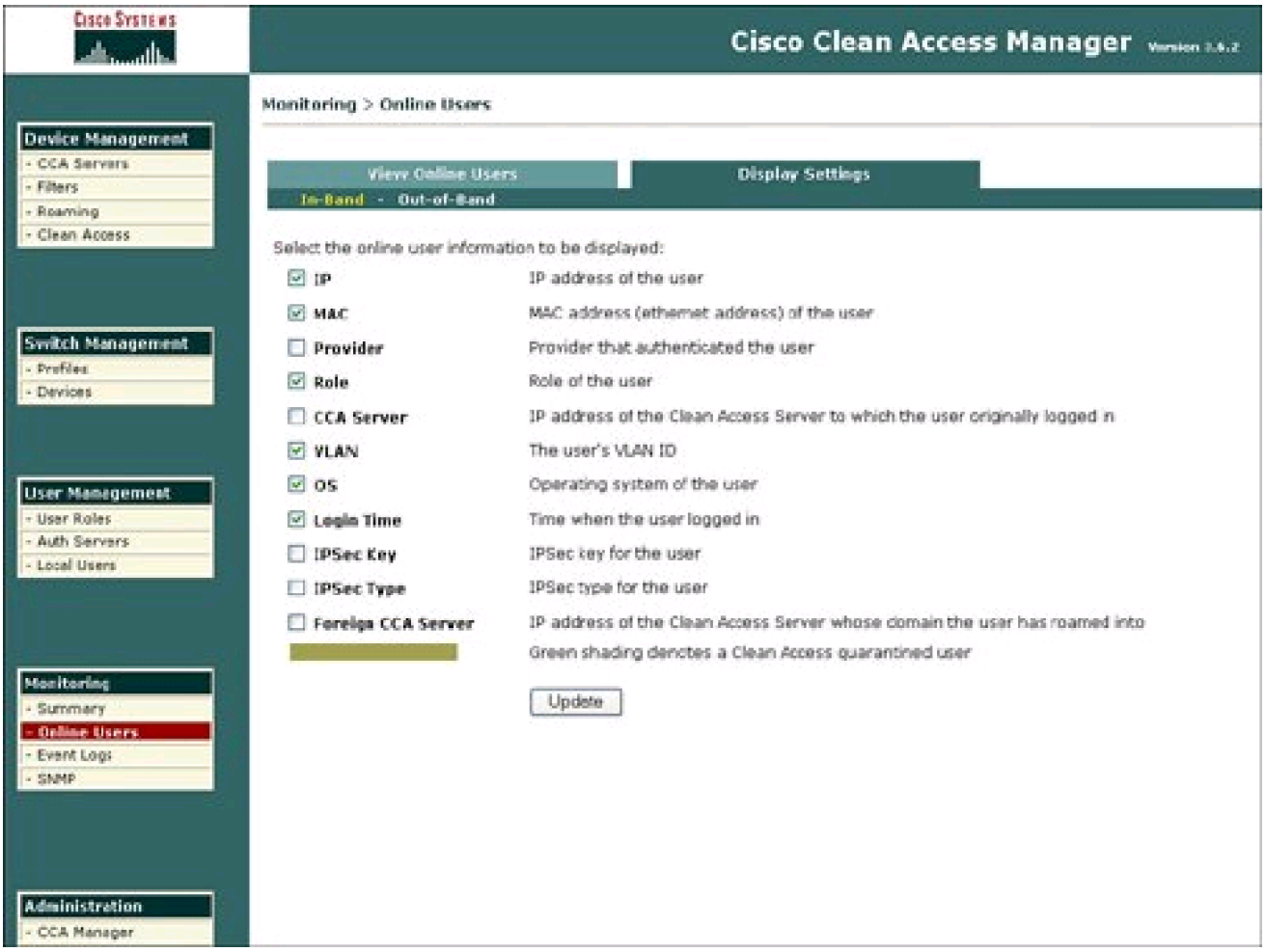


Figure 7-17. Online User Information

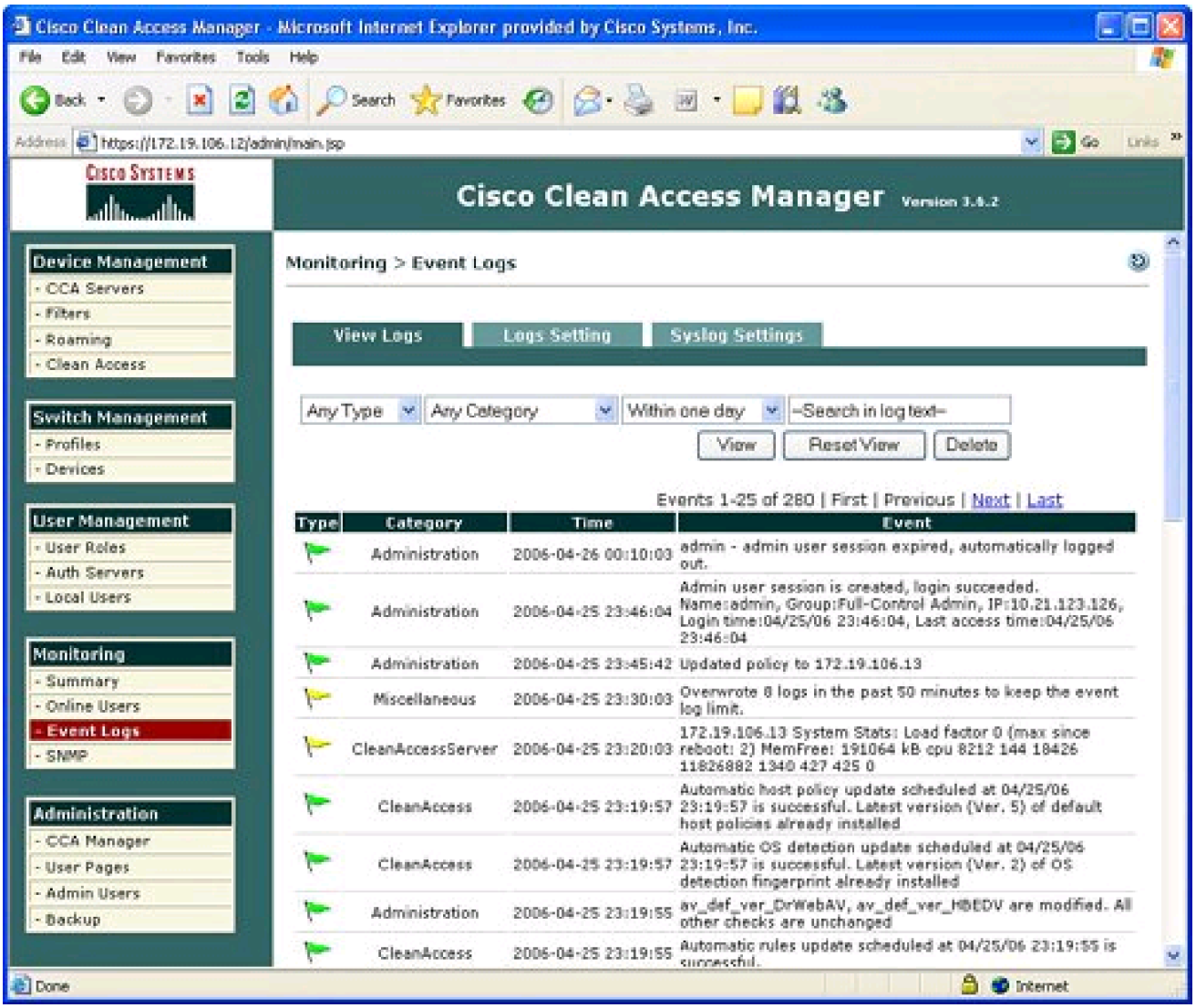
[View full size image]



The NAC appliance manager also features the display of event logs as an option under Monitoring. Event logs can contain items including admin logon, rule creation, policy deployment, and antivirus/antispyware updates. Figure 7-18 displays a sample of events in the event log.

Figure 7-18. Event Log

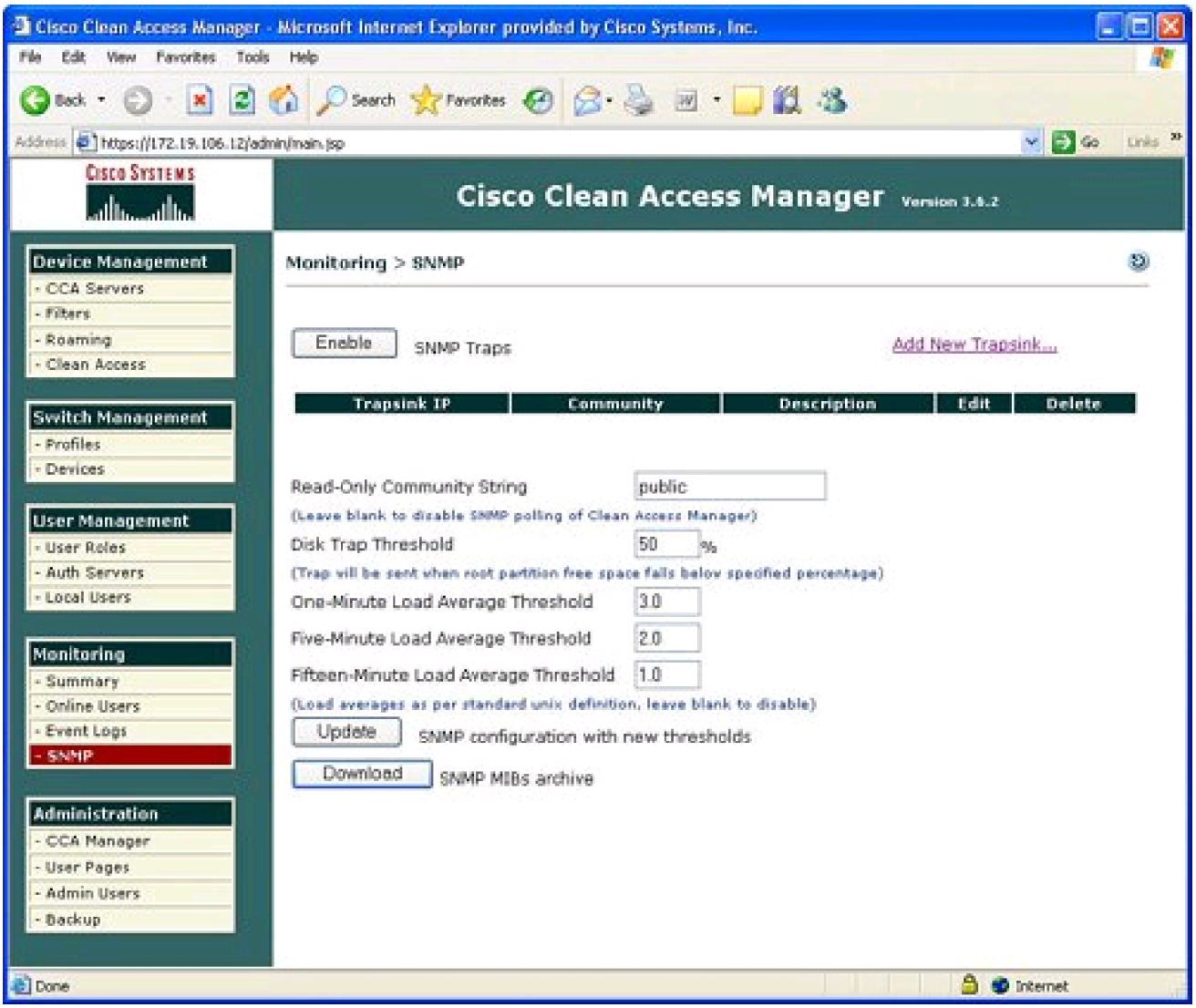
[View full size image]



The Monitoring function also provides the ability to configure SNMP parameters. SNMP parameters that you can configure under Monitoring include community strings and threshold values. The SNMP area under Monitoring also provides the ability to download updated SNMP MIBs for the NAC appliance. Figure 7-19 displays a sample of the configurable SNMP parameters for Monitoring.

Figure 7-19. SNMP

[View full size image]



Administration

The NAC appliance manager also contains an Administration option in the manager GUI. The functions contained under the Administrative option include the traditional IP addressing, the manager, SSL certificates, definition of admin users, and the ability to back up the NAC appliance manager. These administrative features are not described in detail because they are conventional and not the focus of this chapter on the security features of the NAC appliance.

PREV NEXT

Summary

NAC is the process of identifying, authorizing, and verifying the security posture to determine that the user or device does not impose a security risk and can join the network safely. NAC can be implemented as a function of Cisco router/switches as NAC Framework, or NAC, can be implemented as a turn-key NAC appliance. NAC can be deployed in-band, where all data traffic from the user goes through the server, or OOB, where the server is involved only in the authentication, scanning, and remediation process and is removed from the normal data traffic flow of the user. OOB offers higher-scalability deployments because the data throughput is not limited by the capacity of the NAC appliance server.

The NAC appliance is also marketed as CCA. The NAC appliance architecture is composed of a server, manager, and optional access agent. The NAC appliance server is managed by the NAC appliance manager because NAC appliance servers do not have an exposed command-line interface (CLI) for all functions, and there is not a device manager. The optional access agent at the time of this publication is offered as a no-cost option and is designed for Windows end stations. The presence of the agent enables advanced security posture validation on the end station, including the ability to check for specific files, services and applications, and to inspect Windows registry values for specific values or vulnerabilities.

References

Cisco Systems, Inc. Cisco Clean Access Manager Installation and Administration Guide, Release 3.4.
http://www.cisco.com/en/US/products/ps6128/products_user_guide_list.html

Cisco Systems, Inc. Cisco Clean Access Manager Installation and Administration Guide, Release 3.6.
http://www.cisco.com/en/US/products/ps6128/products_user_guide_list.html

Cisco Systems, Inc. Cisco Clean Access Server Installation and Administration Guide, Release 3.4.
http://cisco.com/application/pdf/en/us/guest/products/ps6128/c1626/ccmigration_09186a00803d26d8.pdf

Cisco Systems, Inc. Cisco Clean Access Manager Installation and Administration Guide, Release 3.5.
http://www.cisco.com/application/pdf/en/us/guest/products/ps6128/c1626/ccmigration_09186a00804ce7c3.pdf

Cisco Systems, Inc. Cisco Clean Access Manager Installation and Administration Guide, Release 3.6.
http://www.cisco.com/en/US/products/ps6128/products_user_guide_list.html

Cisco Systems, Inc. Cisco Clean Access Server Installation and Administration Guide, Release 3.5.
http://www.cisco.com/application/pdf/en/us/guest/products/ps6128/c1626/ccmigration_09186a00804ce39d.pdf

Chapter 8. Managing the Cisco Security Agent

The Cisco Security Agent represents the last line of defense in a layered self-defending network. The Cisco Security Agent operates directly on the end station by monitoring the OS kernel and requests to the file system, network resources, and registry keys. The Cisco Security Agent can reside directly on the PC, laptop, or server in the network. Cisco Security Agent is supported on Windows, Solaris, and Linux machines.

Cisco Security Agent can provide a day-zero defense against new network attacks since the Cisco Security Agent is looking for malicious behavior directly on a workstation instead of known worms and viruses that can participate in a network attack. *Day-zero* is a fancy way of saying that an attack can be stopped by looking at the symptoms of an attack, rather than a unique identifier or signature of the attack. For example, a virus may delete a specific system file, but day-zero protection would notify the user that something was trying to delete any system file rather than looking for a specific virus. Day-zero protection does not require any host signatures and is a good complement to other signature-based defenses, such as network IPS.

The Cisco Security Agents are centrally managed by the Management Center. The Management Center features an easy-to-use web GUI and uses HTTPS between the Management Center and the Cisco Security Agent on the end station to ensure security during the configuration process. The Cisco Security Agent Management Center includes support for the following features:

- Day-zero protection against certain attacks
- Host intrusion prevention
- Protection against buffer overflows
- Port scan detection
- Distributed personal firewall protection
- Protection against spyware/adware
- Application inventory
- Location-based polices depending upon whether the machine is on a home network or the corporate network
- Policies to restrict access to removable media, including USB devices
- Support for International Windows
- Native end-station Cisco Security Agent Panel support for French, German, Japanese (Kanji), Chinese, Italian, Spanish, and Korean
- Application inventory and use-tracking
- Hot fix and Service Pack (SP) checking
- File and directory protection
- Enforcing security policies for data on Clipboard
- Antivirus DAT checking
- Windows XP Home Edition support
- Embedded Cisco Trust Agent in Cisco Security Agent
- Auto-enrollment group for Windows, Solaris, and Linux

- QoS marking of applications from Cisco Security Agent
- VMWare qualification
- Tablet PC qualification
- Solaris 9

Cisco Security Agent also contains an optional component known as the network shim. The network shim provides additional protection on end stations, including protection against attacks by detecting SYN floods, port scans, and malformed packets at shim layer on the OS at the end station.

PREV NEXT

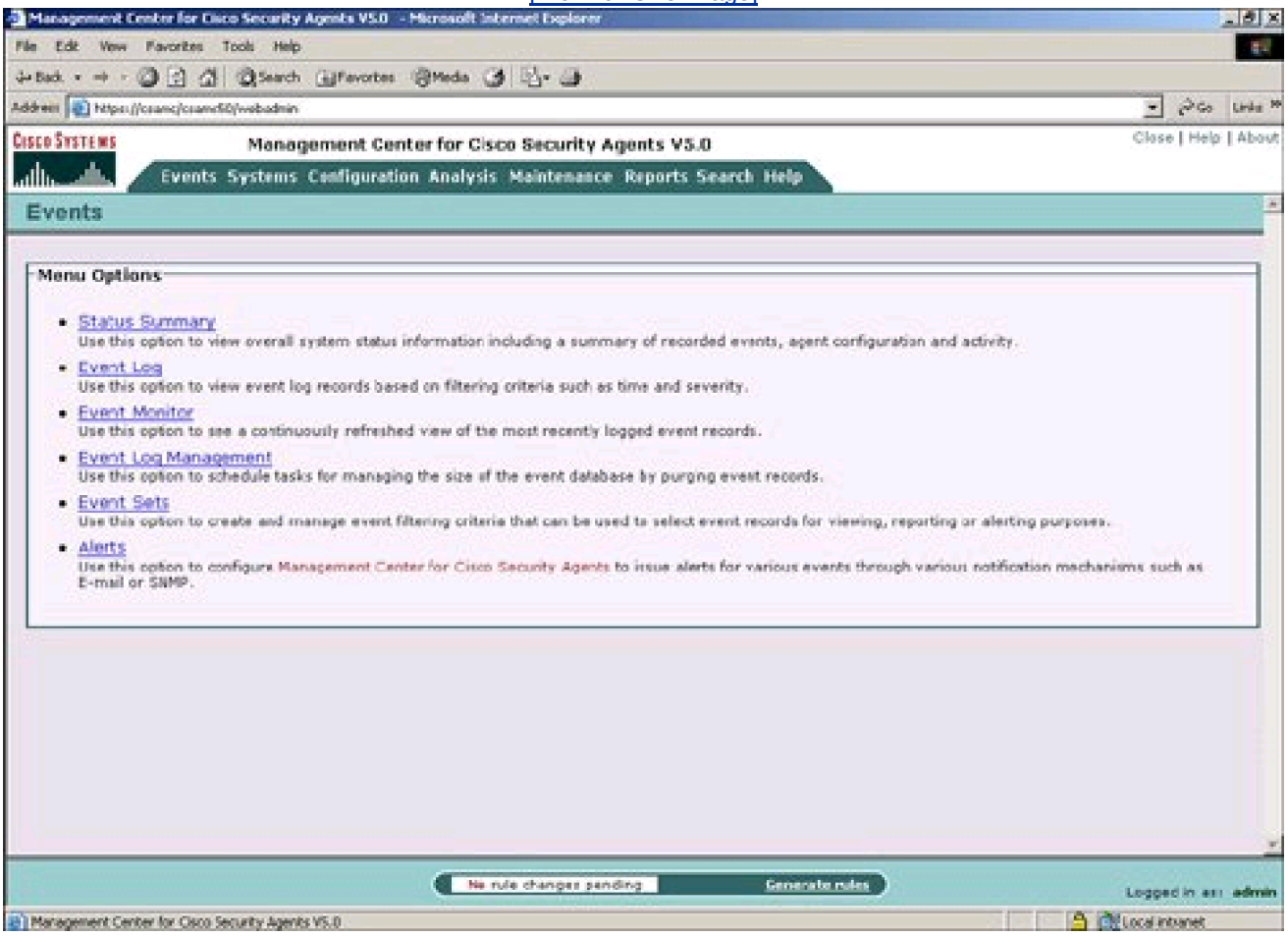
Management Center for Cisco Security Agents

Cisco Security Agents are configured and deployed from the Management Center to the end-station desktop. The Cisco Security Agent Management Center can manage up to 100,000 Cisco Security Agents. The Management Center for Cisco Security Agents is a standalone management product and, like Cisco Incident Control Server (Cisco ICS), is not included in the Cisco Security Manager.

A web browser is used as the GUI to the Management Center. Configuration between the Management Center and the Cisco Security Agent is secured with HTTPS/SSL. The homepage for the Management Center for Cisco Security Agents is displayed in Figure 8-1.

Figure 8-1. Management Center for Cisco Security Agent Homepage

[View full size image]



The Management Center allows the configuration of security policy rules for device groups. The Management Center provides default device groups, such as Linux servers. Hosts or end stations that contain a Cisco Security Agent are included in at least one device group. Security policies are composed of individual rules and are applied to hosts in a device group. Managing the security policies on the Cisco Security Agents can involve the following processes, which are discussed in the following sections:

- Deploying the Cisco Security Agent kit to the end station
- Displaying the end-station hostname in the device group

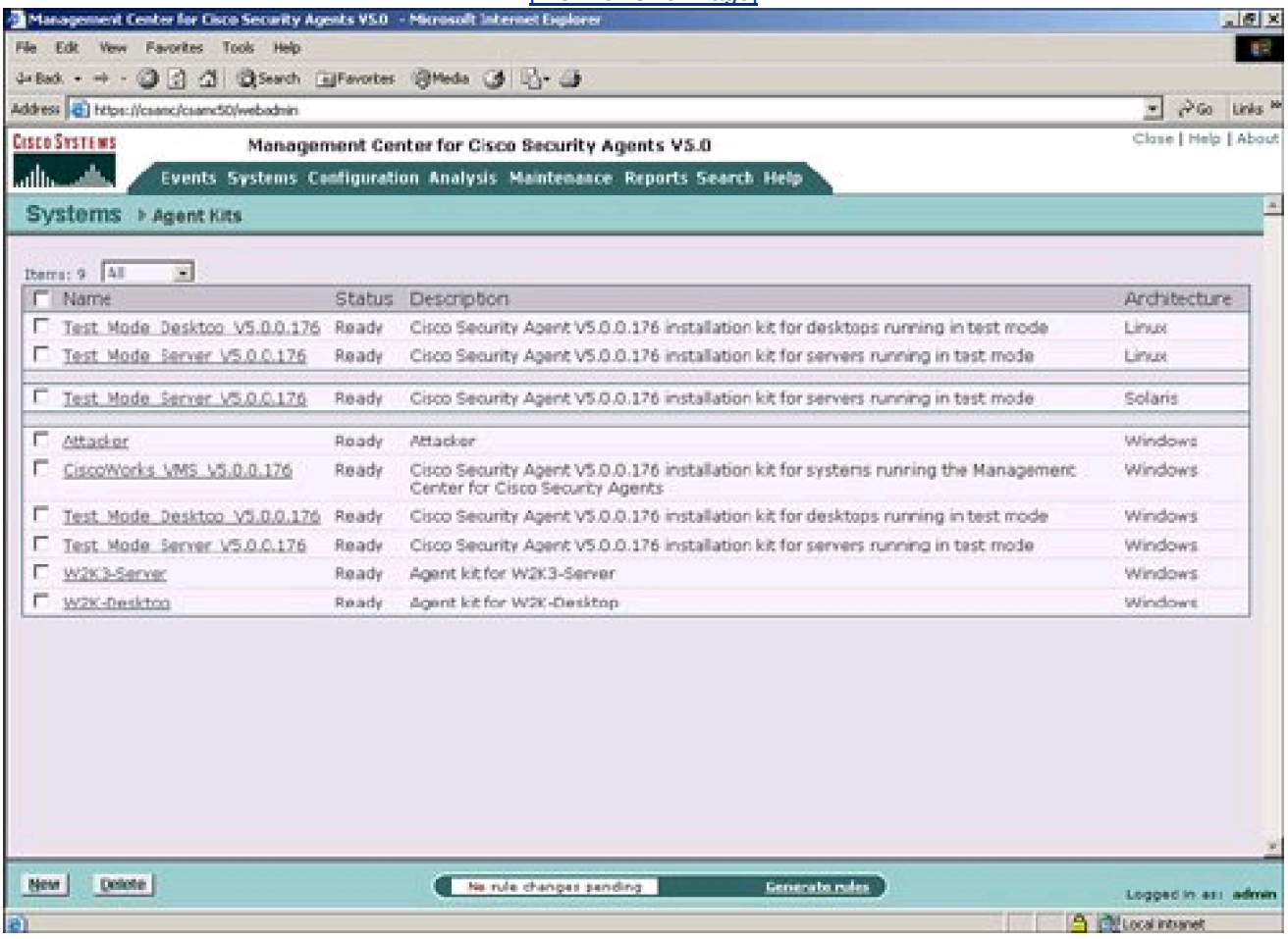
- Reviewing the security policy for a device group
- Attaching rules to the security policy
- Generating rules and deploying to device groups
- Using event monitor and viewing the event log
- Running application analysis

Deploying Cisco Secure Agent Kits

The Management Center can create a Cisco Security Agent Kit for a device or device groups. These agent kits are deployed onto end stations and install the Cisco Security Agent directly on the desktop. The agent kits create a deployment URL, and a user at the end station can type this URL into a web browser to install the Cisco Secure Agent on the endstation desktop. You can create an agent kit by selecting **Systems** > **Agent Kits** from the Management Center homepage, as shown inFigure 8-2. Agent kits can also be installed on an end station with the agent kit zip file on a USB key or CD-ROM. Agent kits can also be bundled and distributed by patch management and application distribution products like SMS or Altiris.

Figure 8-2. Cisco Security Agent Kits

[View full size image]



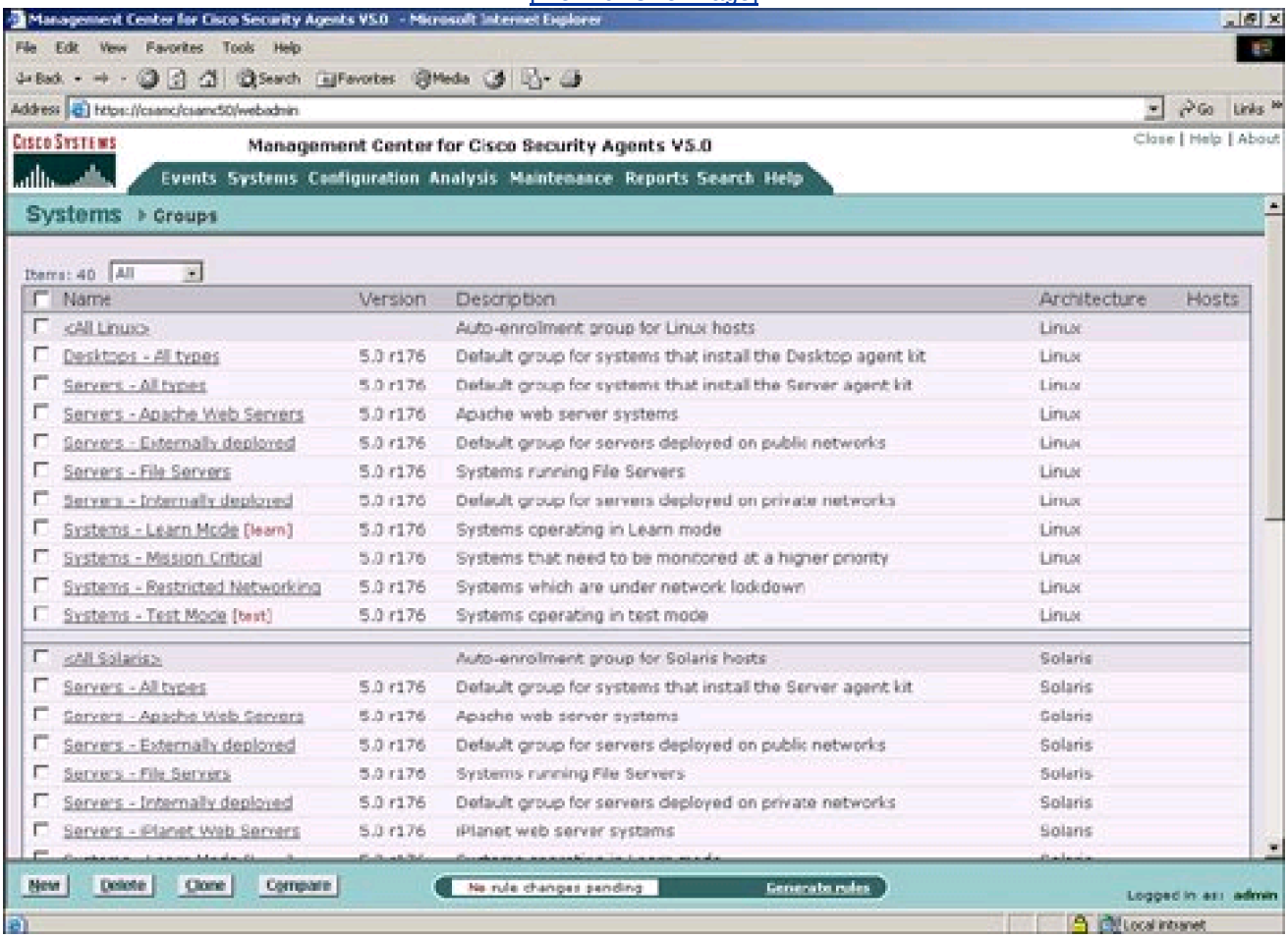
Displaying the End-Station Hostname in the Device Groups

The hostname of the end station must be associated with a device group. A hostname is automatically associated with a device group as indicated in the Cisco Security Agent kit. A hostname can also be added to additional device groups. The ability to associate a hostname, such as a Windows workstation name, with a device group enables common security policies to be deployed to different end stations, including Solaris Web Server, SAP Servers, teleworkers, and so on. For example, a Linux web server in New York City for business-to-business (B2B) can be part of the Linux device group, Web Server device group, New York City data center device group, and the B2B server device group.

The ability to include a host in a device group and apply a security policy to a device group enables common configurations to multiple end stations to be deployed with a common security policy for the device group. A device group can have multiple security policies applied to the device group. The same security policy can also be applied to multiple device groups. Figure 8-3 displays an example of several of the device groups including the auto-enrollment group for Linux and the default group for systems that install the Desktop agent kit.

Figure 8-3. Device Groups

[View full size image]



Reviewing Policies

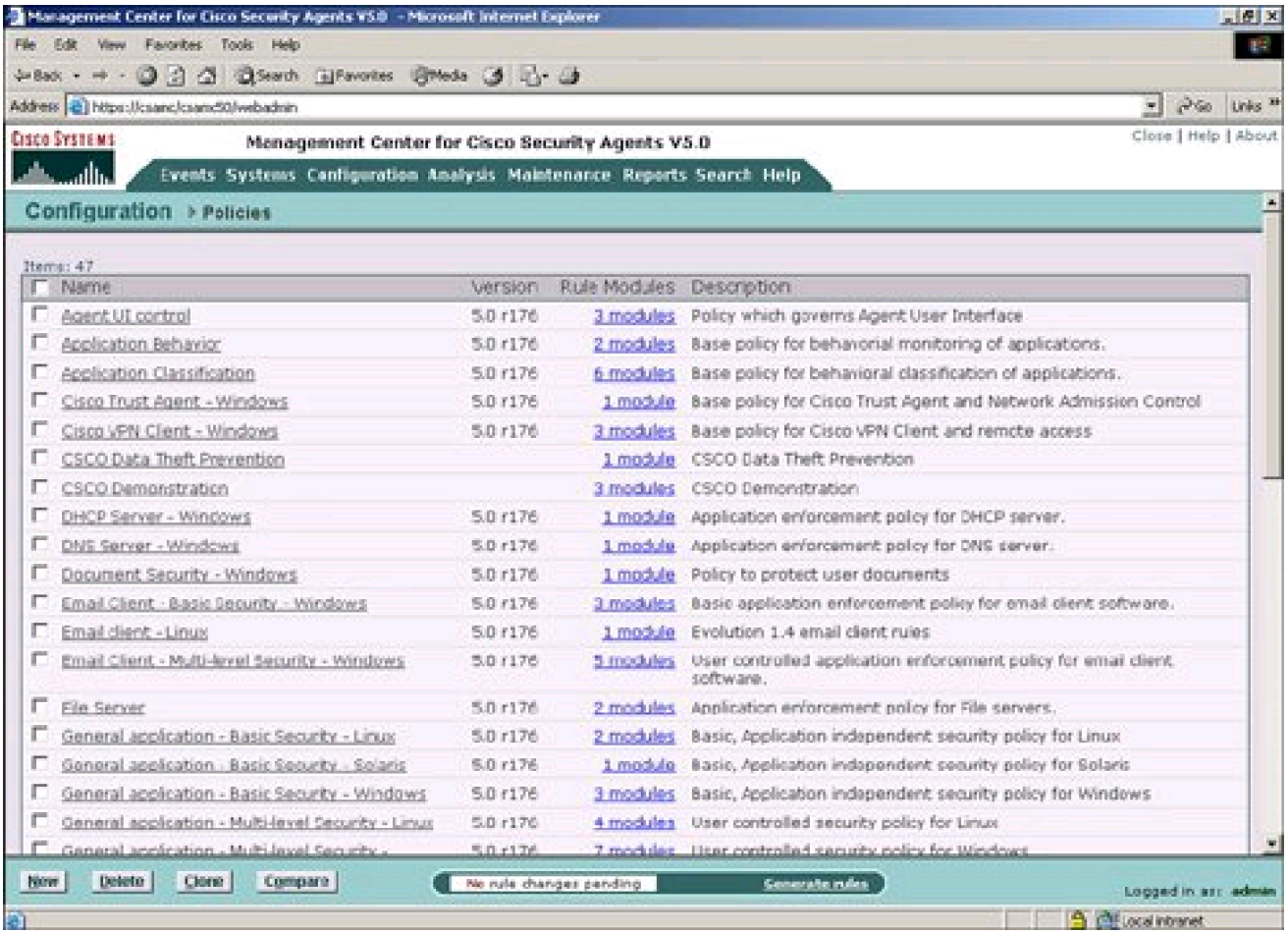
Policies contain the set of security rules that will be attached to a device group. Several default policies are provided to help get users started. These default policies contain a baseline that protects end stations against many day-zero attacks. You can copy and modify default policies or customize your own. Examples of these default policies include a Common Security Module and the Cisco VPN Client Module. The Management Center for Cisco Security Agent also includes support for the following default policy groups:

- Generic Server
- Generic Desktop
- Microsoft IIS v4.0 and v5.0
- Apache v1.3
- Microsoft SQL Server
- Microsoft Exchange
- Sendmail
- Domain Name Server (DNS) servers
- DHCP servers
- Network Time Protocol (NTP) servers
- Domain Controllers
- Distributed Firewall
- Browser protection
- Instant Messenger control
- Microsoft Office protection
- Data theft prevention

Figure 8-4 displays the Management Center with a sample of default policies.

Figure 8-4. Policies

[View full size image]

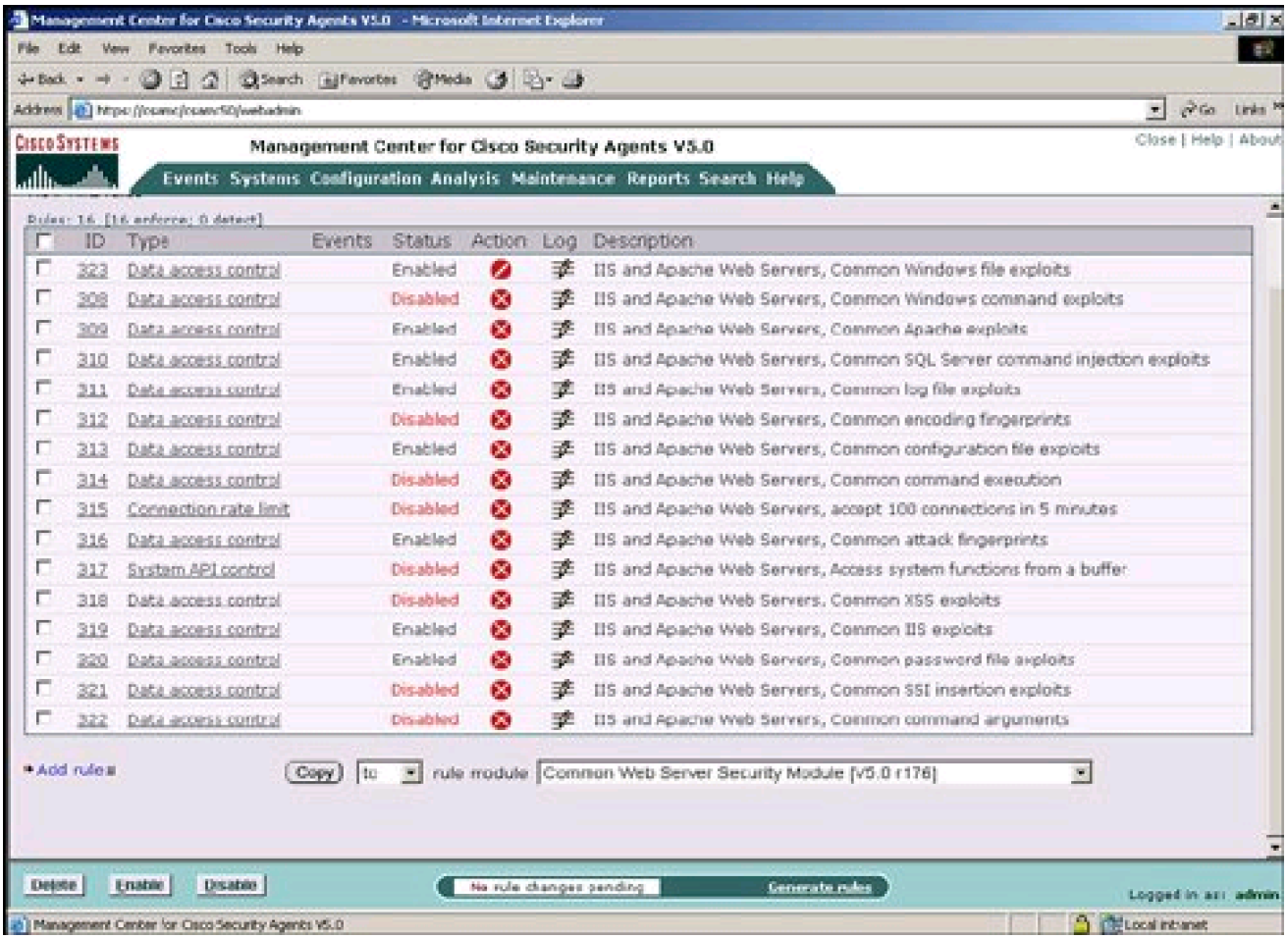


Attaching Rules to a Policy

A policy is composed of individual rules. A collection of rules is named a rule module. Rule modules are generally specific to a particular OS. Rules define each component of the specific security posture in the rule module, which can be attached to a security policy. Rules can also refer to an application class to indicate which applications or processes are policed by the rule. Rules can also be composed with variables, so common information between rules can be defined once and referenced multiple times. Example of variables in rules includes event sets, query settings, file sets, network address sets, network services, registry sets, COM component sets, and data sets. Figure 8-5 displays some the rules that compose the Common Web Server Security Module default policy.

Figure 8-5. Rules of the Common Web Server Security Module Policy

[View full size image]



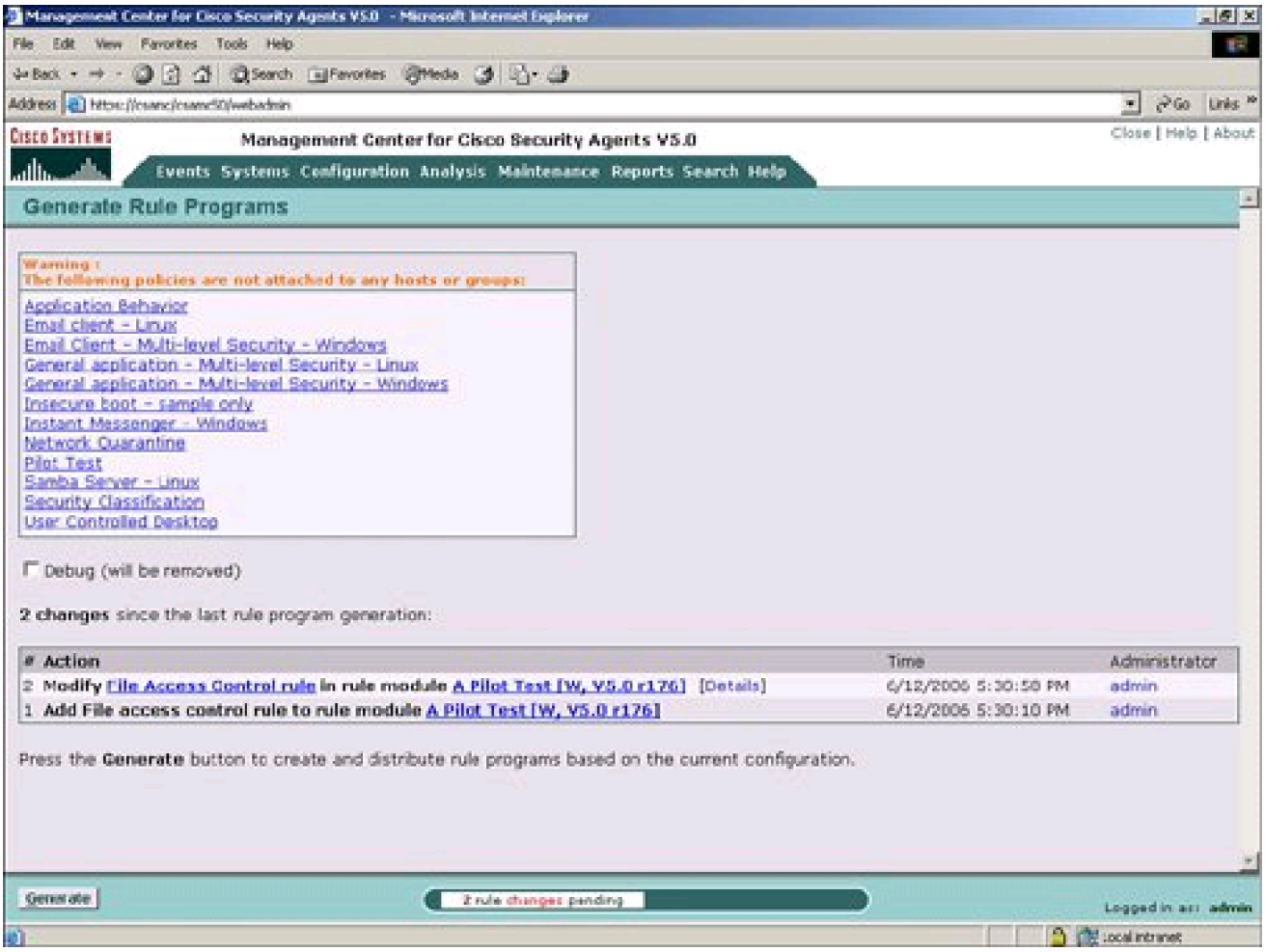
Generating and Deploying Rules

Updating the security policy on an end station requires that the new rules be generated and distributed to the end station. The Management Center for Cisco Security Agents GUI displays the option to Generate Rules at the bottom of the screen and informs the user of the number of new rules that have been configured, but have not yet been generated into a deployable security policy. The Generate Rules process also informs the user of any policies that have been configured but are not associated or attached to any device group.

The Cisco Security Agent on the end station will automatically receive the new security policy from the Generate Rules process during the next automated or manual update cycle. An example of how to initiate the Generate Rules process is provided in Figure 8-6. The end station can elect to poll the Management Center to manually receive the new security policy by selecting the update option directly from the Cisco Security Agent icon on the end-station desktop.

Figure 8-6. Generate Rules

[View full size image]



The Management Center for Cisco Security Agents also features the ability to force connected workstations to poll in and get the latest policy using the "send polling hint" capability. If the user configures the send polling hint on the Management Center for Cisco Security Agents, a User Datagram Protocol (UDP) message can be sent from the Management Center to the host when there is a change in the policy for the host. This UDP message instructs the Cisco Security Agent on the host to download the new security policy prior to the next scheduled polling period.

Using Event Monitor

The Management Center provides an event monitor and event log to view and record significant events that occur at the end-station Cisco Security Agents. It is often advantageous to filter out some of these event logs to reduce false positives and provide a quick mechanism to view a specific event log of interest. Figure 8-7 displays the event monitor in the Management Center, andFigure 8-8 displays the window to configure an event filter to restrict the number of Event Logs that are viewed in the Event Monitor and Event Log.

Figure 8-7. Event Monitor

[View full size image]

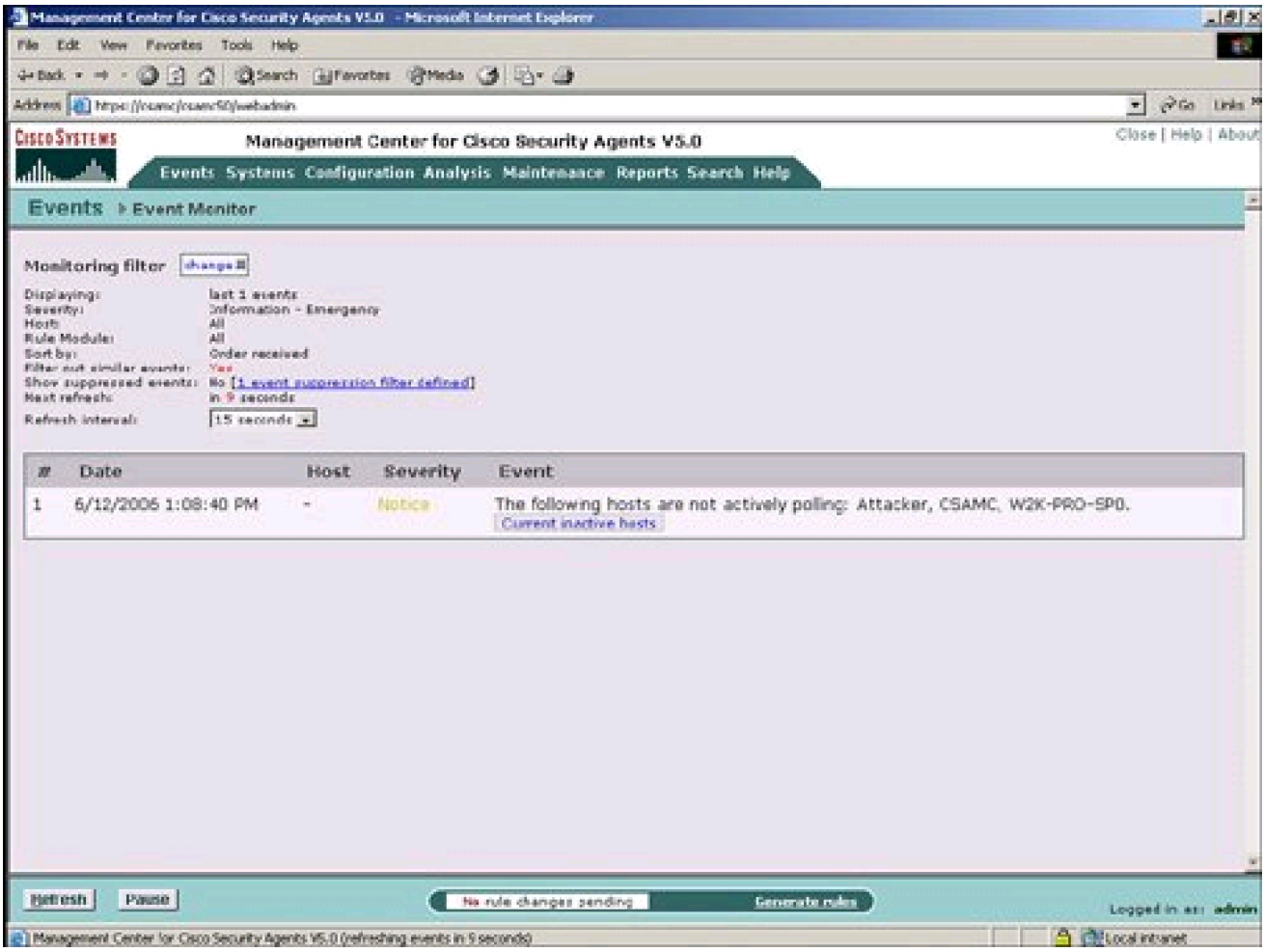
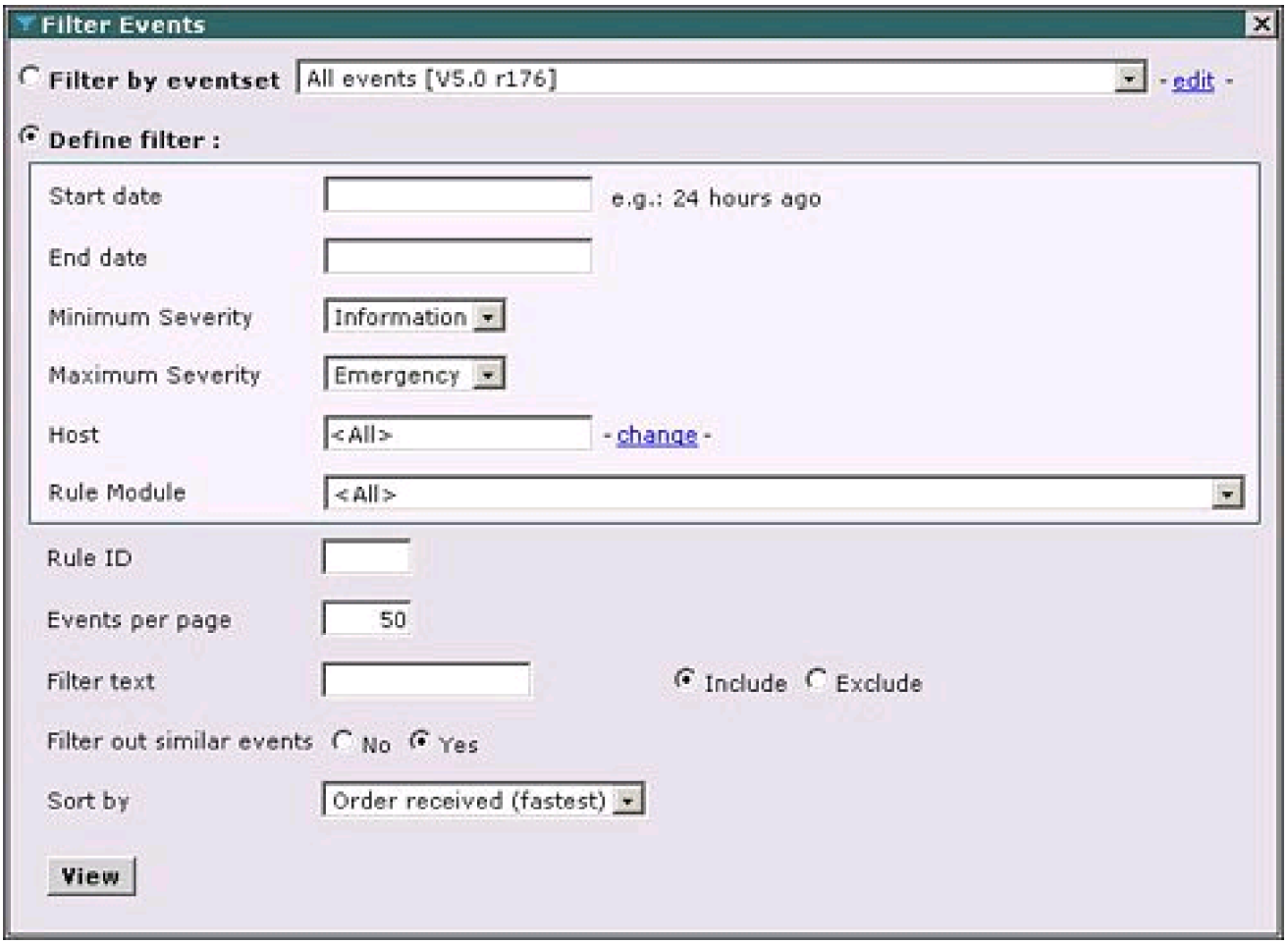


Figure 8-8. Event Filter

[View full size image]



Running Cisco Security Agent Analysis

Cisco Security Agent contains support for an optional application profiler known as Cisco Security Agent Analysis. This application profiler is enabled with a separate license for the Cisco Security Agent Management Center. This feature enables the Management Center and the Cisco Security Agent to determine what applications are deployed on a PC, laptop, or server with the Cisco Security Agent installed on that end station. This feature also enables the Management Center to determine the use pattern of these detected applications on the end stations.

Application analysis is enabled on a per-device group basis and will analyze all hosts in that device group. Application analysis is initiated by selecting the Application Deployment Investigation option under Analysis in the Management Center. Application Deployment Investigation includes a list of reports to display information gained from the application profiling process. The information in the reports that are generated by the Profiler contains statistics about how often an application is used. The reports generated from the analysis also contain network data statistics, including network source, destination, and service traffic patterns. Information in the reports about how applications are used on an end system can provide valuable input into the construction of effective rules and security policies for device groups. Reports that are generated by the application analysis include the following:

- Anti-Virus Installations Report (Norton and McAfee)
- Installed Products Report
- Unprotected Hosts Report (No associated Policy Groups)
- Unprotected Products Report (No Policy to protect that Product)
- Product Usage Report

- Network Data Flows Report, which includes the following information:
    - Number of unique source/destination combinations
    - Number of client hosts
    - Number of server hosts
    - Filter report by source, destination, protocol
- Network Server Application Report, which includes the following information:
    - Associates the application with open service ports
    - Identifies which service ports are not used or are lightly used

Application Deployment Investigation is an optional feature of the Management Center for Cisco Security Agents. The Management Center also contains a feature called Learn Mode. Learn Mode is used as a mechanism to eliminate query-responses for common application and service use on the desktop with the Cisco Security Agent. The Cisco Security Agent will often query the user when a new application is running and ask the user if this is the expected behavior. Learn Mode enables the Cisco Security Agent to learn the normal application and service use on a desktop without having a query-response pop up to the user for each application or service. The Cisco Security Agent is placed in Learn Mode during the first 72 hours of deployment of the Cisco Security Agent on the desktop.

In addition to Learn Mode, there is also an optional Test Mode for a security policy. Test Mode is designed for policies and will log any activity from the policy but will not query or deny network activity, based upon a policy in Test Mode. Test Mode is designed to inform what the effect of a new security policy would be on a host before actually enforcing the new security policy on the end station.

The Analysis module also contains an Application Behavior Investigation feature in addition to Application Deployment Investigation. The user must select the specific application, the time to end the analysis, the application, and the specific host in the Management Center to investigate the behavior of that application. The Management Center will allow the selection of an application class for analysis on a particular host. However, it is recommended that analysis only occur for one specific application at a time on a particular host. The Application Behavior Investigation feature can create a recommended rule module to increase security, based upon the analyzed application behavior on the end station. This rule module generation feature of Application Behavior Investigation will create a new application class in the created rule module for the analyzed application.

PREV NEXT

Cisco Security Agent

The Cisco Security Agent sits directly on the end station. The Cisco Security Agent is often identified by an icon of a red flag at the bottom of the desktop. A waving red flag notifies the user of suspicious behavior that could be indicative of an attack.

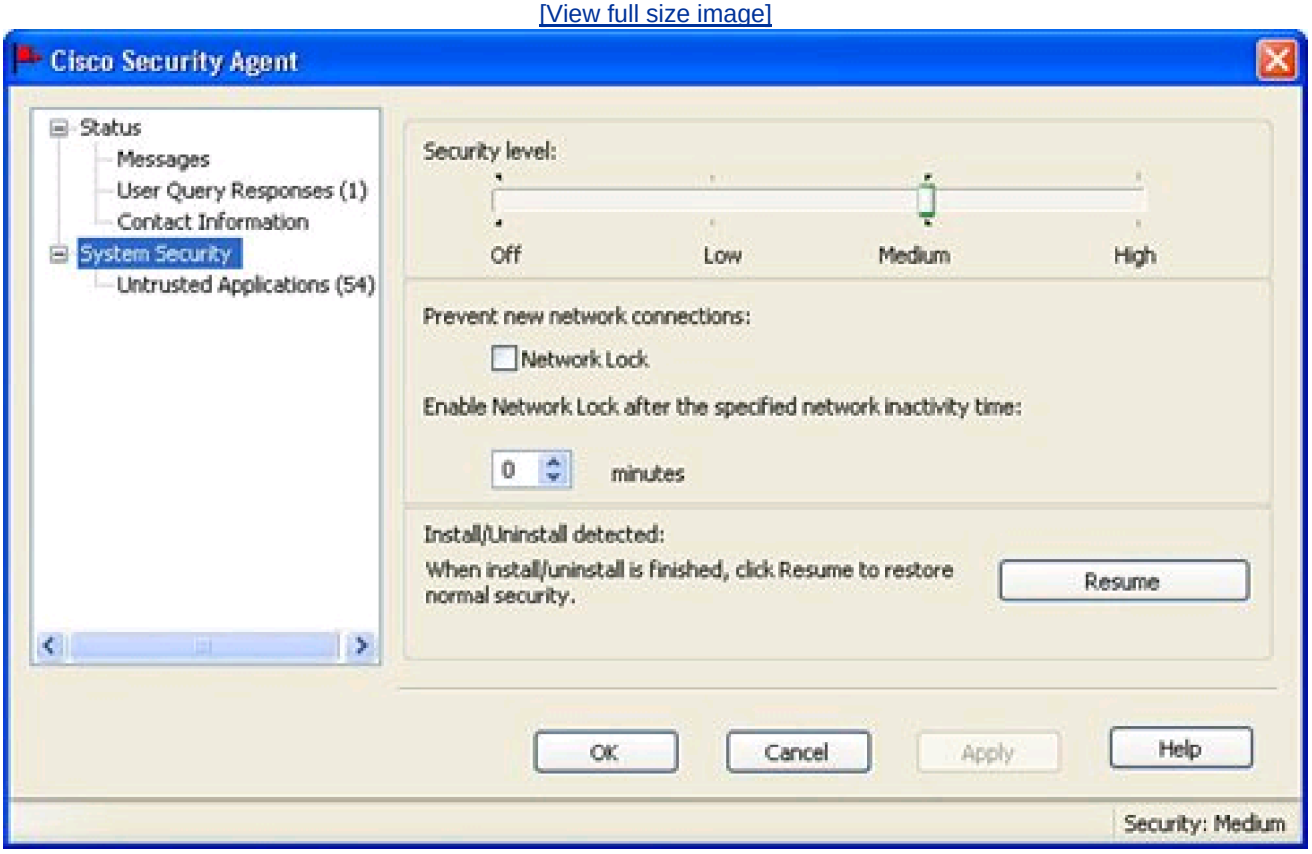
The Cisco Security Agent Panel is composed of the following categories:

- Status
- System Security

Figure 8-9 provides an example of the Cisco Security Agent Panel.

Figure 8-9. Cisco Security Agent Panel

[View full size image]



Status

The Status area of the Cisco Security Agent panel provides information to the end user on what the Cisco Security Agent is doing. This status feedback on the Cisco Security Agent Panel is important because the end user typically does not have any direct access to the Management Center for Cisco Security Agents.

The main Status area provides several items of important information about the Cisco Security Agent including the following:

- Host name
- Management Center
- Registration date
- Last poll time (to check for a new policy configuration)
- Last download time (to download a new policy configuration)
- Software update
- Network Admission Control posture results
- Poll button (to poll Management Center to download a new policy configuration)

The following subcategories are available in the Status category:

- **Messages** The Messages subcategory provides information to the user about what important events have been detected by the Cisco Security Agent.
- **User Query Response** The User Query Response subpanel provides details on what permissions were asked to the user (for example, application *x* attempted to modify memory in process*y*; the user was queried and the response was "Yes").
- **Contact Information** Optional information, including name, phone number, location, and e-mail address to contact the end user on the desktop with the Cisco Security Agent.

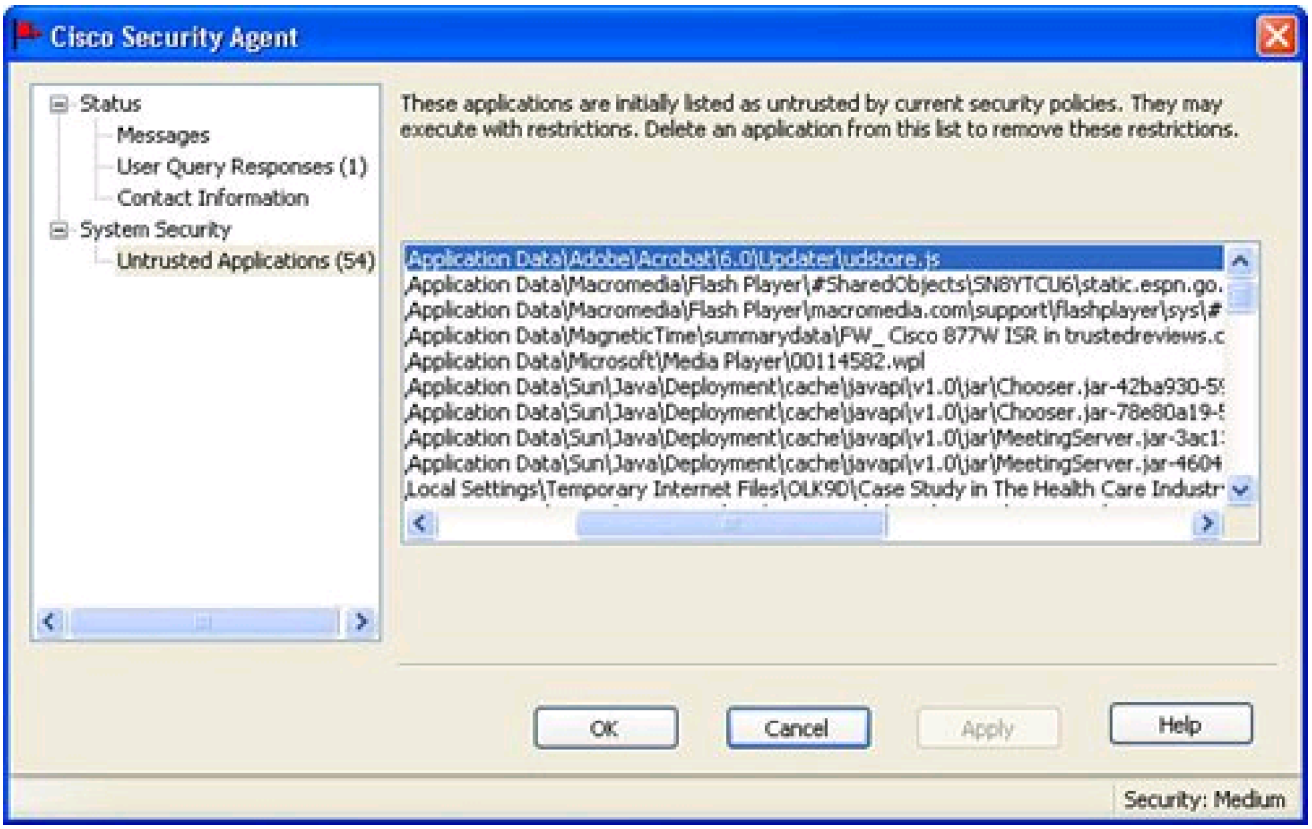
System Security

The System Security area provides a mechanism where certain users can specify a default security policy (high, medium, low) if this option is allowed by the Management Center. The System Security area also provides an option to restrict new network connections after a certain network inactivity timeout.

The System Security area also provides a vehicle to display to the user which applications are natively untrusted by the Cisco Security Agent. These untrusted applications can result in the user being queried about permission to use the application if the application attempts to modify critical system resources. The Cisco Security Agent panel also provides an option to remove applications for the untrusted list, if this option is enabled by the Management Center. Figure 8-10 displays a sample of the display of a few of the untrusted applications on the Cisco Security Agent Panel.

Figure 8-10. Untrusted Applications

[View full size image]


Cisco Security Agent
Status
Messages
User Query Responses (1)
Contact Information
System Security
Untrusted Applications (54)
These applications are initially listed as untrusted by current security policies. They may execute with restrictions. Delete an application from this list to remove these restrictions.
Application Data\Adobe\Acrobat\6.0\Updater\udstore.js
Application Data\Macromedia\Flash Player\#SharedObjects\SN8YTCU6\static.espn.go.
Application Data\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys\#
Application Data\MagneticTime\summarydata\FW_ Cisco 877W ISR in trustedreviews.c
Application Data\Microsoft\Media Player\00114582.wpl
Application Data\Sun\Java\Deployment\cache\javapi\v1.0\jar\Chooser.jar-42ba930-5
Application Data\Sun\Java\Deployment\cache\javapi\v1.0\jar\Chooser.jar-78e80a19-5
Application Data\Sun\Java\Deployment\cache\javapi\v1.0\jar\MeetingServer.jar-3ac1
Application Data\Sun\Java\Deployment\cache\javapi\v1.0\jar\MeetingServer.jar-4604
Local Settings\Temporary Internet Files\OLK9D\Case Study in The Health Care Industr
OK
Cancel
Apply
Help
Security: Medium

PREV NEXT

Summary

The Cisco Security Agent is often the last line of defense in a self-defending network. The Cisco Security Agent sits on the user's desktop and monitors OS kernel activity for suspicious behavior. The Cisco Security Agent can be self-defending, as the Cisco Security Agent can ask user permission or block suspicious activity on the desktop and defend against a network attack. The Cisco Security Agent can prevent "day-zero" attacks because it looks for symptoms of an attack rather than a unique signature of the attack. Cisco Security Agents are a good complement to other signature-based defenses, such as IPS, in a layered self-defending network. The Cisco Security Agent is considered to be a Host IPS (HIPS) product that complements Network IPS and other self-defending components within the network fabric.

The Management Center for Cisco Security Agents is the centralized management product to manage the agents. A Management Center can manage up to 100,000 agents. A host that contains a Cisco Security Agent is placed into a device group in the Management Center. A host can belong to more than one device group. Security policies are attached to device groups and contain a definition of the security policy that is monitored or enforced on the end station. Multiple security policies can be attached to a single device group, and a single security policy can be attached to multiple device groups. Security policies or policy groups are composed of rule modules. A rule module can be applied to multiple security policies. A rule module is fundamentally a named collection or container of individual rules.

References

Cisco Systems, Inc. Cisco Security Agent 4.5 Data Sheet.
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_data_sheet09186a008033a40f.html

Cisco Systems, Inc. Using Management Center for Cisco Security Agents Version 4.5.1.
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_book09186a0080422f08.html

Cisco Systems, Inc. Using Management Center for Cisco Security Agents Version 5.0.
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_book09186a00805ae89c.html

Sullivan, Chad. Cisco Security Agent. Cisco Press 2005.

Sullivan, Chad, Jeff Asher, and Paul Mauvais. Advanced Host Intrusion Prevention with CSA. Cisco Press 2006.

Chapter 9. Cisco Security Manager

This book details how a layered defense is the best defense to protect a network against attacks. A layered defense as part of a self-defending network is similar to layered defenses in sports such as football and soccer. These sports have an initial defense against the opposition followed by additional layers of defense closer to the critical resource of the team. In a soccer or football analogy, the critical resource is the goal, and in a network environment, the critical resource is often a server or remote PC. In the sports analogy, a layered defense is only effective if the different layers are implementing a consistent strategy and are on the same page as to what they are trying to accomplish. For example, a football defense in which the cornerbacks are playing zone defense while the safeties think that everyone is playing man defense is probably not going to be very effective because the layered defense is not coordinated and is inconsistent.

In the network environment, centralized management is an effective way to ensure that the layered defenses are all executing the same plan. Centralized management is also an effective tool to let the security operations manager know when part of the layered defense is behaving incorrectly or is being ineffective.

Centralized management is composed of two main functional areas:

- Configuration
- Monitoring/mitigation

Cisco offers a centralized management product line called the Cisco Security Management Suite. The Cisco Security Management Suite is composed of the Cisco Security Manager and Cisco Security MARS. Cisco Security Manager and Cisco Security MARS are the follow-on products to the CiscoWorks VPN and Security Management Solution (VMS) product.

Getting Started

Cisco Security Manager can centrally manage many of the individual components of the Cisco Self-Defending Network. Examples of devices that can be managed by the Cisco Security Manager include IOS routers, Adaptive Security Appliances (ASA), Intrusion Prevention Systems (IPS), PIX Firewalls, and Catalyst 6500/7600 LAN switches.

The Cisco Security Manager has three main views to manage a :

- Device view
- Map view
- Policy view

Cisco Security Manager is an integrated application because all supported device platforms are managed together. For example, the process to configure an access control list (ACL) is the same for a Cisco IOS router as an ASA security appliance. The process to configure a VPN is also independent of platform type and allows a single VPN with multiple platform types. For example, a single VPN can be created with IOS routers as the hub devices and PIX Firewalls as the spoke devices.

The integrated approach based upon service or function like firewall or VPN is a contrast to the previous product, CiscoWorks VMS. CiscoWorks VMS was platform-based, with a separate Management Center for each platform like IOS routers or PIX firewalls. CiscoWorks VMS also used a separate GUI or web browser for each Management Center or platform while the Cisco Security Manager features a single, integrated GUI. New features in the Cisco Security Manager that were not present in the CiscoWorks VMS product include the following:

- Single client GUI to manage multiple platforms
- Single access control list (ACLs) rule table for PIX, FWSM, IOS CBAC, and IOS ACL
- Catalyst 6500/7600 chassis management
- Topology map view to graphically manage the network
- Ability to import command-line interface (CLI) that has been modified by telnet/ Device Managers
- Coexist with multiple Java Runtime Environments (JREs) on a server
- Mine or filter audit reports based upon admin, date, string
- Flex-config template for nonsecurity IOS features
- Multithreaded backend server for performance increase
- Support up to 5000 devices with a single server
- Manage ASA 7.x
- Import device list from CiscoWorks Resource Management Essentials (RME)
- Hierarchical virtual private network (VPN)
- Apply access control lists (ACLs) to a group of interfaces
- Define access control lists (ACLs) for a specific time-range
- access control list (ACLs) hit count information

- Scheduled configuration deployment at specific date and time
- ASA device status
- Dynamic Multiple VPN (DMVPN)
- Aswan 2.0 (MPLS to IP Security (IPSec) VPN)

Cisco Security Manager provides a JumpStart menu so that new security operations users can quickly learn how to import, configure, and deploy configuration to security devices.

Figure 9-1 displays the JumpStart menu of the Cisco Security Manager.

Figure 9-1. JumpStart

[View full size image]

Cisco Security Manager includes several features to enable the integrated management of 5000 devices of separate platform types. One of these features is the ability to filter a list of devices by platform type. Another integrated feature is the ability to create a single device group with mixed device platforms. These device groups can be used to apply security and VPN configuration settings to a group of devices. Device groups can be based upon categories such as data center locations (for example, Los Angeles, San Francisco) or functional groups (for example, Engineering, Finance, ACME Corp, and so on).

PREV NEXT

Device View

This section describes how to add a device in Device View. You also learn how to configure access control lists (ACLs) from Device View.

Add Device

Cisco Security Manager can add a new device in several ways. The most common way is to import a device and its existing configuration from a live device on a network. Cisco Security Manager can also import a list of devices from other CiscoWorks applications through a Device Credentials Repository (DCR). Cisco Security Manager can also "hotstage" a new device and then deploy the configuration for that new device once the device in activated and placed in the network with its bootstrap configuration.

Figure 9-2 displays an example of initiating the process to create a new ASA device, and Figure 9-3 indicates how to place this new device into a device group. It is common practice to place a device into a device group based upon device location or functional group. However, any type of device group based upon function, asset cost, and so on can be created and used.

Figure 9-2. Add New ASA Device

[View full size image]

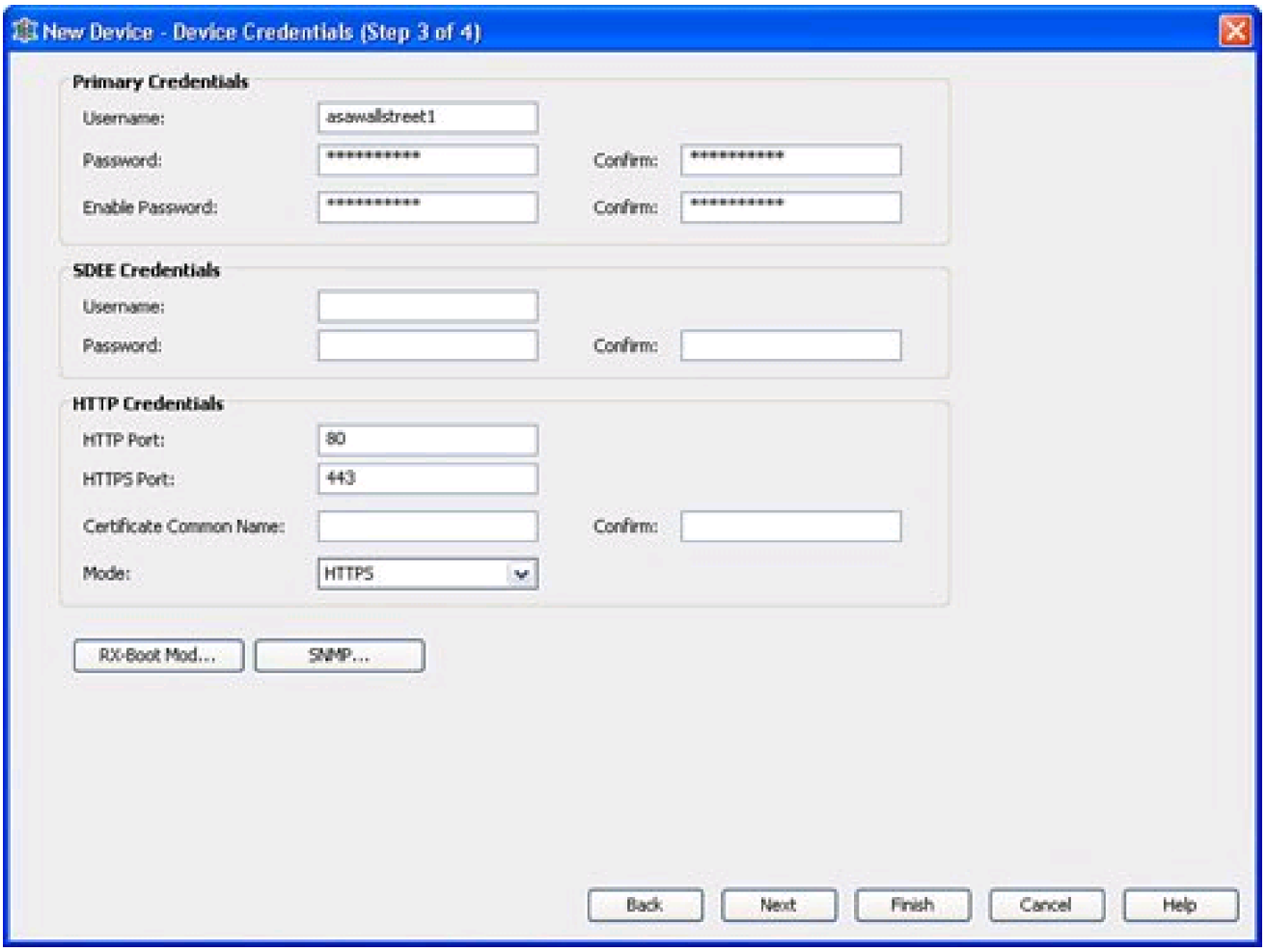
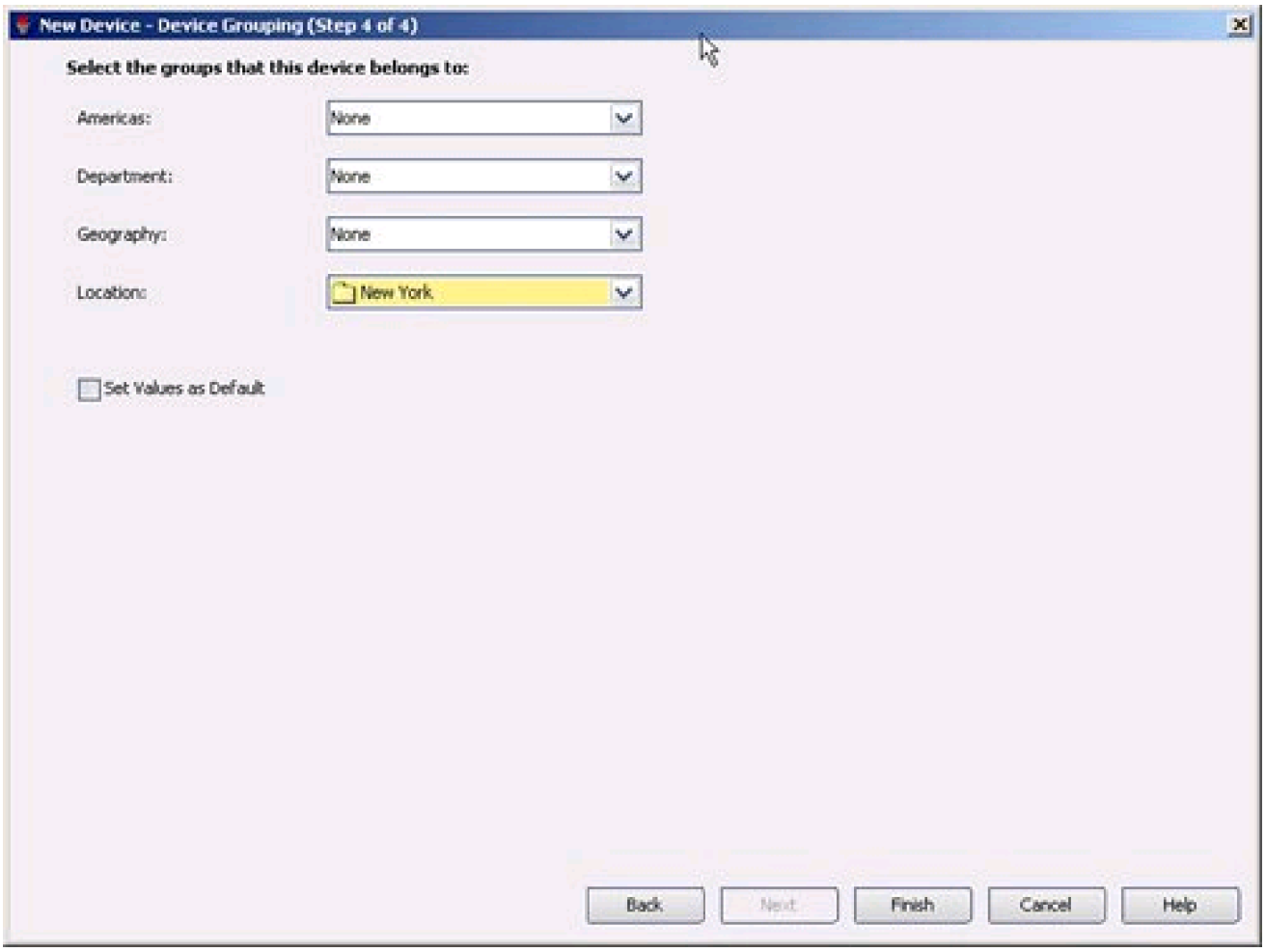


Figure 9-3. Place New Device in Device Group

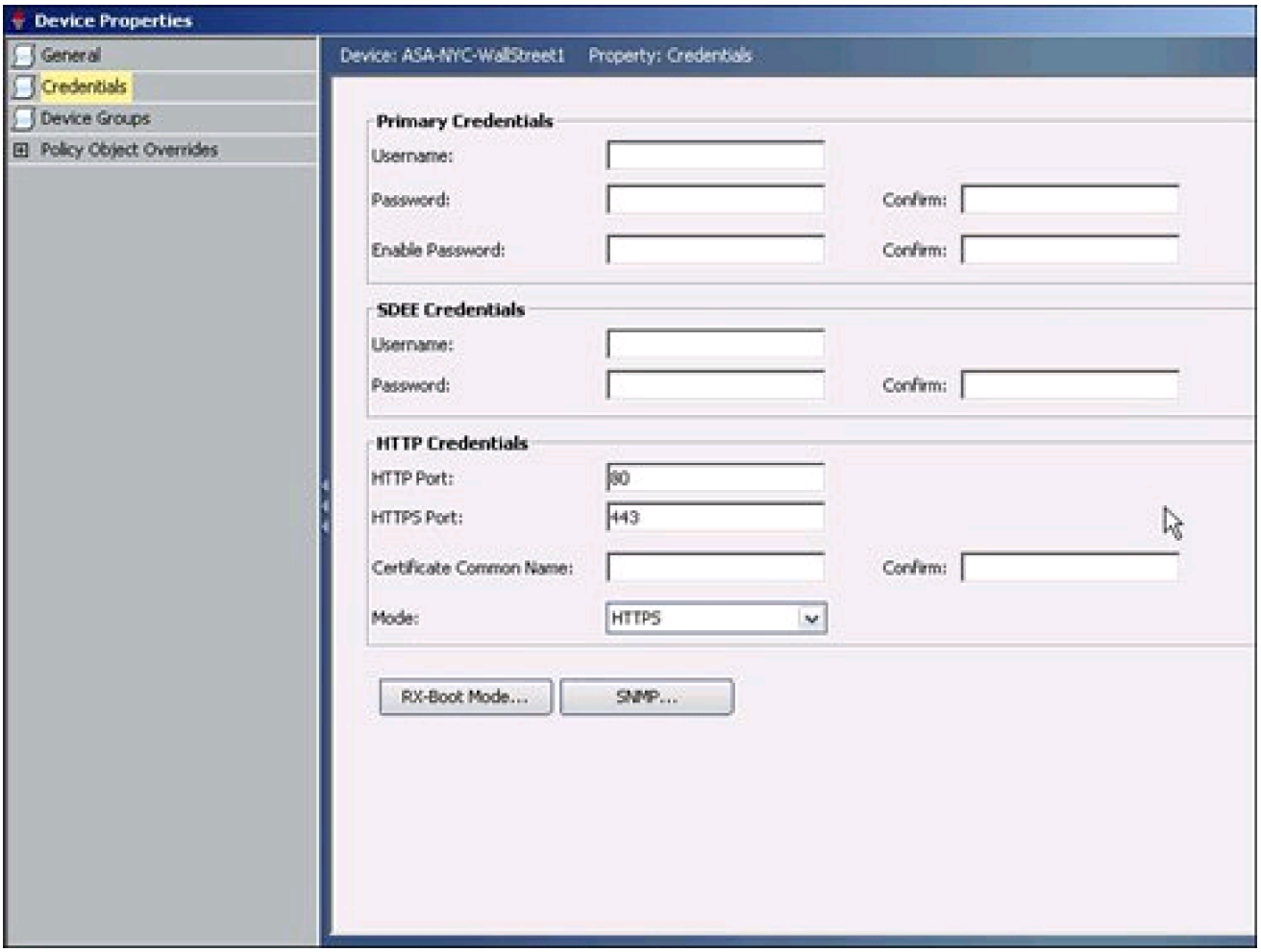
[View full size image]



Each device in the Cisco Security Manager contains the set of management credentials shown in Figure 9-4. Some of the most used primary credentials include the username, password, and enable password. These primary device credentials can also be stored in a separate device identity server like Cisco ACS. Cisco Security Manager can natively store primary credentials for a device or retrieve these primary credentials from an external Cisco ACS server.

Figure 9-4. Device Credentials

[View full size image]



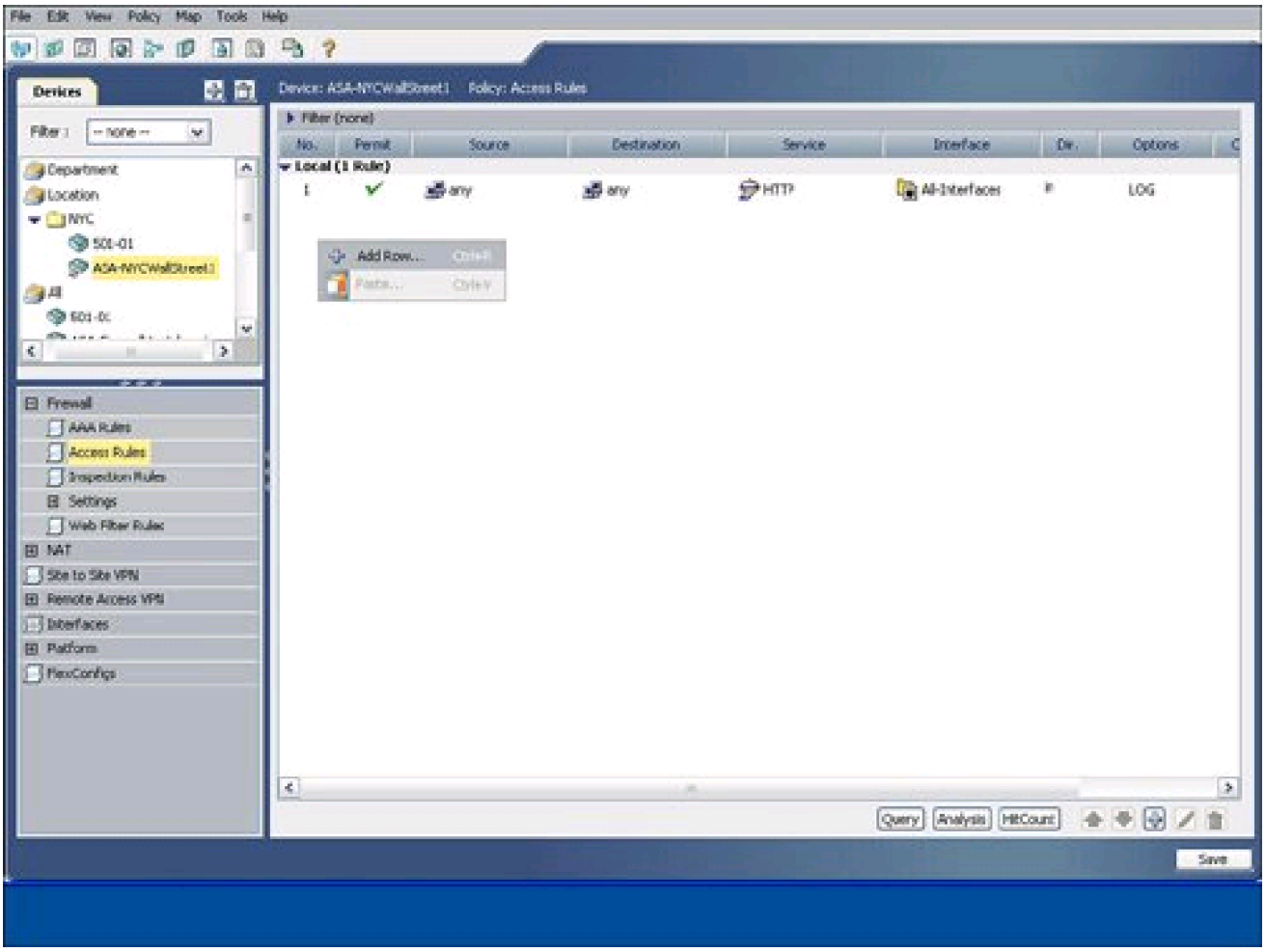
Device credentials are required for the Cisco Security Manager to communicate with the device. Many Cisco security products that use device managers also use HTTPS for centralized management with the Cisco Security Manager.

Configure Access Conrol Lists (ACLs) from Device View

One of the most popular tasks in security operations or security management is configuration and deployment of access control list (ACLs) rules. The selection of a device in Cisco Security Manager from the device list will by default display the access control list (ACLs) rule table for that device. Users can initiate the process to add an access control list (ACLs) to that device by right-clicking on the access control list (ACLs) rule table as displayed in Figure 9-5.

Figure 9-5. Add an Access Control List (ACLs) to a Device

[View full size image]

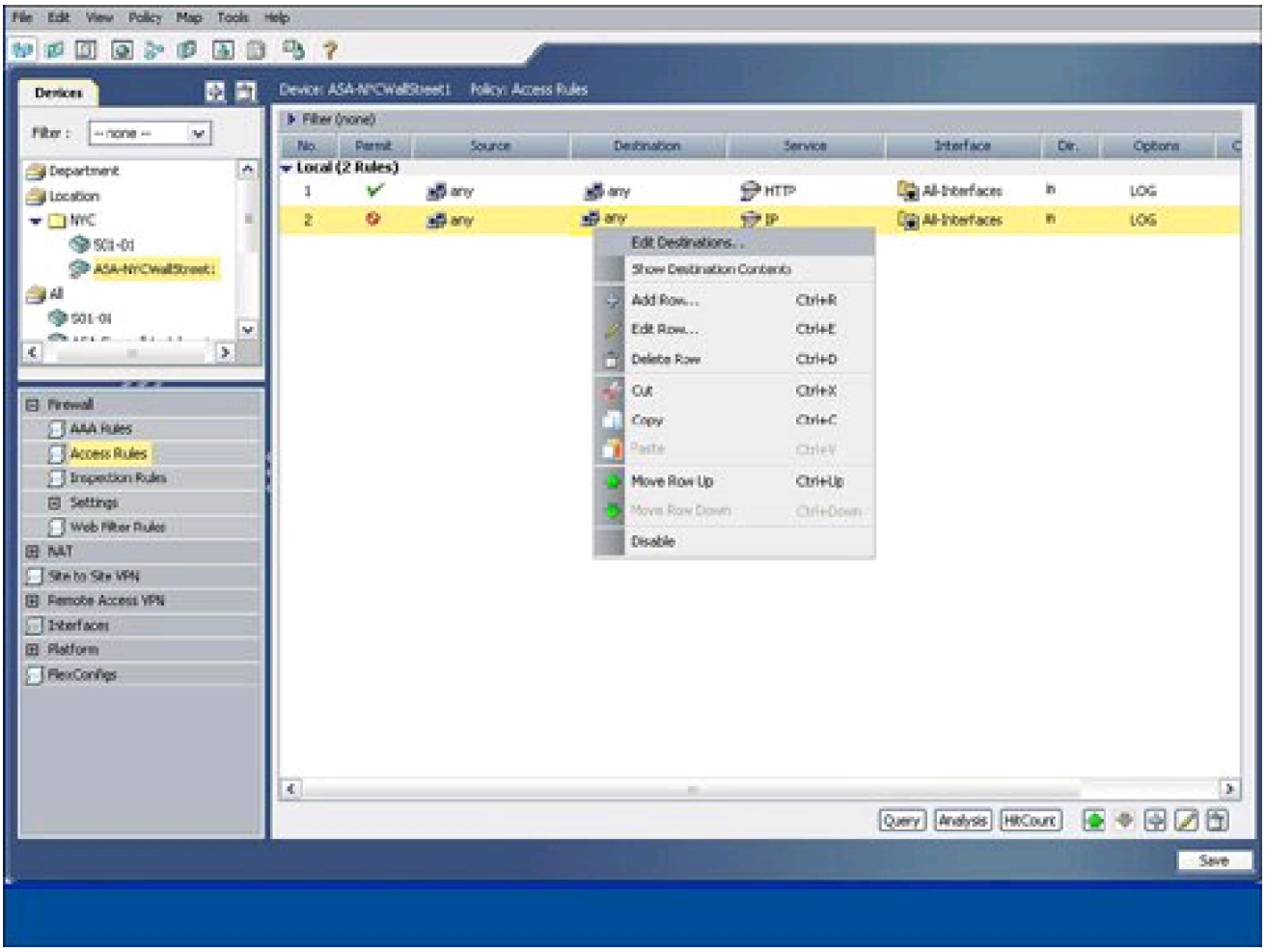


This process to add an access control list (ACLs) results in the display of the Add Firewall Rule wizard. This wizard includes fields for permit/deny, source, destination, service, interfaces, and logging. The Firewall Rule wizard also supplies default values for these parameters. These parameters can be modified, deleted, or added directly in the wizard. You also have the option to select the OK button to create the access control list (ACLs) with the default values.

Cisco Security Manager enables the user to right-click and edit a specific column in the access control list (ACLs) to create the new access control list (ACLs), as shown in Figure 9-6. This figure shows a modification to the destination field in the access control list (ACLs) rule.

Figure 9-6. Right-Click and Edit a Column in the Rule Table

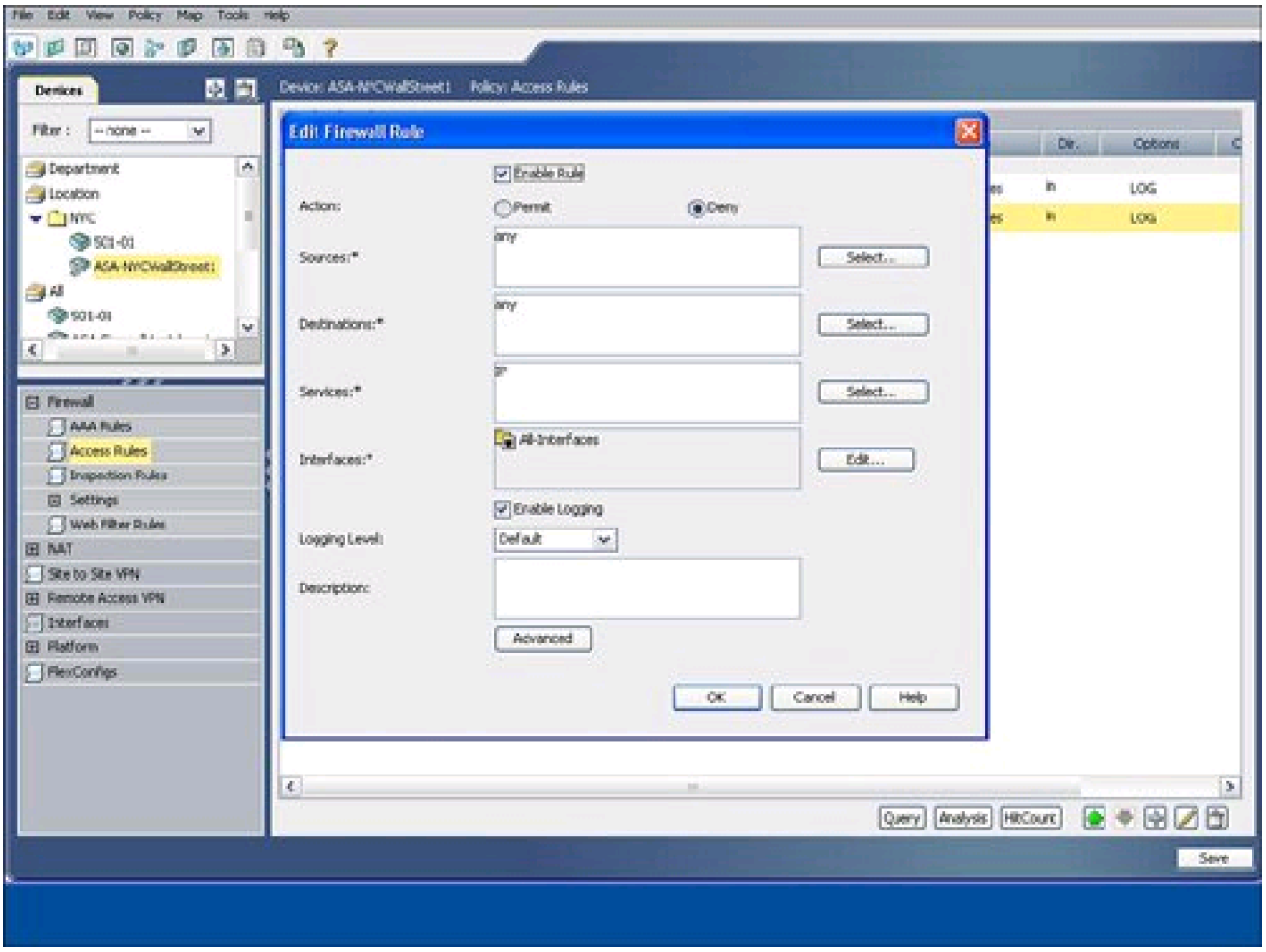
[View full size image]



Alternately, you can also select the rule number and then edit the fields of the access control list (ACLs) rule with the Edit Firewall Rule wizard shown in Figure 9-7. The Edit Firewall Rule wizard contains the same fields as the Add Firewall Rule wizard. The Edit Firewall Rule wizard enables the user to manually edit the fields or to add predefined objects for source, destination, and service fields in the access control list (ACLs) rule.

Figure 9-7. Edit Firewall Rule Wizard

[View full size image]



Configuring Interface Roles

Cisco Security Manager introduces a feature that enables you to configure an access control list (ACLs) rule for multiple interfaces. The ability to configure an access control list (ACLs) rule for multiple interfaces reduces the administrative burden on security groups and increases security because rules can now be defined for a group of interfaces rather than a single interface. Interface groups or roles are created by matching a name pattern in the interface name. For example, the External interface group or role includes any interface that contains the name "Outside."

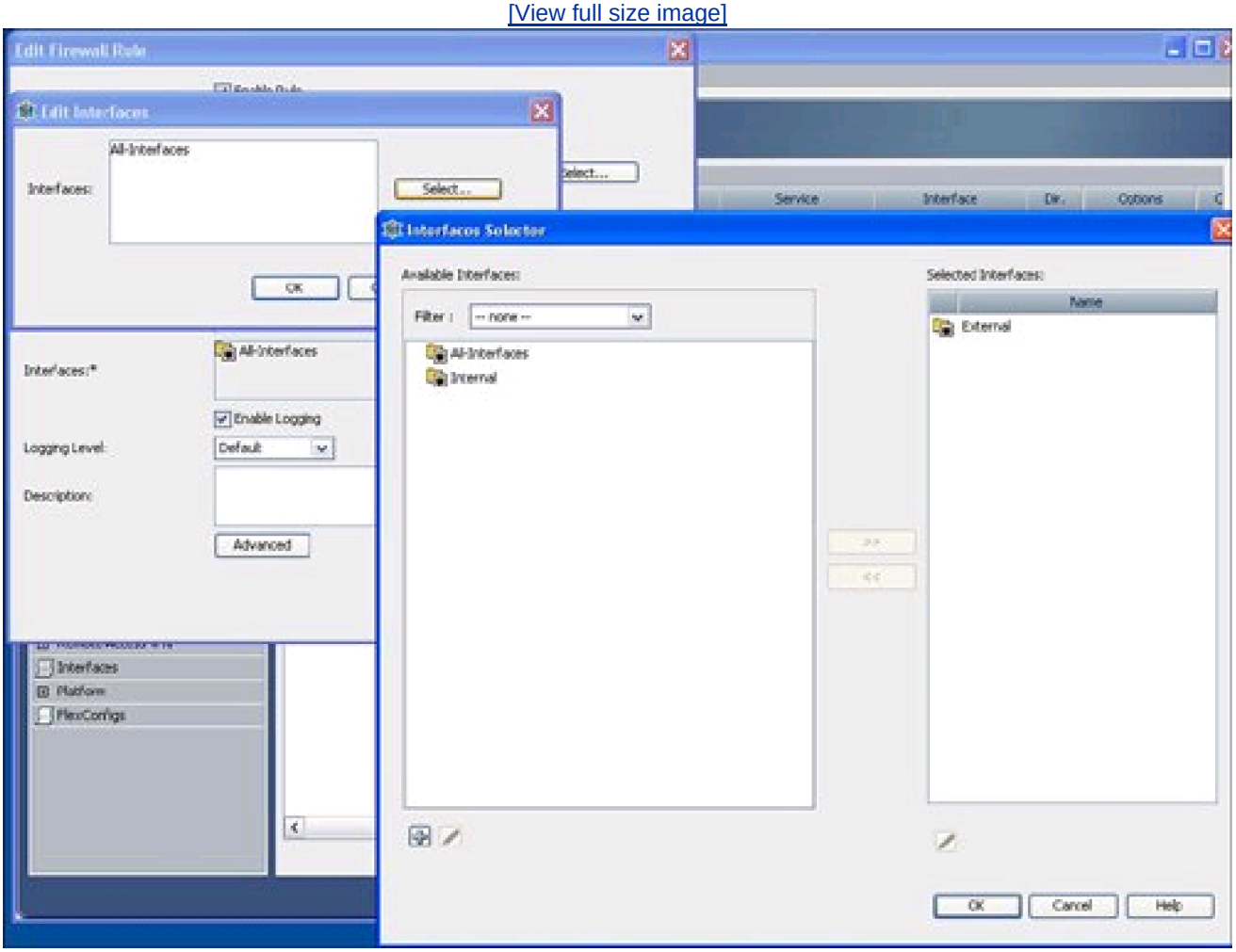
Cisco Security Manager creates many default interface groups or roles. In addition to the default roles, users can also manually create any customized interface role. An example of the interface roles that are provided by default includes the following:

- All Interfaces
- External
- Internal

Figure 9-8 provides an example of how to select the External interfaces in the definition of an access control list (ACL) rule. Be sure to examine all the name patterns that are included in any default interface role prior to deploying access control list (ACLs) rules that reference a default interface role. For example, the External interface role group may include Ethernet1 by default, while the Internal interface role may include Ethernet0. Any customized interface role can be created in the Interface Role object in the Policy Object Manager. Interface roles that are created in the Policy Object Manager can be selected in the access control list (ACL) rule table.

Figure 9-8. Apply an Access Control List (ACL) Rule to External Interfaces

[View full size image]



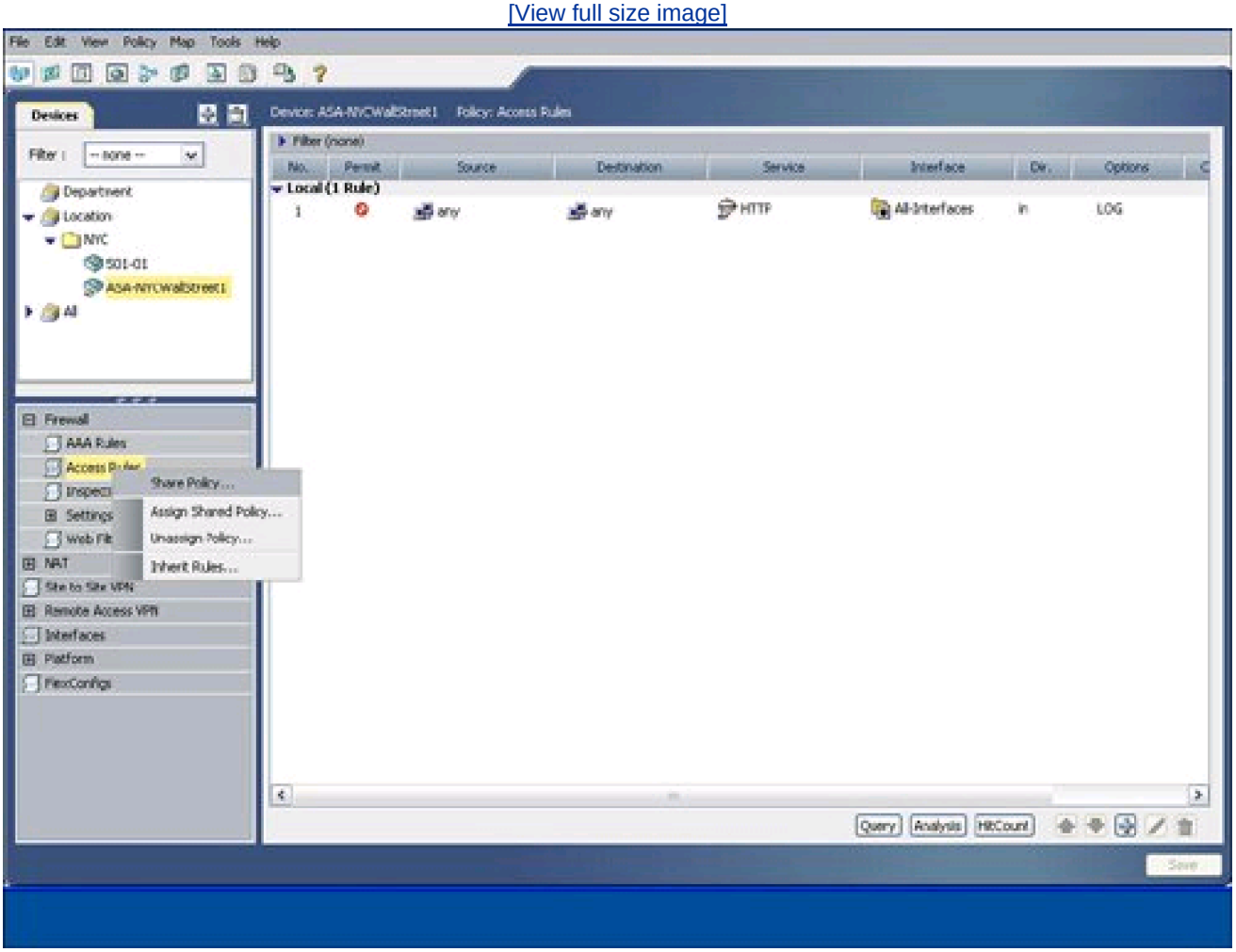
Apply Access Control List (ACL) Rules to Multiple Devices

Cisco Security Manager offers several mechanisms to apply a list of access rules to a group of devices. Once you are satisfied with the access control lists (ACLs) that are configured for one device, you can share and copy the access control lists (ACLs) to multiple devices from the Device View. The ability to share policy between multiple devices types is a powerful feature because you can apply this firewall access-rule table policy to a wide variety of devices, including a Cisco IOS router without the IOS firewall feature set. The IOS firewall feature set is also known as Context-Based Access-Control (CBAC). The security policy contained in the access control list (ACL) rule table will be configured with plain access control lists (ACLs) (TCP state information is not maintained for the connection) if the CBAC firewall feature set is not installed on the IOS router.

To share or apply firewall rules to multiple devices from the Device View, you can select a rule table and then initiate the share policy process. The process to share an access control list (ACL) rule policy from one device in the device view to multiple devices is initiated by right-clicking on the access-rule tab for the device and selecting the share policy option. Figure 9-9 displays an example of how to define a policy to be shared or applied to multiple devices. The shared policy must be given a name in order to be referenced and applied to multiple devices.

Figure 9-9. Mark an Access Control List (ACLs) Rule Table to Be Shared

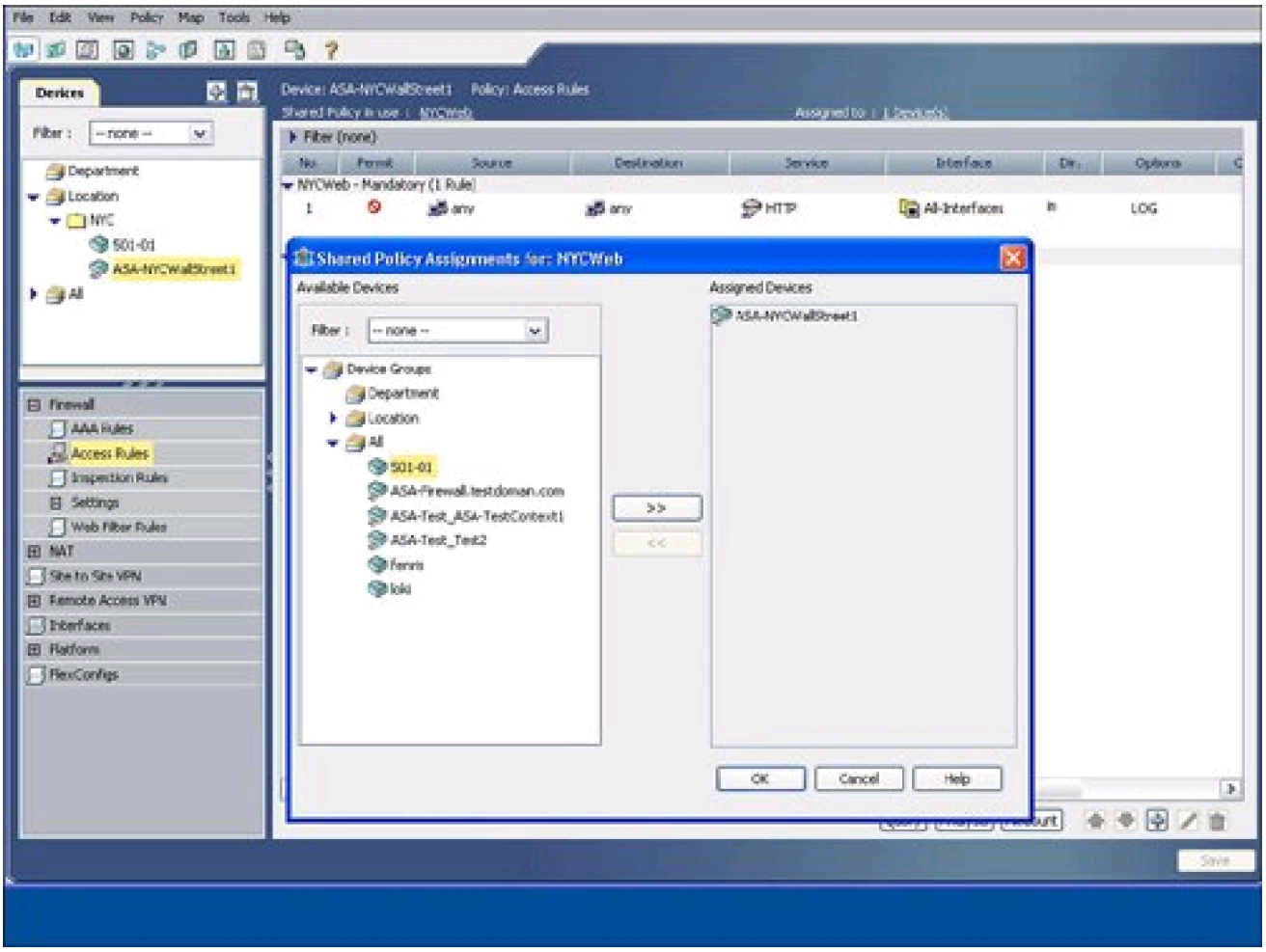
[View full size image]



The shared policy in the example shown in Figure 9-10 is named NYCWeb Policy and is composed of all access control list (ACL) rules in the rule table for a particular device. To apply NYCWeb Policy to multiple devices, select the policy assignment option and select the devices, group of devices, or all device options.

Figure 9-10. Assign Shared Access Control List (ACLs) Rule Policy to Multiple Devices

[View full size image]



Invoking the Policy Query

As you have learned in this chapter, the Cisco Security Manager product provides the flexibility to apply a policy from one device to a group of devices. The end configuration of a device can be the result of several applied security polices. The access control list (ACLs) rule table for a device will display all the applied policies to that device. Cisco Security Manager contains a policy query function to indicate what specific policies have been applied to a device. The policy query function is invoked from the bottom of the firewall access control list (ACLs) rule table. Invocation of the policy query function enables the user to interactively display any particular rule combinations that have been configured for the device. Examples of the rule types that can be used in a policy query include the following:

- **AAA rules** The AAA rules determine what traffic will be sent to the AAA server for authentication.
- **Access rules**access control list (ACLs) rules have been discussed in this chapter and previously in this book.
- **Inspection rules** Inspection rules are protocol or application inspection rules like the kind you learned about in Chapter 3, "Cisco Adaptive Security Appliance Overview," for HTTP protocol inspection.
- **Web filter rules** Web filter rules determine what traffic will be sent from the device to an external web filter URL server.

Figure 9-11 provides an example of the type of information that can be used in a policy query for a device. A policy query is initiated by selecting the Query button at the bottom of the rule table for a device. This example is for a policy query of the access control lists (ACLs) that match a particular source, destination, service, and interface query. Wildcards can also be used for the fields in a policy query. Both full-matches and partial matches of a query are displayed. Figure 9-12 displays the result of the policy query and the matching access control list (ACL). In addition to Policy Query, there is also the rule analysis and hit count functions available in the access control list

(ACL) rule table for a device.

Figure 9-11. Policy Query Definition

[View full size image]

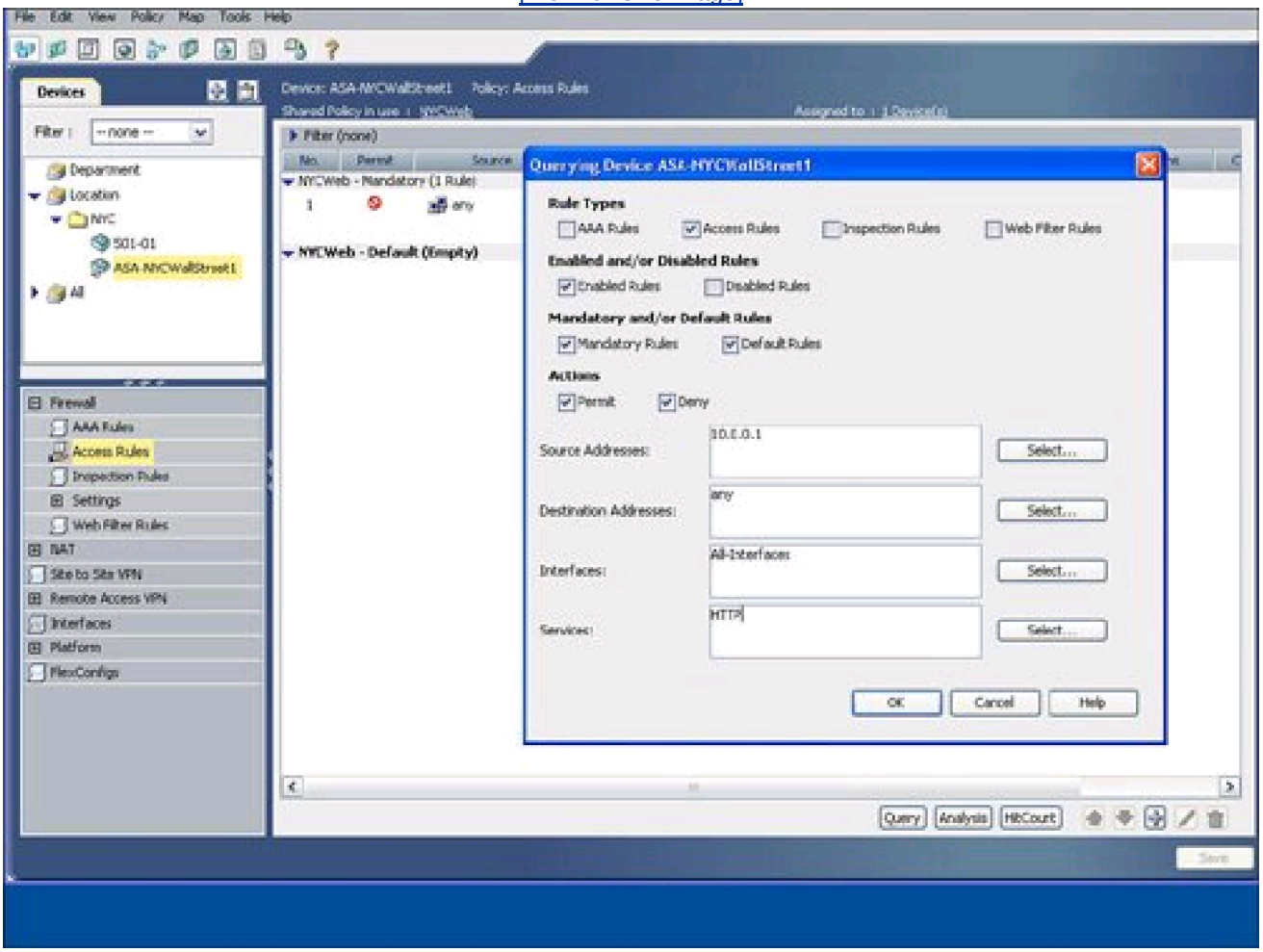
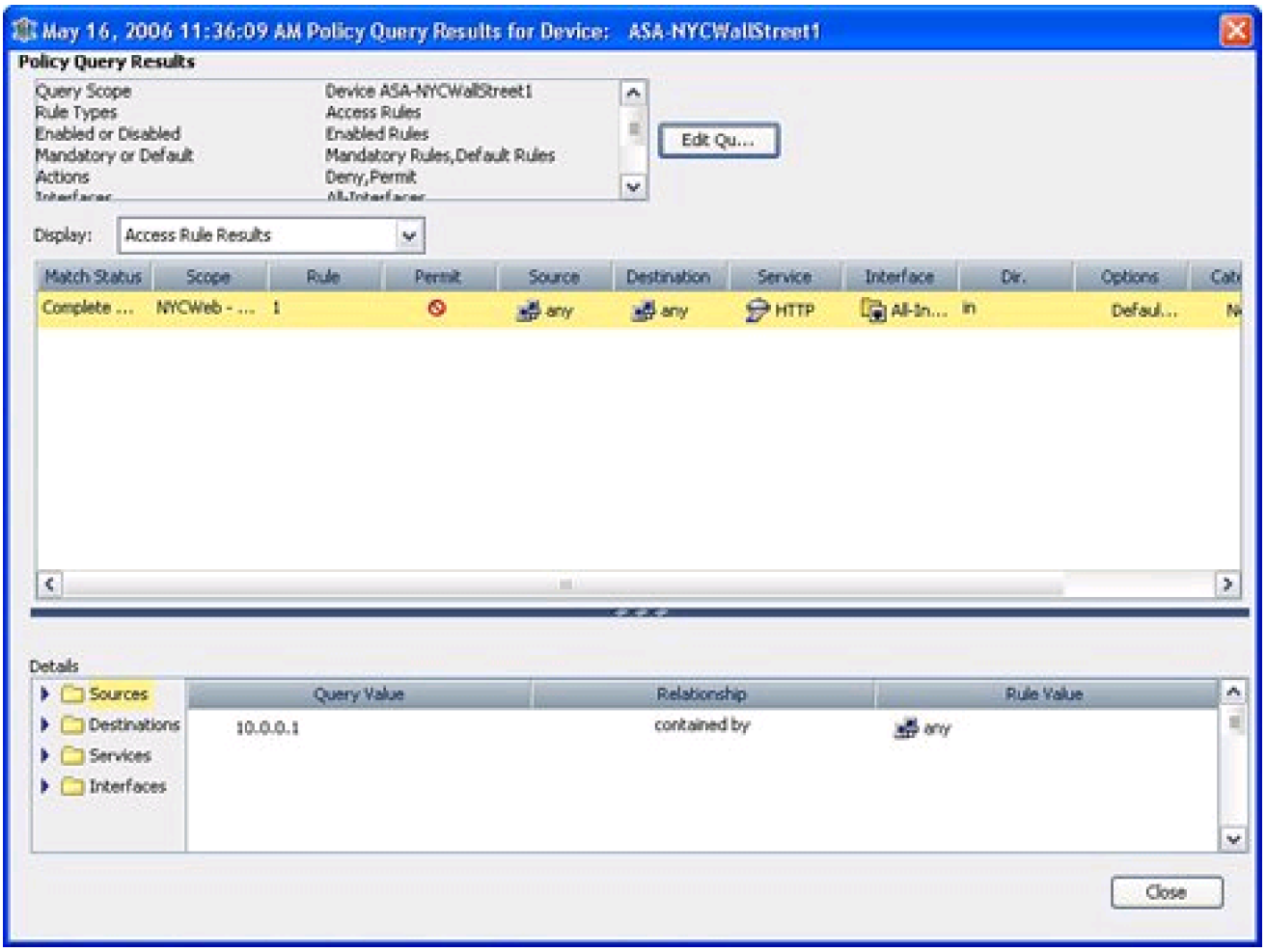


Figure 9-12. Policy Query Results

[View full size image]

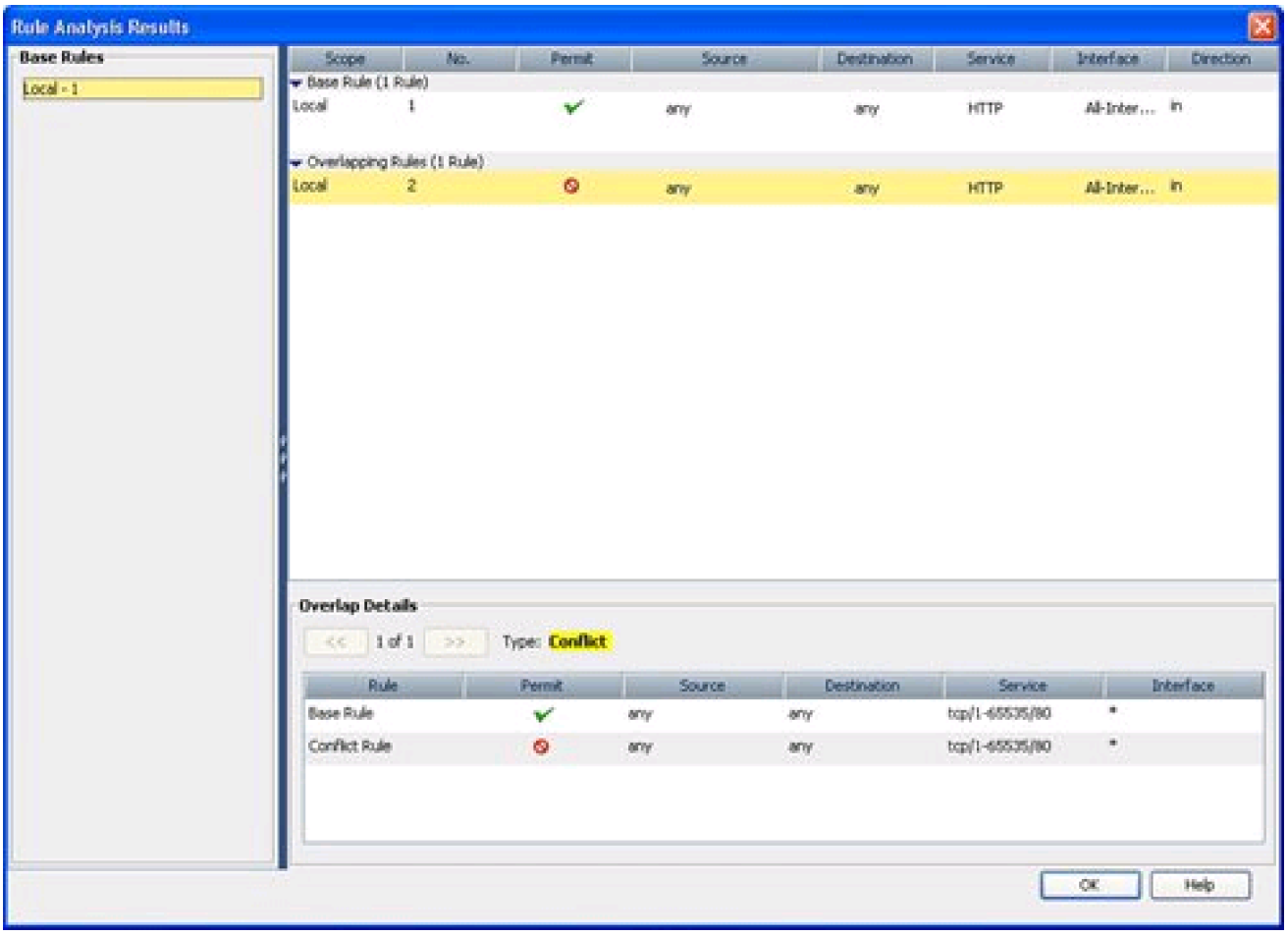


Using Analysis and Hit Count Functions

The Analysis and Hit Count buttons are located next to the Query button at the bottom of the access control list (ACL) rule table for a device. The Analysis function performs an analysis on the access control list (ACL) rules in the rule table for the device. The rule Analysis function will display access control list (ACL) rules that conflict or overlap. For example, say that someone has configured a rule to permit any traffic to the web server destination object for web service (in other words, permit source of any destination of "web server" object for service of HTTP). Let's also say that several weeks later another admin added a rule to deny any traffic to the web server destination object for web service further down in the rule table. The Analysis function would display that these rules are in mutual conflict. An example of how Analysis would display a conflict for these access control list (ACLs) rules is provided in Figure 9-13.

Figure 9-13. Analysis

[View full size image]



The Hit Count function displays how many times the access control list (ACLs) has been "hit" or triggered on the device. Hit Count statistics are very valuable in debugging scenarios because the user can see which access control list (ACLs) rules are being used on the device to determine which access control list (ACLs) rule is affecting network traffic. The Hit Count functionality is reset to zero when the device is rebooted. The Hit Count utility in the Cisco Security Manager also displays a delta or the number of times that the access control list (ACLs) rule has been triggered on the device since the last time the Hit Count utility was used for that device. In the previous example of the analysis of an access control list (ACLs) rule conflict, one rule would never receive any hits or be triggered on the device because it would be in conflict or superseded by the other conflicting and higher-priority rule.

PREV NEXT

Map View

Cisco Security Manager features an easy-to-use topology map to manage a network, including networks that are self-defending. Several default background maps are provided, and a customization feature enables users to create their own background map on the topology by importing a JPG, BMP, or GIF file. To access a topology map, click the Map View icon, which is the second icon on the left and next to the Device View icon on the main homepage. Figure 9-14 displays an example of how to launch the map view.

Figure 9-14. Launch Map View

[View full size image]

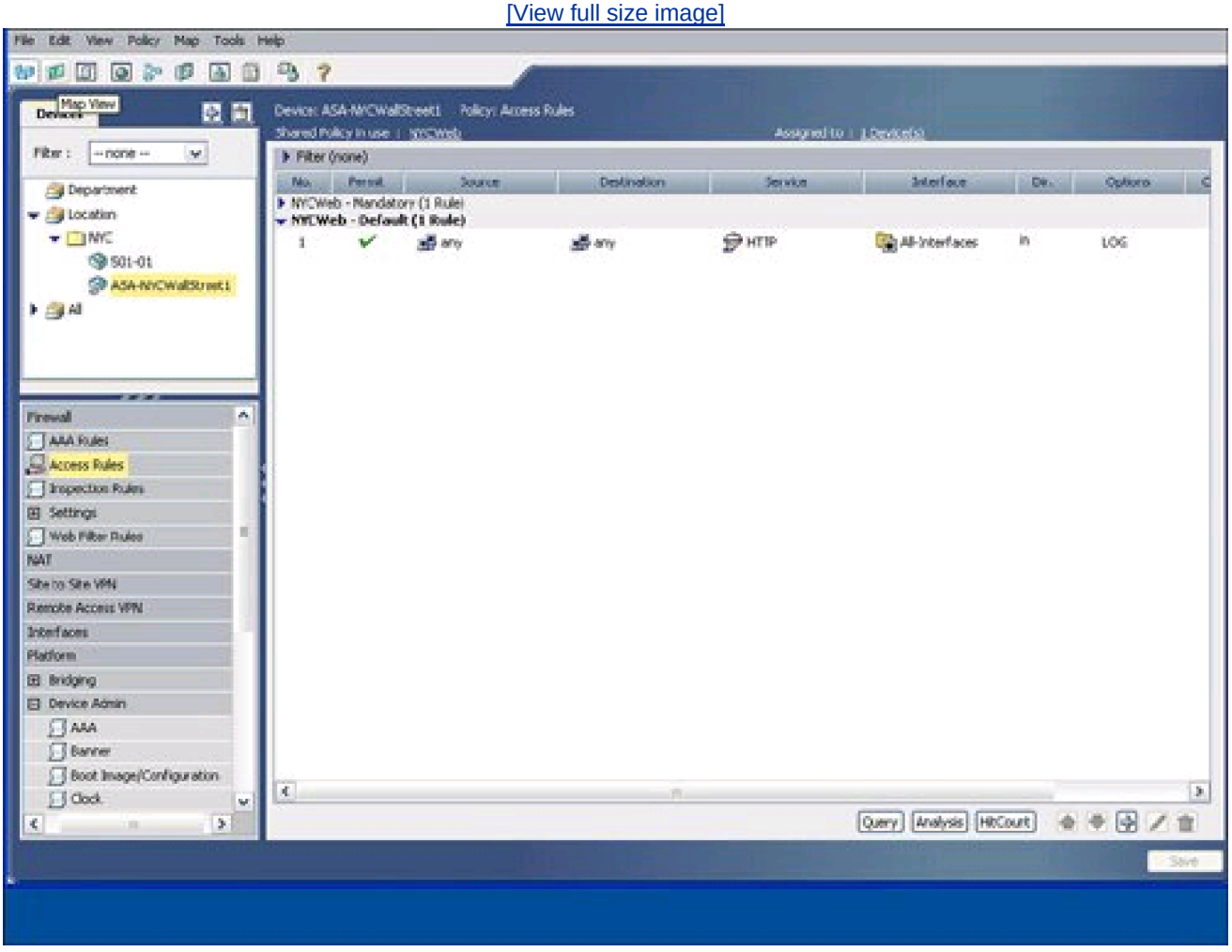
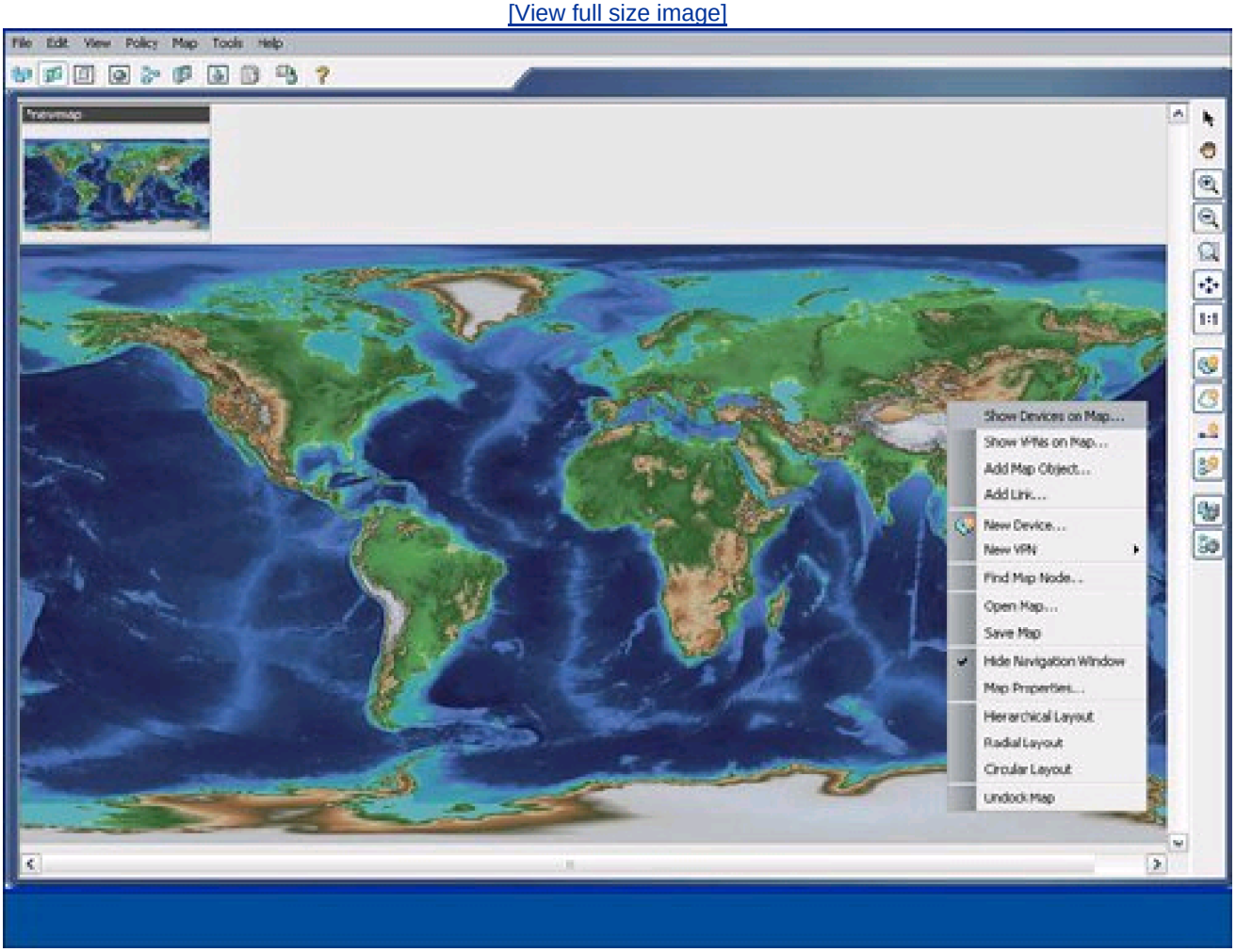


Figure 9-15 displays a sample topology map background. Cisco Security Manager uses a right-click methodology like many other Windows applications. The drop-down list that appears by right-clicking directly on the topology map enables you to add a device or change the background map.

Figure 9-15. Topology Map Background

[View full size image]



As you learn in the next sections, devices and other nodes like networks and hosts can be added to the topology map. You also learn how to configure a firewall from the topology map.

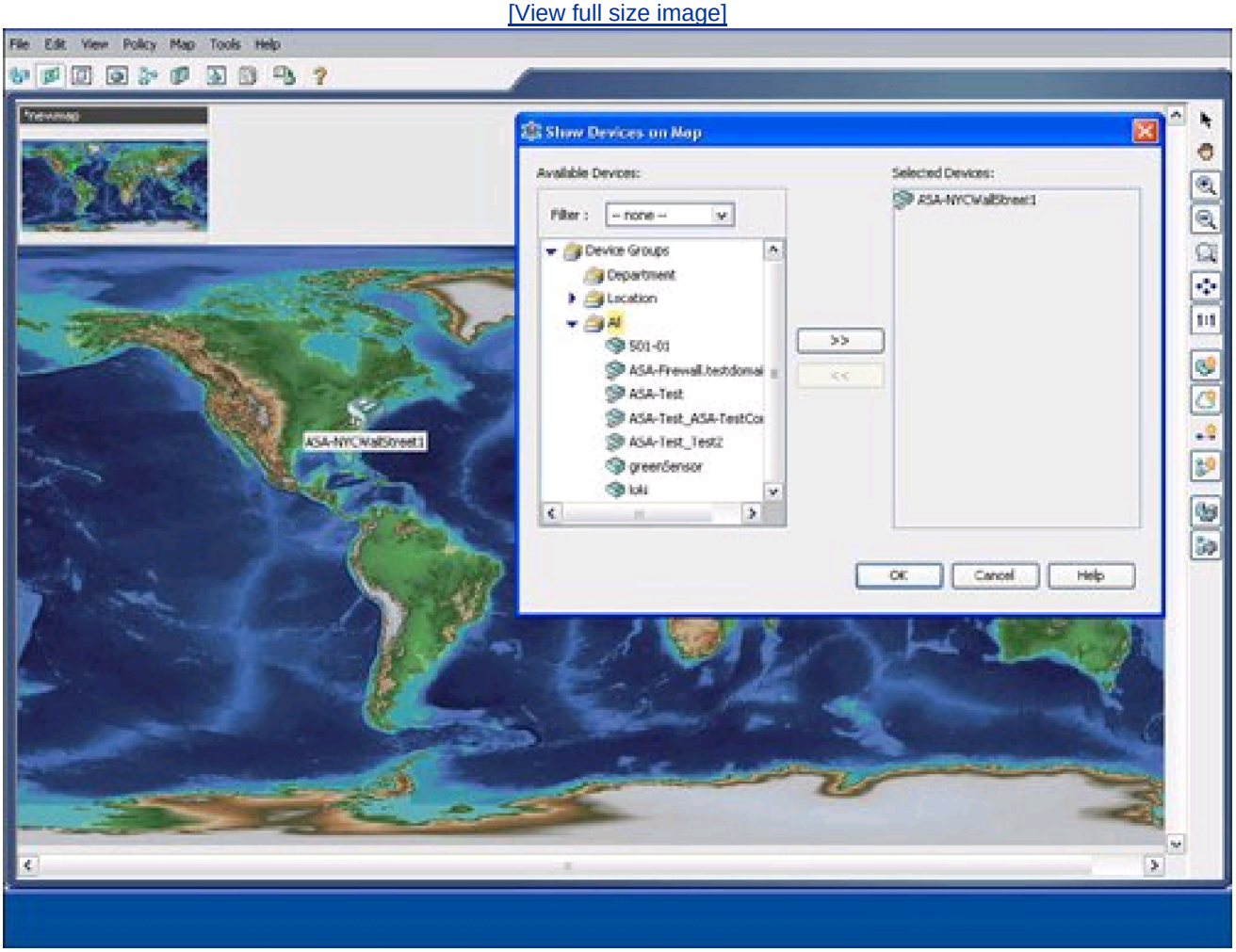
Showing Devices on the Topology Map

Cisco Security Manager provides a mechanism to easily add devices from device groups to the topology map. Users can right-click on the topology map to show a device to the topology map by using the Device Selector option from the drop-down menu after the right-click select. The show device feature for a topology map involves displaying a device that is already imported into the Cisco Security Manager. The New Device option is designed to add or import a new device into Cisco Security Manager directly through a topology map.

Figure 9-16 displays an example of showing a device on the topology map by selecting the Show Devices on Map option. The user may manually place the device at the desired location on the map, for example a security appliance at the Wall Street office may be placed in the NYC region on the map. The show device option will also add the networks that are directly connected to each interface on the device to the topology map.

Figure 9-16. Show Device on the Topology Map

[View full size image]

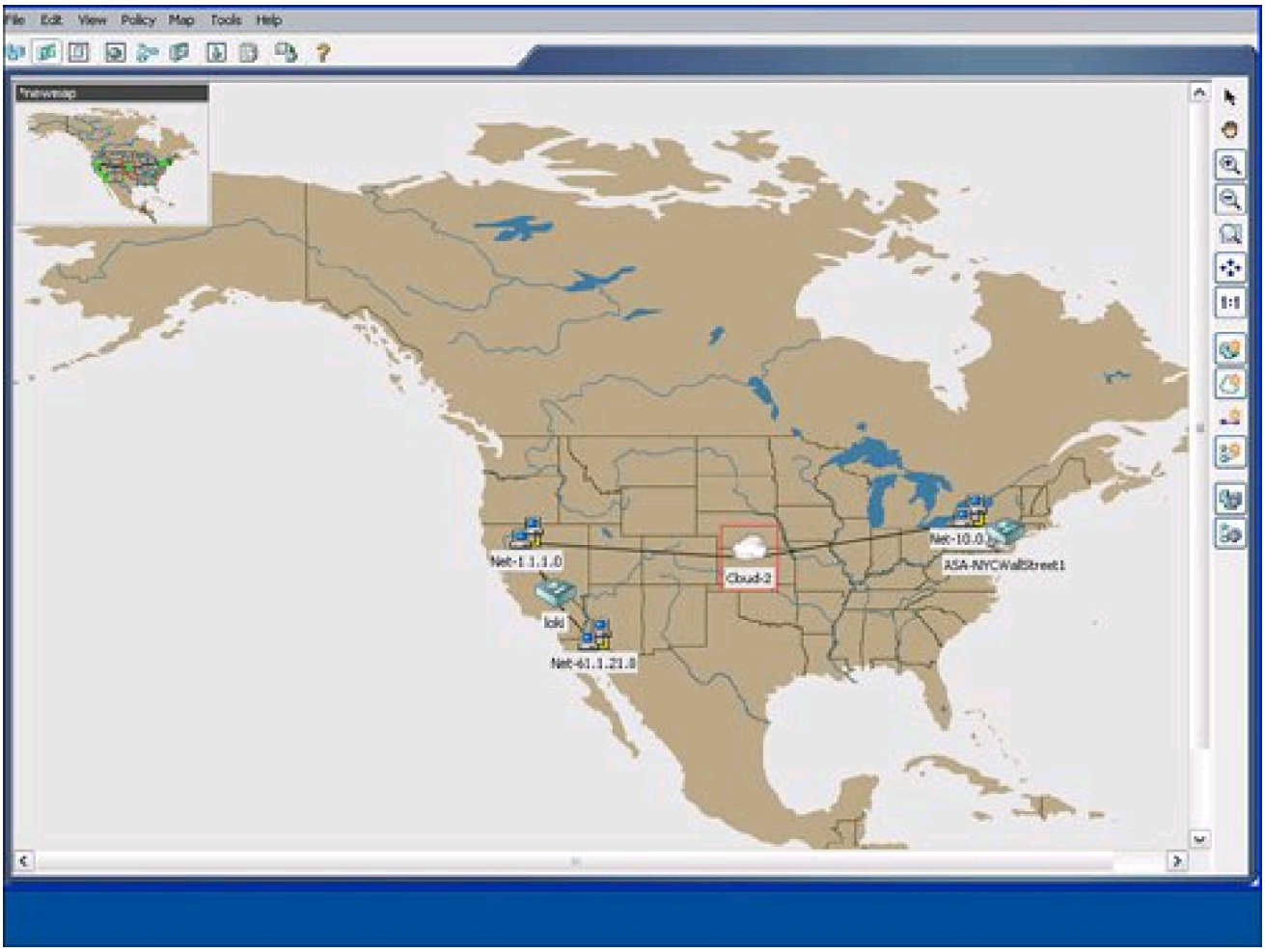


Adding Cloud Networks and Hosts to the Topology Map

The Cisco Security Manager examines the interface IP addresses to determine if devices are located on the same subnet. As shown in Figure 9-17, the Cisco Security Manager features the Add Link icon on the right side of the map to draw the connections between devices on the map. If the user tries to add a link between two managed devices on the map that are not on the same subnet, the Cisco Security Manager will create a cloud network between the devices to indicate that the devices are not on the same subnet.

Figure 9-17. Create a Link Between Devices on the Topology Map

[View full size image]



The process to manually add additional networks and hosts to the topology map is initiated by selecting the Add Map Objects to Map icon on the right-hand side of the topology map. Networks and hosts can be manually defined, or they can be selected from existing network objects. Network objects can be used in the access control list (ACLs) rule table and in other configuration options in the Cisco Security Manager. Hosts are typically nonmanaged devices to the Cisco Security Manager and can be added to a topology map to help create a visual picture of the management and critical resources in the self-defending network.

Configuring Firewall Access Control List (ACLs) Rules from Topology Map

The "Device View" section of this chapter detailed how to add an access control list (ACLs) to a device from the device view. You can also configure access control list (ACLs) rules on a firewall device from a topology map in the map view. The topology map view is a good fit for smaller networks or for security or network operators who prefer to view their network graphically with a topology map. In addition to smaller networks, topology maps can also be a good fit for the commercial or smallmedium business customers.

From the topology map, a user can select a firewall by right-clicking it and then select the firewall access control list (ACLs) option for it. Figure 9-18 provides an example of how right-clicking the ASA-NYC-WallStreet1 firewall icon enables the user to select the access-rules configuration option for that device. Figure 9-19 displays an example of the rule table for that firewall. The access control list (ACLs) rule table for the device that is launched from the topology map is identical to the access control list (ACLs) rule table that is displayed for the device in the device view, as discussed previously in this chapter. Users can display, add, edit, or delete access control list (ACLs) rules for a device directly from the topology map. Users can also access the advanced functions of the access control list (ACLs) rule table, including policy query, rule analysis, and access control list (ACLs) hit count.

Figure 9-18. Configure Access Control List (ACLs) Rules from the Topology Map

[View full size image]

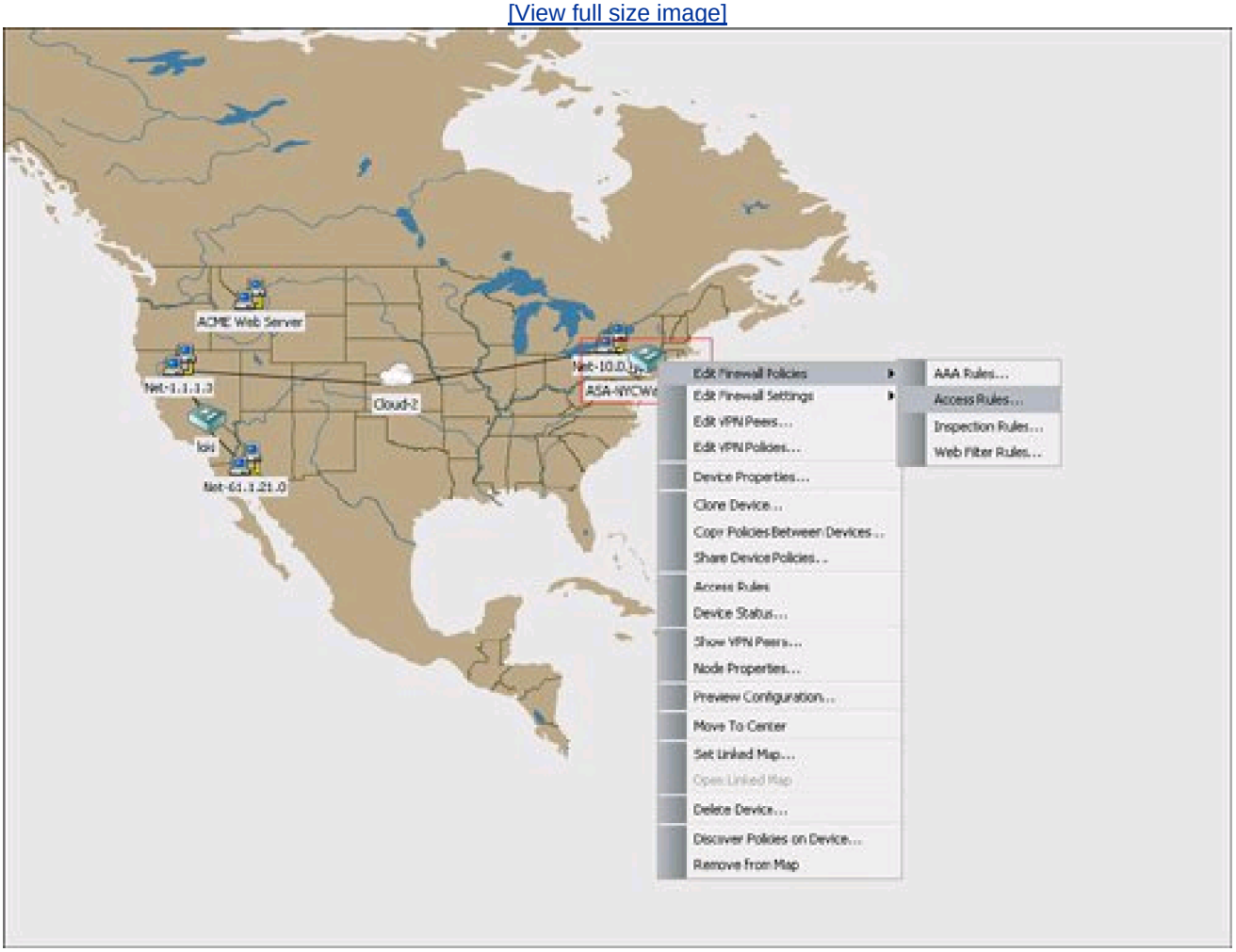
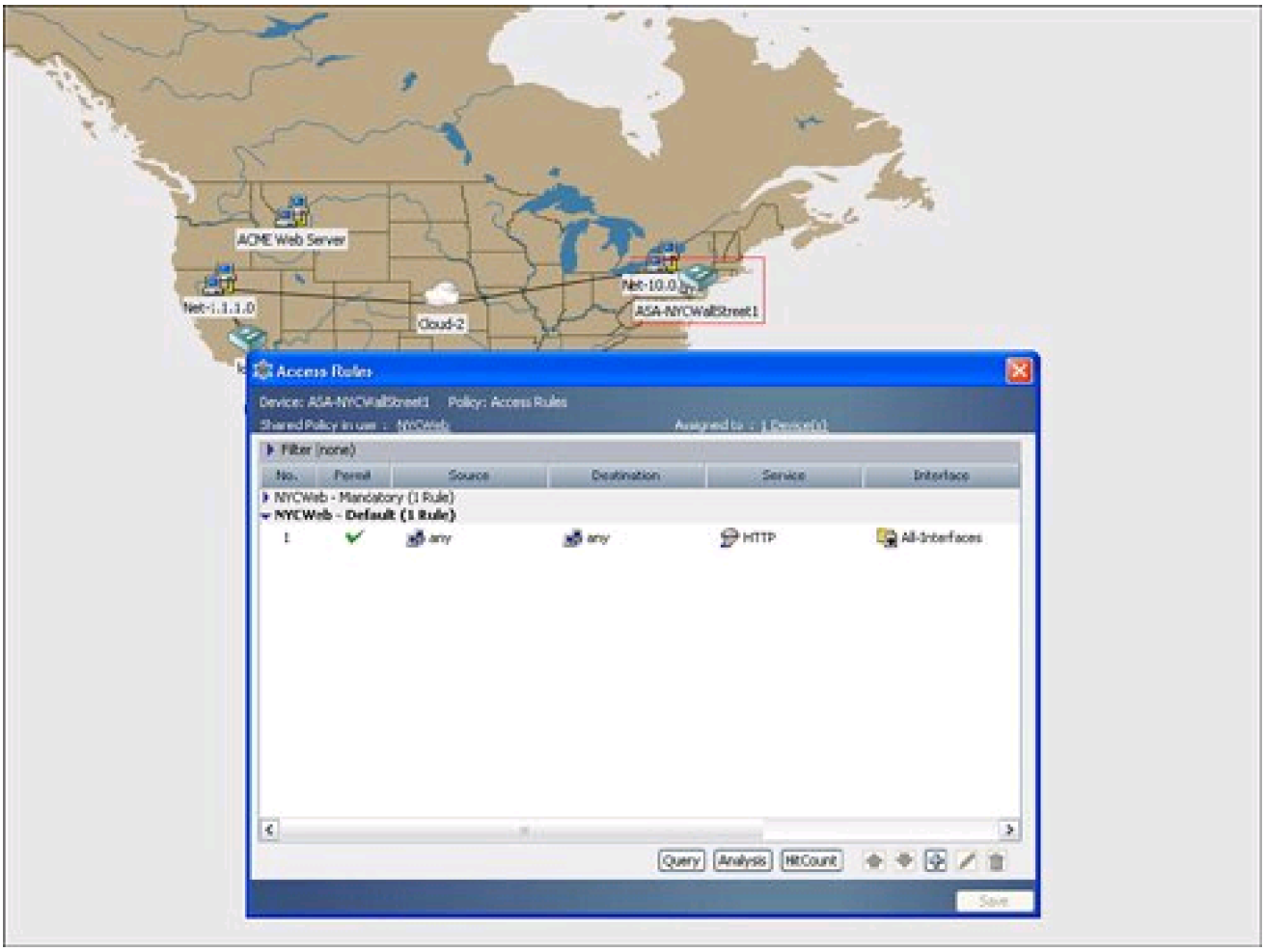


Figure 9-19. Access Control List (ACL) Rule Table for Device from the Topology Map

[View full size image]


ACME Web Server
Net-1.1.1.0
Cloud-2
Net-10.0.0.0
ASA-NYCWallStreet1
Access Rules
Device: ASA-NYCWallStreet1
Policy: Access Rules
Filter (none)
No.
Permit
Source
Destination
Service
Interface
NYCWeb - Mandatory (1 Rule)
NYCWeb - Default (1 Rule)
1
any
any
HTTP
All-Interfaces
Query
Analysis
HitCount
Save

PREV

NEXT

Policy View

The Policy View, the Map View, and the Device View are the three main areas in the Cisco Security Manager to define and enforce the security configuration of a device in a Cisco Self-Defending Network. The previous example in the Device View detailed how a security policy or access control list (ACL) to permit HTTP or web traffic could be copied, or shared between multiple devices. Any shared policies that are created in the device view are also displayed in the Policy View.

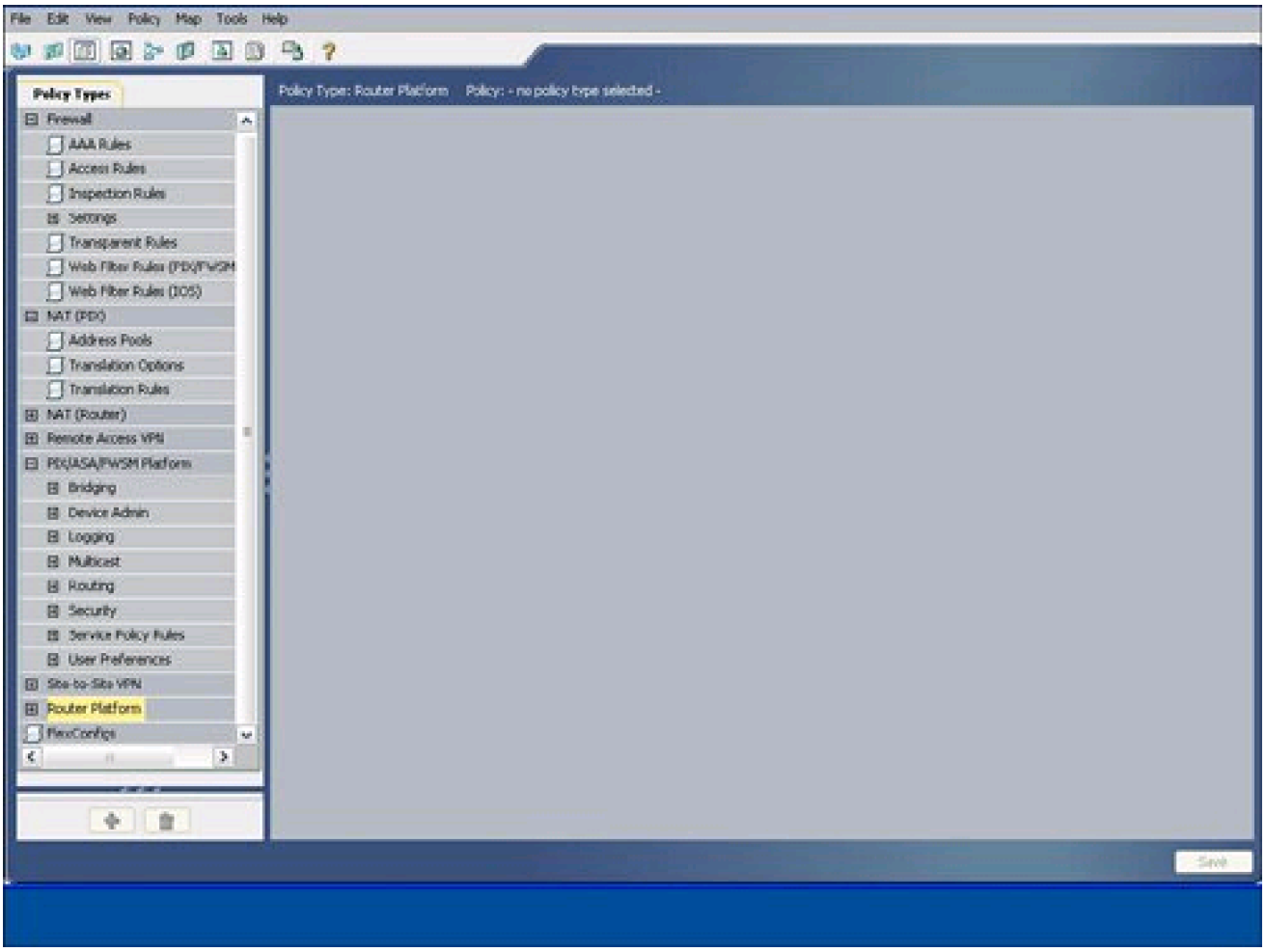
Some users will want to select a device from either the device view or map view and configure a security policy for that device. Other users may want to start by selecting a security policy and then applying this security policy to multiple devices. The Policy View allows the user to first select or create the security policy and then apply the policy to the multiple devices.

The icon to launch the Policy View is located next to the Device View and Map View icons. Policy View, in addition to the Device View and Map View, can also be launched from the view drop-down tab on the main Cisco Security Manager homepage.

Figure 9-20 displays the policy types that can be configured in the Policy View. Policy types include Firewall (access rules, inspection rules, and so on), Network Address Translation (NAT), remote-access VPN, PIX/ASA/FWSM platform (bridging, routing, and so on), site-to-site VPN, router platform (802.1x, NAC, QoS, and so on), and FlexConfigs. FlexConfigs is a CLI template that enables a user to manually define CLI to be deployed to a device or group of devices. There are also predefined FlexConfig templates for common deployments that involve nonsecurity features, including how to configure voice over IP (VoIP) on IOS routers. FlexConfig also supports network and service objects, which can also use the Cisco Security Manager rule tables and VPN components.

Figure 9-20. Policy View Feature Set

[View full size image]

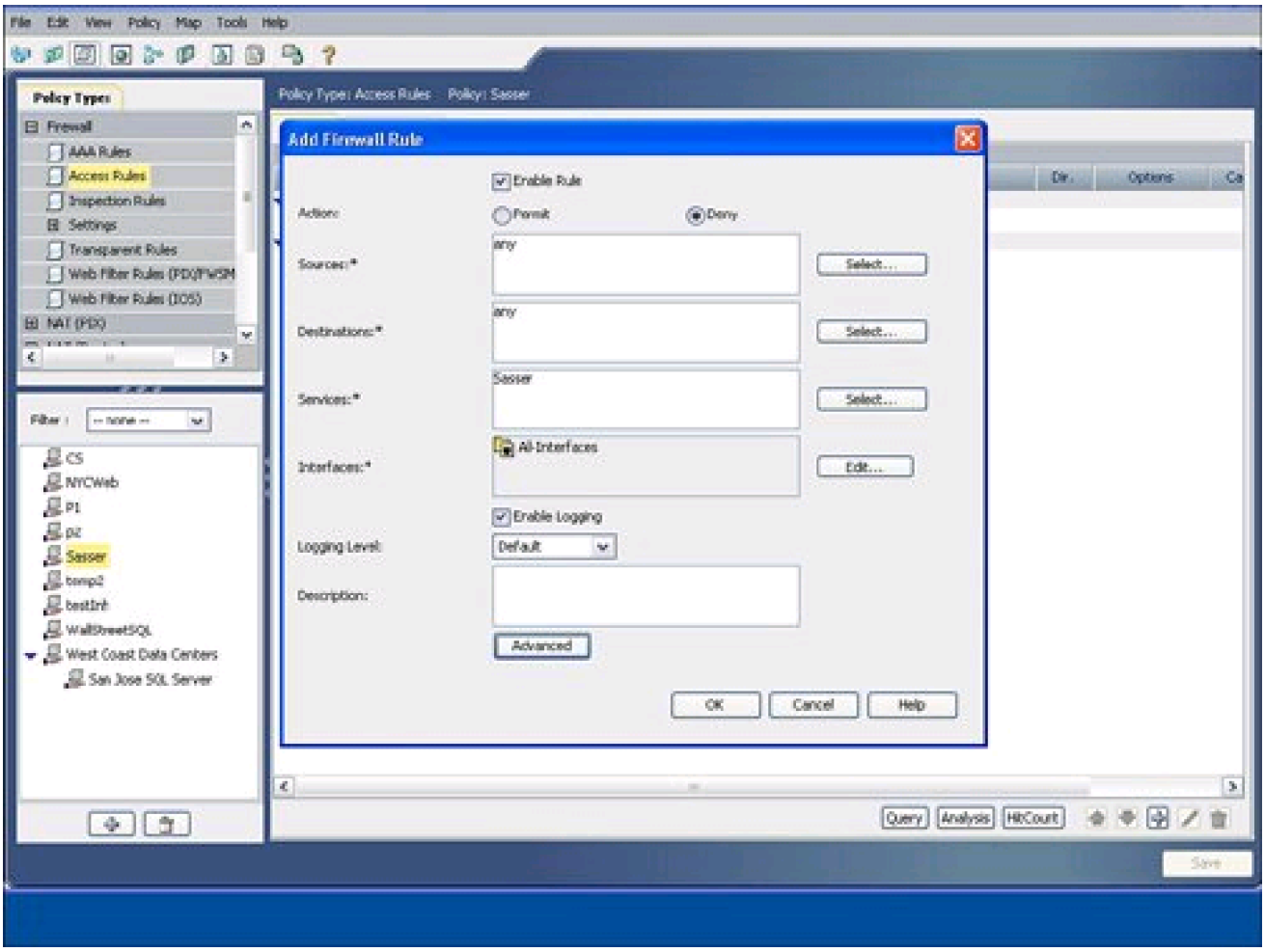


Access Control List (ACL) Rules Security Policy

Let's say that a security operator wants to define a security policy to block the nasty Sasser virus on all devices in the . This operator can simply create a firewall access control list (ACL) rules policy from the Policy View to block Sasser and apply this policy to all interfaces of all devices with a single rule. Figure 9-21 displays how a rule to block the Sasser virus can be configured from the Policy View.

Figure 9-21. Policy Rule to Block the Sasser Virus

[View full size image]

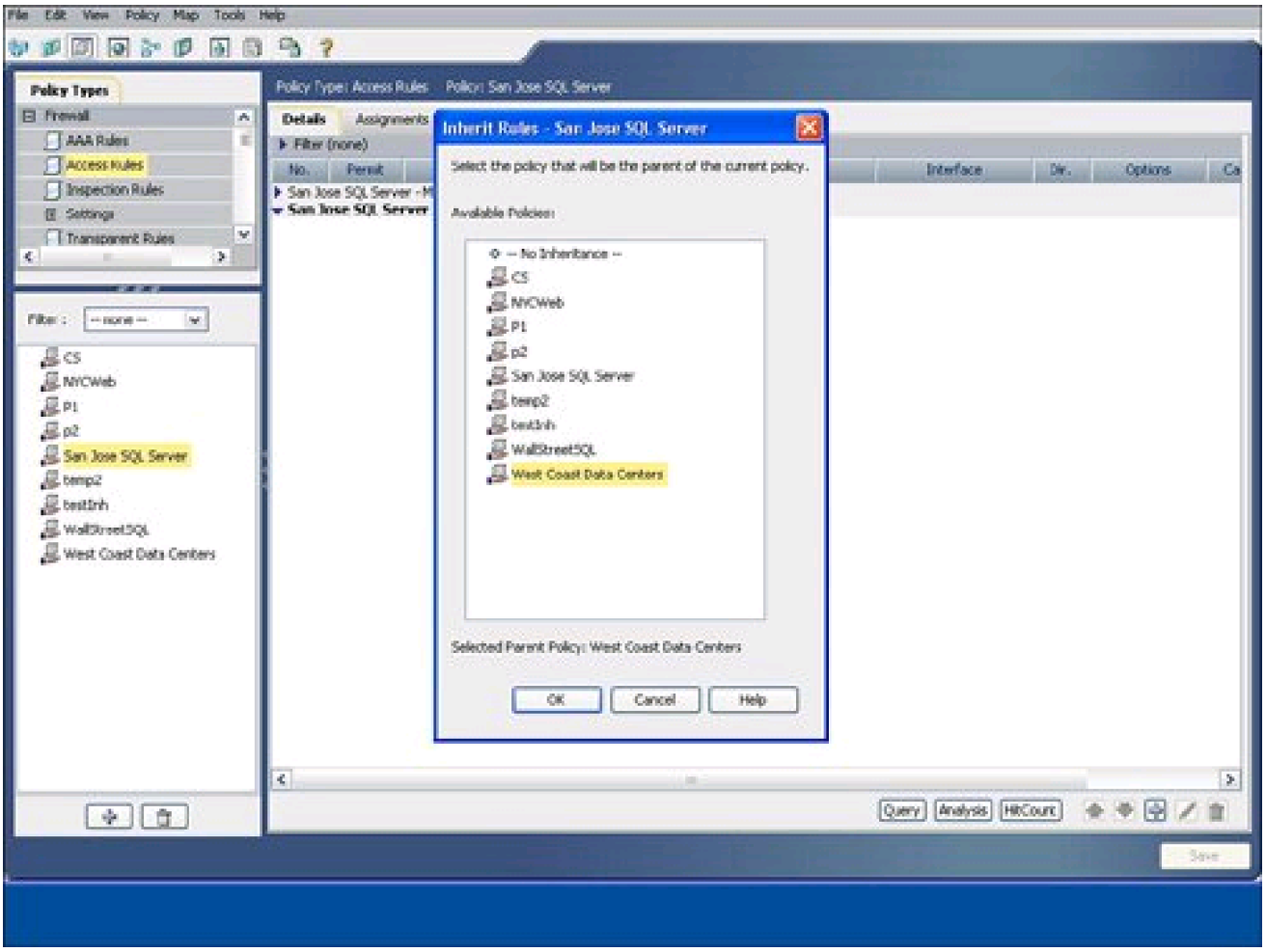


Policy Inheritance and Mandatory Security Policies

Security policies can be applied to all devices, a group of devices, or a single device. Security policies can also be implemented in a hierarchy. For example, say that a user wants to define a security policy to protect an SQL server in a data center in San Jose. The user may want to construct a common high-level security policy and then have the security policy for the San Jose SQL server inherit all the access control list (ACLs) rules defined for the common high-level security policy. The advantage of a policy hierarchy is that the common, course-grained security policy can be defined once and leveraged many times while being maintained or managed in a single, common policy. An example of how to create a policy hierarchy by allowing a policy type to inherit the security policy from a parent policy type is displayed in Figure 9-22.

Figure 9-22. Policy Inheritance

[View full size image]



A security policy created from the Policy View can be either mandatory or default. Mandatory security policies take precedence over default security policies. Mandatory security policies can also be applied to specific administrative privileges. The ability to have mandatory security policies allows for multiple security operations and the network operations group to view and configure the same set of devices. For example, a senior security operator may define the security policy to deny IPSec VPN traffic received on an inside interface as mandatory because it may be required by corporate policy. Another security operator may have the ability to add default security policies to that device but cannot delete or modify the mandatory security policy.

PREV NEXT

IPS Management

Cisco Security Manager also provides centralized IPS management. Cisco Security Manager allows you to add an IPS System device to the centralized device list. Cisco Security Manager also supports the ability to select an IPS device, including the AIP-SSM on the ASA or the IPS feature set on IOS and then select the IPS signatures, like the IPS antispyware signatures that you learned about in Chapter 3. IPS signatures can be applied to a device as demonstrated inChapter 3, or IPS signatures can be copied to a group of devices. The Cisco Security Manager can also import the IPS signatures that were deployed by the Cisco Incident Control Service (Cisco ICS) product discussed in Chapter 4, "Cisco Incident Control Service," on worm mitigation.

Object Manager

Cisco Security Manager enables a wide variety of objects to be created and configured for any supported platform. For example, a single network object can be used in the rule table for a Firewall Services Module (FWSM), ASA, and for the remote-access VPN configuration on an IOS router. The types of reusable objects that are supported in Cisco Security Manager include the following:

- **Networks/hosts** Objects for source/destination fields
- **Service objects** Objects for service fields
- **Service groups** Combination of service objects (for example, IPSec)
- **Interface roles (groups)** Combine interfaces from a device into a group
- **Authentication, authorization, and accounting (AAA) server groups** List of AAA servers for failover, and so on
- **AAA server objects** AAA server details including RADIUS/ TACACS+, and IP
- **Access control lists (ACLs)** Reuse ACL between components including quality of service (QoS)
- **ASA group policy** Define system policy/preferences for ASA
- **Certificate authority (CA) servers** CA configuration
- **Dynamic Host Configuration Protocol (DHCP) servers** DHCP parameters including IP address, timeout, and so on
- **FTP Map** Deep packet protocol inspection of FTP parameters
- **HTTP Map** Deep packet protocol inspection of HTTP parameters (for example, GET)
- **IPSec transform sets** Define AES/3DES, SHA, and so on, for IPSec VPN
- **TCP Map** Deep packet inspection of TCP, including Checksum
- **GPRS Tunneling Protocol (GTP) map** Deep packet inspection of tunneled network packets over 3G phone networks
- **Time range objects** Define ACLs for a specific time range
- **Domain name rules matching** Configuration domain name matching for digital certificates
- **User group** Group configuration for remote-access VPN
- **Traffic flow objects** Define packet matching for deep packet inspection
- **User templates** Templates for CLI tokens
- **Categories** Apply colors to rules and objects to find/filter

Figure 9-23 provides an example of launching the object manager, and Figure 9-24 shows the resulting object management homepage it is displayed in. Note the object manager supports the ability to find and filter objects based upon fields including name, group, and description.

Figure 9-23. Manage Objects

[View full size image]

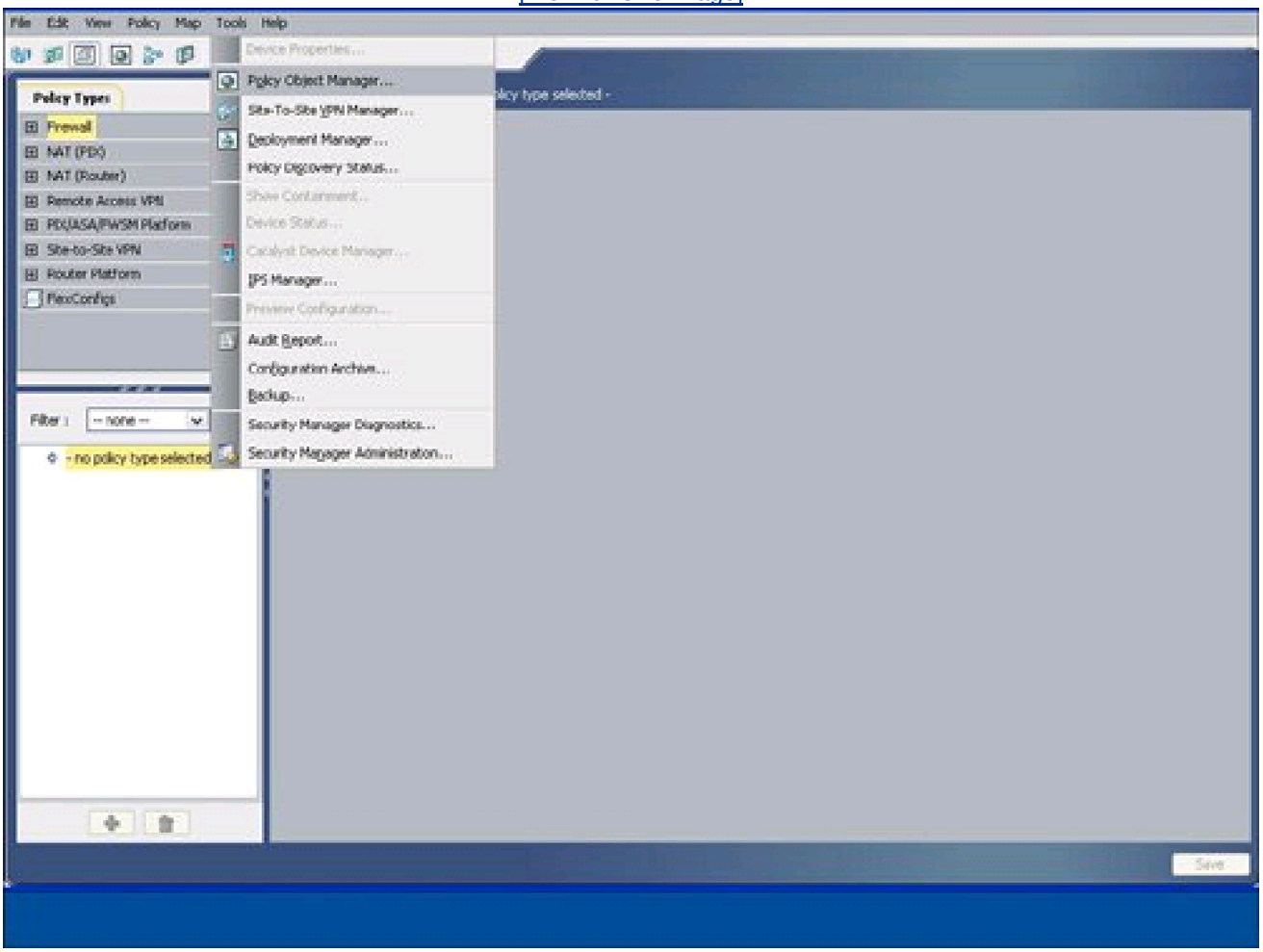
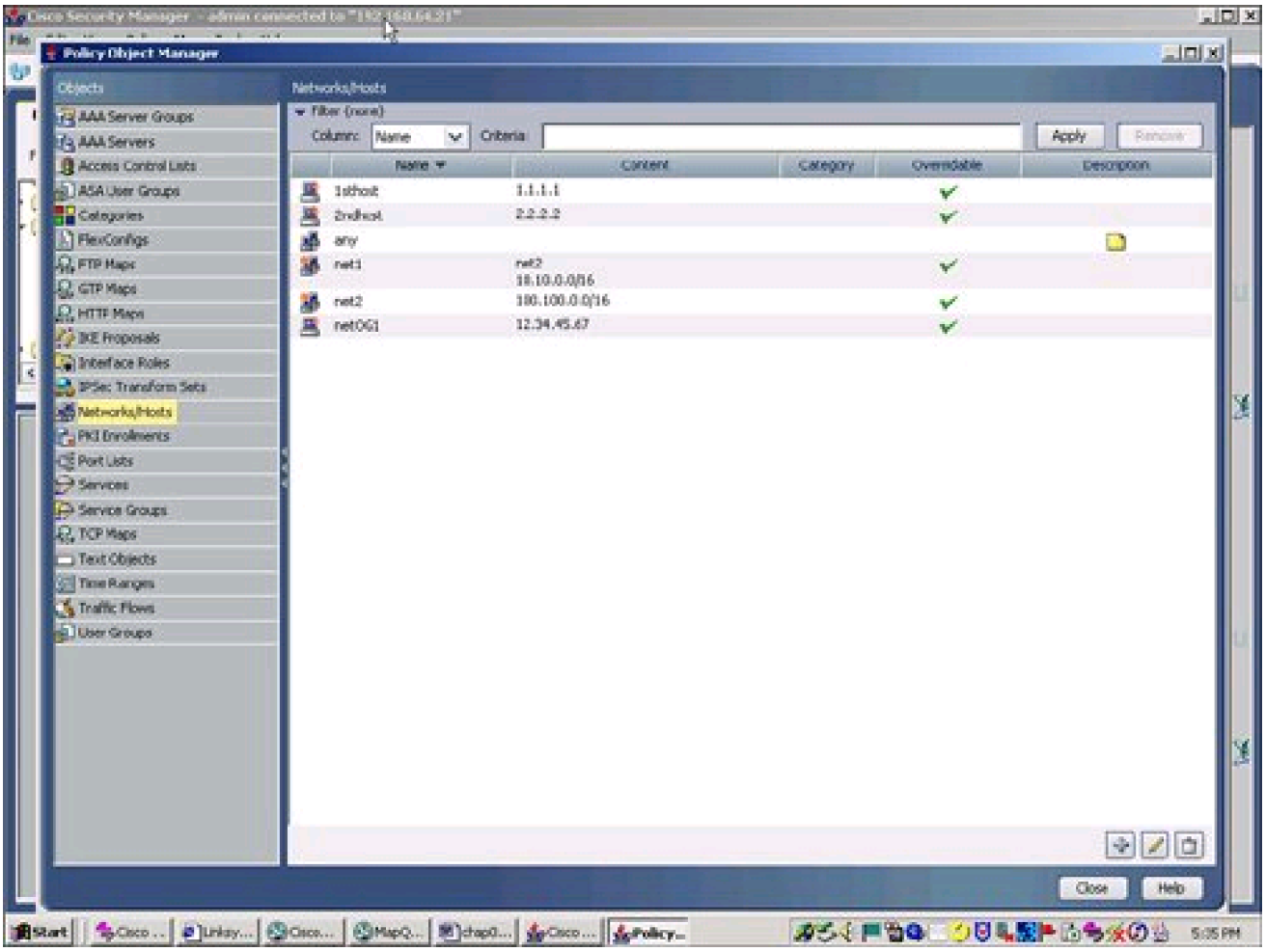


Figure 9-24. Object Homepage

[View full size image]



Network and service objects can be created directly from the access control list (ACLs) rule table, or they can be created directly from the Policy Object Manager. Objects can be nested and contain other objects. Network objects can be a single IP address, a single network, multiple IP addresses, multiple networks, or a collection of objects, or a combination of IP addresses, networks, and objects.

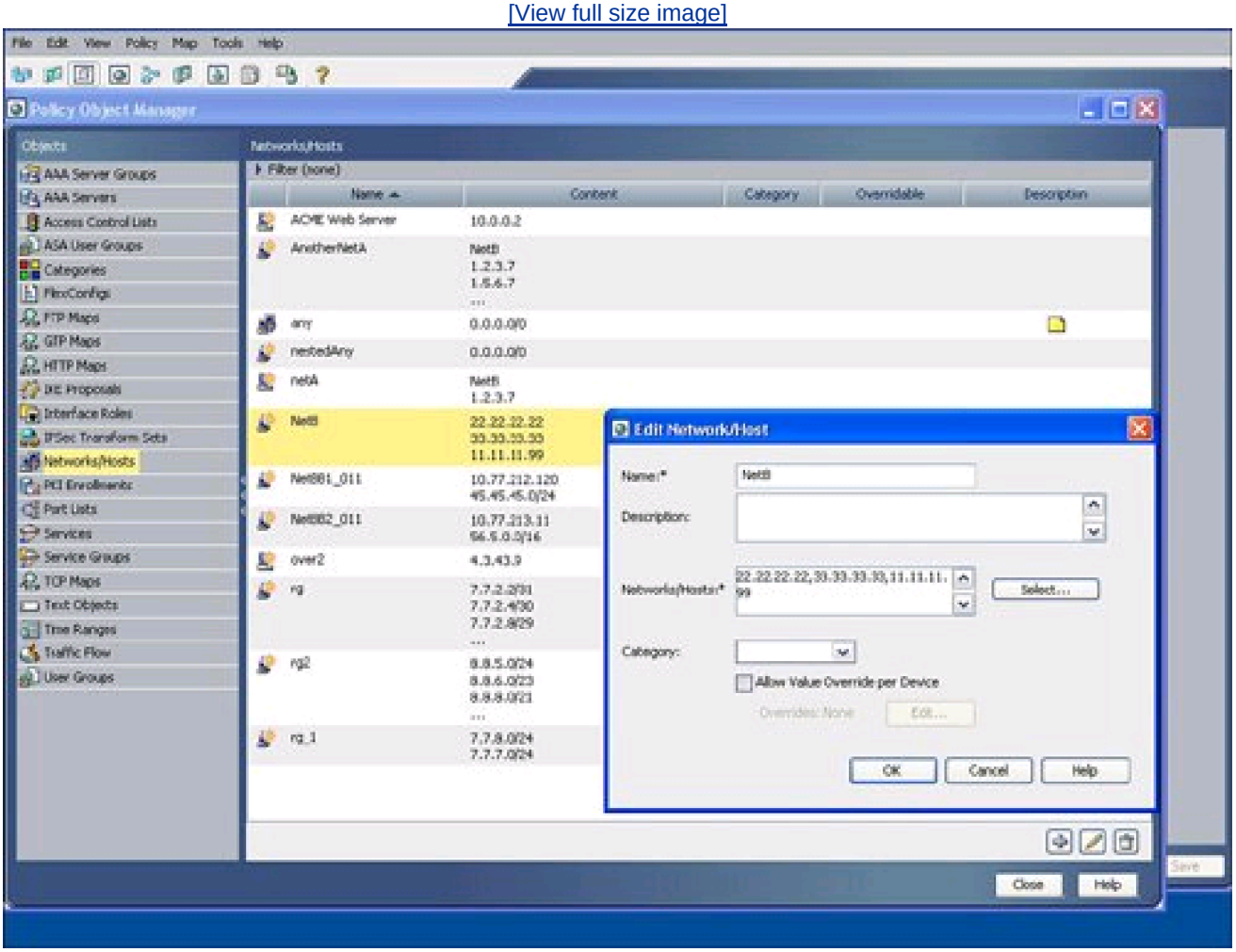
PREV NEXT

Value Override Per Device

Cisco Security Manager contains an object management feature called value override per device. Value override allows the same object name to have different values or contents for different devices. For example, say that the user wants to have a common security policy to allow HTTP from all inside networks to all destinations. A single network object with the entire list of inside networks could be a very large object. A more attractive and more secure approach would be to have a single security policy with a source object named "inside networks" and then have the contents of "inside networks" be a variable that contains only the inside networks that are protected by each device. The per-device object override features allow a single access control list (ACLs) rule with a network object to be defined for multiple devices, but with the contents or value of the network object, such as the "inside network" example, to be defined uniquely for each device. A display of the value override per device check box is displayed in Figure 9-25.

Figure 9-25. Value Override Per Device

[View full size image]



Summary

The Cisco Security Management Suite provides configuration and monitoring of a . The Cisco Security Manager product is the configuration component of the Cisco Security Management Suite, and the Cisco Security MARS product is the monitoring component of the security management suite. Cisco Security Manager is a centralized management product that can configure up to 5000 security devices. Cisco Security Manager supports many of the products previously discussed in this book, including the ASA, IOS routers, and IPS sensors. Cisco Security Manager also supports Catalyst 6500/7600 chassis configuration and security linecard modules, including the FWSM, VPN SPA, and the IPS services linecard module (IPSM).

Cisco Security Manager features three main views: Device View, Map View, and Policy View. The Device View is similar in ease-of-use and scope to that of a device manager, such as the ASA Device Manager (ASDM). The Device View also features the ability to share or copy policies from one device to another. The Map View allows users to place devices and hosts on to a topology map and graphically configure their . The Map View enables a user to select a device from the topology map and configure the device directly from the topology map. The Map View can be advantageous for smaller networks. The Policy View enables the user to select or configure the policy first and then apply the policy to multiple devices. The Policy View is designed to enable the user to configure and apply a single security policy to hundreds or thousands of security devices.

References

Cisco Systems, Inc. Cisco Security Manager 3.0 Data Sheet.
http://www.cisco.com/en/US/products/ps6498/products_data_sheet0900aecd803ffd5c.html

Chapter 10. Cisco Security Monitoring, Analysis, and Response System

Chapter 9 discussed Cisco Security Manager in detail. Cisco Security Manager is the centralized configuration management product for a self-defending network. The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) product is the monitoring and mitigation platform for a self-defending network. Cisco Security Manager creates and deploys configurations to self-defending network devices including Cisco IOS routers, Catalyst 6500/7600 Firewall Services Modules, and Adaptive Security Appliances. Cisco Security MARS complements the Cisco Security Manager by providing best-of-breed monitoring of the self-defending network.

This chapter provides an overview of Cisco Security MARS. You learn about Cisco Security MARS features, the dashboard, how Cisco Security MARS displays a security incident, and how Cisco Security MARS can mitigate an attack or allow a network to be self-defending. This chapter also provides details on Cisco Security MARS integration with Cisco Security Manager, including how to select a syslog from an incident in Cisco Security MARS and receive a display of the access control list (ACL) rule in Cisco Security Manager that created the syslog.

Understanding Cisco Security MARS Features

Cisco Security MARS is different from the conventional Security Information Management Solution (SIMS) or other traditional security monitoring products. Cisco Security MARS offers several advantages based upon the following features:

- Import Netflow data
- Create baseline of normal network traffic
- Import configurations of monitored devices
- Understand traffic flow across Network Address Translation (NAT) boundaries
- Integrated Nessus Vulnerability Scanner input
- Display topology map of network and attack vectors
- Reduce false positives by reporting incidents
- Provide mitigation by deploying configuration to shut specific ports to stop an attack
- Provide mitigation by displaying an access list to stop an attack close the source of the attack

Cisco Security MARS is offered as a turnkey appliance. Cisco Security MARS includes an integrated Oracle database and can handle up to 10,000 events per second. The Cisco Security MARS product line also features different appliance form-factors including a lowend model that supports 500 events per second, excluding Netflow data. A turnkey appliance allows the Cisco Security MARS product to be up-and-running quickly without an extensive installation or tuning process. Cisco Security MARS displays a security incident during an attack, based upon input and events from devices within the selfdefending network. A partial list of the sources from which Cisco Security MARS can accept input and events includes the following:

- Cisco IOS routers
- Cisco Catalyst LAN Switches (Catalyst 0S 6.x)
- Cisco PIX Firewalls
- Checkpoint Firewalls
- Cisco VPN Concentrators
- Netscreen Firewalls
- Cisco IPS Sensors
- Enterasys Dragon IPS Sensors
- Snort IPS Sensors
- ISS IPS Sensors
- eEye REM
- Foundstone
- Cisco Security Agent

- Symantec Anti-Virus
- Cisco ACS
- Windows Host Log
- Solaris Host Log
- Linux Host Log
- IIS Web Server Log
- Apache Web Server Log
- Oracle Audit Logs
- NetApp Logs

Cisco Security MARS has the ability to see the entire self-defending network based upon input and events from the preceding sources. This diverse selection of input, combined with the network configurations and baseline traffic, allows Cisco Security MARS to report on specific, high-level, actionable security incidents rather than displaying and reporting based upon individual and voluminous firewall syslog and IPS Sensor events. Cisco Security MARS also supports a global controller functionality. The global controller provides a centralized management station for multiple Cisco Security MARS local controllers.

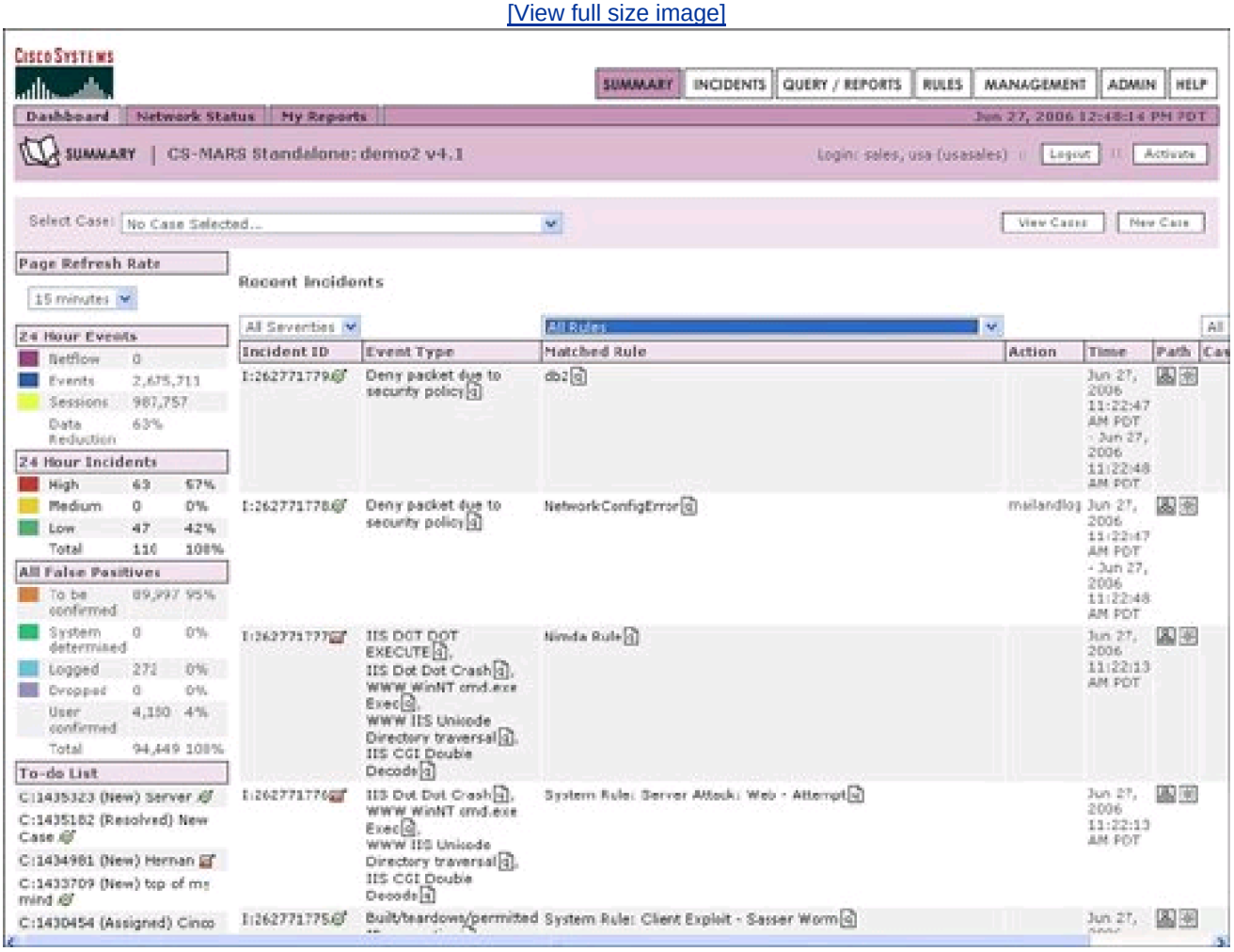
PREV NEXT

Summary Dashboard

Cisco Security MARS uses a web browser for the client GUI. Cisco Security MARS also facilitates the download of Adobe SVG to display the topology graphs. Cisco Security MARS requires Internet Explorer for the web browser and uses HTTPS to ensure secure monitoring. After a successful logon to Cisco Security MARS, you are presented with the dashboard under the Summary tab. Figure 10-1 displays an example of the top of the Cisco Security MARS dashboard.

Figure 10-1. Cisco Security MARS Dashboard

[View full size image]



The dashboard includes a summary of security incidents, or a high-level indication of a possible network attack or vulnerability based upon input from devices and hosts in the self-defending network. In addition to incidents, the dashboard also includes information on events within the last 24 hours, false positives that are detected, a hotspot, and an attack diagram including source and destination of the attack.

Incidents

The focal point of the Cisco Security MARS dashboard is a list of recent incidents. In addition to the dashboard, incident information is also available by selecting the Incident tab at the top of the Cisco Security MARS GUI. All incidents are supplied with an incident ID, event type, matched rule, time, and path information. Figure 10-2 provides an example of an incident ID selected from the dashboard (highlighted). In addition to selecting an incident from the Summary Dashboard, incidents can also be selected from the Incident tab at the top of the Cisco Security MARS GUI. Figure 10-3 displays the resulting information from the incident selection in Figure 10-2. Figure 10-3 also provides an example of how an incident is displayed with the matching rule that triggered the incident and the subcomponents of the incident. Subcomponents of the incident include the following fields:

- Event Type
- Source IP/Port
- Destination IP/Port
- Protocol
- Time
- Reporting Device
- Reported User
- Path/Mitigate
- False Positive

Figure 10-2. Select Incident from Dashboard

[View full size image]

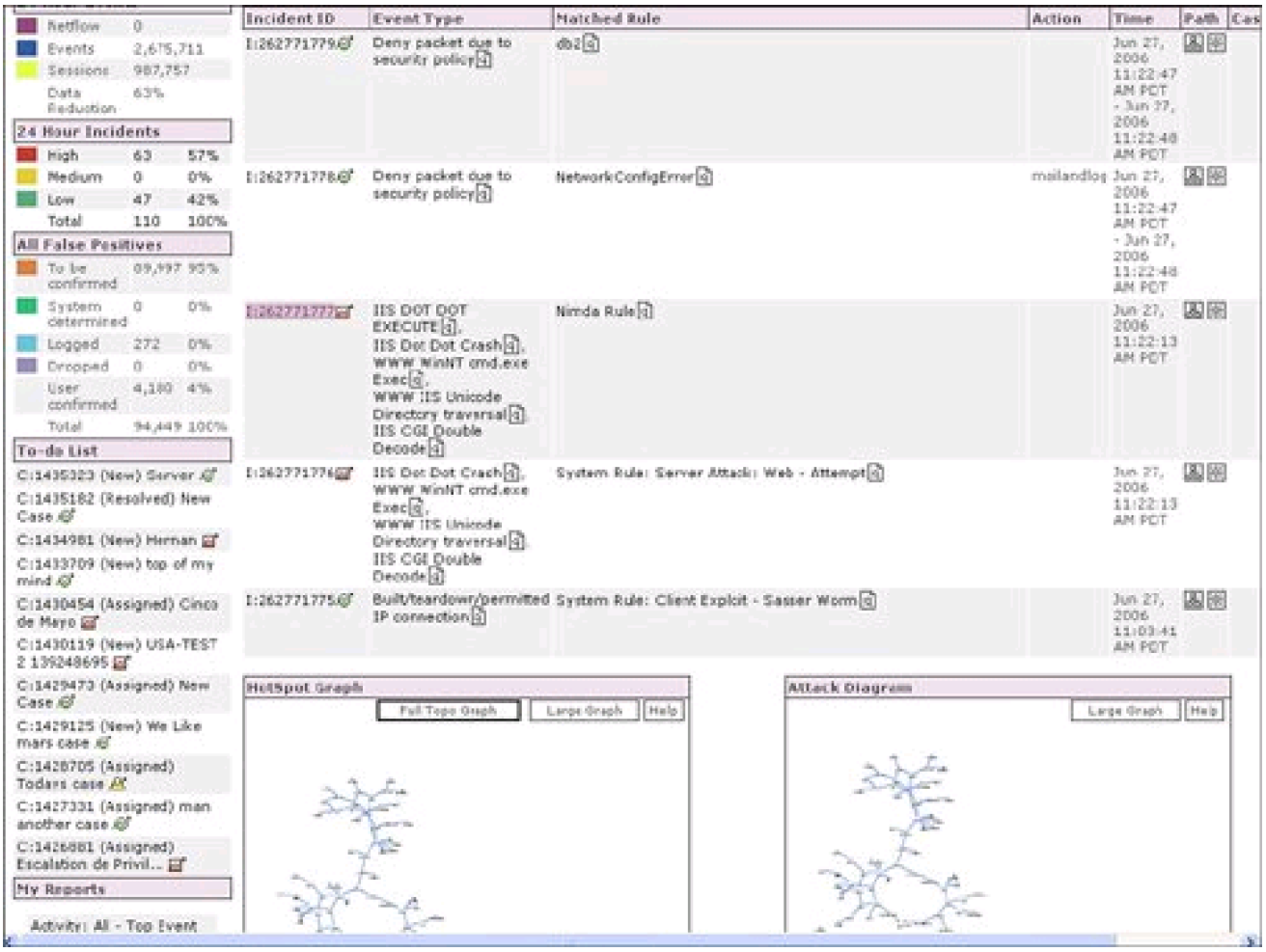
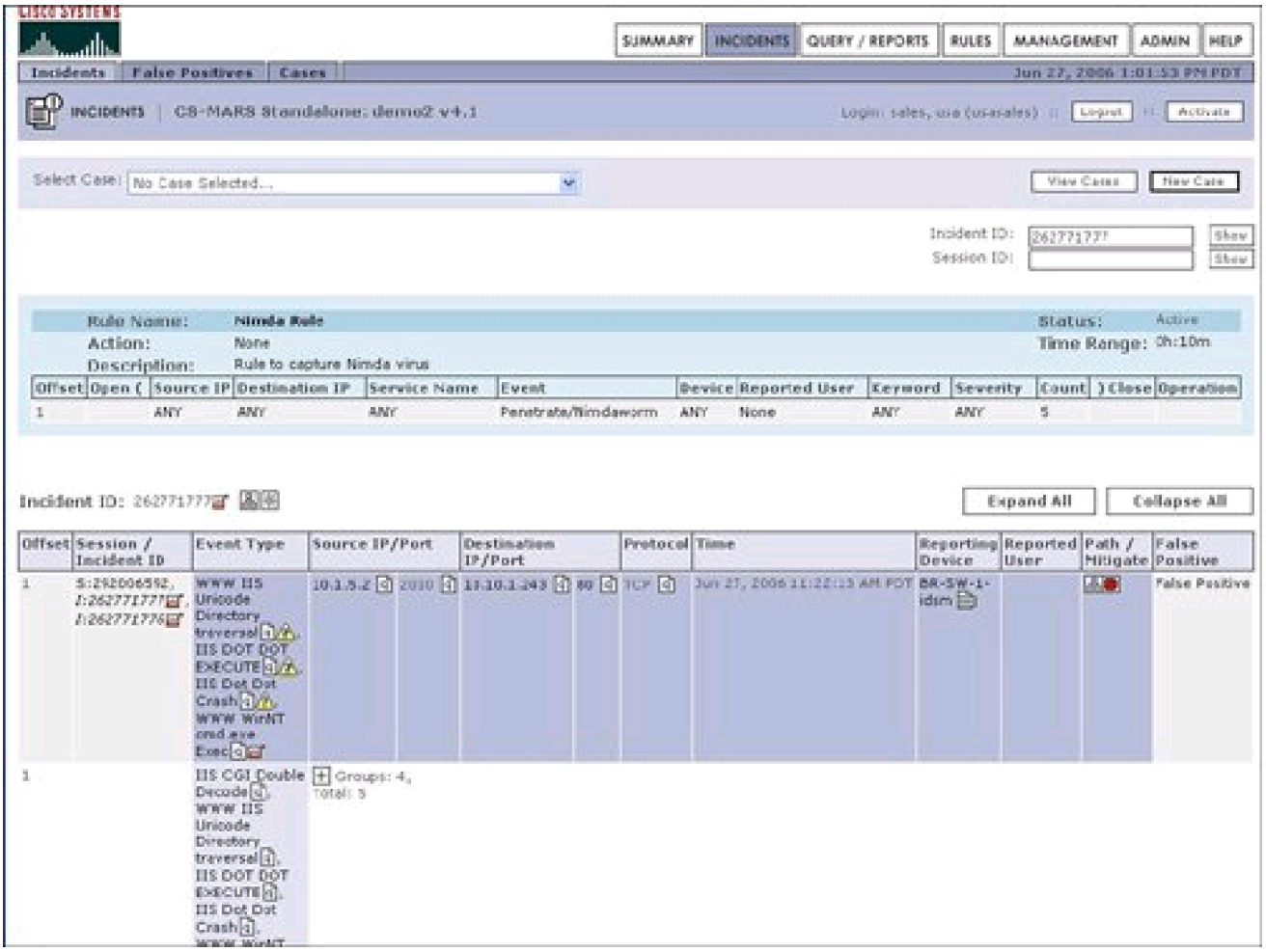


Figure 10-3. Incident Details

[View full size image]



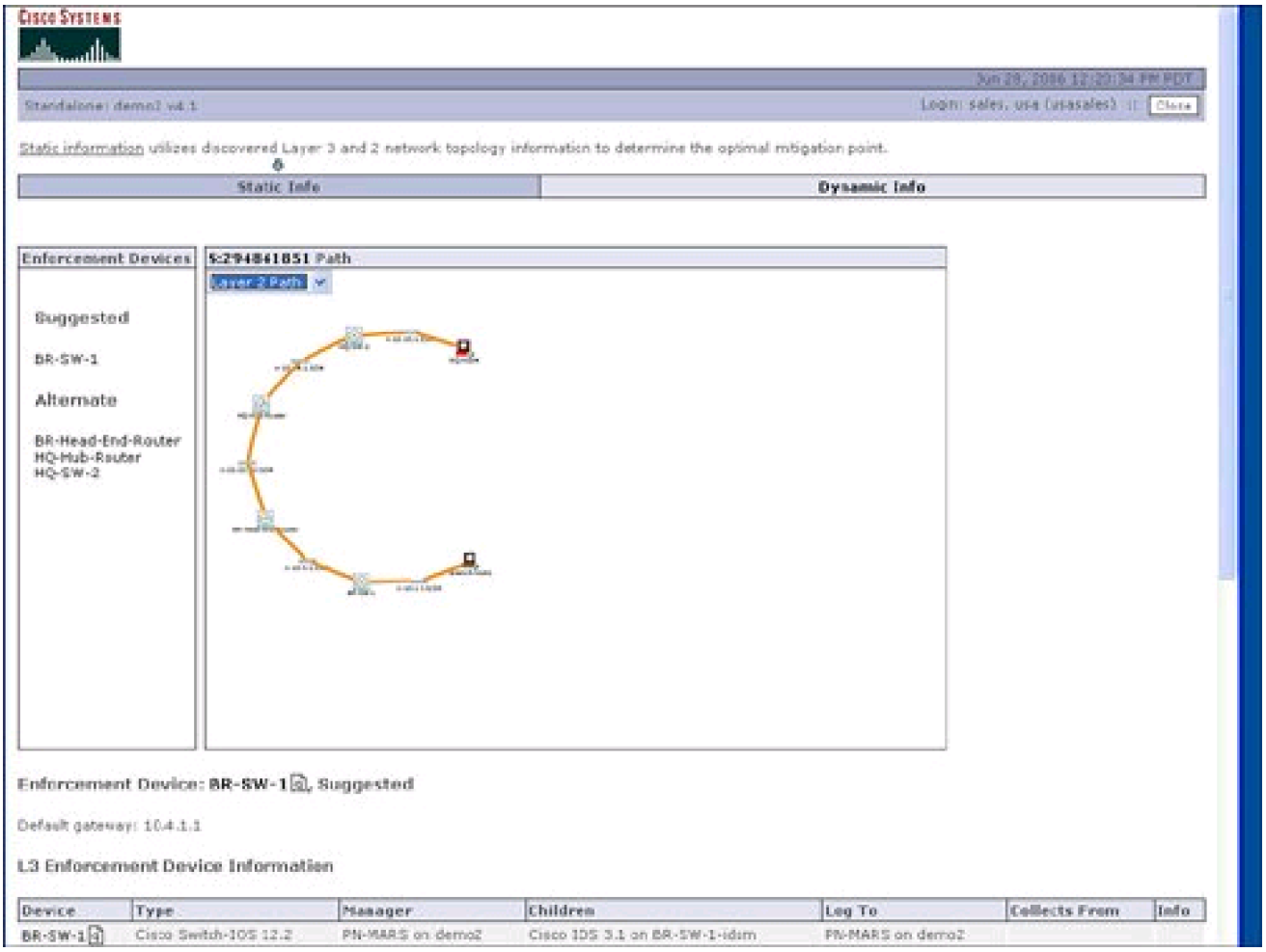
Cisco Security MARS displays security incidents to the user that may require action as opposed to simply providing a real-time viewer of IDS and firewall events. In addition to providing high-level security incidents to the user, another powerful feature of Cisco Security MARS is the ability to recommend or apply a mitigation action to stop the incident or attack.

Displaying Path of Incident and Mitigating the Attack

Figure 10-3 displayed details of the security incident for a Nimda worm. Selecting the red icon in the Path/Mitigate field for this incident results in the display of the path of the network attack. Figure 10-4 provides the resulting display of the path of the security incident through the network.

Figure 10-4. Path of Incident

[View full size image]



In addition to displaying the path of the network attack, Cisco Security MARS can also generate the command-line interface (CLI) commands to mitigate or stop the network attack. The CLI commands used to mitigate an attack are displayed with the path by selecting the path/mitigate option in the incident. Cisco Security MARS has the ability to automatically shut a LAN port to mitigate the attack. Cisco Security MARS will generate the CLI for an access control list (ACL) rule to stop an attack, but will not deploy the CLI. The suggested CLI recommendation is typically based upon the device closest to the source of the attack. This choice may not be the optimal mitigation point based upon the user's point of view. Cisco Security MARS allows the selection of alternate devices within the path of the network attack in case the user does not wish to mitigate the attack at the device that is closest to the source of the network attack. Figure 10-5 displays the suggested CLI to configure an access list to stop the Nimda attack.

Figure 10-5. Suggested CLI to Mitigate the Attack

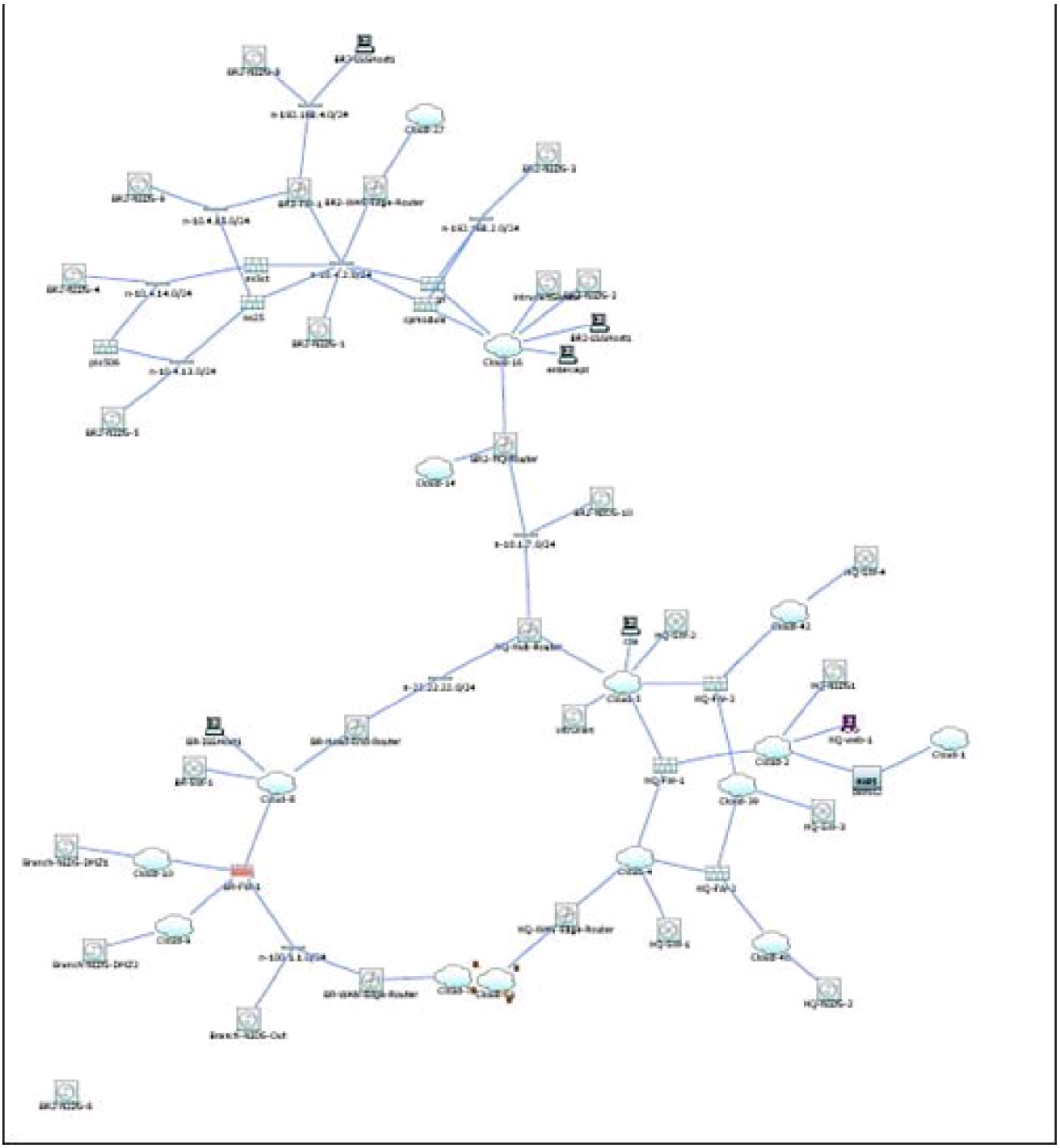
[View full size image]

Hotspot Graph and Attack Diagram

Cisco Security MARS relies heavily on SNMP to gain topological awareness of the network. Cisco Security MARS requires SNMP read access to construct a Layer 3 and Layer 2 topological map of the network. Cisco Security MARS uses Simple Network Management Protocol (SNMP) to gather information about the device. Cisco Security MARS also uses SNMP and a seed device to discover the neighboring devices for each known device in the network. A seed device is a starting device to discover the network by attempting to discover every device known by the seed device and then attempting to discover every device known by each newly discovered device.

SNMP allows Cisco Security MARS to create the hotspot graph and the attack diagrams. Use of SNMP by Cisco Security MARS is complemented by the integrated network scanner. The integrated network scanner is used to gain information about the hosts and applications that exist on the network. Cisco Security MARS combines the device discovery of SNMP with the scanning information about the hosts and applications to construct the hotspot graph. Cisco Security MARS uses the host scanning for OS and application fingerprinting. OS and application fingerprinting is used to assist in ensuring that an incident is relative to the target and valid. For example, a detected Windows exploit attack against a Linux server is not a valid incident. Both the hotspot graph and the attack diagram can be displayed on the main Cisco Security MARS dashboard. Figure 10-6 provides a sample of a hotspot topology graph. In our example, the hotspot diagram displays the network for the Nimda incident on the dashboard.

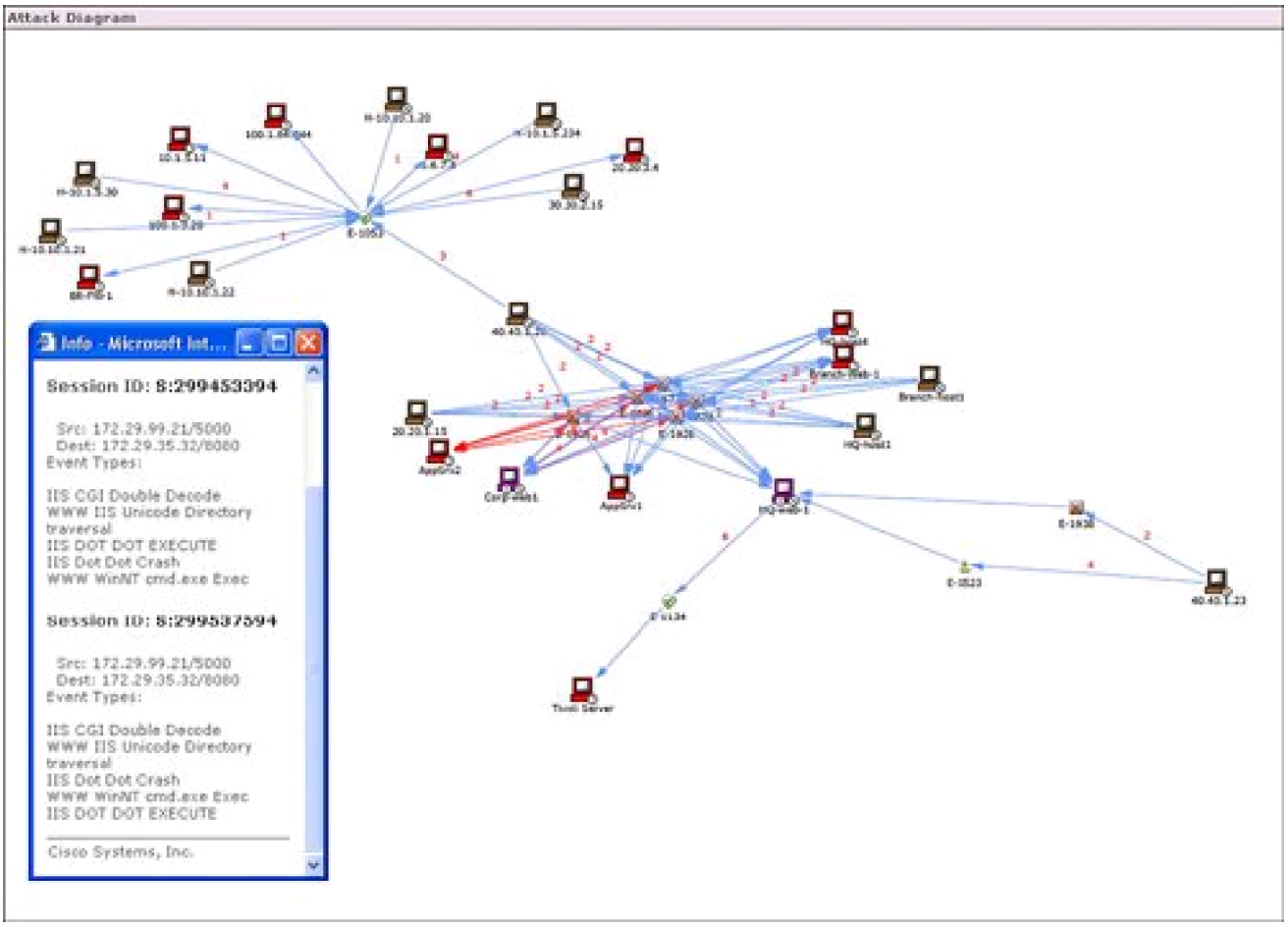
Figure 10-6. Hotspot Graph



The hotspot graph displays the path of the incident or attack across the network. An attack diagram allows the user to highlight a vulnerable path between two points in the network and receive a display of the session IDs of the events that are incorporated into the security incident. Figure 10-7 provides an example of an attack diagram for the Nimda incident. Both the hotspot graph and the attack diagram are launched from the icons next to the incident ID from the details on the incident. The hotspot graph and attack diagram on the dashboard typically correspond with the latest incident listed on the dashboard.

Figure 10-7. Attack Diagram

[View full size image]


Attack Diagram
Info - Microsoft Int...
Session ID: 8:299453394
Src: 172.29.99.21/5000
Dest: 172.29.35.32/8080
Event Types:
IIS CGI Double Decode
WWW IIS Unicode Directory traversal
IIS DOT DOT EXECUTE
IIS Dot Dot Crash
WWW WinNT cmd.exe Exec
Session ID: 8:299537594
Src: 172.29.99.21/5000
Dest: 172.29.35.32/8080
Event Types:
IIS CGI Double Decode
WWW IIS Unicode Directory traversal
IIS Dot Dot Crash
WWW WinNT cmd.exe Exec
IIS DOT DOT EXECUTE
Cisco Systems, Inc.

PREV

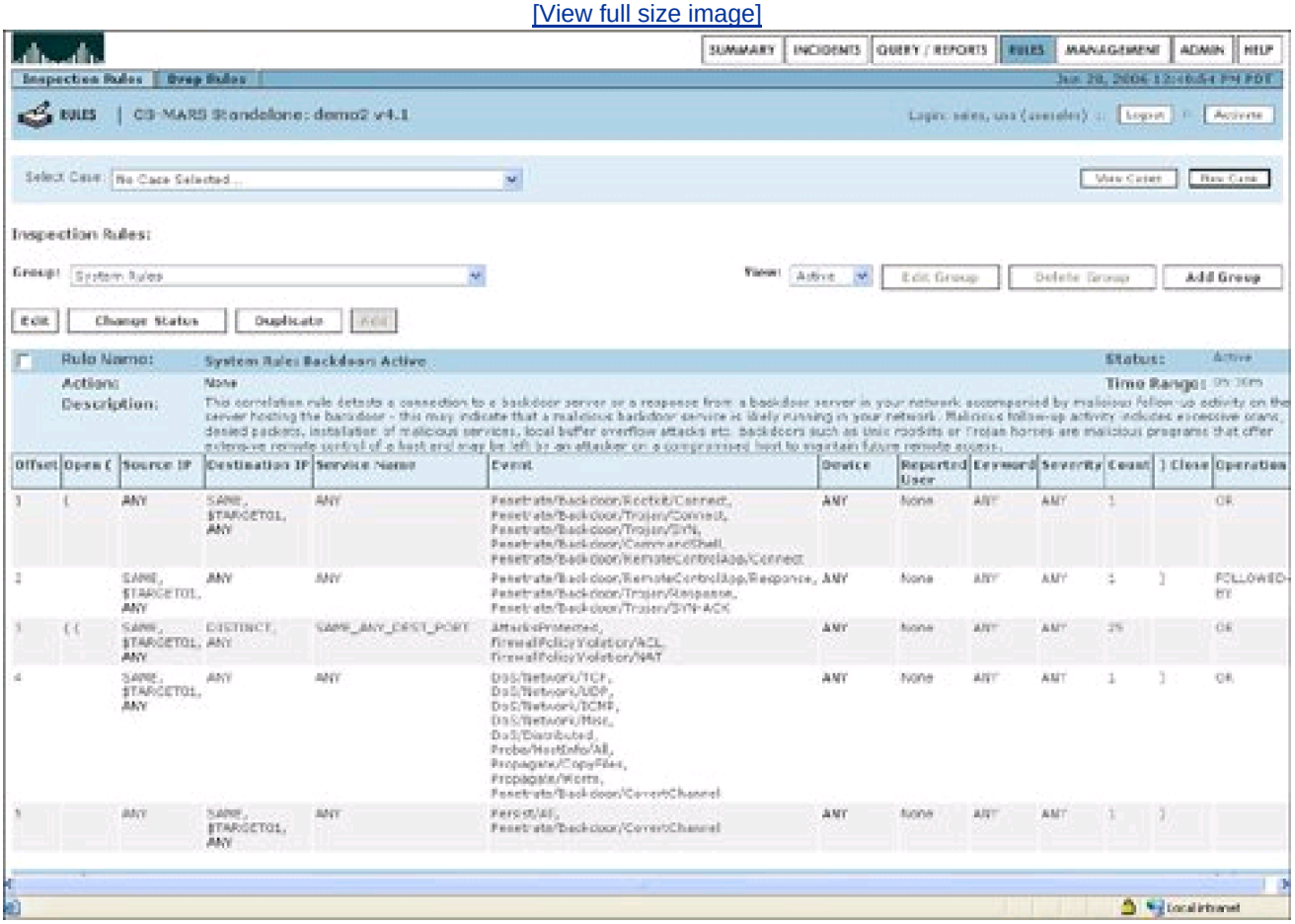
NEXT

Rules

To display an incident, a matching rule was used to trigger that a possible security incident or attack was in progress. Cisco Security MARS includes a set of system rules that are automatically configured and applied to detect security incidents or attacks. Figure 10-8 displays a system rule to detect an active backdoor connection. An active backdoor connection typically signifies that a host has been attacked and that a connection is open for someone to remotely access and control this host, perhaps for use in a botnet.

Figure 10-8. System Inspection Rule to Detect an Active Backdoor Connection

[View full size image]



In addition to the active backdoor system rule, some of the automatic or system inspection rules include detection of client exploits, firewall configuration issues, password attacks, scans, viruses found, viruses cleaned, worm propagation, and sudden traffic increases to a port.

In addition to the canned or predefined system inspection rules, Cisco Security MARS also features the ability to create customized or user inspection rules. User inspection rules can be ideal for homegrown or custom applications. These customized rules are created with the following parameters or fields:

- Source IP
- Destination IP
- Service
- Event
- Device
- User
- Keyword
- Count
- Operation

Rule information for a specific incident is available by selecting the incident details from the dashboard. General rule information is also available by selecting the Rules tab from the top of the Cisco Security MARS GUI. Cisco Security MARS was one of the first security monitoring products on the market to incorporate Netflow data. Netflow is a feature of Cisco IOS routers and Catalyst LAN switches. Netflow is essentially a record of a traffic flow between a particular source and destination through the IOS router. Netflow contains a high-level record of the source IP address, destination IP address, the time of the connection, and the duration of the connection.

Cisco IOS routers and Catalyst LAN switches running IOS periodically send a Netflow record to a Netflow collector such as Cisco Security MARS. This Netflow record is sent over User Datagram Protocol (UDP) and is highly efficient because it is merely a record of a traffic flow as opposed to a packet-by-packet dump of the traffic flow. Netflow contains the following information:

- Source IP address
- Destination IP address
- Ports/protocol
- Total packets
- Total bytes

Netflow is used by Cisco Security MARS to create a baseline of normal network traffic. This baseline is used to identify anomalous network behavior that can be indicative of several types of network attacks, including distributed denial-of-service (DDoS) attacks and worms that are sending large amounts of network traffic. Cisco Security MARS also contains integrated system inspection rules for IPS (Intrusion Prevention Service) that leverage Netflow information to signify a security incident or network attack, thus reducing the false positives that are sometimes associated with IPS. Netflow information, including the number of Netflow events received in the last 24 hours, is available on the dashboard.

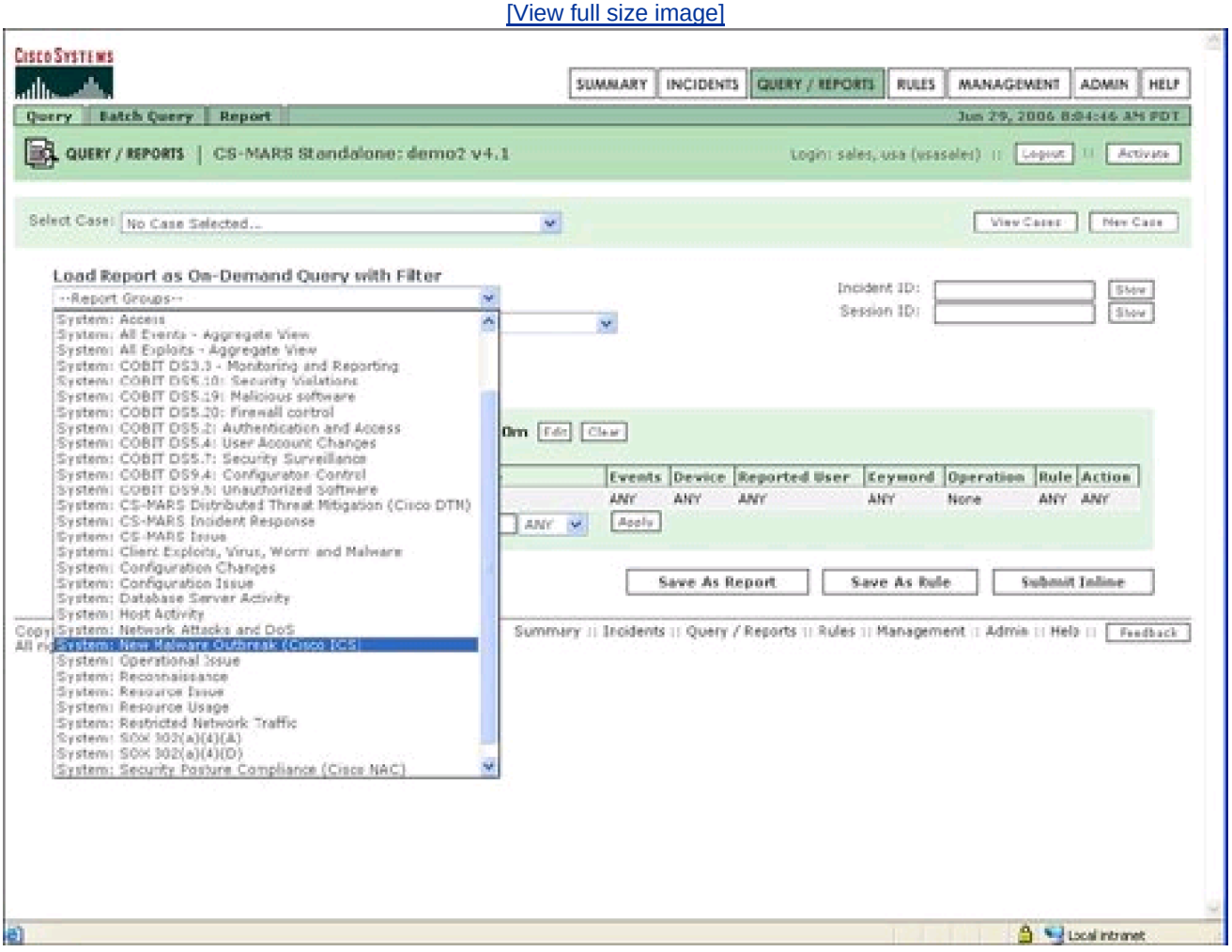
PREV NEXT

Query/Reports

Cisco Security MARS features a collection of predefined reports in addition to the ability to create a custom report. Reports are generated from the event data in Cisco Security MARS that is collected from the devices in the self-defending network, including routers, LAN switches, firewalls, IPS sensors, and hosts. Cisco Security MARS also features groups of reports. Figure 10-9 displays a sample of the report groups in Cisco Security MARS.

Figure 10-9. Report Groups

[View full size image]



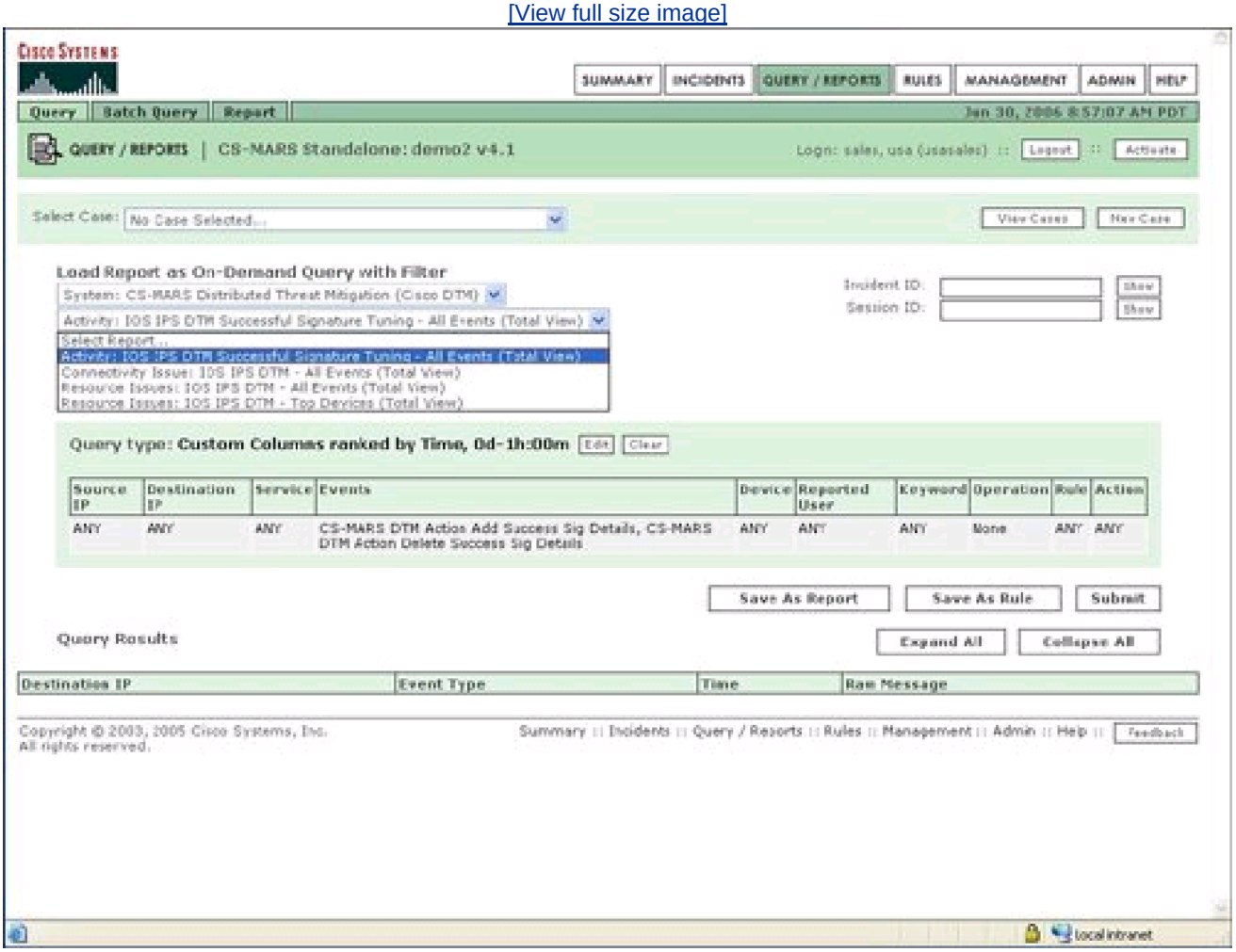
There are several report groups in Cisco Security MARS for topics that you have previously learned about in this book. For example, there are report groups for attacks and DoS, firewall control, malware outbreak (Cisco ICS), and security posture compliance (Cisco NAC). In addition to the topics previously discussed in this book, Cisco Security MARS also features a report group for Distributed Threat Mitigation (DTM).

DTM is designed to enable branch IOS routers, specifically Integrated Services Routers (ISRs), to dynamically configure themselves with the necessary IPS signatures to reduce the risk of an attack at the branch office in an automated, self-defending fashion. DTM is an emerging technology, and it is strongly recommended that DTM be tested in a small pilot network to verify scalability prior to any deployments in production networks.

In addition to the DTM report group, Cisco Security MARS also includes the option to be a DTM controller. The DTM controller is essentially the brains behind the DTM battlefield. The DTM controller in Cisco Security MARS receives input in the form of IPS Security Device Event Exchange (SDEE) events and syslogs to help to determine what specific attack is occurring in the branch network. Cisco Security MARS can then automatically enable the identified and necessary IPS signature on the branch IOS ISR. Figure 10-10 provides an example of the reports that are available as part of the DTM report group.

Figure 10-10. DTM Reports

[View full size image]



Cisco IOS ISRs can implement many features, including voice, routing, and security in a single device at a very cost-effective price point. The combination of feature-richness and low price point enables ISR routers to be deployed in remote branch offices in environments where an organization may have thousands of remote branches. To keep the price point of the ISRs attractive, their memory footprint, or capacity, is often substantially less than that of a dedicated security appliance such as an ASA (Advanced Security Appliance). The reduced memory footprint of the ISR creates a situation in which the entire IPS signature set cannot be simultaneously enabled on the ISR. The branch environment is often remote, and there may be no security or IT professionals resident at the remote branch to manage these devices. The combination of the remoteness of the branch and the limited memory capacity of the ISR can be addressed in certain, small-scale situations by managing the IPS signatures on the ISR with a DTM in Cisco Security MARS. DTM is currently not scalable to

large networks, and DTM should be implemented only on select remote ISRs with Cisco Security MARS.

ISRs contain a file called named attack-drop.sdf. This attack-drop.sdf file lists all the IPS signatures that are enabled on that ISR device. In addition to the attack-drop.sdf file, some of the larger ISR routers may also run the 128MB.sdf or 256MB.sdf signature files if they have enough memory. These attack-drop.sdf, 128MB.sdf, and 256MB.sdf files are frequently updated on Cisco.com to contain the latest, most relevant IPS signatures.

DTM can automatically enable the desired IPS signature on the ISR by monitoring network events that originate from networks around the ISR and updating the attack.sdf file on the ISR with the desired IPS signature. The monitored network events that are used by Cisco Security MARS to apply dynamically apply IPS signatures to ISR to mitigate a threat can originate from an IPS appliance, ASA IPS (AIP-SSM), a Catalyst 6500/7600 IPS service module, or an ISR router.

Cisco Security MARS cannot create the initial attack-drop.sdf file on the router. This attack-drop.sdf file must be initially created by CLI, Security Device Manager (SDM), or Cisco Security Manager.

PREV NEXT

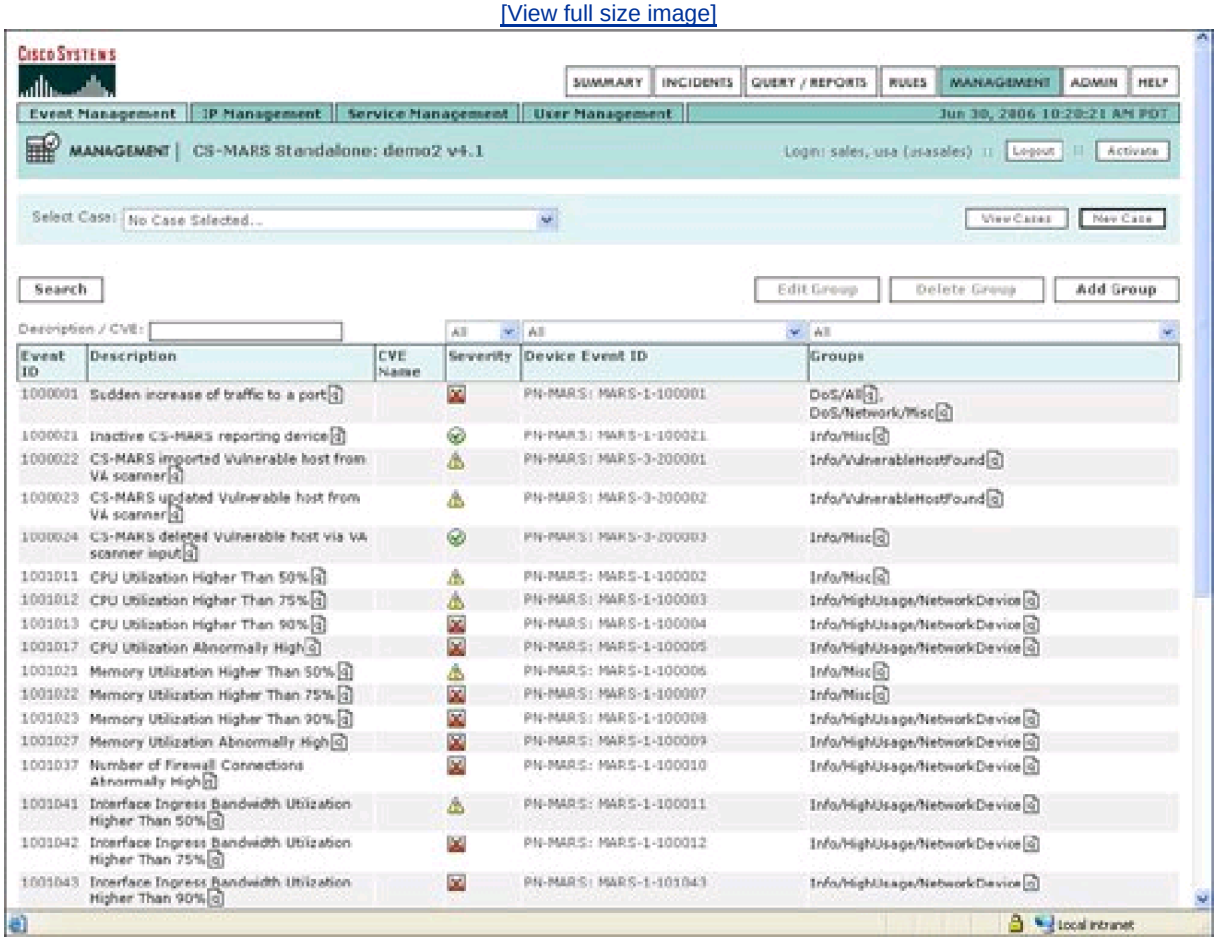
Management

The Management tab in the Cisco Security MARS graphical user interface (GUI) enables the user to view events and create IP addresses, services (ports or protocols), and admin accounts in Cisco Security MARS through the following tabs:

- Event Management displays the network events that are seen by Cisco Security MARS that can be used to trigger an incident. The event management tab is one of the more commonly used management tabs in Cisco Security MARS. An example of the event display in event management is provided in Figure 10-11.

Figure 10-11. Event Management

[View full size image]



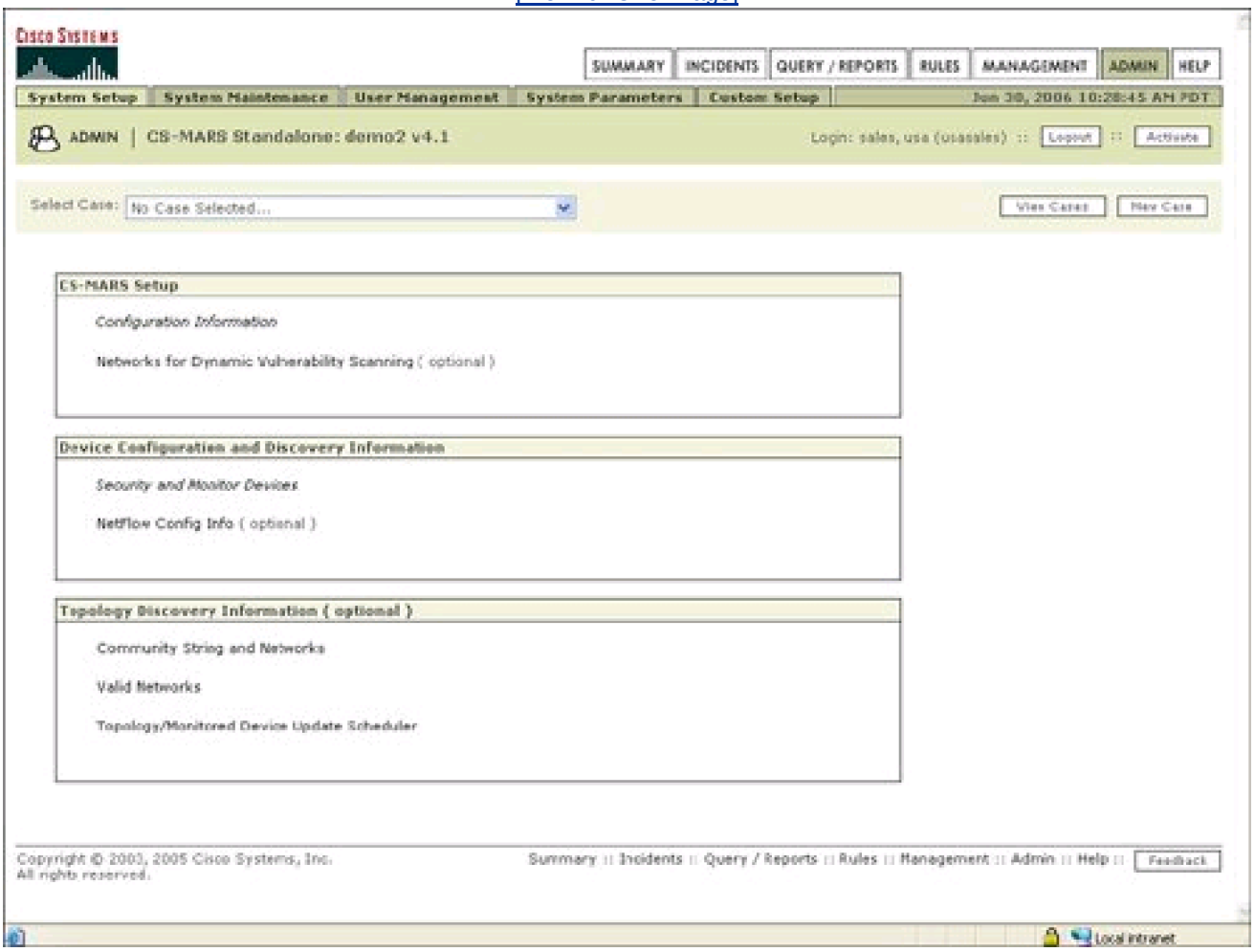
- IP Management displays what IP addresses or networks are known by Cisco Security MARS.
- Service Management displays what ports or protocols can be used in rules.
- User Management tab enables the creation or modification of a user account in Cisco Security MARS.

Admin

The Admin tab of the Cisco Security MARS GUI enables the configuration of administrative functions like system setup, maintenance, user management, system parameters, and custom setup. System setup is a critical step because system setup controls how devices are discovered or imported into Cisco Security MARS. Figure 10-12 provides a display of the system setup options.

Figure 10-12. System Setup

[View full size image]



Cisco Security Manager Linkages

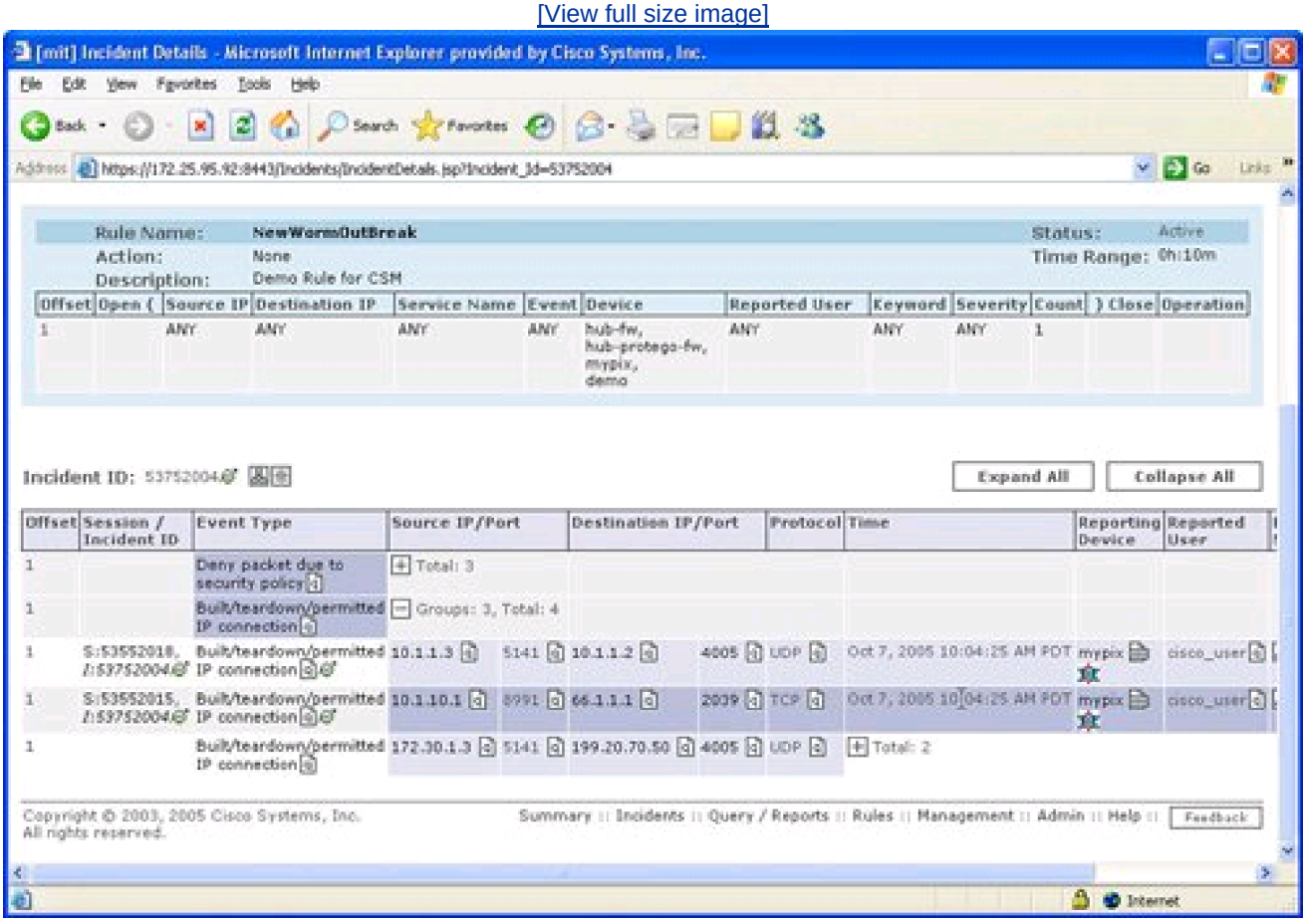
Cisco Security MARS supports integration or "linkages" with Cisco Security Manager. The ability to directly integrate between Cisco Security MARS and Cisco Security Manager enables security operators to cross-launch between the monitoring and configuration components. The ability to correlate or cross-launch between monitoring and configuration components can be especially useful in debugging or trouble-ticket situations.

Cisco Security MARS contains a feature that directly links an incident with a security policy in Cisco Security Manager. Specifically, Cisco Security MARS enables the user to select a syslog from a security incident and display the access control list (ACL) rule in Cisco Security Manager that generated the syslog.

Cisco Security MARS provides an incident to signify to the security operator that something of significance is occurring within the network. The incident is composed of various events that are reported by the devices within the self-defending network. Cisco Security MARS contains an entry under Reporting Devices in the Event entries for the incident. Figure 10-13 displays an example of how an incident can indicate that a reporting device has a policy link to Cisco Security Manager.

Figure 10-13. Incident with Cisco Security Manager Policy Entry

[View full size image]



This policy entry is supported only for Cisco devices that are configured by Cisco Security Manager to deploy access list rules to these devices. Selecting this policy entry displays the access list configured by the Cisco Security Manager that generated the syslog in the

security event. The ability to display the access list rules from the security event in Cisco Security MARS allows for quick debugging of many security situations and can allow the user to quickly address and rectify the security event that is reported by Cisco Security MARS.

The policy link in Cisco Security MARS displays a copy of the desired access list rules configured in Cisco Security Manager. Figure 10-14 displays an example of how to launch the policy link from the reporting device in Cisco Security MARS, and Figure 10-15 displays the resulting access control list (ACL) rule table from Cisco Security Manager.

Figure 10-14. Launch Policy Link from Cisco Security MARS

[View full size image]

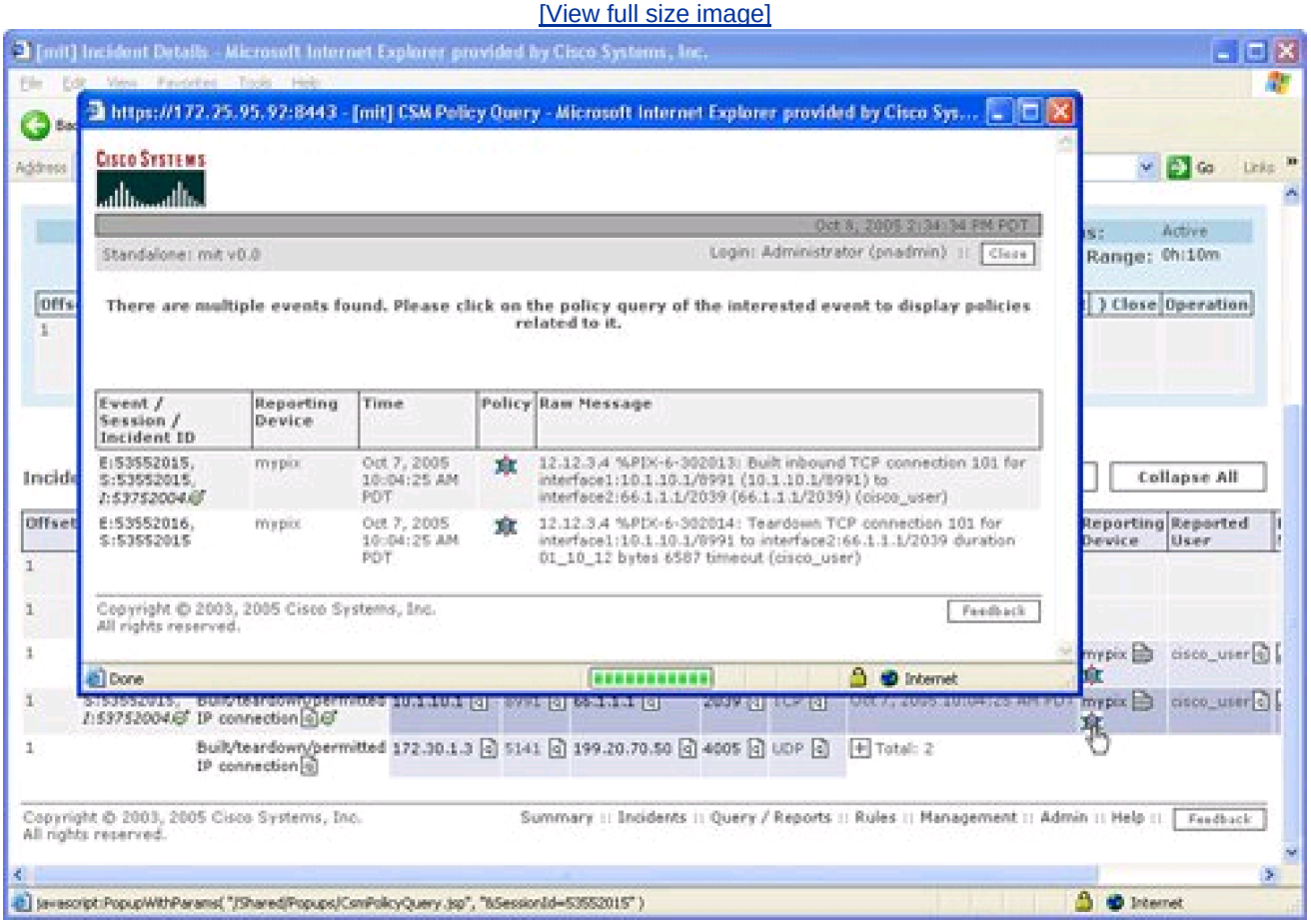
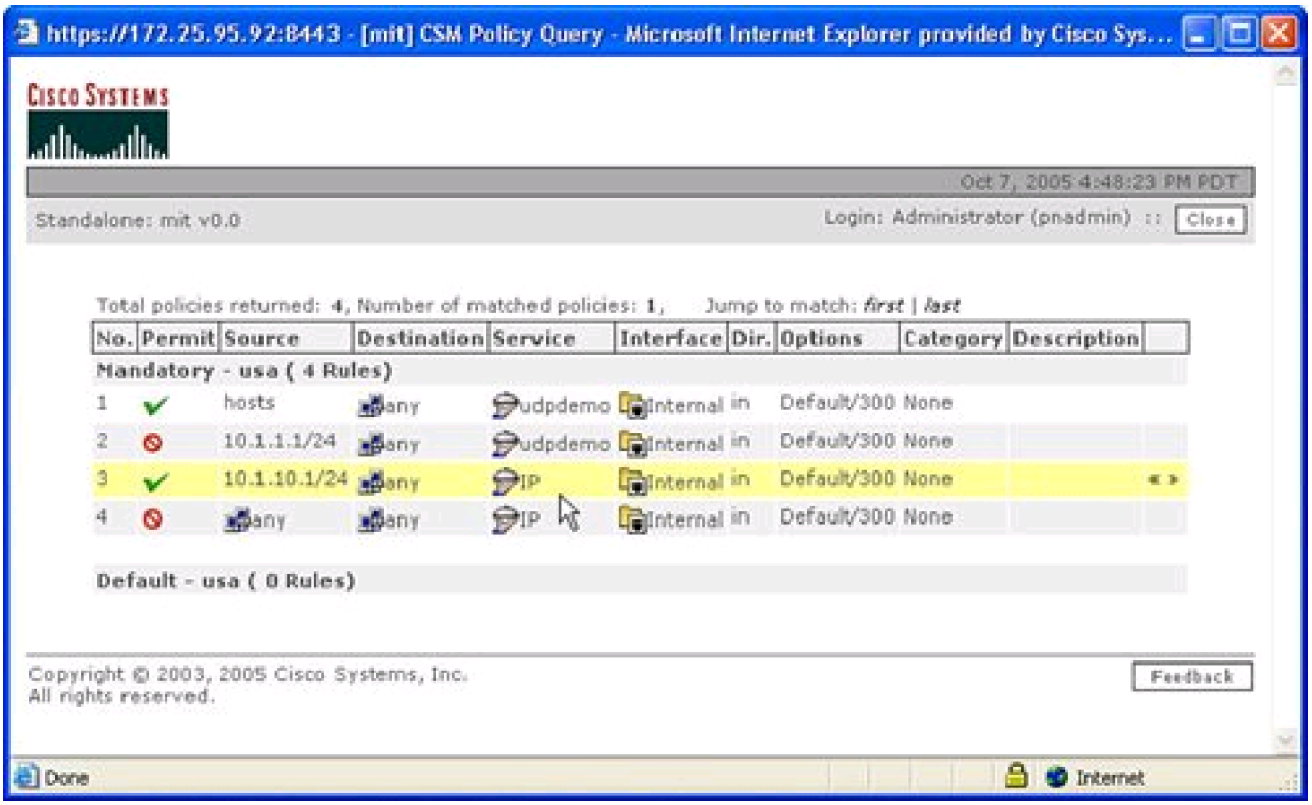


Figure 10-15. Access Control List (ACL) Rule Table Display

[View full size image]



The linkages between Cisco Security MARS and Cisco Security Manager provide another example of how centralized management is the "coach" that allows the self-defending network to be deployed and managed in an integrated and holistic fashion.

PREV NEXT

Summary

Cisco Security MARS is a monitoring and reporting component of a self-defending network. Cisco Security MARS can also mitigate or generate configurations that can stop certain attacks and can allow the network to be self-defending. Some of the configurations that can be generated by Cisco Security MARS include the CLI to shut a LAN port, enable an IPS signature on an IOS ISR or an access control list (ACL) rule. Cisco Security MARS can automatically generate CLI to reduce the risk of an attack, or Cisco Security MARS can recommend the CLI to be manually deployed by SSH (Secure Shell) or the Cisco Security Manager. Cisco Security MARS will only recommend and will not deploy the CLI to configure an access control list (ACL) rule.

Cisco Security MARS contains a high-level summary dashboard that includes incidents, hotspot graphs, and attack diagrams. An incident can be an indication that a high-level security attack, such as a Nimda attack, has been detected on the network. An incident is composed of security events and monitoring data that is received from known devices in the self-defending network, including routers, LAN switches, firewalls, IPS devices, hosts, databases, and storage appliances. Netflow data can be used to establish a baseline of normal traffic on a network. Netflow can be used to identify and filter false positives from valid security incidents. Rules are used to trigger a security incident. Cisco Security MARS contains many default or system inspection rules. Cisco Security MARS also features the ability to create custom or user-defined rules.

The dashboard lists actionable, high-level security incidents. A hotspot graph and attack diagram are also created for a significant security incident. A hotspot graph contains the path of the network attack, including the source, destination, and known devices within the attack path. The attack diagram displays the session IDs reported by devices for the incident. Cisco Security MARS and Cisco Security Manager are components of the Cisco Security Management suite. Cisco Security MARS contains linkages with Cisco Security Manager. For example, a user can select a syslog from an incident and see the access control list (ACL) rule policy in Cisco Security Manager that generated the syslog.

References

Cisco Systems, Inc. Cisco Security Monitoring, Analysis and Response System 4.2 Data Sheet.
http://www.cisco.com/en/US/products/ps6241/products_data_sheet0900aecd80272e64.html

Cisco Systems, Inc. *Cisco Security Monitoring, Analysis and Response System Q&A.*
http://www.cisco.com/en/US/products/ps6241/products_qanda_item0900aecd8027a051.shtml

Cisco Systems, Inc. Cisco Router and Security Device Manager.http://www.cisco.com/en/US/products/sw/secursw/ps5318/index.html

Cisco Systems, Inc. Technology Preview: Configuring Distributed Threat Mitigation in Cisco Security MARS.
http://www.cisco.com/en/US/products/ps6241/products_configuration_example09186a008067a2b0.shtml

Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [Z]

Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [Z]

802.1x 2nd
- authentication server
- authenticators
- EAP
  - *EAP FAST*
  - *EAP MD5*
  - *EAP TLS*
  - *LEAP*
  - *messages*
  - *PEAP*
- IBNS
- machine authentication
- NAC
- PPP connections
- supplicants
- VPN

Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [Z]

ACL (Access Control List) rules
- firewall rules configuring from topology maps
- security policies Cisco Security Manager

Action filters (Guard)
Add Device function (Cisco ICS)
Admin tab (Cisco Security MARS)
Administration option (NAC Appliance Manager)
agentless host admission process (NAC)
AIP-SSM (Advanced Inspection and Protection Security Services Module)
Analysis button (Cisco Security Manager)
antispoofing (ASA)
antivirus programs
Appliance (NAC) customer preferences comparison chart 2nd
Appliance Manager (NAC appliance)
- Administration option
- Device Management category
  - *CCA Servers option*
  - *Clean Access section*
  - *filters*
- Event log
- homepage organization
- Monitoring function
- monitoring summary
- switch management function
- user management function
  - *quarantine roles*
  - *user authentication*
  - *user roles list*

Application analysis (Cisco Security Agent Management Center)
Application Behavior Investigation option (Cisco Security Agent Management Center)
Application Deployment Investigation option (Cisco Security Agent Management Center)
ASA (Adaptive Security Appliance)
- antispoofing
- ASDM
  - *Content Security tab*
  - *IPS* 2nd

threat graphs
CSC-SSM
antispam configurations
configuring
file blocking
file transfers
InterScan (Trend Micro) 2nd
mail
phishing
scanning
URL filtering
web/http functions
HTTP inspection engine
attacks
HTTP maps 2nd
HTTP/Web service inspections
protocol inspections
RFC compliance
TCP inspections
TCP maps
URL length
IPS signatures
attack signatures
configuring
spyware detection signatures
subcategories
protocol inspection services
Randomize Sequence Number feature
Service Policy Rules 2nd 3rd
SYN Cookie feature
ASDM (Adaptive Security Device Manager)
Content Security tab
IPS
configuring
connecting to
inline IPS
inspections
preventions
Service Policy rules 2nd 3rd
signatures
threat graphs
attack diagrams (Cisco Security MARS)
attack reports (Guard) generating
attack signatures (IPS)
attack-drop.sdf files
Audit admission validations (Cisco Secure ACS)

authentication
machine-based (802.1x)
NAC Appliance Manager
authentication server (802.1x)
authenticator (802.1x)
Automatic Outbreak Management Task (Cisco ICS)

PREV NEXT

Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [Z]

behavior diagrams (Cisco ICS)
bootstrapping (Guard)
bump-in-the-wire
Burst filters (Guard)
bypass filters (Traffic Anomaly Detector)

Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [Z]

Catalyst Anomaly Guard service module (Guard)
CCA (Cisco Clean Access) [See **NAC (Network Admission Control)**.]
CCA Servers option (NAC Appliance Manager)
Checkup posture states
Cisco ICS (Incident Control Service) 2nd
Add Device function
Device List
Global Settings tab
logs
Event Log Query function
Incident Log Query function
Log Maintenance function
Outbreak Log Query function
New Outbreak Management Task list2nd
OPACL
automatic deployment of
information displaying
target devices selecting
OPSig
outbreak management 2nd
outbreak reports
outbreak settings
accessing
Automatic Outbreak Management Task
Exception Lists
OPACL
Report
watch list
summary page
threats
behavior diagrams
statistics
technical details
Update Settings tab
Cisco Secure ACS
admission control policy comparisons

admission validations
Checkup posture states
enforcement actions
Healthy posture states
Infected posture states
network admission decisions
Policy decision point
policy servers forwarding endpoint information to
Quarantine posture states
enforce quarantine access actions
enforce redirection (optional) actions
Healthy posture states changing to
Transition posture states
Unknown posture states
Cisco Security Agent
day-zero protection
features of
Management Center
analysis running
Application analysis
Application Behavior Investigation option
Application Deployment Investigation option
attaching rules to security policies
deploying device/device group kits
displaying device group end-station hostnames
Event Log
Event Monitor
generating/deploying rules
Learn mode
reviewing security policies
send polling hintcapabilities
Test mode
Status area
System Security area
Cisco Security Manager 2nd
Cisco Security MARS linkages
Device View
ACLs 2nd
adding devices
Analysis button
firewalls
Hit Count button
interface roles configuring
policy queries invoking
features of
Map View

- Object Manager
- Policy View
  - *ACL rules security policies*
  - *IPS management*
  - *policy inheritance*
  - *security policies*
- value override per device

Cisco Security MARS (Cisco Security Monitoring Analysis and Response System)
- Admin tab
- Cisco Security Manager linkages
- CLI commands
- dashboard
- features of
- incidents
  - *attack diagrams*
  - *displaying paths of*
  - *hotspot graphs*
  - *mitigating attacks*
- input/event sources
- Management tab
- Netflow
- report groups
- rules 2nd

CiscoWorks VMS [See **Cisco Security Manager**.]

Clean Access section (NAC Appliance Manager)

CLI (command-line interface) commands
- commands Cisco Security MARS
- Service Policy rules

cloud networks adding topology maps to

content filtering (mail) CSC-SSM

Content Security tab (ASDM)

CSC-SSM (Content Security and Control Security Service Module)
- configuring
- file blocking
- file transfers
- InterScan (Trend Micro) 2nd
- mail
- phishing
- scanning
- URL filtering
- web/http functions

CTA (Cisco Trust Agent)

Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [Z]

dashboard (Cisco Security MARS)
- attack diagrams
- hotspot graphs
- incidents

day-zero protection (Cisco Security Agent)

DDoS (distributed denial-of-service) attacks 2nd
- Guard 2nd
  - *attach reports generating*
  - *bootstrapping*
  - *Catalyst Anomaly Guard service module*
  - *WBM*
  - *zone creation*
  - *zone filters*
  - *zone learning phases*
  - *zone protect mode*
  - *zone synchronization*
  - *zone traffic diversion*
- HTTP inspection engine
- mitigation
- mitigation overview
- Traffic Anomaly Detector
  - *configuring*
  - *detecting anomalies*
  - *diagnostic information*
  - *dynamic filters*
  - *policy templates*
  - *zone creation*
  - *zone filters*
  - *zone learning phases*
  - *zone policy construction phase*
  - *zone threshold-tuning phase*
- types of

device filters (NAC Appliance Manager)

Device List (Cisco ICS)

Device Management category (NAC Appliance Manager)
- CCA Servers option

NAT Gateway mode
OOB deployments
Real IP Gateway mode
Virtual IP Gateway mode
Clean Access section
filters
Device View (Cisco Security Manager)
ACLs 2nd
adding devices
Analysis button
firewalls
Hit Count button
interface roles configuring
policy queries invoking
DoS (denial-of-service) attacks
Dst Port filters (Guard)
DTM report groups (Cisco Security MARS)
dynamic filters (Traffic Anomaly Detector)

PREV NEXT

Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [Z]

EAP (Extensible Authentication Protocol) 802.1x
- EAP FAST
- EAP MD5
- EAP TLS
- LEAP
- messages
- PEAP

endpoint security application

enforce quarantine access actions (Quarantine posture states)

enforce redirection (optional) actions (Quarantine posture states)

enforcement actions (NAD)

Event log
- Cisco Security Agent
- NAC Appliance Manager
- Query function (Cisco ICS)

Event Monitor (Cisco Security Agent)

Exception Lists (Cisco ICS)

Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [Z]

false positives
files (CSC-SSM)
- blocking
- transfers security

filters
- flex filters (Traffic Anomaly Detector)
- Fragments filters (Guard)
- NAC Appliance Manager

firewalls
- ACL rules configuring from topology maps
- Device View (Cisco Security Manager)

Fragments filters (Guard)
Framework (NAC)
- agentless host admission process
- benefits of
- components of
- customer preferences comparison chart
- deployment
  - *LAN access compliance*
  - *remote access compliance*
  - *rules for*
  - *WAN access compliance*
- endpoint security application
- management systems
- network access devices
- noncompliant endpoint admission process
  - *admission control policy comparisons*
  - *Cisco Secure ACS decisions*
  - *Cisco Secure ACS enforcement actions*
  - *endpoint change from Quarantine to Healthy posture state*
  - *endpoint compliance change polls*
  - *endpoint network access*
  - *NAD enforcement of actions*
  - *NAD policy server notifications*
  - *policy servers forwarding endpoint information to*
  - *posture agent actions*

operational overview
policy servers
posture agents 2nd
reporting tools
Revalidation configurable timers
Status Query configurable timers
web resources

PREV NEXT

Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [Z]

Global Settings tab (Cisco ICS)
Guard
- attack reports generating
- bootstrapping
- Catalyst Anomaly Guard service module
- DDoS attacks
- WBM
- zones
  - *creating*
  - *filters*
  - *learning phase*
  - *protect mode*
  - *synchronizing*
  - *traffic diversion*

Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [Z]

Healthy posture states
Hit Count button (Cisco Security Manager)
hotspot graphs (Cisco Security MARS)
HTTP insepction engine
- attacks
- HTTP maps 2nd
- HTTP/Web server inspections
- protocol inspections
- RFC compliance
- TCP inspections
- TCP maps
- URL length

Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [Z]

IBNS (Identity-Based Networking Services)
ICS (Incident Control Service)[See **Cisco ICS (Incident Control Service)**]
Identity admission validations (Cisco Secure ACS)
IDS (intrusion detection systems)
Incident Log Query function (Cisco ICS)
incidents Cisco Security MARS
- attack diagrams
- displaying paths of
- hotspot graphs
- mitigating attacks

Infected posture states
inheritance policies (Cisco Security Manager)
inline IPS (Intrusion Prevention Service)
InterScan (Trend Micro)
- antispam configurations
- CSC-SSM

IPS (Intrusion Prevention Service)2nd
- ASDM connections to
- configuring
- inline IPS
- inspections
- Policy View (Cisco Security Manager) managing via
- preventions
- Service Policy rules 2nd 3rd
- signatures
  - *attack signatures*
  - *configuring*
  - *spyware detection signatures*
  - *subcategories*

ISR (Integrated Services Routers)

Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [Z]

LEAP (802.1x)

Learn mode (Cisco Security Agent Management Center)

learning phase (zones)

- Guard
- Traffic Anomaly Detector

Log Maintenance function (Cisco ICS)

Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [Z]

machine authentication (802.1x)
mail security
Management Center (Cisco Security Agent)
- analysis running
- Application analysis
- Application Behavior Investigation option
- Application Deployment Investigation option
- attaching rules to security policies
- deploying device/device group kits
- displaying device group end-station hostnames
- Event Log
- Event Monitor
- generating/deploying rules
- Learn mode
- reviewing security policies
- send polling hintcapabilities
- Test mode

Management tab (Cisco Security MARS)
Map View (Cisco Security Manager) topology maps
- adding cloud networks to
- firewall ACL rules
- showing devices on

maximum services option (policy templates)
minimum threshold option (policy templates)
Monitoring function (NAC Appliance Manager)

Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [Z]

NAC (Network Admission Control) 2nd
- 802.1x
- Appliance customer preferences comparison chart2nd
- Appliance Manager
  - *Administration option*
  - *Device Management category*
  - *Event log*
  - *homepage organization*
  - *Monitoring function*
  - *monitoring summary*
  - *switch management function*
  - *user authentication*
  - *user management function*
- Framework
  - *agentless host admission process*
  - *benefits of*
  - *components of*
  - *customer preferences comparison chart*
  - *deployment*
  - *endpoint security application*
  - *management systems*
  - *network access devices*
  - *noncompliance endpoint admission process*
  - *operational overview*
  - *policy servers*
  - *posture agents* 2nd
  - *reporting tools*
  - *Revalidation configurable timers*
  - *Status Query configurable timers*
  - *web resources*
- overview of

NAD (Network Admission Devices)
- Cisco Secure ACS actions enforcement of
- enforcement actions

NAT Gateway mode (CCA Servers option)

Netflow Cisco Security MARS

network access devices (NAC Framework)
network attacks
- attacks 2nd
- DoS attacks
- phishing
- spyware
- Trojan horses
- viruses
- worms

network defenses
- antivirus programs
- firewalls
- IDS
- router ACLs
- VPN

New Outbreak Management Task list (Cisco ICS) 2nd

PREV NEXT

Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [Z]

Object Manager (Cisco Security Manager)
OOB (out-of-band) deployments (CCA Servers option)
OPACL (outbreak prevention access control lists) 2nd
- automatic deployment of
- information displaying
- target devices selecting

OPSig (outbreak prevention signatures)
Outbreak Log Query function (Cisco ICS)
outbreak management (Cisco ICS)
- behavior diagrams
- New Outbreak Management Task list 2nd
- OPACL 2nd 3rd
- outbreak reports
- outbreak settings
- overview of
- statistics (threats)
- summary page
- tasks running/stopping
- technical details (threats)

outbreak reports (Cisco ICS)

Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [Z]

PEAP (802.1x)
phishing 2nd
policies
- construction phase (zones)
- inheritance CS Manager
- queries
  - *Device View (Cisco Security Manager)*
  - *wildcards*
- templates

Policy decision point (Cisco Secure ACS)
Policy servers
- endpoint information forwarding to (NAC)
- NAD notifications

Policy View (Cisco Security Manager)
- ACL rules security policies
- IPS management
- policy inheritance
- security policies

Posture admission validations (Cisco Secure ACS)
posture agents
- actions of
- CTA

PPP connections (802.1x)
protect mode (zones) Guard
Protocol filters (Guard)
protocol inspection services

Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [Z]

Quarantine posture states
enforce quarantine access actions
enforce redirection (optional) actions
Healthy posture states changing to
quarantine roles (NAC appliance)

Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [Z]

Randomize Sequence Number feature (ASA)
Rate filters (Guard)
Real IP Gateway mode (CCA Servers option)
report groups Cisco Security MARS
Report Settings (Cisco ICS)
reports generating attack reports (Guard)
Revalidation configurable timers (NAC)
RFC HTTP inspection engine
routers
- ACLs
- ISR

RTP (Real-Time Protocol)
rules Cisco Security MARS2nd

Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [Z]

Secure ACS (Cisco)
admission validations
Policy decision point
security
ASA
antispoofing
ASDM 2nd
CSC-SSM 2nd
HTTP inspection engine 2nd
IPS 2nd
protocol inspection services
Randomize Sequence Number geature
Service Policy rules 2nd 3rd
attacks HTTP inspection engine
Cisco ICS
Add Device function
behavior diagrams
Device List
Event Log Query function
Global Settings tab
Incident Log Query function
Log Maintenance function
New Outbreak Management Task list 2nd
OPACL 2nd 3rd
OPSig
Outbreak Log Query function
outbreak management
Outbreak Management tab
outbreak management tasks
outbreak reports
outbreak settings
statistics (threats)
summary page
technical details (threats)
Update Settings tab
Cisco Security Agent

day-zero protection
features of
Management Center
Status area
System Security area
files
blocking
transfers CSC-SSM
mail
phishing
policies
ACL rules
Policy View
TrendLabs (Trend Micro) role in outbreak managment
URL
blocking InterScan (Trend Micro)
filtering
Security Manager (Cisco) [See **Cisco Security Manager**.]
self-defending networks
802.1x
ASA
CSA
Cisco Security Manager
ICS
IPS
mitigation
NAC
Service Policy rules (ASA) 2nd 3rd
show module command (AIP-SSM)
SMTP mail scanning
Source IP filters (Guard)
Source Subnet filters (Guard)
spam (mail)
spyware 2nd
state option (policy templates)
Status area (Cisco Security Agent)
Status Query configurable timers (NAC)
subnet filters (NAC Appliance Manager)
summary page (Cisco ICS)
supplicants (802.1x)
switch management function (NAC Appliance Manager)
SYN Cookie feature (ASA)
System Security area (Cisco Security Agent)

Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [Z]

TCP (transfer control protocol) HTTP inspection engine
Test mode (Cisco Security Agent Management Center)
threats (security)
- behavior diagrams
- Cisco ICS
  - *statistics*
  - *technical details*
- graphs ASDM

threshold-tuning phase (zones)
topology maps
- adding cloud networks to
- firewall ACL rules
- showing devices on

Traffic Anomaly Detector
- configuring
- DDoS attacks
- detecting anomalies
- diagnostic information
- dynamic filters
- policy templates
- zones
  - *creating*
  - *filters*
  - *learning phase*
  - *policy construction phase*
  - *threshold-tuning phase*

Transition posture states
TrendLabs (Trend Micro) role in outbreak management
Trojan horses

Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [Z]

Unknown posture states
Update Settings tab (Cisco ICS)
URL (uniform resource locators)
- blocking InterScan (Trend Micro)
- filtering
- HTTP inspection engine

user filters (Traffic Anomaly Detector)
user management function (NAC Appliance Manager)
- quarantine roles
- user authentication
- user roles list

Index

[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [Z]

value override per device (Cisco Security Manager)
Virtual IP Gateway mode (CCA Servers option)
viruses 2nd
VPN (Virtual Private Networks)2nd

Index

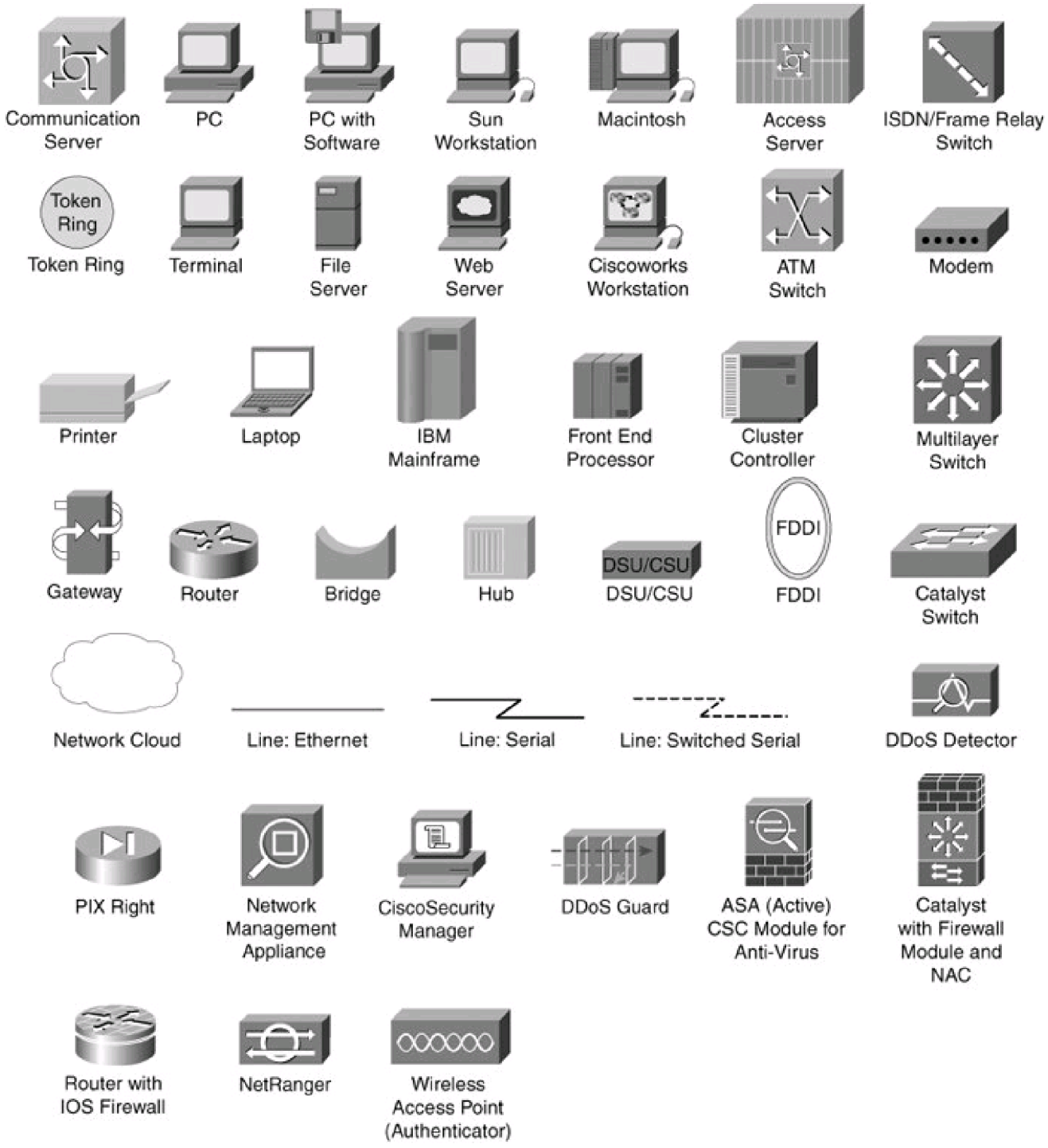
[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [Z]

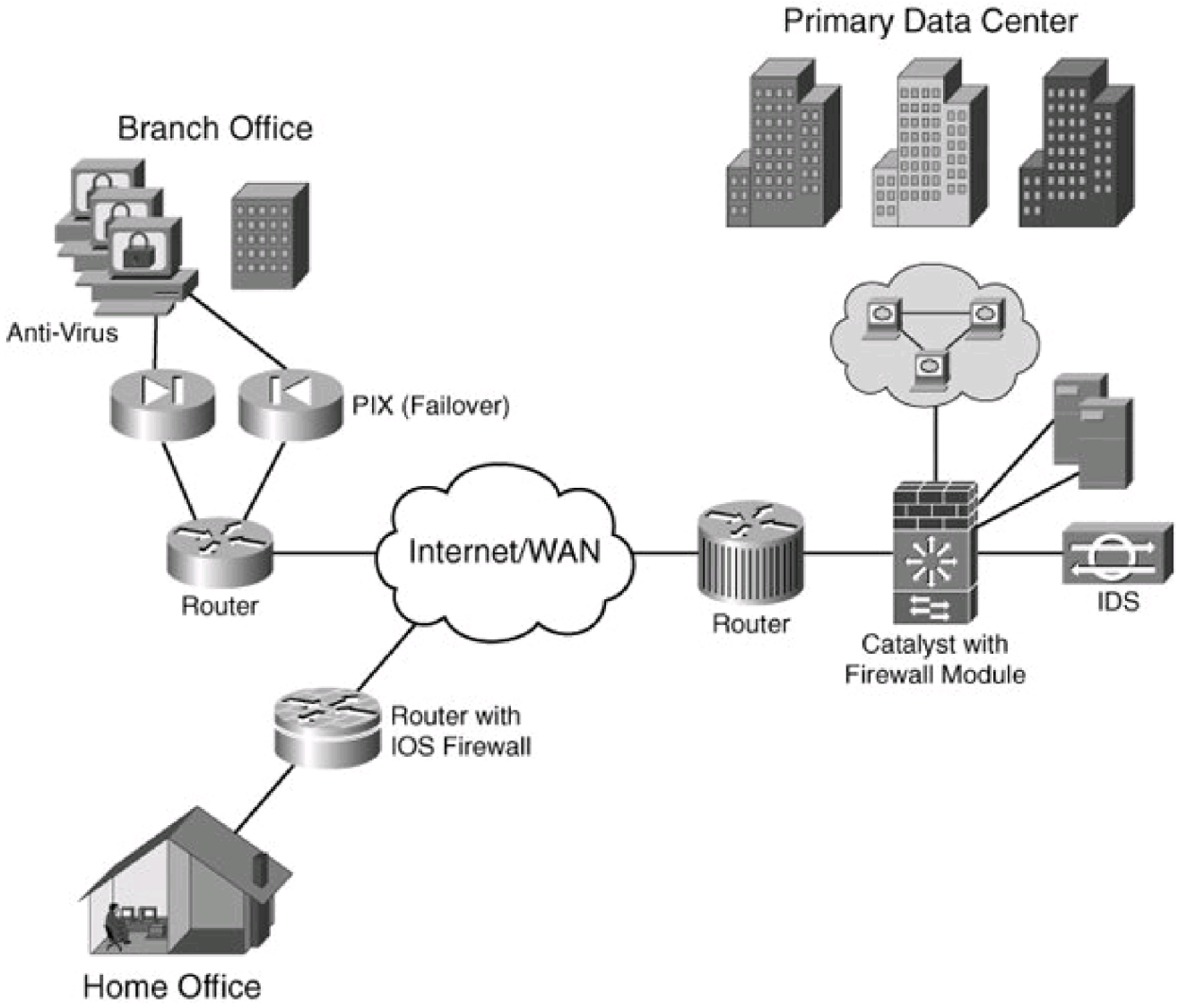
watch list settings (Cisco ICS)
wildcards policy queries
worms

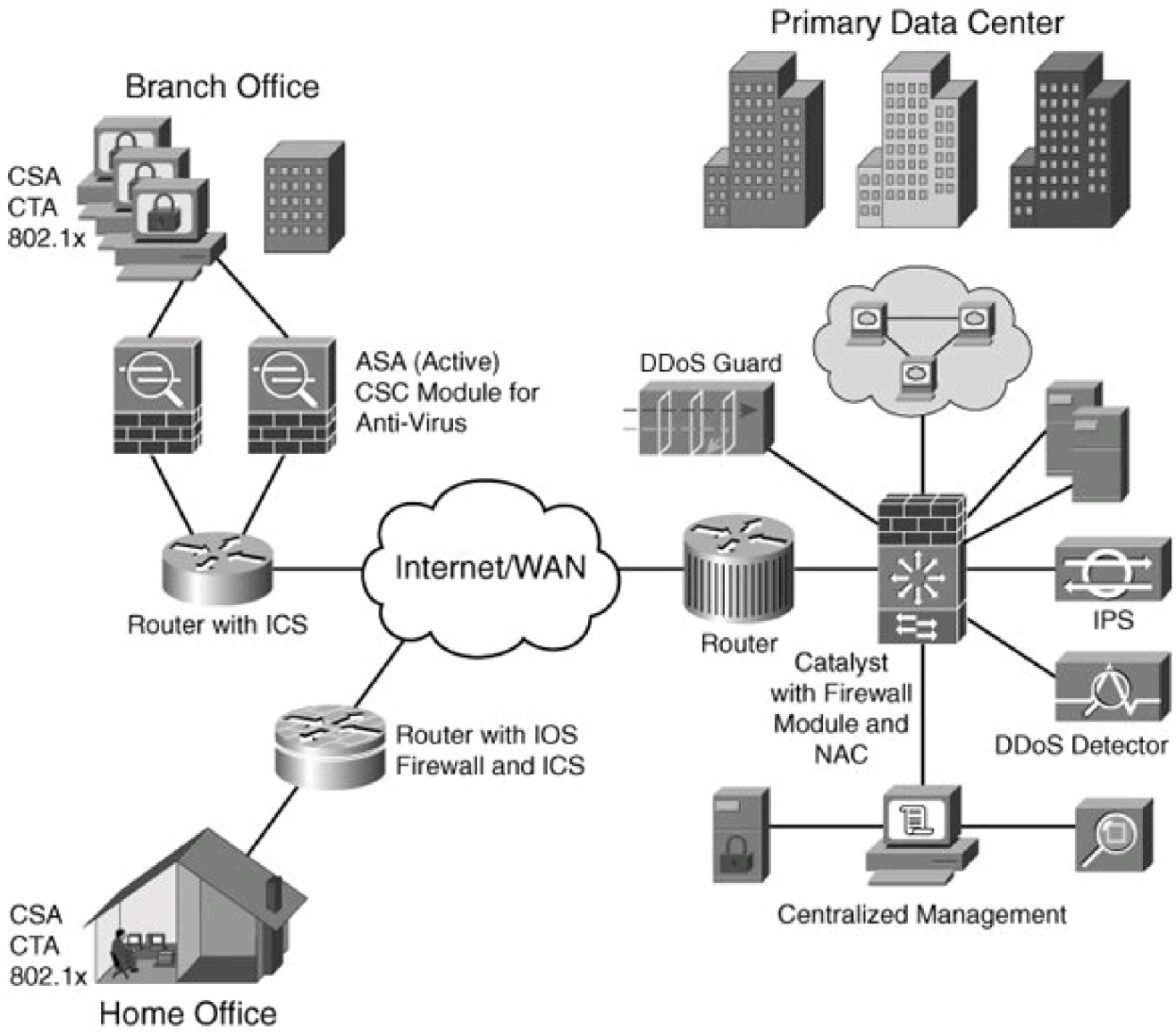
Index

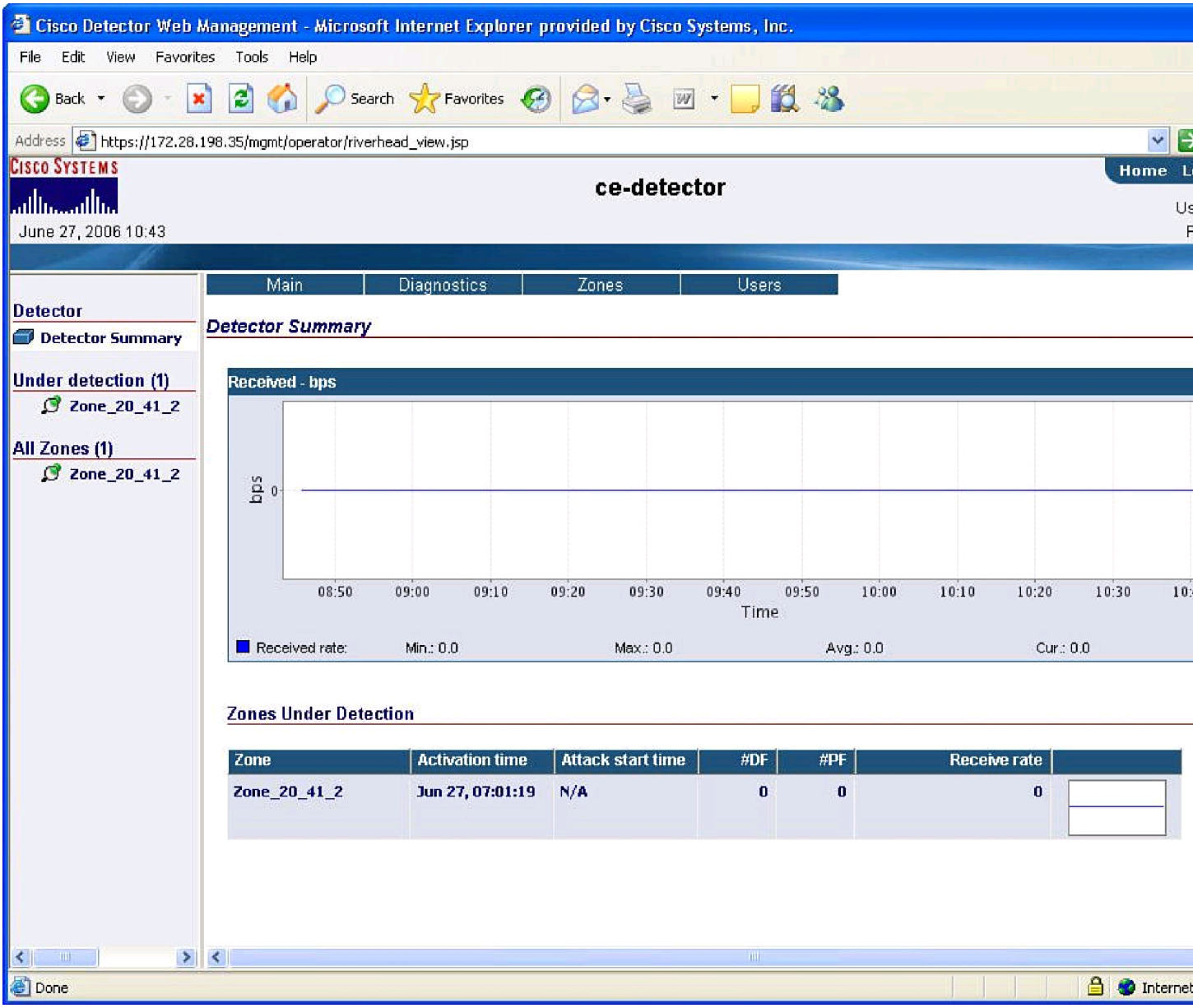
[SYMBOL] [A] [B] [C] [D] [E] [F] [G] [H] [I] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [Z]

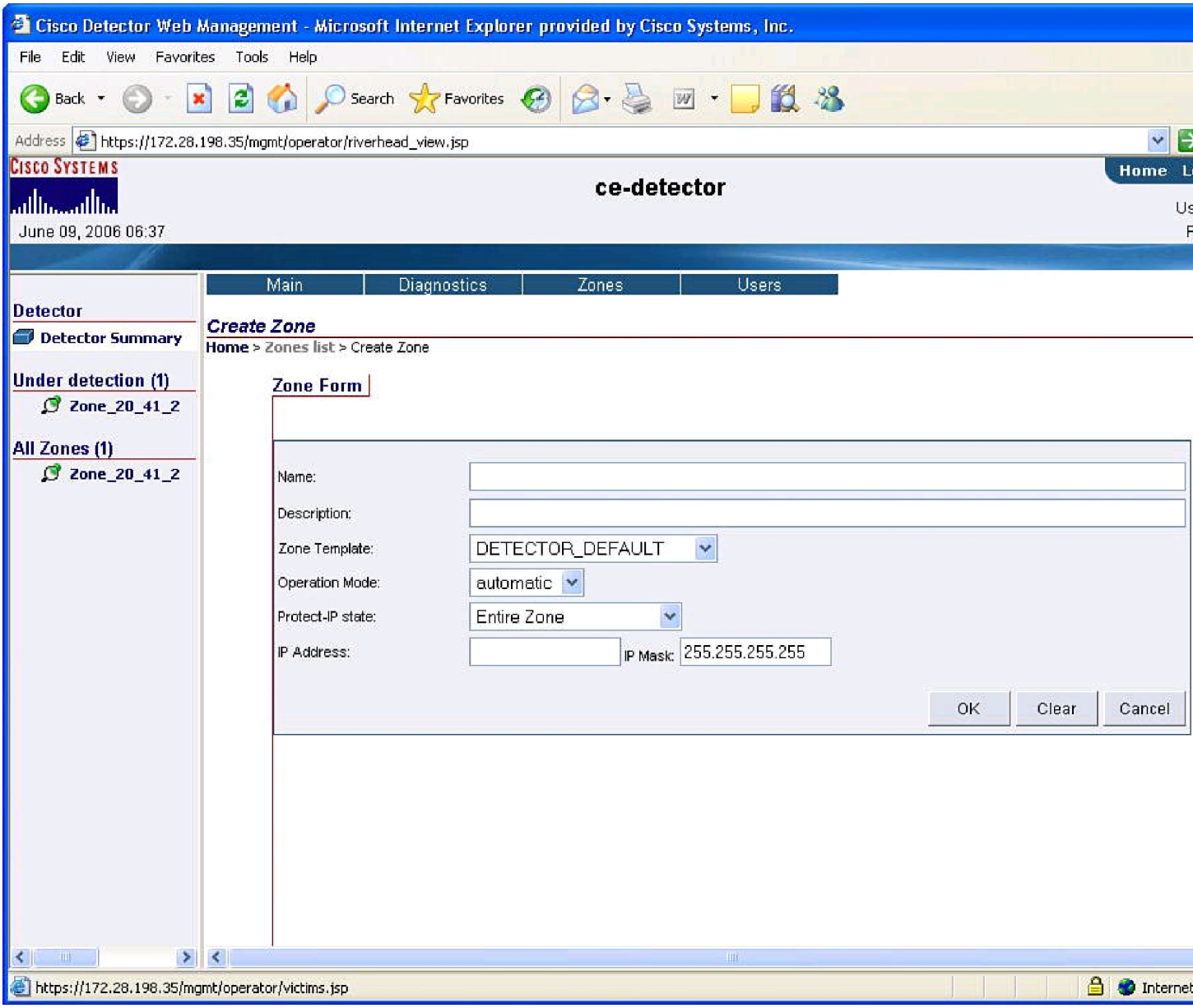
zombies
zones
- Guard
  - *creating in*
  - *filters*
  - *learning phase*
  - *protect mode*
  - *synchronizing in*
  - *traffic diversion*
- policies
  - *construction phase*
  - *templates*
- threshold-tuning phase
- Traffic Anomaly Detector
  - *creating in*
  - *filters*
  - *learning phase*

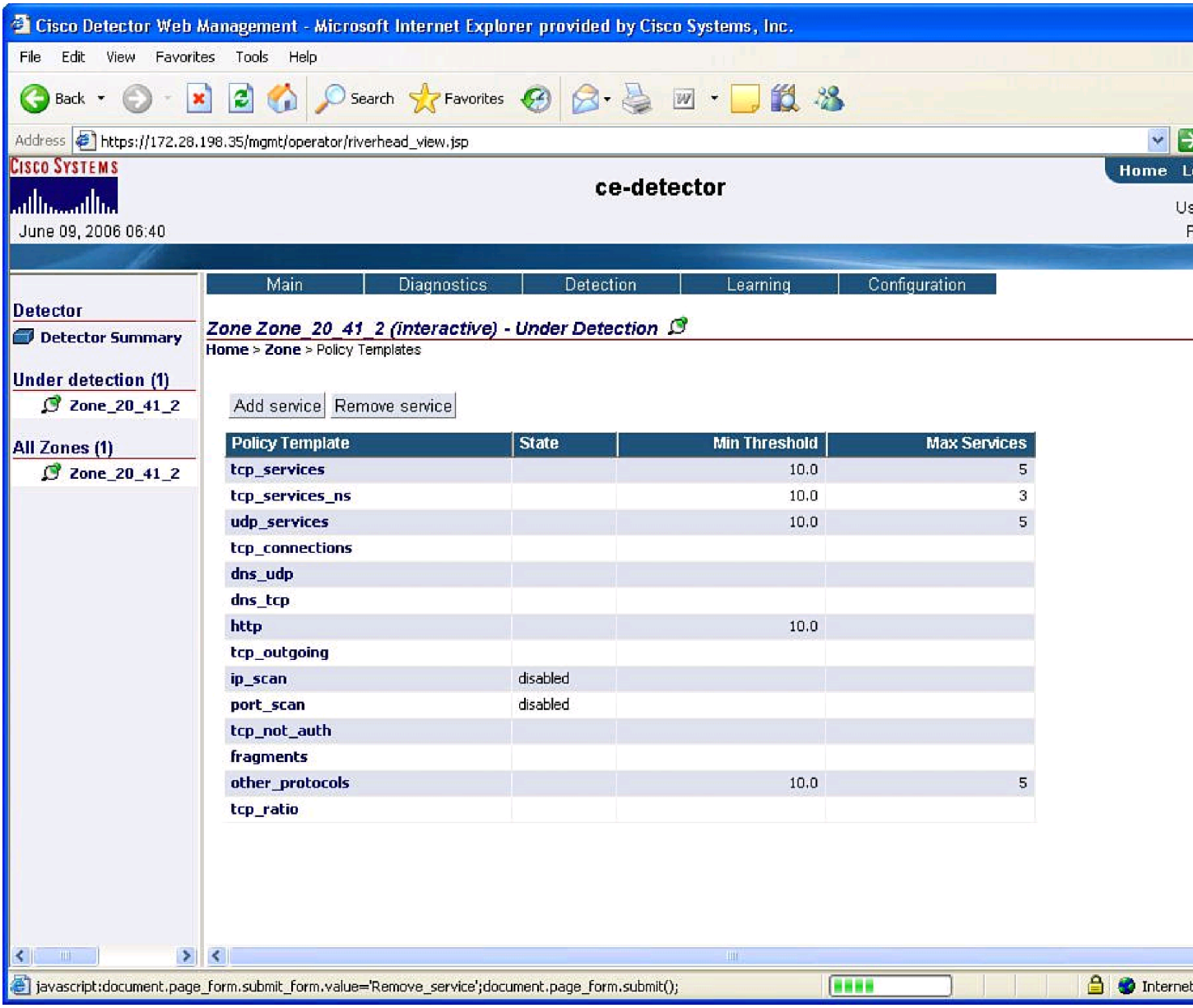

Communication Server
PC
PC with Software
Sun Workstation
Macintosh
Access Server
ISDN/Frame Relay Switch
Token Ring
Token Ring
Terminal
File Server
Web Server
Ciscoworks Workstation
ATM Switch
Modem
Printer
Laptop
IBM Mainframe
Front End Processor
Cluster Controller
Multilayer Switch
Gateway
Router
Bridge
Hub
DSU/CSU
DSU/CSU
FDDI
FDDI
Catalyst Switch
Network Cloud
Line: Ethernet
Line: Serial
Line: Switched Serial
DDoS Detector
PIX Right
Network Management Appliance
CiscoSecurity Manager
DDoS Guard
ASA (Active) CSC Module for Anti-Virus
Catalyst with Firewall Module and NAC
Router with IOS Firewall
NetRanger
Wireless Access Point (Authenticator)

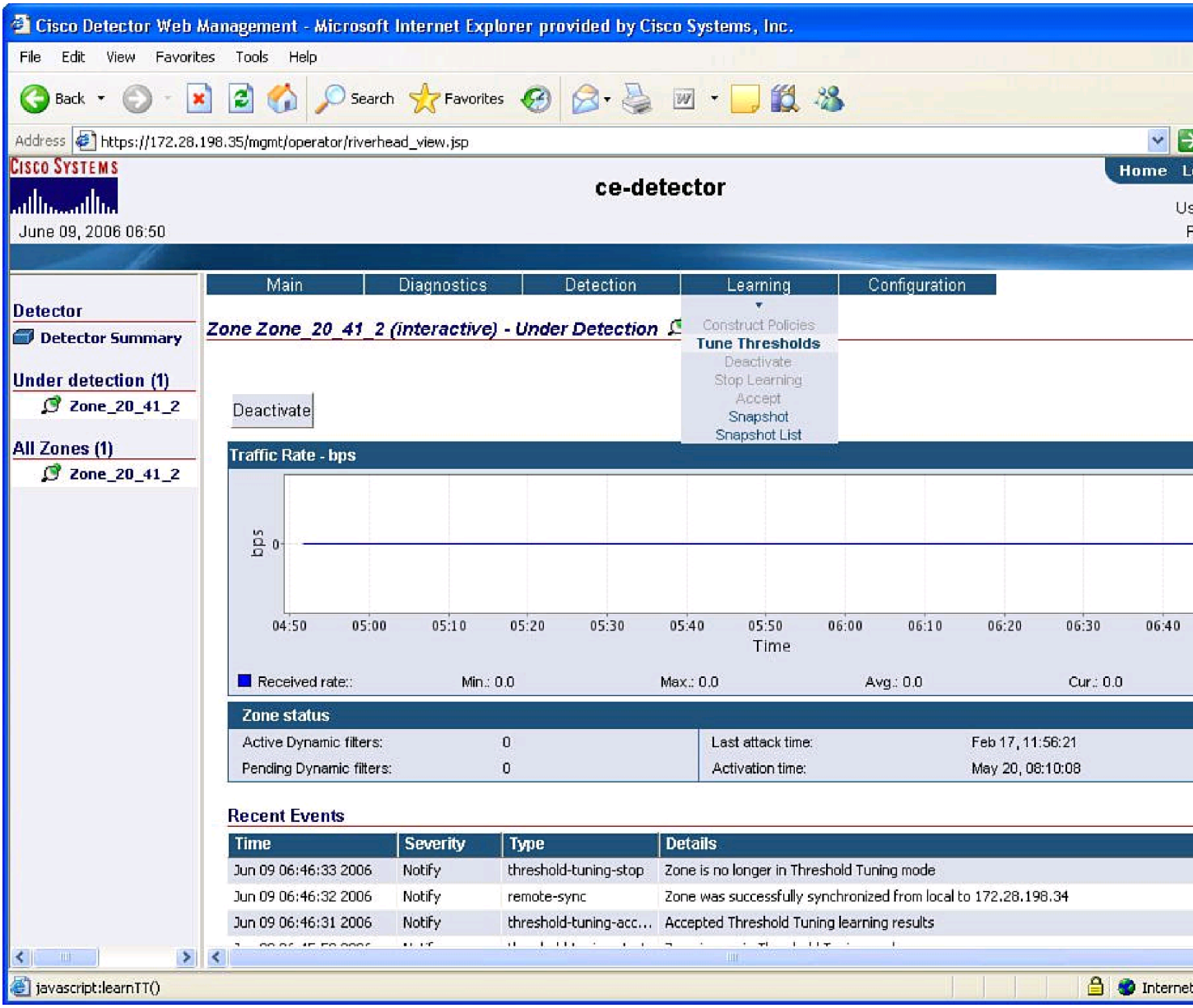

Primary Data Center
Branch Office
Anti-Virus
PIX (Failover)
Internet/WAN
Router
Router
Catalyst with
Firewall Module
IDS
Router with
IOS Firewall
Home Office

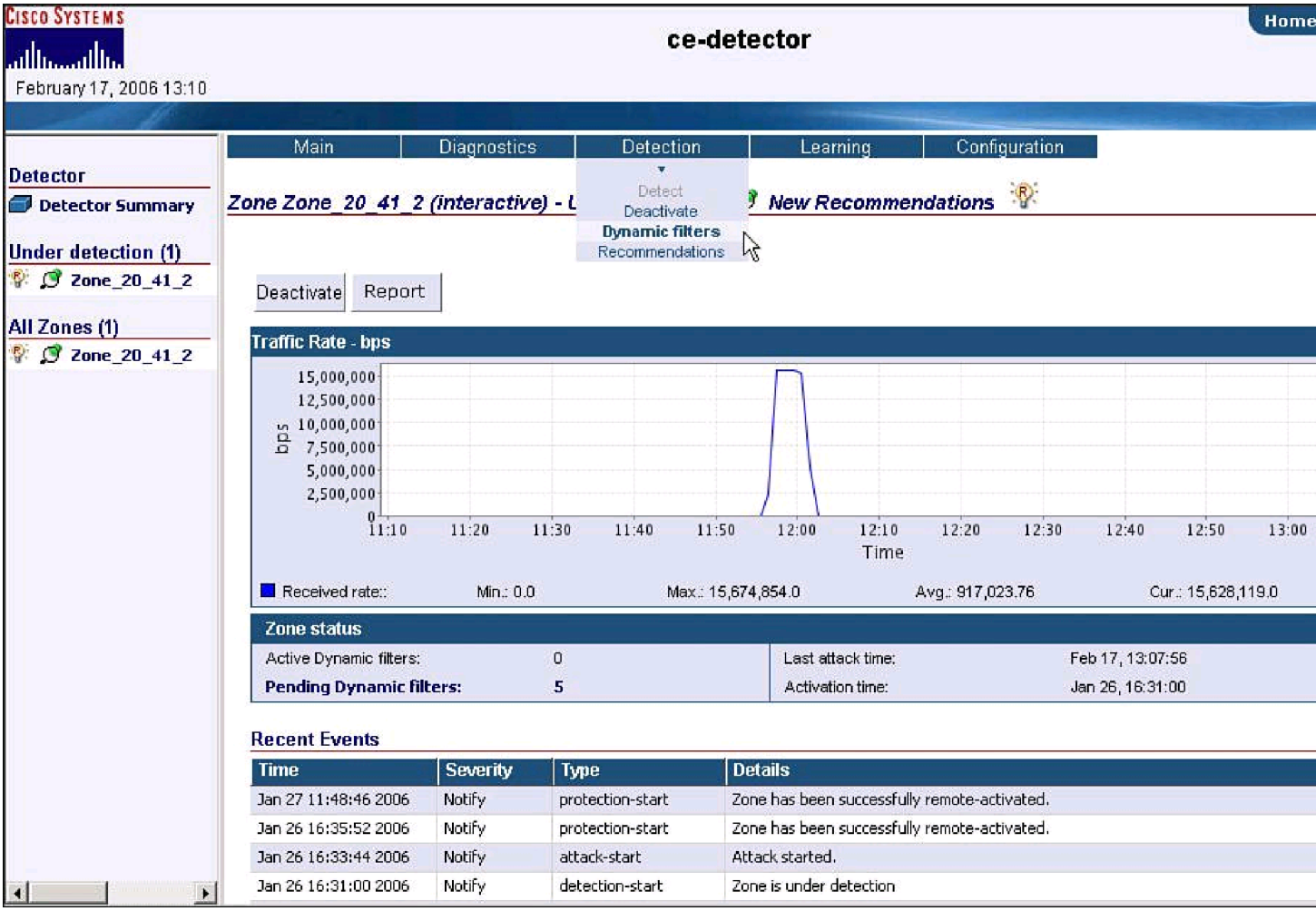

Primary Data Center
Branch Office
CSA
CTA
802.1x
ASA (Active)
CSC Module for
Anti-Virus
DDoS Guard
Internet/WAN
Router with ICS
Router
IPS
Catalyst
with Firewall
Module and
NAC
DDoS Detector
Router with IOS
Firewall and ICS
Centralized Management
CSA
CTA
802.1x
Home Office

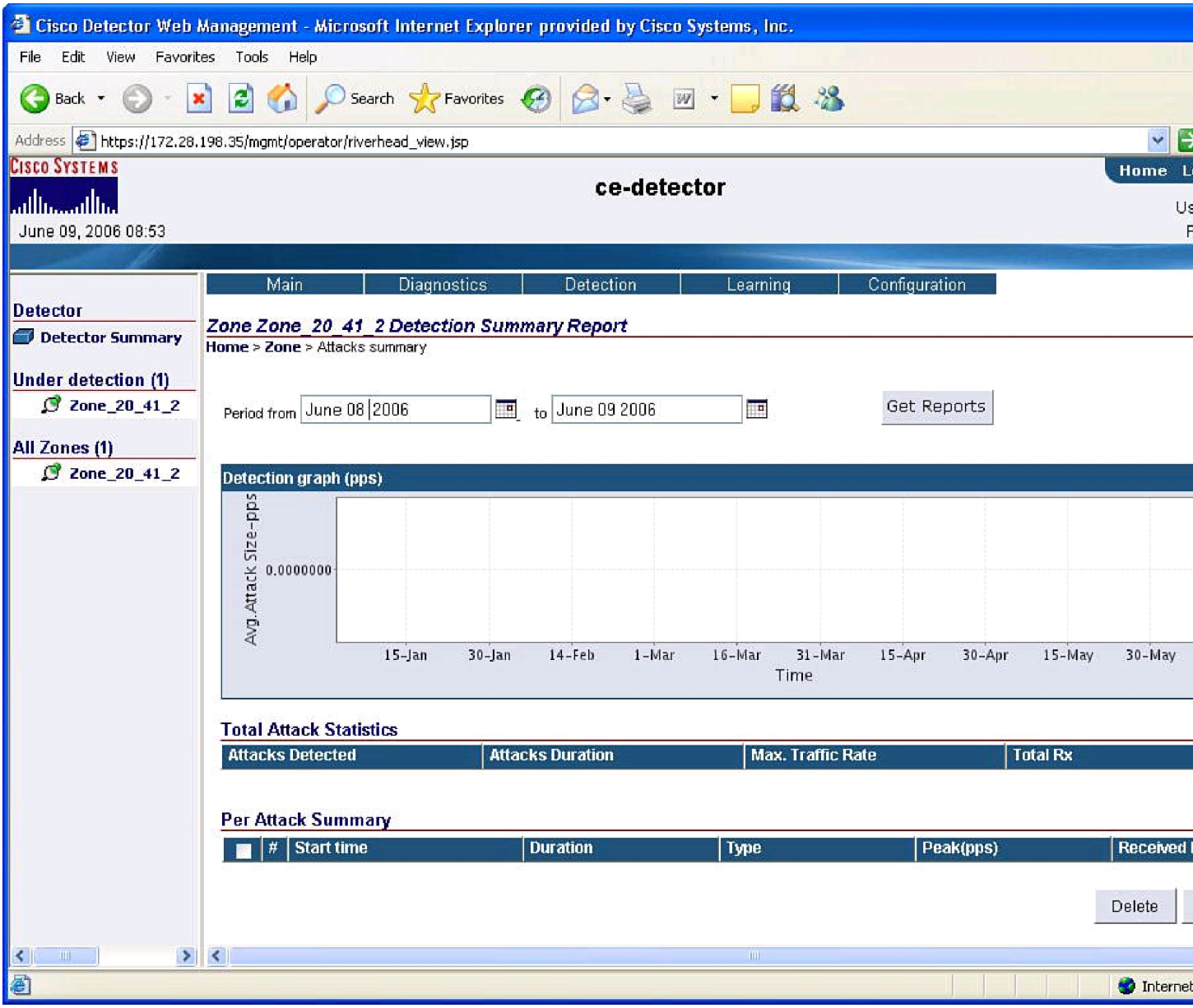

Cisco Detector Web Management - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.28.198.35/mgmt/operator/riverhead_view.jsp
Cisco Systems
ce-detector
Home
June 27, 2006 10:43
Main Diagnostics Zones Users
Detector
Detector Summary
Under detection (1)
Zone_20_41_2
All Zones (1)
Zone_20_41_2
Detector Summary
Received - bps
bps
0
08:50 09:00 09:10 09:20 09:30 09:40 09:50 10:00 10:10 10:20 10:30
Time
Received rate: Min.: 0.0 Max.: 0.0 Avg.: 0.0 Cur.: 0.0
Zones Under Detection
Zone
Activation time
Attack start time
#DF
#PF
Receive rate
Zone_20_41_2
Jun 27, 07:01:19
N/A
0
0
0
Done
Internet

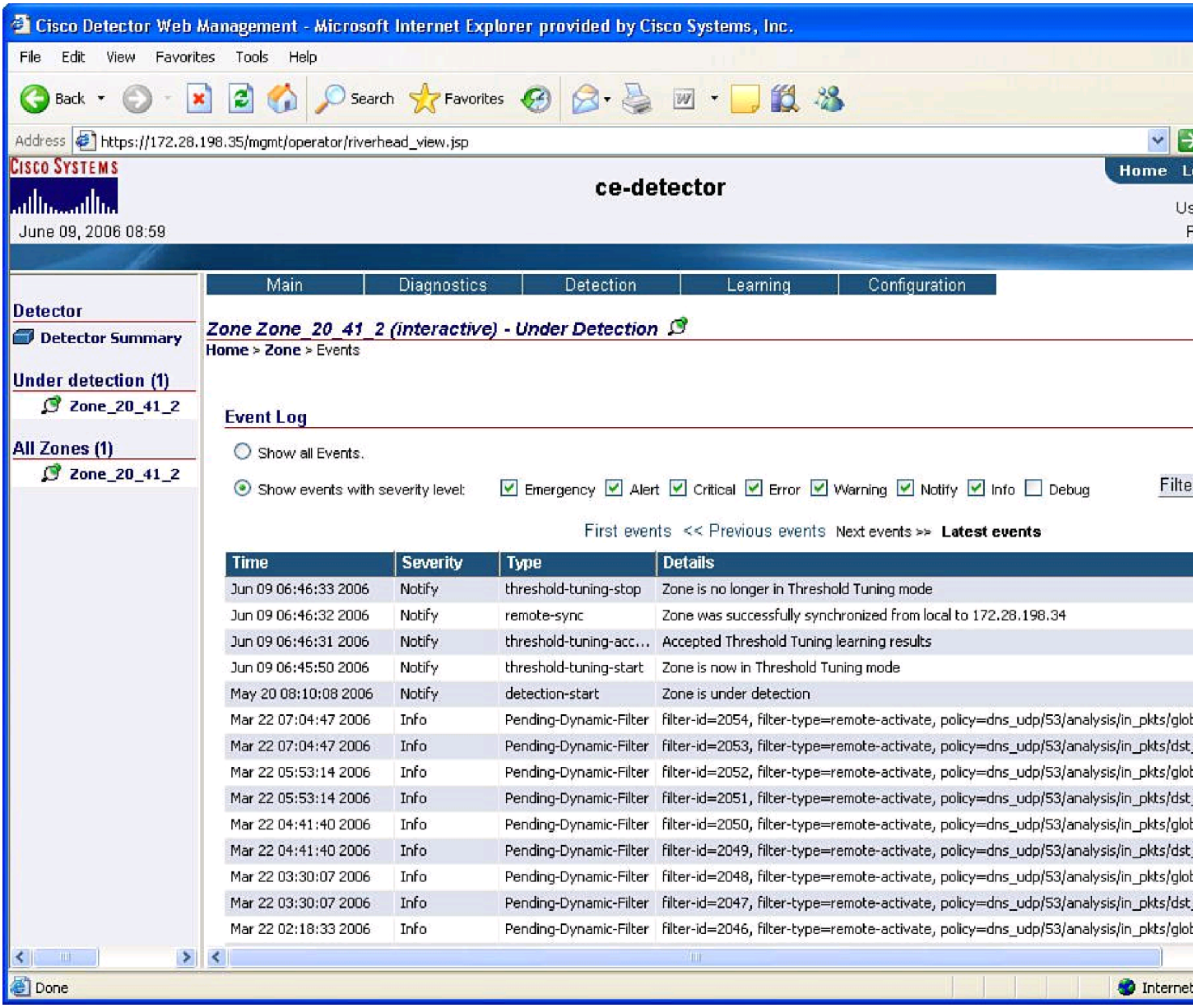

Cisco Detector Web Management - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.28.198.35/mgmt/operator/riverhead_view.jsp
Cisco Systems
ce-detector
Home
June 09, 2006 06:37
Main Diagnostics Zones Users
Detector
Detector Summary
Under detection (1)
Zone_20_41_2
All Zones (1)
Zone_20_41_2
Create Zone
Home > Zones list > Create Zone
Zone Form
Name:
Description:
Zone Template: DETECTOR_DEFAULT
Operation Mode: automatic
Protect-IP state: Entire Zone
IP Address:
IP Mask: 255.255.255.255
OK Clear Cancel
https://172.28.198.35/mgmt/operator/victims.jsp
Internet

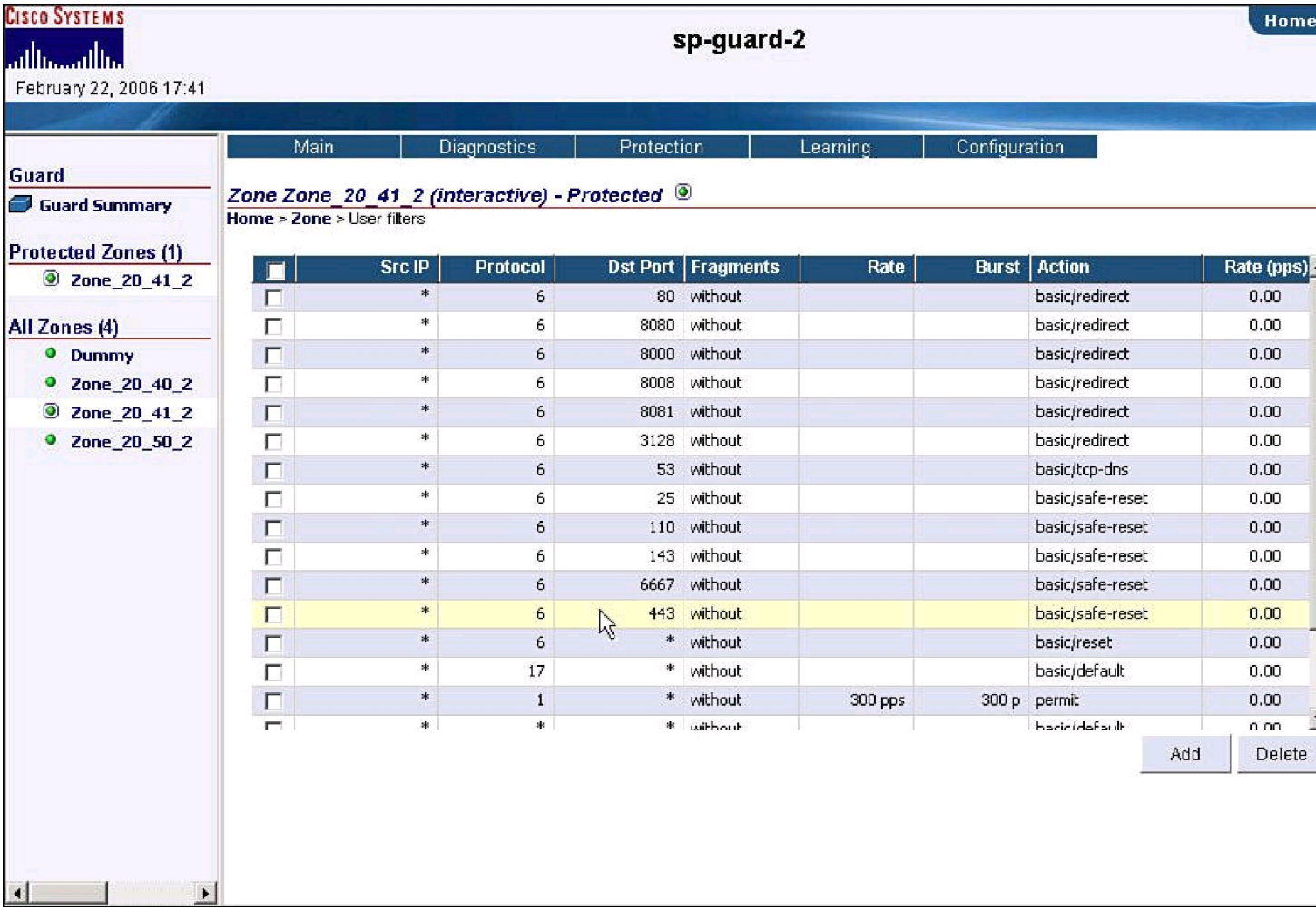

Cisco Detector Web Management - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.28.198.35/mgmt/operator/riverhead_view.jsp
Cisco Systems
ce-detector
Home
June 09, 2006 06:40
Main Diagnostics Detection Learning Configuration
Detector
Detector Summary
Under detection (1)
Zone_20_41_2
All Zones (1)
Zone_20_41_2
Zone Zone_20_41_2 (interactive) - Under Detection
Home > Zone > Policy Templates
Add service Remove service
Policy Template State Min Threshold Max Services
tcp_services 10.0 5
tcp_services_ns 10.0 3
udp_services 10.0 5
tcp_connections
dns_udp
dns_tcp
http 10.0
tcp_outgoing
ip_scan disabled
port_scan disabled
tcp_not_auth
fragments
other_protocols 10.0 5
tcp_ratio
javascript:document.page_form.submit_form.value='Remove_service';document.page_form.submit();
Internet

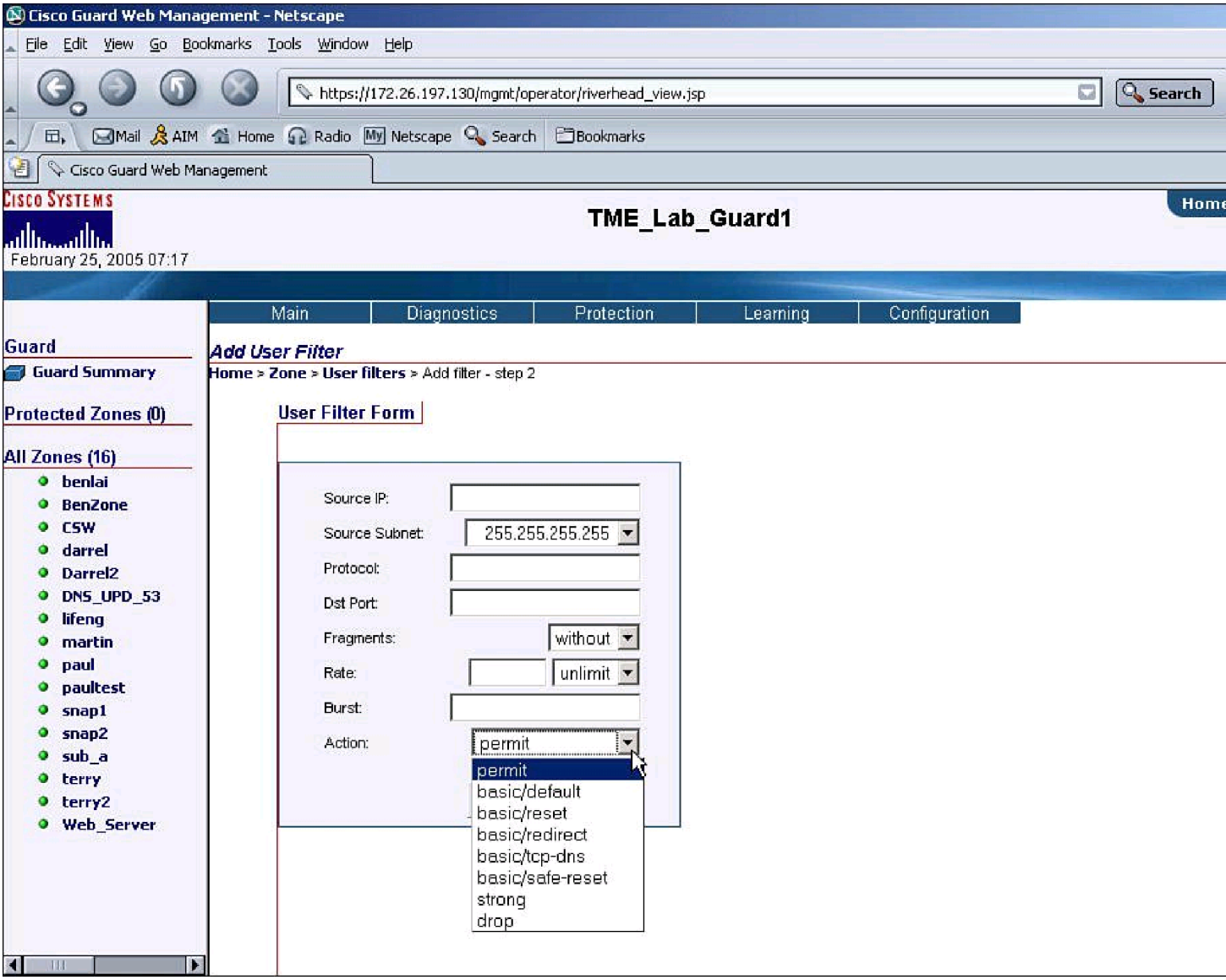

Cisco Detector Web Management - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.28.198.35/mgmt/operator/riverhead_view.jsp
Cisco Systems
ce-detector
Home
June 09, 2006 06:50
Main Diagnostics Detection Learning Configuration
Construct Policies
Tune Thresholds
Deactivate
Stop Learning
Accept
Snapshot
Snapshot List
Detector
Detector Summary
Under detection (1)
Zone_20_41_2
All Zones (1)
Zone_20_41_2
Zone Zone_20_41_2 (interactive) - Under Detection
Deactivate
Traffic Rate - bps
bps
0
04:50 05:00 05:10 05:20 05:30 05:40 05:50 06:00 06:10 06:20 06:30 06:40
Time
Received rate:: Min.: 0.0 Max.: 0.0 Avg.: 0.0 Cur.: 0.0
Zone status
Active Dynamic filters: 0
Pending Dynamic filters: 0
Last attack time: Feb 17, 11:56:21
Activation time: May 20, 08:10:08
Recent Events
Time Severity Type Details
Jun 09 06:46:33 2006 Notify threshold-tuning-stop Zone is no longer in Threshold Tuning mode
Jun 09 06:46:32 2006 Notify remote-sync Zone was successfully synchronized from local to 172.28.198.34
Jun 09 06:46:31 2006 Notify threshold-tuning-acc... Accepted Threshold Tuning learning results
javascript:learnTT()
Internet

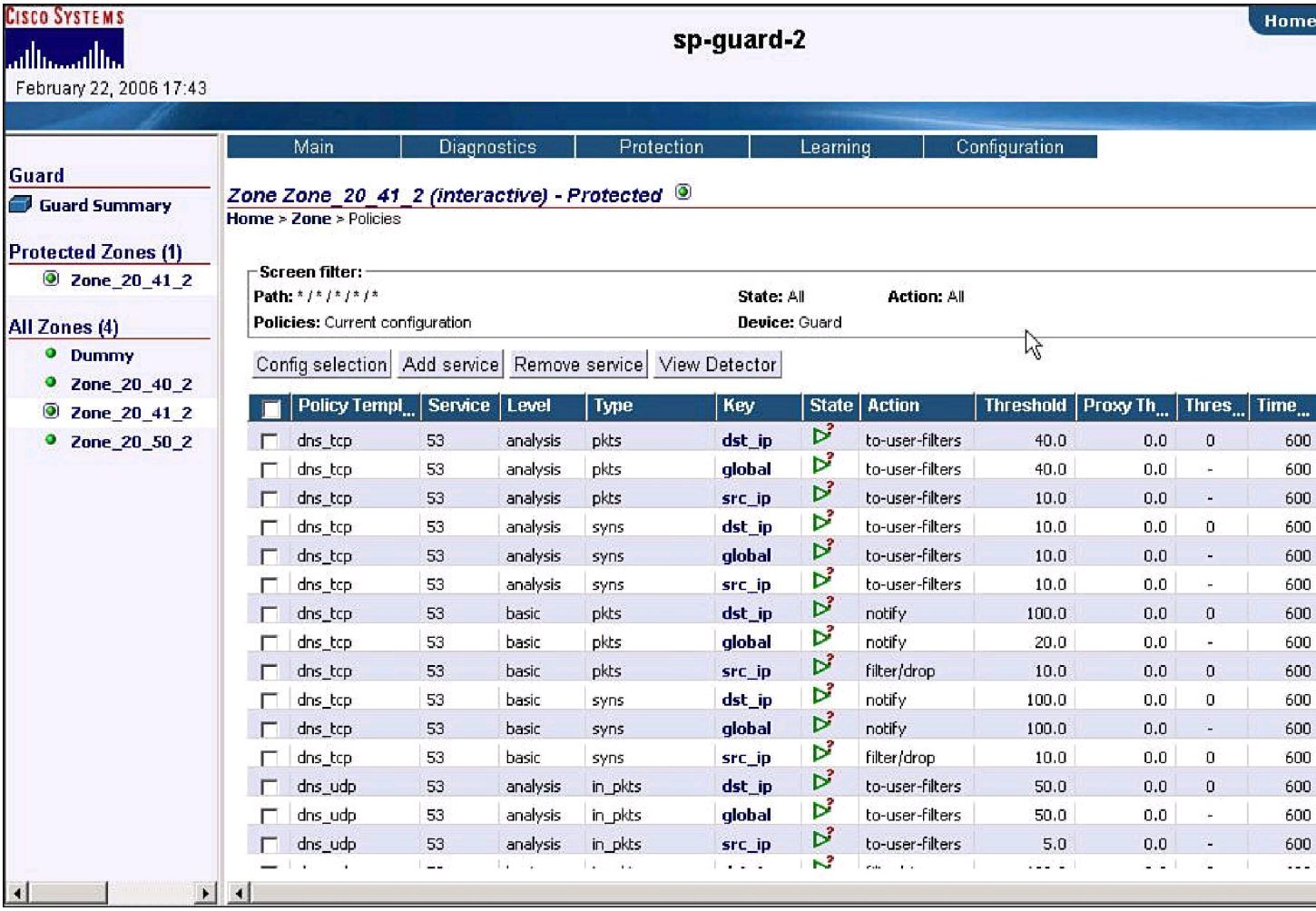

Cisco Systems
ce-detector
Home
February 17, 2006 13:10
Main
Diagnostics
Detection
Learning
Configuration
Detect
Deactivate
Dynamic filters
Recommendations
Detector
Detector Summary
Under detection (1)
Zone_20_41_2
All Zones (1)
Zone_20_41_2
Zone Zone_20_41_2 (interactive) - L
New Recommendations
Deactivate
Report
Traffic Rate - bps
15,000,000
12,500,000
10,000,000
7,500,000
5,000,000
2,500,000
0
bps
11:10
11:20
11:30
11:40
11:50
12:00
12:10
12:20
12:30
12:40
12:50
13:00
Time
Received rate::
Min.: 0.0
Max.: 15,674,854.0
Avg.: 917,023.76
Cur.: 15,628,119.0
Zone status
Active Dynamic filters: 0
Pending Dynamic filters: 5
Last attack time: Feb 17, 13:07:56
Activation time: Jan 26, 16:31:00
Recent Events
Time
Severity
Type
Details
Jan 27 11:48:46 2006
Notify
protection-start
Zone has been successfully remote-activated.
Jan 26 16:35:52 2006
Notify
protection-start
Zone has been successfully remote-activated.
Jan 26 16:33:44 2006
Notify
attack-start
Attack started.
Jan 26 16:31:00 2006
Notify
detection-start
Zone is under detection

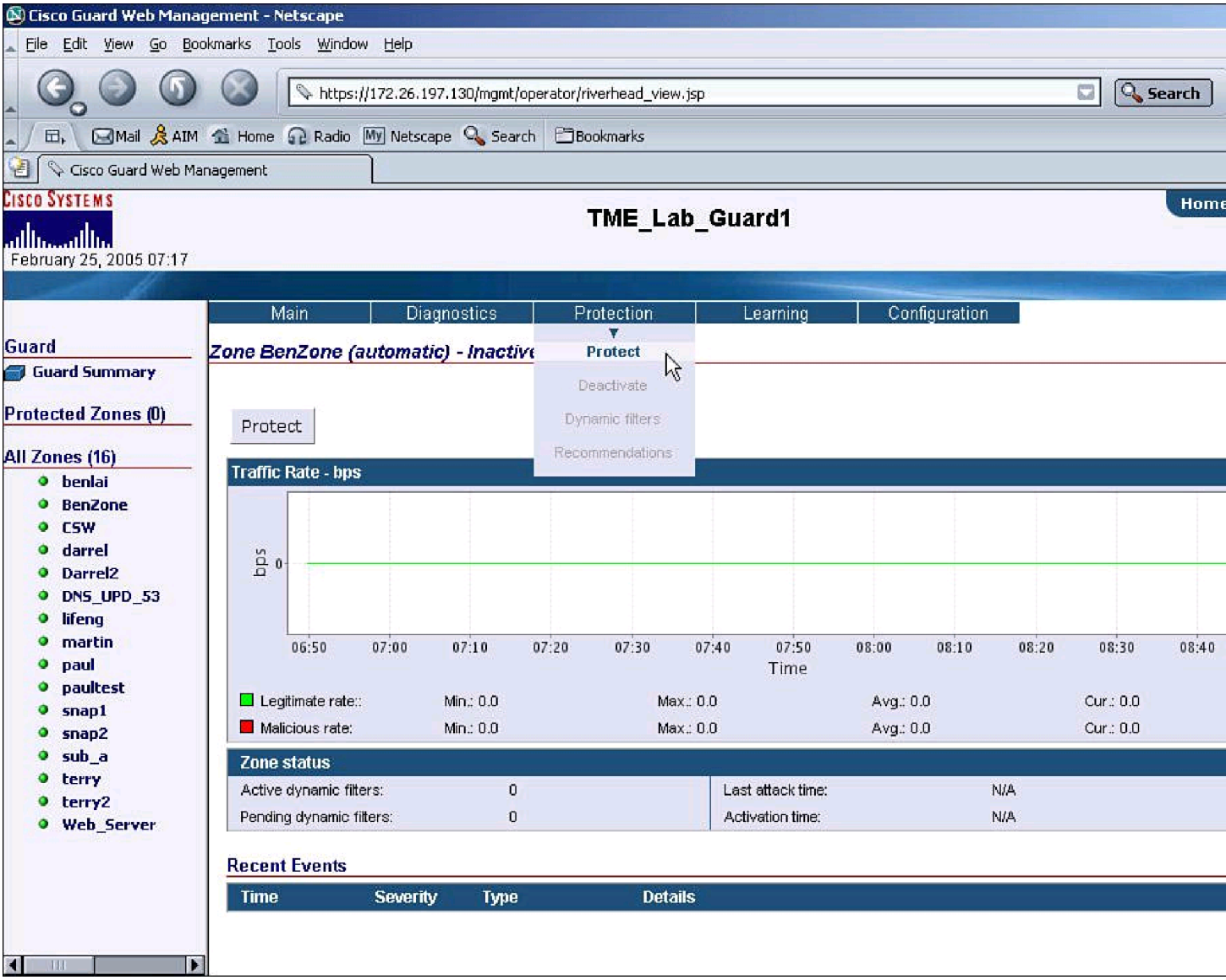

Cisco Detector Web Management - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.28.198.35/mgmt/operator/riverhead_view.jsp
Cisco Systems
ce-detector
Home
June 09, 2006 08:53
Main Diagnostics Detection Learning Configuration
Detector
Detector Summary
Under detection (1)
Zone_20_41_2
All Zones (1)
Zone_20_41_2
Zone Zone_20_41_2 Detection Summary Report
Home > Zone > Attacks summary
Period from June 08 2006 to June 09 2006
Get Reports
Detection graph (pps)
Avg.Attack Size-pps
0.0000000
15-Jan 30-Jan 14-Feb 1-Mar 16-Mar 31-Mar 15-Apr 30-Apr 15-May 30-May
Time
Total Attack Statistics
Attacks Detected
Attacks Duration
Max. Traffic Rate
Total Rx
Per Attack Summary
#
Start time
Duration
Type
Peak(pps)
Received
Delete
Internet

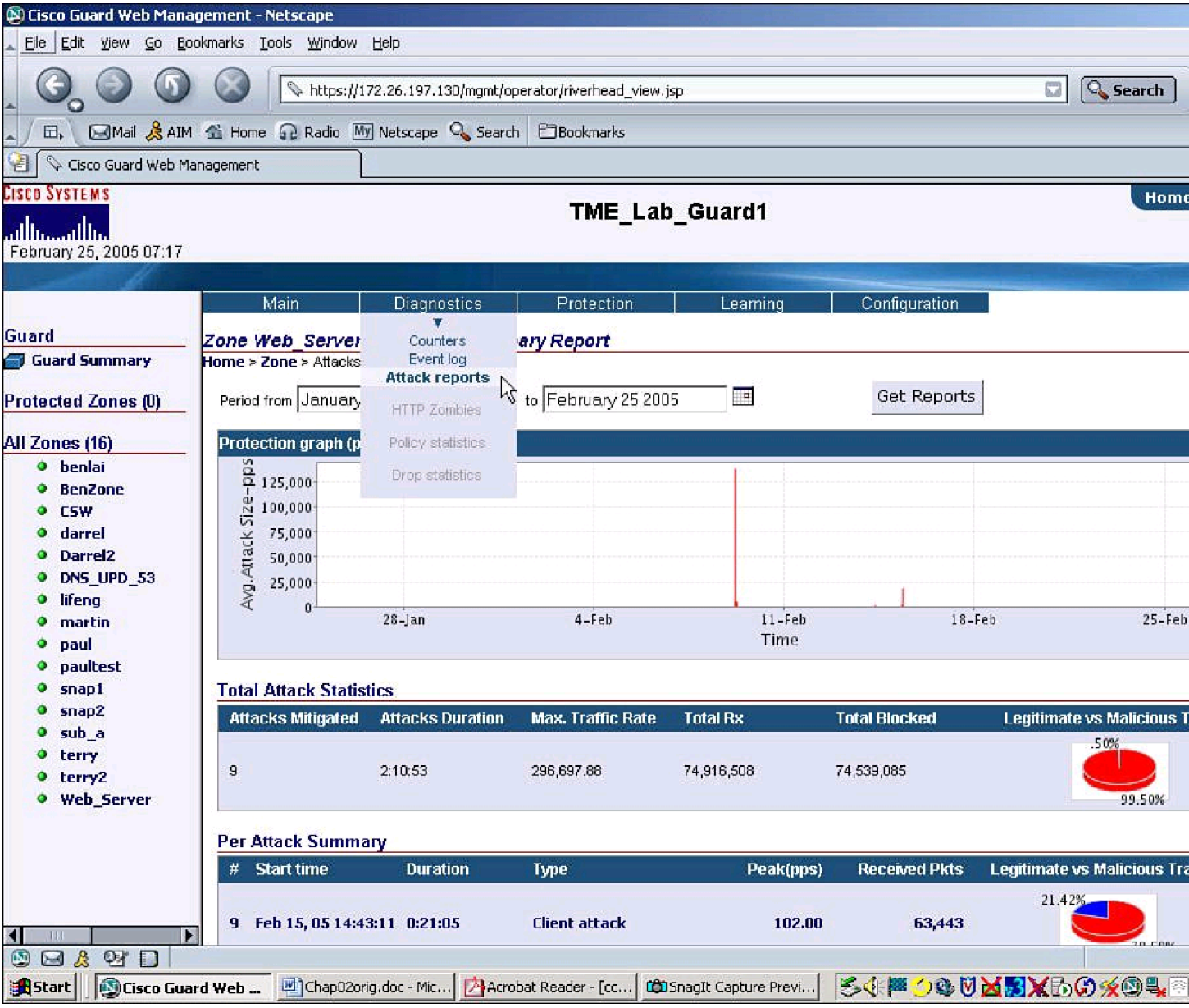

Cisco Detector Web Management - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.28.198.35/mgmt/operator/riverhead_view.jsp
Cisco Systems
ce-detector
Home
June 09, 2006 08:59
Main Diagnostics Detection Learning Configuration
Detector
Detector Summary
Under detection (1)
Zone_20_41_2
All Zones (1)
Zone_20_41_2
Zone Zone_20_41_2 (interactive) - Under Detection
Home > Zone > Events
Event Log
Show all Events.
Show events with severity level: Emergency Alert Critical Error Warning Notify Info Debug
First events << Previous events Next events >> Latest events
Time Severity Type Details
Jun 09 06:46:33 2006 Notify threshold-tuning-stop Zone is no longer in Threshold Tuning mode
Jun 09 06:46:32 2006 Notify remote-sync Zone was successfully synchronized from local to 172.28.198.34
Jun 09 06:46:31 2006 Notify threshold-tuning-acc... Accepted Threshold Tuning learning results
Jun 09 06:45:50 2006 Notify threshold-tuning-start Zone is now in Threshold Tuning mode
May 20 08:10:08 2006 Notify detection-start Zone is under detection
Mar 22 07:04:47 2006 Info Pending-Dynamic-Filter filter-id=2054, filter-type=remote-activate, policy=dns_udp/53/analysis/in_pkts/glob
Mar 22 07:04:47 2006 Info Pending-Dynamic-Filter filter-id=2053, filter-type=remote-activate, policy=dns_udp/53/analysis/in_pkts/dst_
Mar 22 05:53:14 2006 Info Pending-Dynamic-Filter filter-id=2052, filter-type=remote-activate, policy=dns_udp/53/analysis/in_pkts/glob
Mar 22 05:53:14 2006 Info Pending-Dynamic-Filter filter-id=2051, filter-type=remote-activate, policy=dns_udp/53/analysis/in_pkts/dst_
Mar 22 04:41:40 2006 Info Pending-Dynamic-Filter filter-id=2050, filter-type=remote-activate, policy=dns_udp/53/analysis/in_pkts/glob
Mar 22 04:41:40 2006 Info Pending-Dynamic-Filter filter-id=2049, filter-type=remote-activate, policy=dns_udp/53/analysis/in_pkts/dst_
Mar 22 03:30:07 2006 Info Pending-Dynamic-Filter filter-id=2048, filter-type=remote-activate, policy=dns_udp/53/analysis/in_pkts/glob
Mar 22 03:30:07 2006 Info Pending-Dynamic-Filter filter-id=2047, filter-type=remote-activate, policy=dns_udp/53/analysis/in_pkts/dst_
Mar 22 02:18:33 2006 Info Pending-Dynamic-Filter filter-id=2046, filter-type=remote-activate, policy=dns_udp/53/analysis/in_pkts/glob
Done
Internet

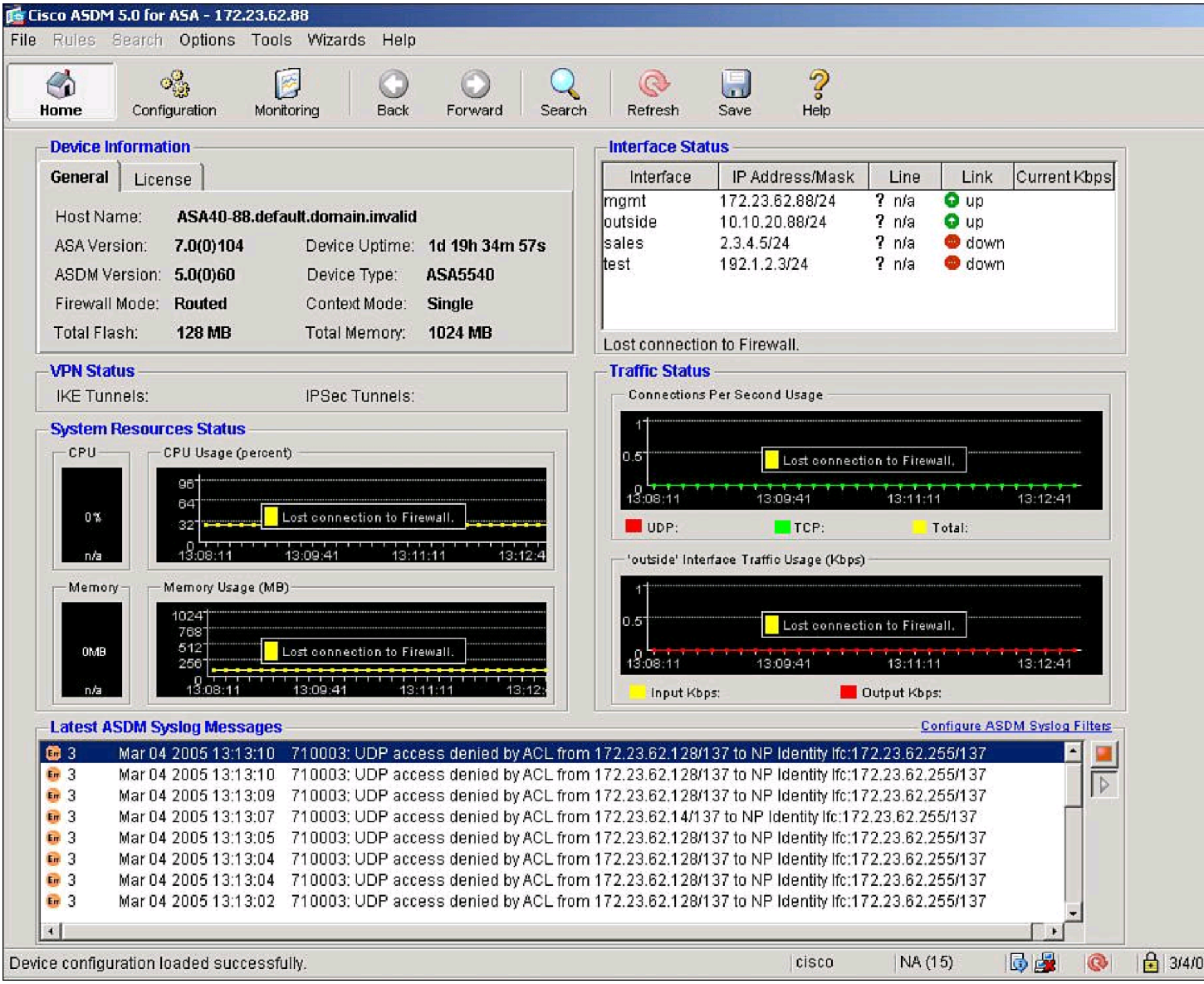

Cisco Systems
sp-guard-2
Home
February 22, 2006 17:41
Main
Diagnostics
Protection
Learning
Configuration
Guard
Guard Summary
Protected Zones (1)
Zone_20_41_2
All Zones (4)
Dummy
Zone_20_40_2
Zone_20_41_2
Zone_20_50_2
Zone Zone_20_41_2 (interactive) - Protected
Home > Zone > User filters
Src IP | Protocol | Dst Port | Fragments | Rate | Burst | Action | Rate (pps)
* | 6 | 80 | without | basic/redirect | 0.00
* | 6 | 8080 | without | basic/redirect | 0.00
* | 6 | 8000 | without | basic/redirect | 0.00
* | 6 | 8008 | without | basic/redirect | 0.00
* | 6 | 8081 | without | basic/redirect | 0.00
* | 6 | 3128 | without | basic/redirect | 0.00
* | 6 | 53 | without | basic/tcp-dns | 0.00
* | 6 | 25 | without | basic/safe-reset | 0.00
* | 6 | 110 | without | basic/safe-reset | 0.00
* | 6 | 143 | without | basic/safe-reset | 0.00
* | 6 | 6667 | without | basic/safe-reset | 0.00
* | 6 | 443 | without | basic/safe-reset | 0.00
* | 6 | * | without | basic/reset | 0.00
* | 17 | * | without | basic/default | 0.00
* | 1 | * | without | 300 pps | 300 p | permit | 0.00
Add
Delete

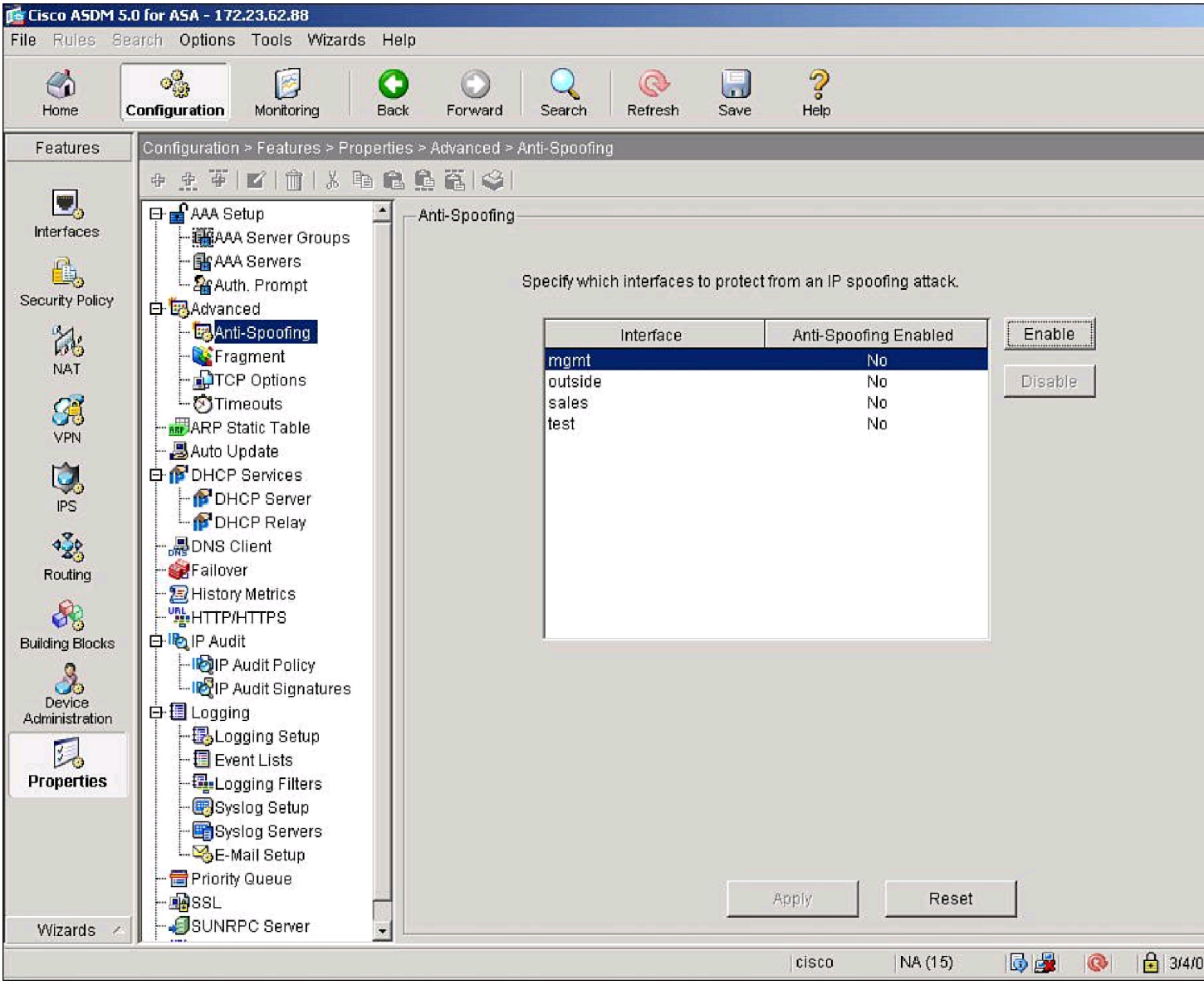

Cisco Guard Web Management - Netscape
File Edit View Go Bookmarks Tools Window Help
https://172.26.197.130/mgmt/operator/riverhead_view.jsp
Search
Mail AIM Home Radio Netscape Search Bookmarks
Cisco Guard Web Management
Cisco Systems
February 25, 2005 07:17
TME_Lab_Guard1
Home
Main Diagnostics Protection Learning Configuration
Guard
Guard Summary
Protected Zones (0)
All Zones (16)
benlai
BenZone
CSW
darrel
Darrel2
DNS_UPD_53
lifeng
martin
paul
paultest
snap1
snap2
sub_a
terry
terry2
Web_Server
Add User Filter
Home > Zone > User filters > Add filter - step 2
User Filter Form
Source IP:
Source Subnet: 255.255.255.255
Protocol:
Dst Port:
Fragments: without
Rate: unlimit
Burst:
Action: permit
permit
basic/default
basic/reset
basic/redirect
basic/tcp-dns
basic/safe-reset
strong
drop

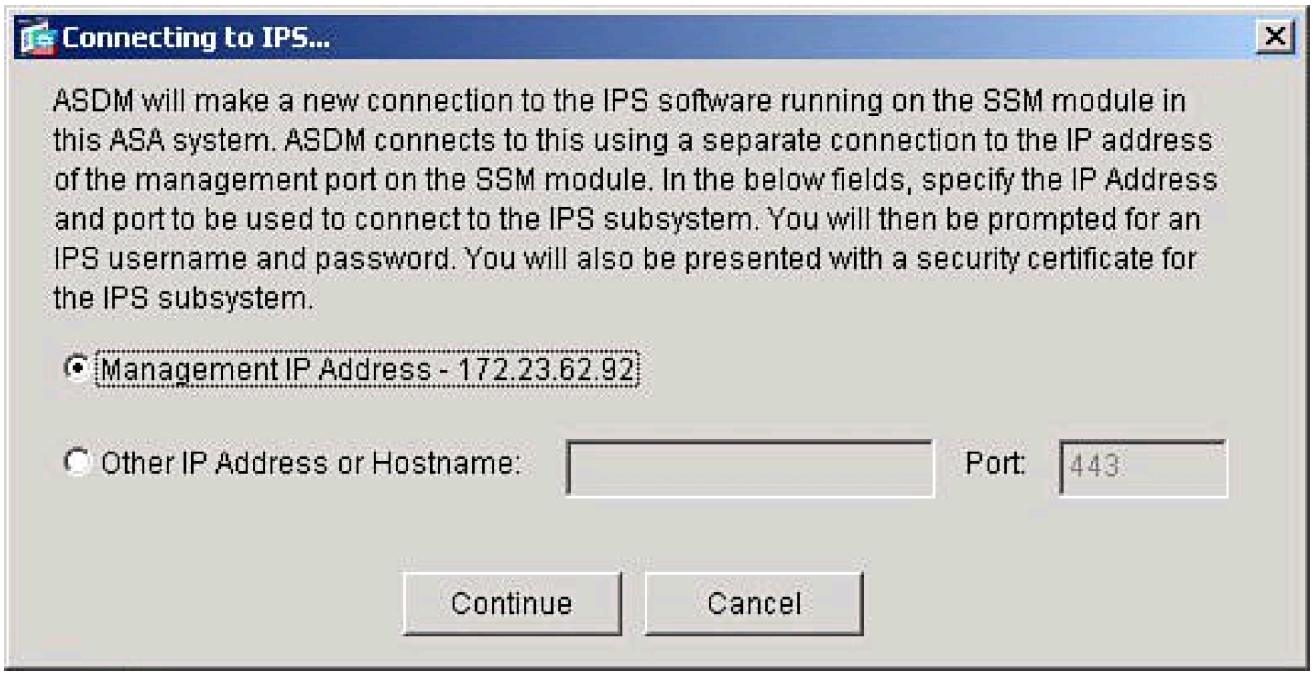

Cisco Systems
sp-guard-2
Home
February 22, 2006 17:43
Main
Diagnostics
Protection
Learning
Configuration
Guard
Guard Summary
Protected Zones (1)
Zone_20_41_2
All Zones (4)
Dummy
Zone_20_40_2
Zone_20_41_2
Zone_20_50_2
Zone Zone_20_41_2 (interactive) - Protected
Home > Zone > Policies
Screen filter:
Path: * / * / * / * / *
State: All
Action: All
Policies: Current configuration
Device: Guard
Config selection
Add service
Remove service
View Detector
Policy Templ...
Service
Level
Type
Key
State
Action
Threshold
Proxy Th...
Thres...
Time...
dns_tcp 53 analysis pkts dst_ip to-user-filters 40.0 0.0 0 600
dns_tcp 53 analysis pkts global to-user-filters 40.0 0.0 - 600
dns_tcp 53 analysis pkts src_ip to-user-filters 10.0 0.0 - 600
dns_tcp 53 analysis syns dst_ip to-user-filters 10.0 0.0 0 600
dns_tcp 53 analysis syns global to-user-filters 10.0 0.0 - 600
dns_tcp 53 analysis syns src_ip to-user-filters 10.0 0.0 - 600
dns_tcp 53 basic pkts dst_ip notify 100.0 0.0 0 600
dns_tcp 53 basic pkts global notify 20.0 0.0 - 600
dns_tcp 53 basic pkts src_ip filter/drop 10.0 0.0 0 600
dns_tcp 53 basic syns dst_ip notify 100.0 0.0 0 600
dns_tcp 53 basic syns global notify 100.0 0.0 - 600
dns_tcp 53 basic syns src_ip filter/drop 10.0 0.0 0 600
dns_udp 53 analysis in_pkts dst_ip to-user-filters 50.0 0.0 0 600
dns_udp 53 analysis in_pkts global to-user-filters 50.0 0.0 - 600
dns_udp 53 analysis in_pkts src_ip to-user-filters 5.0 0.0 - 600

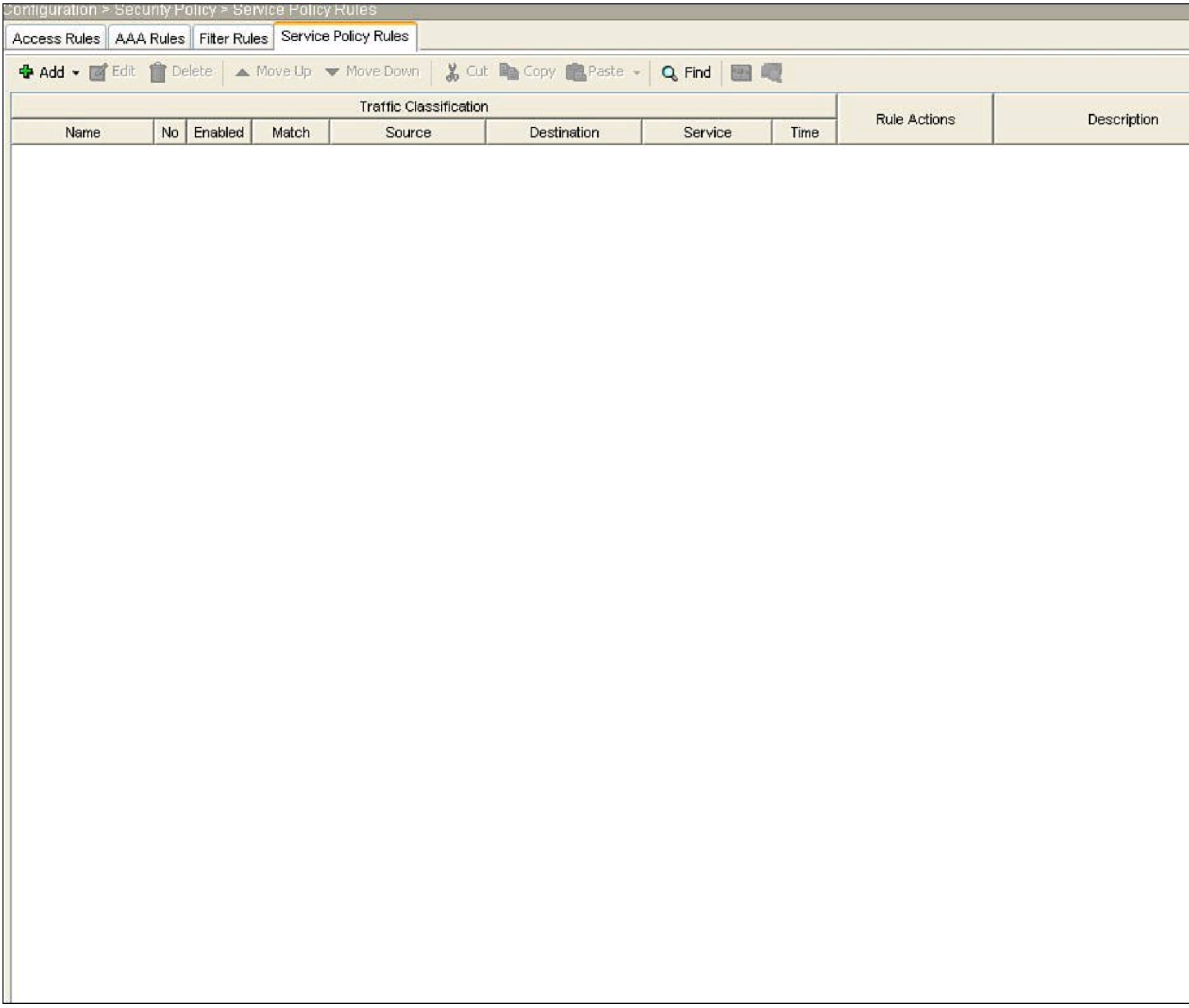

Cisco Guard Web Management - Netscape
File Edit View Go Bookmarks Tools Window Help
https://172.26.197.130/mgmt/operator/riverhead_view.jsp
Search
Mail AIM Home Radio Netscape Search Bookmarks
Cisco Guard Web Management
Cisco Systems
February 25, 2005 07:17
TME_Lab_Guard1
Home
Main
Diagnostics
Protection
Learning
Configuration
Protect
Deactivate
Dynamic filters
Recommendations
Guard
Guard Summary
Protected Zones (0)
All Zones (16)
benlai
BenZone
CSW
darrel
Darrel2
DNS_UPD_53
lifeng
martin
paul
paultest
snap1
snap2
sub_a
terry
terry2
Web_Server
Zone BenZone (automatic) - Inactive
Protect
Traffic Rate - bps
bps
0
06:50
07:00
07:10
07:20
07:30
07:40
07:50
08:00
08:10
08:20
08:30
08:40
Time
Legitimate rate:: Min.: 0.0 Max.: 0.0 Avg.: 0.0 Cur.: 0.0
Malicious rate: Min.: 0.0 Max.: 0.0 Avg.: 0.0 Cur.: 0.0
Zone status
Active dynamic filters: 0
Pending dynamic filters: 0
Last attack time: N/A
Activation time: N/A
Recent Events
Time
Severity
Type
Details

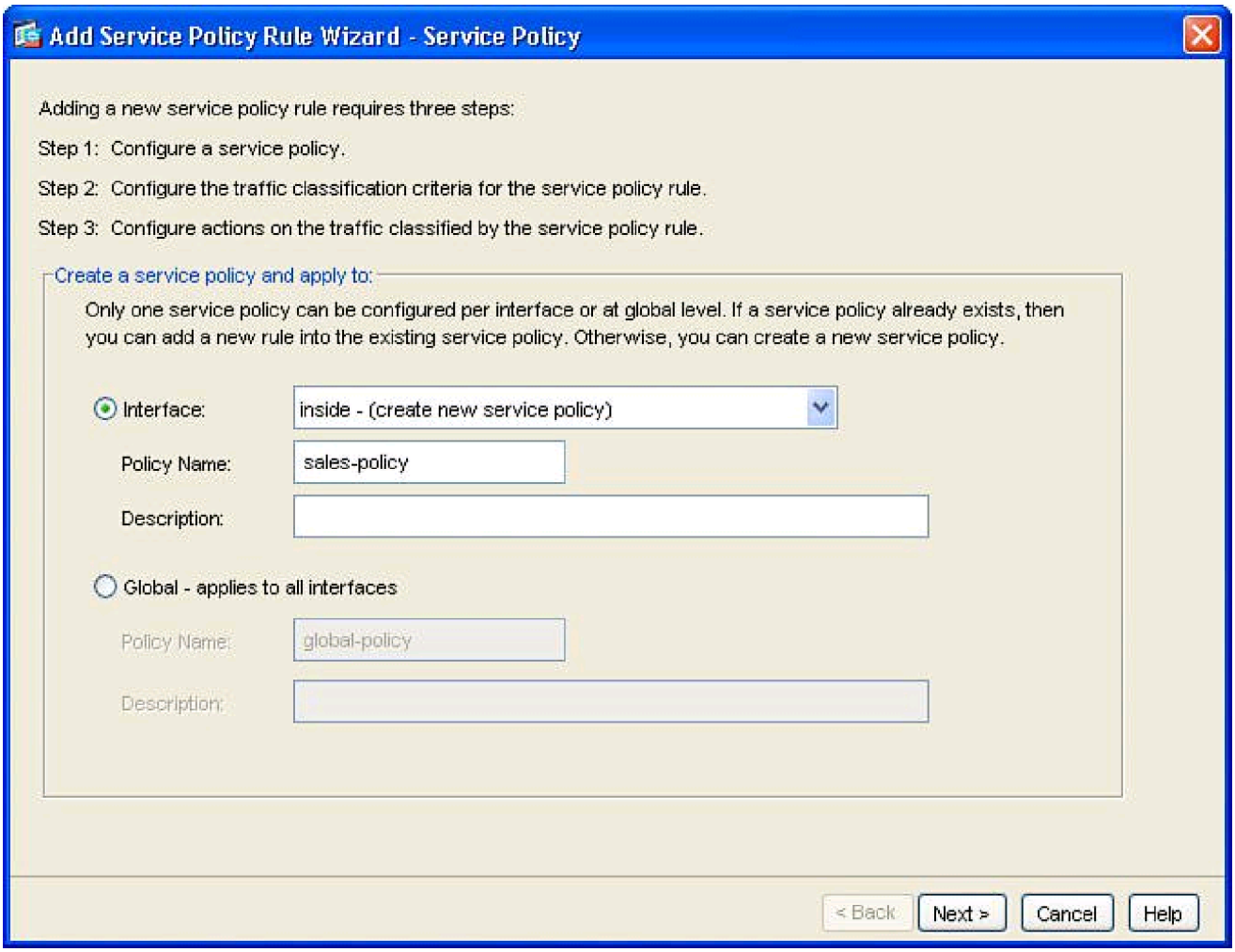

Cisco Guard Web Management - Netscape
File Edit View Go Bookmarks Tools Window Help
https://172.26.197.130/mgmt/operator/riverhead_view.jsp
Search
Mail AIM Home Radio Netscape Search Bookmarks
Cisco Guard Web Management
Cisco Systems
February 25, 2005 07:17
TME_Lab_Guard1
Home
Main
Diagnostics
Protection
Learning
Configuration
Counters
Event log
Attack reports
HTTP Zombies
Policy statistics
Drop statistics
Guard
Guard Summary
Protected Zones (0)
All Zones (16)
benlai
BenZone
CSW
darrel
Darrel2
DNS_UPD_53
lifeng
martin
paul
paultest
snap1
snap2
sub_a
terry
terry2
Web_Server
Zone Web_Server
ary Report
Home > Zone > Attacks
Period from January
to February 25 2005
Get Reports
Protection graph (p
Avg.Attack Size-pps
125,000
100,000
75,000
50,000
25,000
0
28-Jan
4-Feb
11-Feb
18-Feb
25-Feb
Time
Total Attack Statistics
Attacks Mitigated
Attacks Duration
Max. Traffic Rate
Total Rx
Total Blocked
Legitimate vs Malicious T
9
2:10:53
296,697.88
74,916,508
74,539,085
.50%
99.50%
Per Attack Summary
Start time Duration Type Peak(pps) Received Pkts Legitimate vs Malicious Tra
9 Feb 15, 05 14:43:11 0:21:05 Client attack 102.00 63,443
21.42%
Start
Cisco Guard Web ...
Chap02orig.doc - Mic...
Acrobat Reader - [cc...
SnagIt Capture Previ...

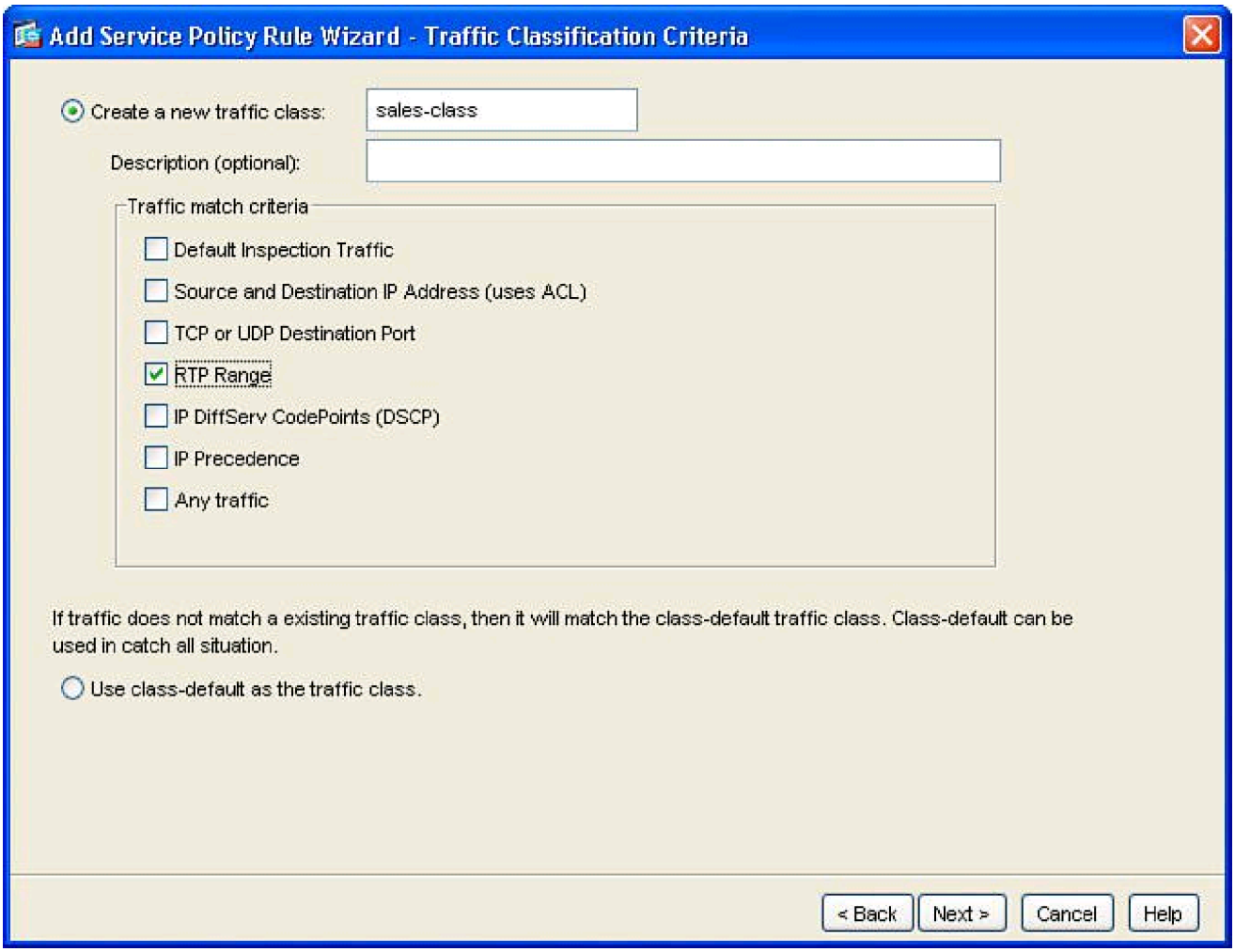

Cisco ASDM 5.0 for ASA - 172.23.62.88
File Rules Search Options Tools Wizards Help
Home
Configuration
Monitoring
Back
Forward
Search
Refresh
Save
Help
Device Information
General
License
Host Name: ASA40-88.default.domain.invalid
ASA Version: 7.0(0)104
Device Uptime: 1d 19h 34m 57s
ASDM Version: 5.0(0)60
Device Type: ASA5540
Firewall Mode: Routed
Context Mode: Single
Total Flash: 128 MB
Total Memory: 1024 MB
Interface Status
Interface
IP Address/Mask
Line
Link
Current Kbps
mgmt 172.23.62.88/24 ? n/a up
outside 10.10.20.88/24 ? n/a up
sales 2.3.4.5/24 ? n/a down
test 192.1.2.3/24 ? n/a down
Lost connection to Firewall.
VPN Status
IKE Tunnels:
IPSec Tunnels:
System Resources Status
CPU
CPU Usage (percent)
Lost connection to Firewall.
Memory
Memory Usage (MB)
Traffic Status
Connections Per Second Usage
UDP:
TCP:
Total:
'outside' Interface Traffic Usage (Kbps)
Input Kbps:
Output Kbps:
Latest ASDM Syslog Messages
Configure ASDM Syslog Filters
3 Mar 04 2005 13:13:10 710003: UDP access denied by ACL from 172.23.62.128/137 to NP Identity Ifc:172.23.62.255/137
3 Mar 04 2005 13:13:10 710003: UDP access denied by ACL from 172.23.62.128/137 to NP Identity Ifc:172.23.62.255/137
3 Mar 04 2005 13:13:09 710003: UDP access denied by ACL from 172.23.62.128/137 to NP Identity Ifc:172.23.62.255/137
3 Mar 04 2005 13:13:07 710003: UDP access denied by ACL from 172.23.62.14/137 to NP Identity Ifc:172.23.62.255/137
3 Mar 04 2005 13:13:05 710003: UDP access denied by ACL from 172.23.62.128/137 to NP Identity Ifc:172.23.62.255/137
3 Mar 04 2005 13:13:04 710003: UDP access denied by ACL from 172.23.62.128/137 to NP Identity Ifc:172.23.62.255/137
3 Mar 04 2005 13:13:04 710003: UDP access denied by ACL from 172.23.62.128/137 to NP Identity Ifc:172.23.62.255/137
3 Mar 04 2005 13:13:02 710003: UDP access denied by ACL from 172.23.62.128/137 to NP Identity Ifc:172.23.62.255/137
Device configuration loaded successfully.
cisco
NA (15)
3/4/0

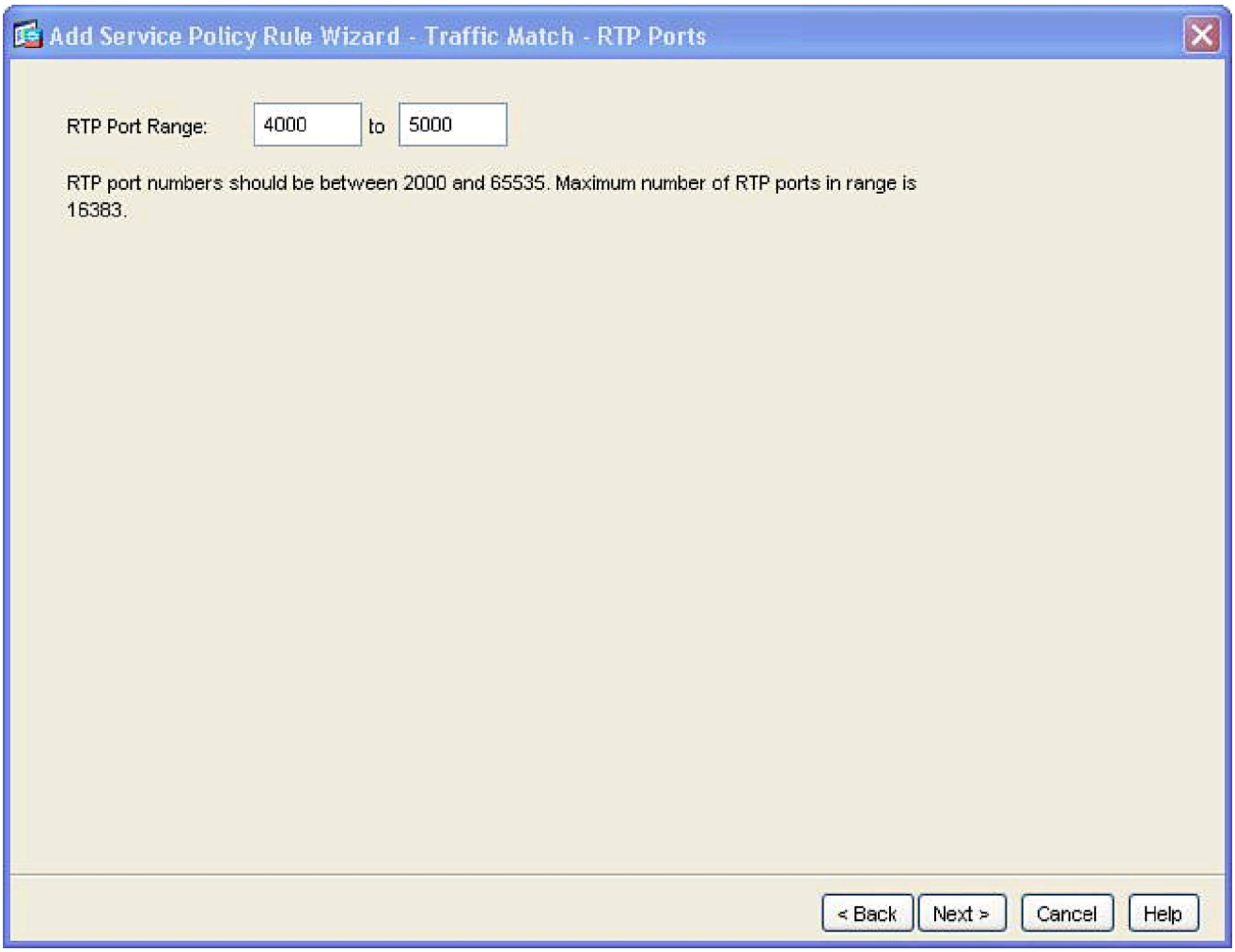

Cisco ASDM 5.0 for ASA - 172.23.62.88
File Rules Search Options Tools Wizards Help
Home
Configuration
Monitoring
Back
Forward
Search
Refresh
Save
Help
Features
Interfaces
Security Policy
NAT
VPN
IPS
Routing
Building Blocks
Device Administration
Properties
Wizards
Configuration > Features > Properties > Advanced > Anti-Spoofing
AAA Setup
AAA Server Groups
AAA Servers
Auth. Prompt
Advanced
Anti-Spoofing
Fragment
TCP Options
Timeouts
ARP Static Table
Auto Update
DHCP Services
DHCP Server
DHCP Relay
DNS Client
Failover
History Metrics
HTTP/HTTPS
IP Audit
IP Audit Policy
IP Audit Signatures
Logging
Logging Setup
Event Lists
Logging Filters
Syslog Setup
Syslog Servers
E-Mail Setup
Priority Queue
SSL
SUNRPC Server
Anti-Spoofing
Specify which interfaces to protect from an IP spoofing attack.
Interface
Anti-Spoofing Enabled
mgmt No
outside No
sales No
test No
Enable
Disable
Apply
Reset
cisco
NA (15)
3/4/0

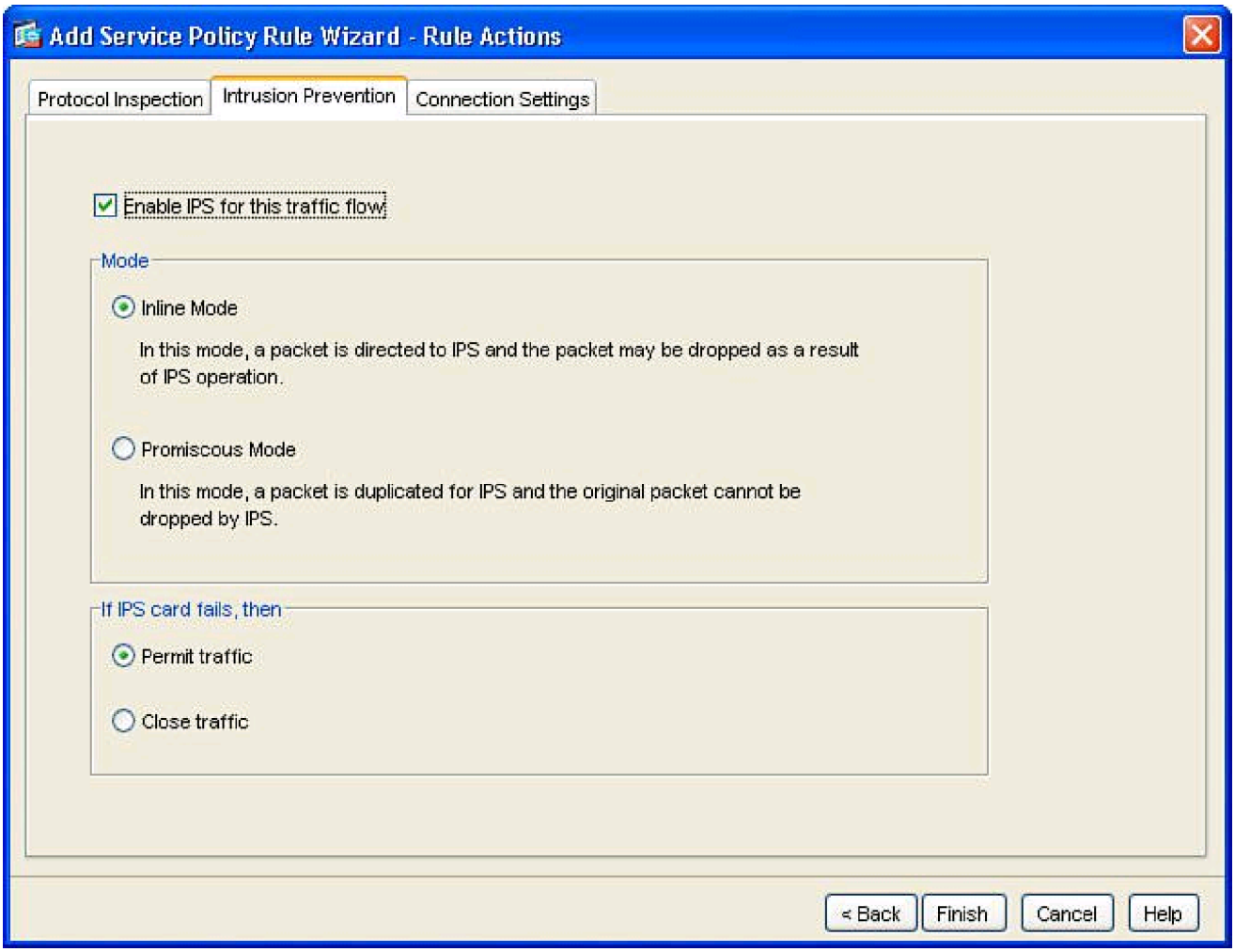

Connecting to IPS...
ASDM will make a new connection to the IPS software running on the SSM module in this ASA system. ASDM connects to this using a separate connection to the IP address of the management port on the SSM module. In the below fields, specify the IP Address and port to be used to connect to the IPS subsystem. You will then be prompted for an IPS username and password. You will also be presented with a security certificate for the IPS subsystem.
Management IP Address - 172.23.62.92
Other IP Address or Hostname:
Port:
443
Continue
Cancel

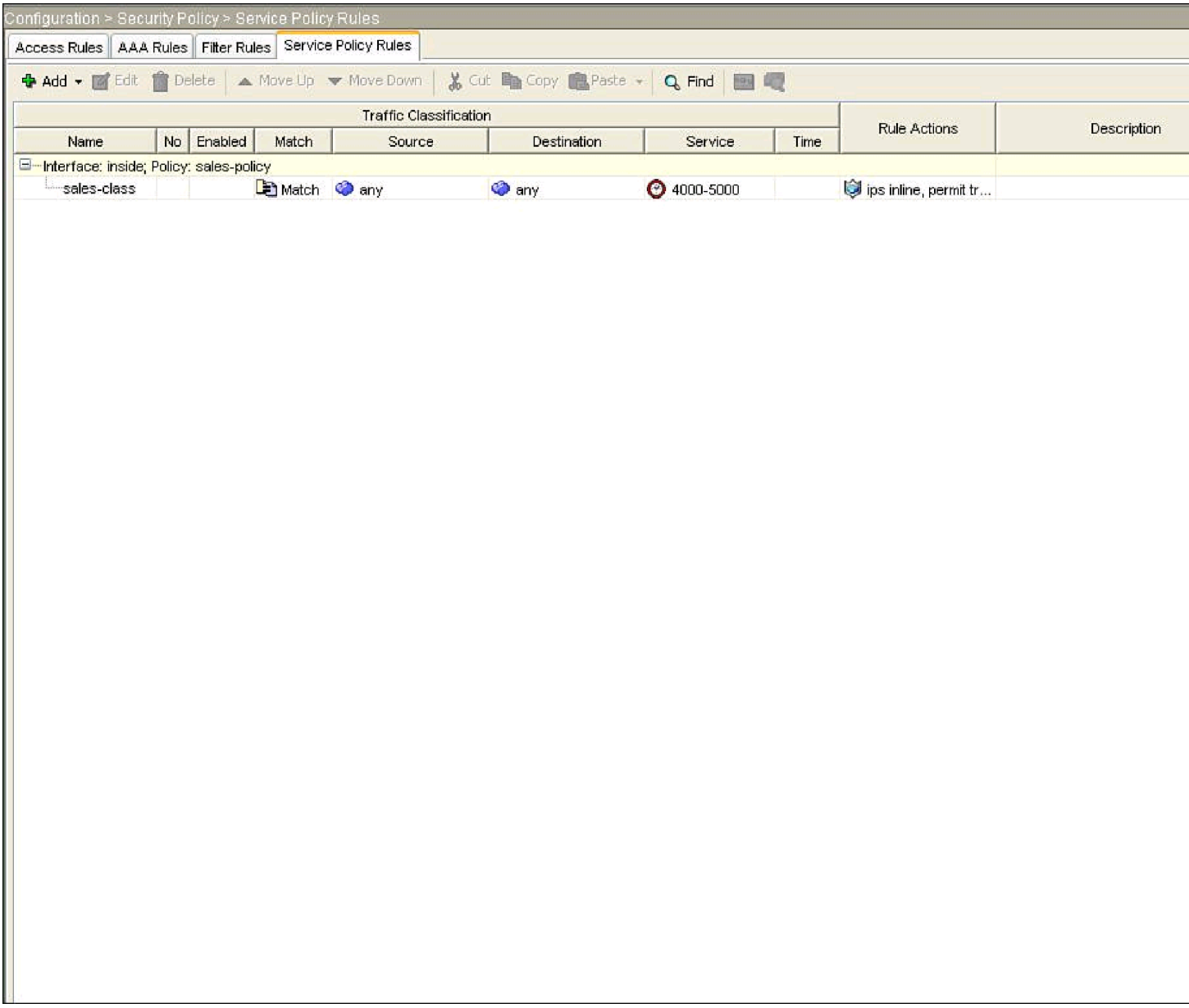

Configuration > Security Policy > Service Policy Rules
Access Rules
AAA Rules
Filter Rules
Service Policy Rules
Add
Edit
Delete
Move Up
Move Down
Cut
Copy
Paste
Find
Traffic Classification
Name
No
Enabled
Match
Source
Destination
Service
Time
Rule Actions
Description

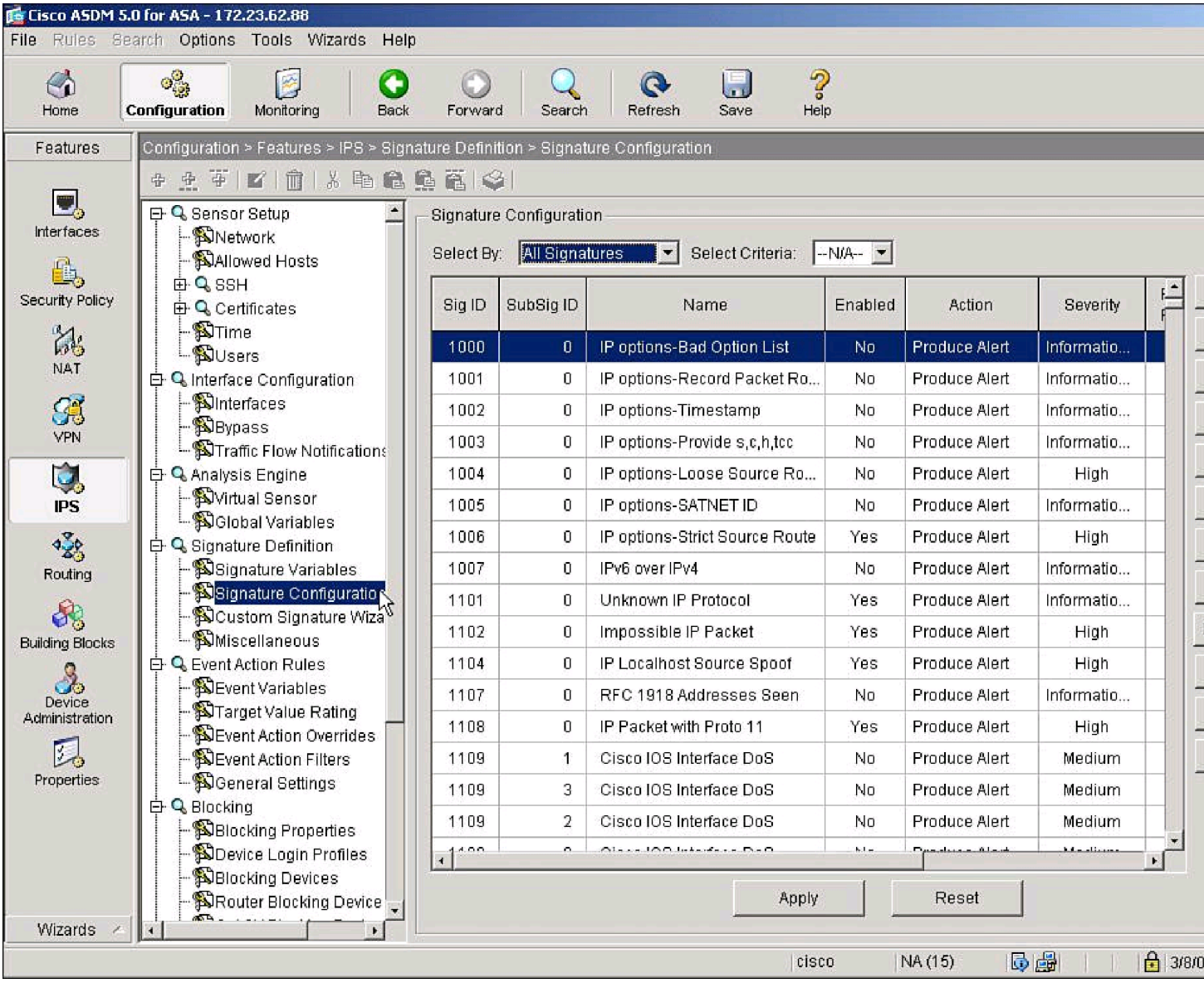

Add Service Policy Rule Wizard - Service Policy
Adding a new service policy rule requires three steps:
Step 1: Configure a service policy.
Step 2: Configure the traffic classification criteria for the service policy rule.
Step 3: Configure actions on the traffic classified by the service policy rule.
Create a service policy and apply to:
Only one service policy can be configured per interface or at global level. If a service policy already exists, then you can add a new rule into the existing service policy. Otherwise, you can create a new service policy.
Interface:
inside - (create new service policy)
Policy Name:
sales-policy
Description:
Global - applies to all interfaces
Policy Name:
global-policy
Description:
< Back
Next >
Cancel
Help

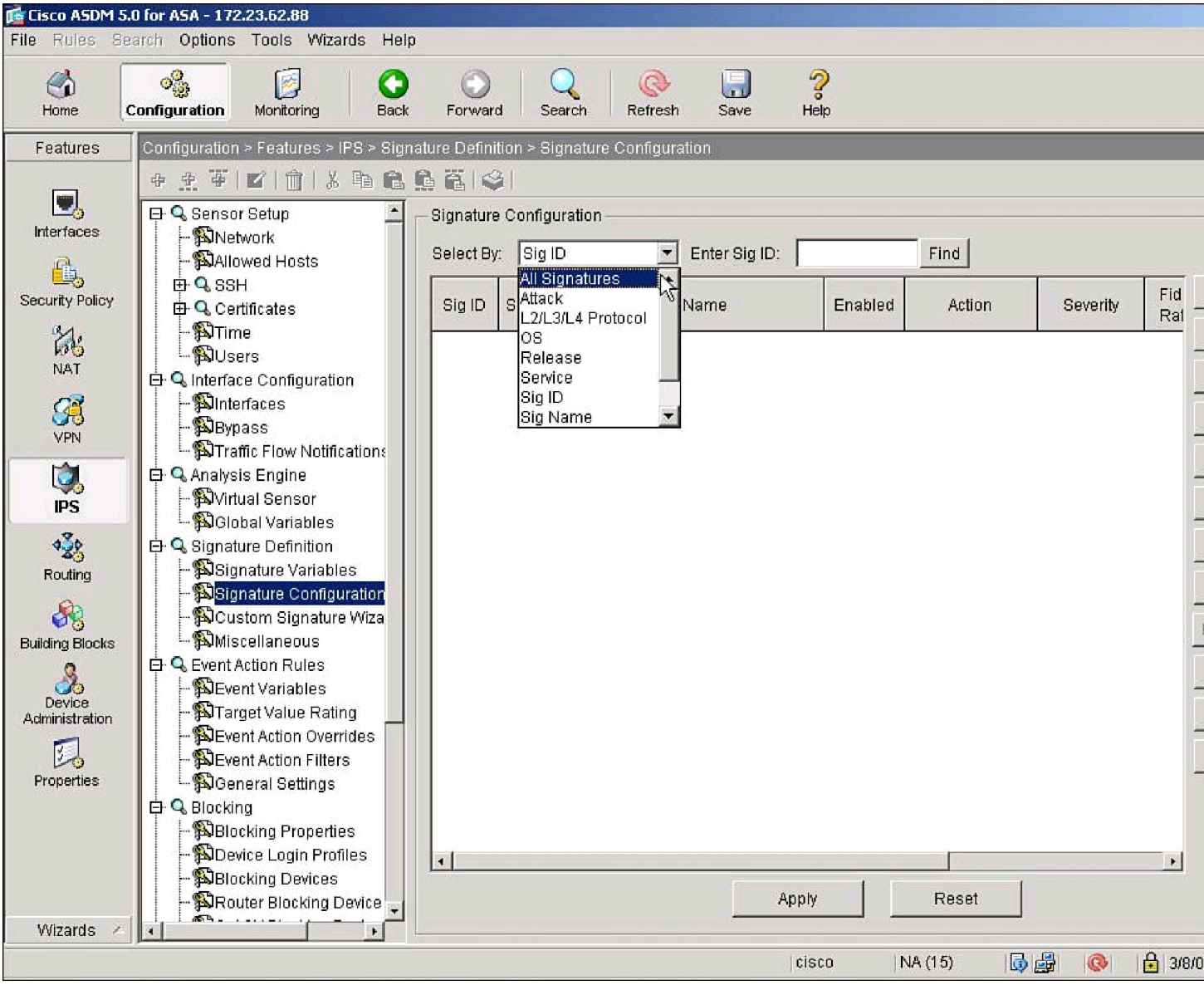

Add Service Policy Rule Wizard - Traffic Classification Criteria
Create a new traffic class:
sales-class
Description (optional):
Traffic match criteria
Default Inspection Traffic
Source and Destination IP Address (uses ACL)
TCP or UDP Destination Port
RTP Range
IP DiffServ CodePoints (DSCP)
IP Precedence
Any traffic
If traffic does not match a existing traffic class, then it will match the class-default traffic class. Class-default can be used in catch all situation.
Use class-default as the traffic class.
< Back
Next >
Cancel
Help

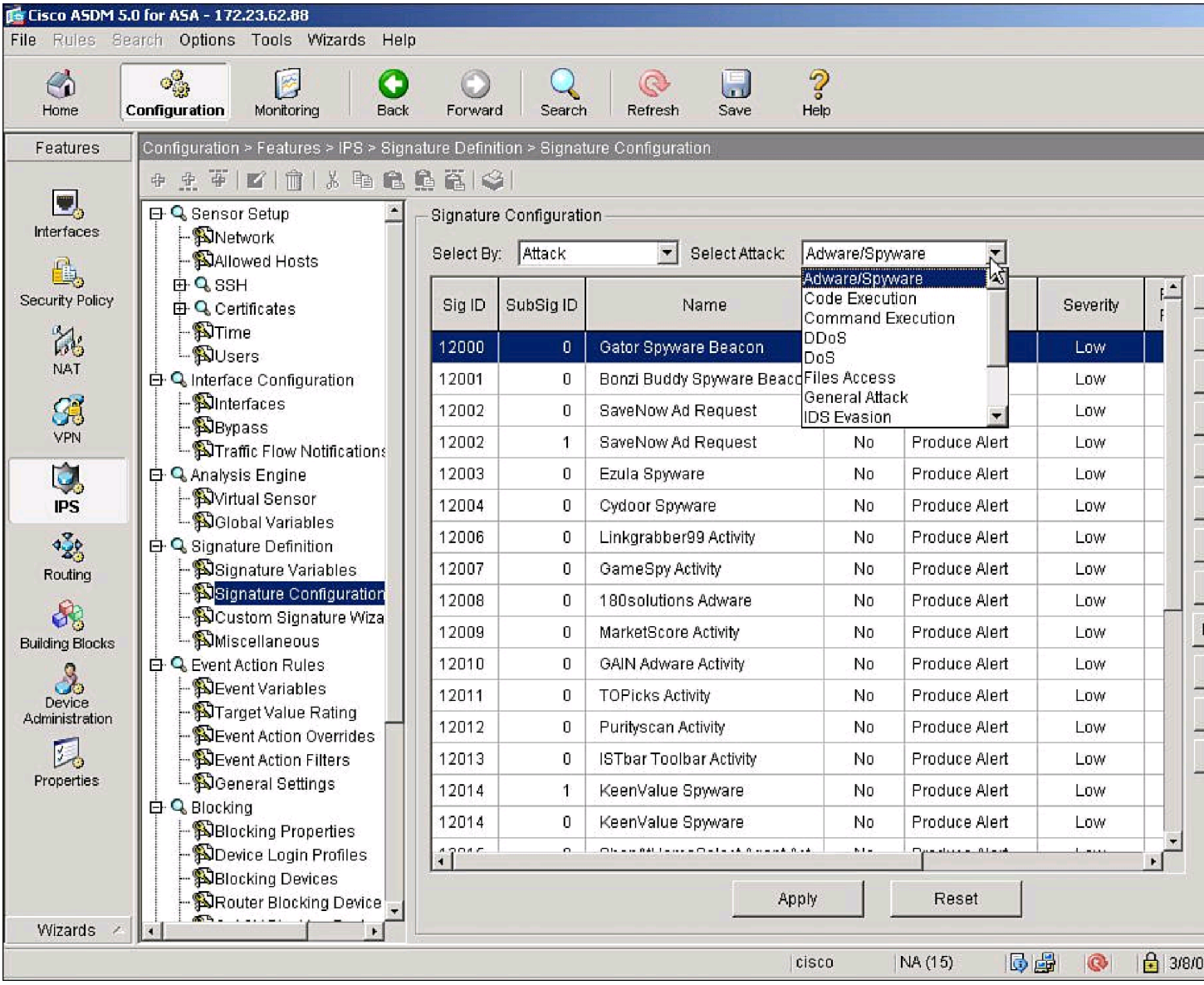

Add Service Policy Rule Wizard - Traffic Match - RTP Ports
RTP Port Range:
4000
to
5000
RTP port numbers should be between 2000 and 65535. Maximum number of RTP ports in range is 16383.
< Back
Next >
Cancel
Help

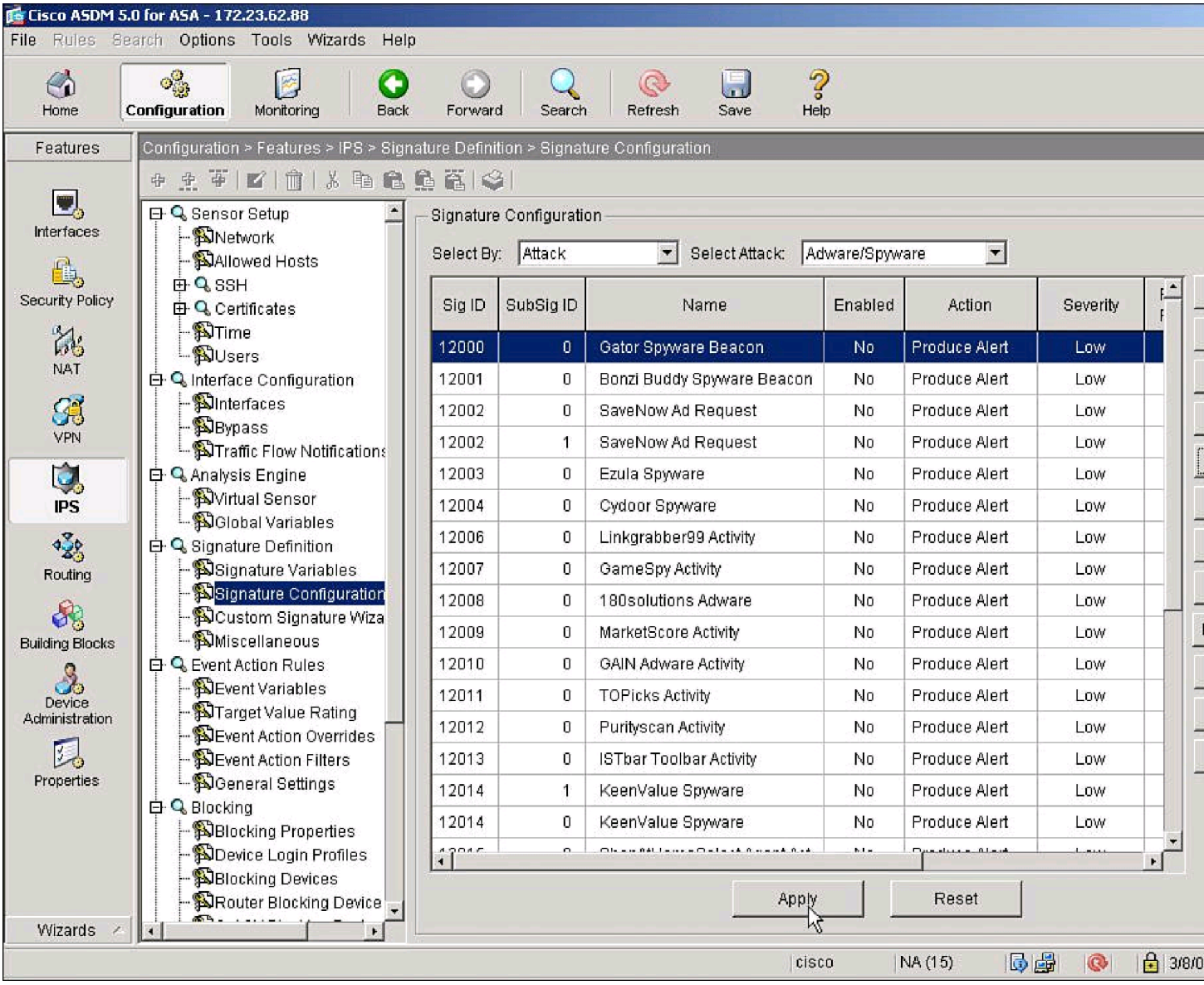

Add Service Policy Rule Wizard - Rule Actions
Protocol Inspection
Intrusion Prevention
Connection Settings
Enable IPS for this traffic flow
Mode
Inline Mode
In this mode, a packet is directed to IPS and the packet may be dropped as a result of IPS operation.
Promiscous Mode
In this mode, a packet is duplicated for IPS and the original packet cannot be dropped by IPS.
If IPS card fails, then
Permit traffic
Close traffic
< Back
Finish
Cancel
Help

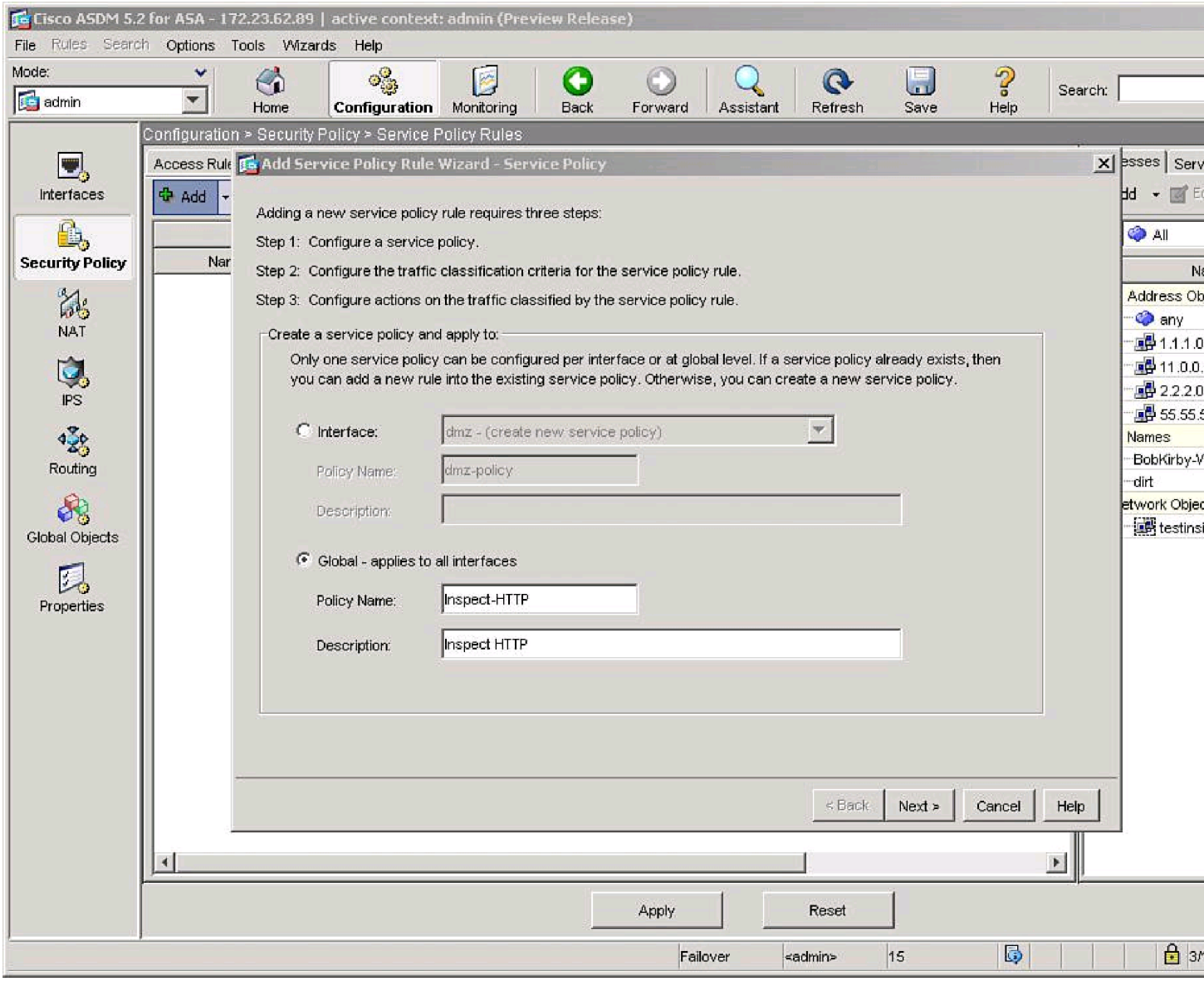

Configuration > Security Policy > Service Policy Rules
Access Rules
AAA Rules
Filter Rules
Service Policy Rules
Add
Edit
Delete
Move Up
Move Down
Cut
Copy
Paste
Find
Traffic Classification
Name
No
Enabled
Match
Source
Destination
Service
Time
Rule Actions
Description
Interface: inside; Policy: sales-policy
sales-class
Match
any
any
4000-5000
ips inline, permit tr...

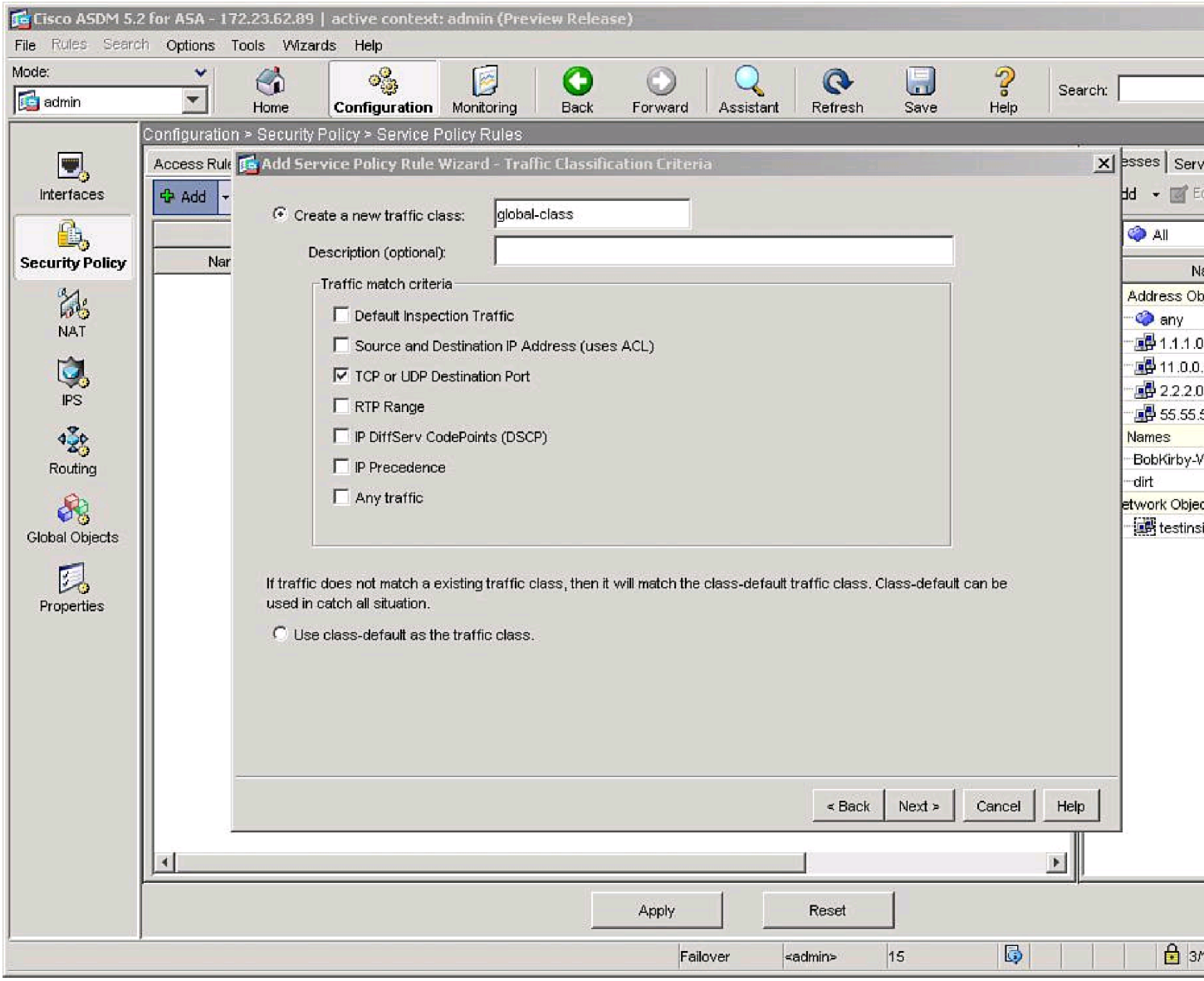

Cisco ASDM 5.0 for ASA - 172.23.62.88
File Rules Search Options Tools Wizards Help
Home
Configuration
Monitoring
Back
Forward
Search
Refresh
Save
Help
Features
Interfaces
Security Policy
NAT
VPN
IPS
Routing
Building Blocks
Device Administration
Properties
Wizards
Configuration > Features > IPS > Signature Definition > Signature Configuration
Sensor Setup
Network
Allowed Hosts
SSH
Certificates
Time
Users
Interface Configuration
Interfaces
Bypass
Traffic Flow Notifications
Analysis Engine
Virtual Sensor
Global Variables
Signature Definition
Signature Variables
Signature Configuration
Custom Signature Wiza
Miscellaneous
Event Action Rules
Event Variables
Target Value Rating
Event Action Overrides
Event Action Filters
General Settings
Blocking
Blocking Properties
Device Login Profiles
Blocking Devices
Router Blocking Device
Signature Configuration
Select By: All Signatures
Select Criteria: --N/A--
Sig ID | SubSig ID | Name | Enabled | Action | Severity
1000 | 0 | IP options-Bad Option List | No | Produce Alert | Informatio...
1001 | 0 | IP options-Record Packet Ro... | No | Produce Alert | Informatio...
1002 | 0 | IP options-Timestamp | No | Produce Alert | Informatio...
1003 | 0 | IP options-Provide s,c,h,tcc | No | Produce Alert | Informatio...
1004 | 0 | IP options-Loose Source Ro... | No | Produce Alert | High
1005 | 0 | IP options-SATNET ID | No | Produce Alert | Informatio...
1006 | 0 | IP options-Strict Source Route | Yes | Produce Alert | High
1007 | 0 | IPv6 over IPv4 | No | Produce Alert | Informatio...
1101 | 0 | Unknown IP Protocol | Yes | Produce Alert | Informatio...
1102 | 0 | Impossible IP Packet | Yes | Produce Alert | High
1104 | 0 | IP Localhost Source Spoof | Yes | Produce Alert | High
1107 | 0 | RFC 1918 Addresses Seen | No | Produce Alert | Informatio...
1108 | 0 | IP Packet with Proto 11 | Yes | Produce Alert | High
1109 | 1 | Cisco IOS Interface DoS | No | Produce Alert | Medium
1109 | 3 | Cisco IOS Interface DoS | No | Produce Alert | Medium
1109 | 2 | Cisco IOS Interface DoS | No | Produce Alert | Medium
Apply
Reset
cisco
NA (15)

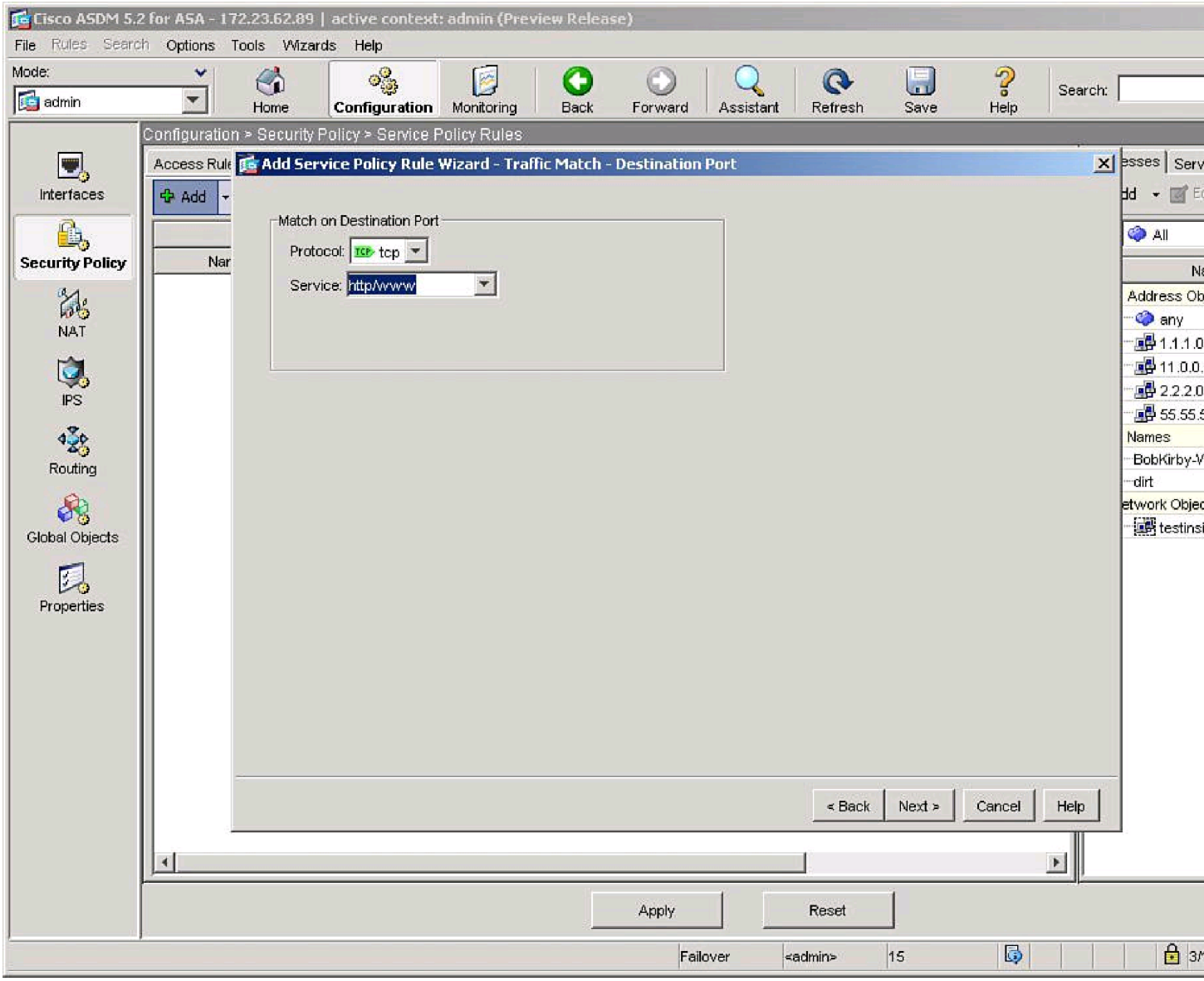

Cisco ASDM 5.0 for ASA - 172.23.62.88
File Rules Search Options Tools Wizards Help
Home
Configuration
Monitoring
Back
Forward
Search
Refresh
Save
Help
Features
Interfaces
Security Policy
NAT
VPN
IPS
Routing
Building Blocks
Device Administration
Properties
Wizards
Configuration > Features > IPS > Signature Definition > Signature Configuration
Sensor Setup
Network
Allowed Hosts
SSH
Certificates
Time
Users
Interface Configuration
Interfaces
Bypass
Traffic Flow Notifications
Analysis Engine
Virtual Sensor
Global Variables
Signature Definition
Signature Variables
Signature Configuration
Custom Signature Wiza
Miscellaneous
Event Action Rules
Event Variables
Target Value Rating
Event Action Overrides
Event Action Filters
General Settings
Blocking
Blocking Properties
Device Login Profiles
Blocking Devices
Router Blocking Device
Signature Configuration
Select By:
Sig ID
Enter Sig ID:
Find
All Signatures
Attack
L2/L3/L4 Protocol
OS
Release
Service
Sig ID
Sig Name
Sig ID
Name
Enabled
Action
Severity
Apply
Reset
cisco
NA (15)

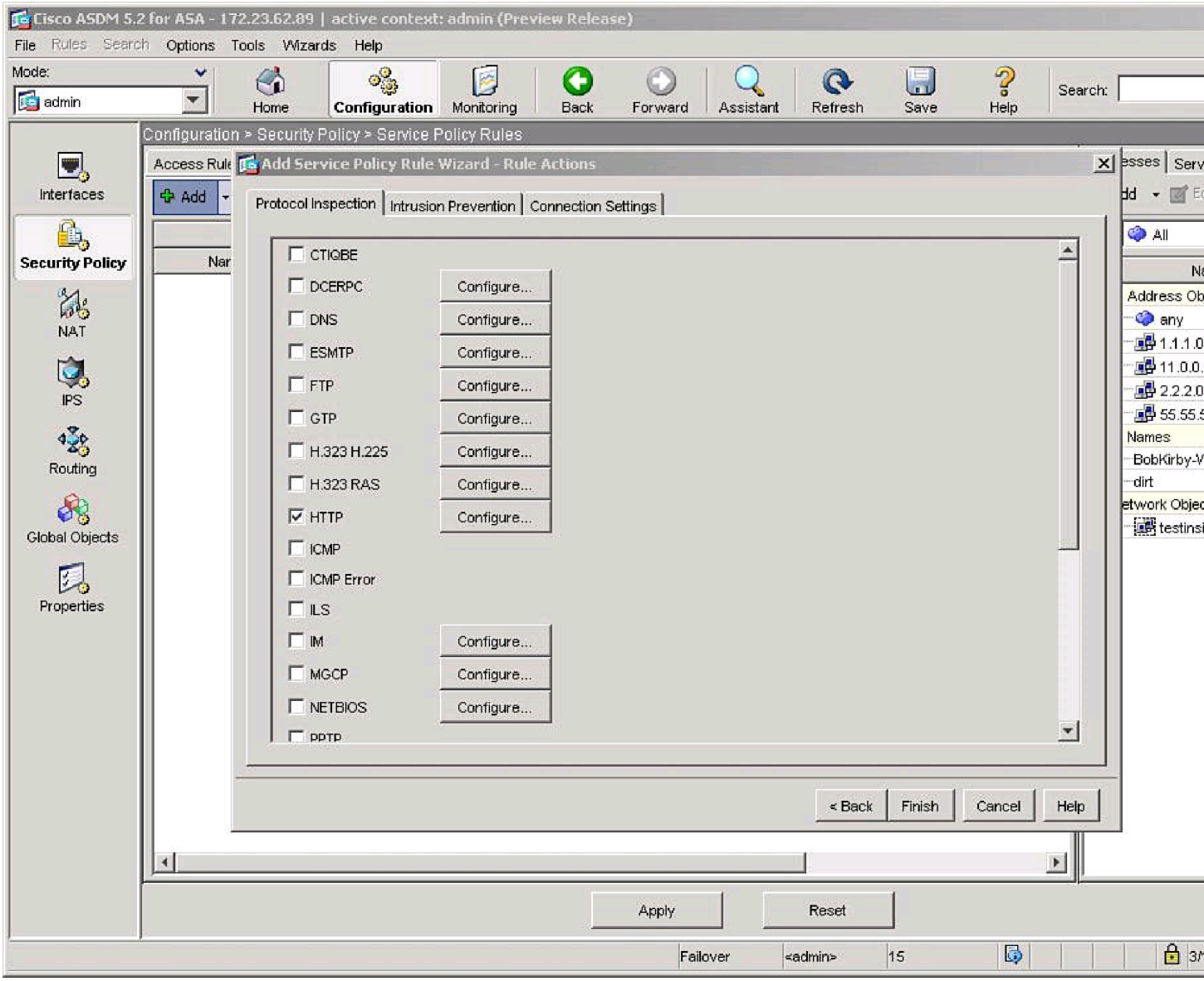

Cisco ASDM 5.0 for ASA - 172.23.62.88
File Rules Search Options Tools Wizards Help
Home
Configuration
Monitoring
Back
Forward
Search
Refresh
Save
Help
Features
Interfaces
Security Policy
NAT
VPN
IPS
Routing
Building Blocks
Device Administration
Properties
Wizards
Configuration > Features > IPS > Signature Definition > Signature Configuration
Sensor Setup
Network
Allowed Hosts
SSH
Certificates
Time
Users
Interface Configuration
Interfaces
Bypass
Traffic Flow Notifications
Analysis Engine
Virtual Sensor
Global Variables
Signature Definition
Signature Variables
Signature Configuration
Custom Signature Wiza
Miscellaneous
Event Action Rules
Event Variables
Target Value Rating
Event Action Overrides
Event Action Filters
General Settings
Blocking
Blocking Properties
Device Login Profiles
Blocking Devices
Router Blocking Device
Signature Configuration
Select By: Attack
Select Attack: Adware/Spyware
Adware/Spyware
Code Execution
Command Execution
DDoS
DoS
Files Access
General Attack
IDS Evasion
Sig ID
SubSig ID
Name
Severity
12000 0 Gator Spyware Beacon Low
12001 0 Bonzi Buddy Spyware Beacc Low
12002 0 SaveNow Ad Request Low
12002 1 SaveNow Ad Request No Produce Alert Low
12003 0 Ezula Spyware No Produce Alert Low
12004 0 Cydoor Spyware No Produce Alert Low
12006 0 Linkgrabber99 Activity No Produce Alert Low
12007 0 GameSpy Activity No Produce Alert Low
12008 0 180solutions Adware No Produce Alert Low
12009 0 MarketScore Activity No Produce Alert Low
12010 0 GAIN Adware Activity No Produce Alert Low
12011 0 TOPicks Activity No Produce Alert Low
12012 0 Purityscan Activity No Produce Alert Low
12013 0 ISTbar Toolbar Activity No Produce Alert Low
12014 1 KeenValue Spyware No Produce Alert Low
12014 0 KeenValue Spyware No Produce Alert Low
Apply
Reset
cisco
NA (15)

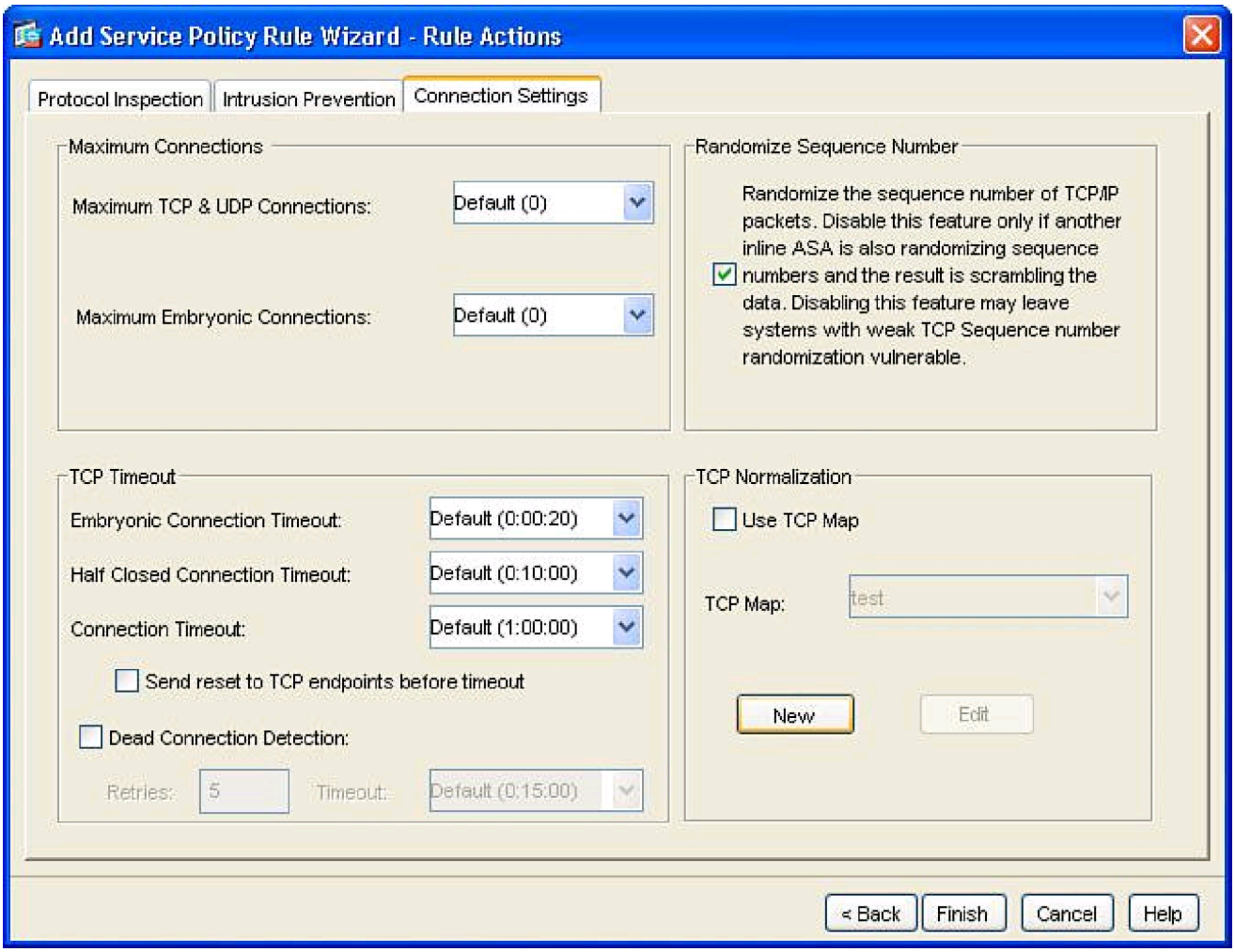

Cisco ASDM 5.0 for ASA - 172.23.62.88
File Rules Search Options Tools Wizards Help
Home
Configuration
Monitoring
Back
Forward
Search
Refresh
Save
Help
Features
Interfaces
Security Policy
NAT
VPN
IPS
Routing
Building Blocks
Device Administration
Properties
Wizards
Configuration > Features > IPS > Signature Definition > Signature Configuration
Sensor Setup
Network
Allowed Hosts
SSH
Certificates
Time
Users
Interface Configuration
Interfaces
Bypass
Traffic Flow Notifications
Analysis Engine
Virtual Sensor
Global Variables
Signature Definition
Signature Variables
Signature Configuration
Custom Signature Wiza
Miscellaneous
Event Action Rules
Event Variables
Target Value Rating
Event Action Overrides
Event Action Filters
General Settings
Blocking
Blocking Properties
Device Login Profiles
Blocking Devices
Router Blocking Device
Signature Configuration
Select By: Attack
Select Attack: Adware/Spyware
Sig ID | SubSig ID | Name | Enabled | Action | Severity
12000 | 0 | Gator Spyware Beacon | No | Produce Alert | Low
12001 | 0 | Bonzi Buddy Spyware Beacon | No | Produce Alert | Low
12002 | 0 | SaveNow Ad Request | No | Produce Alert | Low
12002 | 1 | SaveNow Ad Request | No | Produce Alert | Low
12003 | 0 | Ezula Spyware | No | Produce Alert | Low
12004 | 0 | Cydoor Spyware | No | Produce Alert | Low
12006 | 0 | Linkgrabber99 Activity | No | Produce Alert | Low
12007 | 0 | GameSpy Activity | No | Produce Alert | Low
12008 | 0 | 180solutions Adware | No | Produce Alert | Low
12009 | 0 | MarketScore Activity | No | Produce Alert | Low
12010 | 0 | GAIN Adware Activity | No | Produce Alert | Low
12011 | 0 | TOPicks Activity | No | Produce Alert | Low
12012 | 0 | Purityscan Activity | No | Produce Alert | Low
12013 | 0 | ISTbar Toolbar Activity | No | Produce Alert | Low
12014 | 1 | KeenValue Spyware | No | Produce Alert | Low
12014 | 0 | KeenValue Spyware | No | Produce Alert | Low
Apply
Reset
cisco
NA (15)

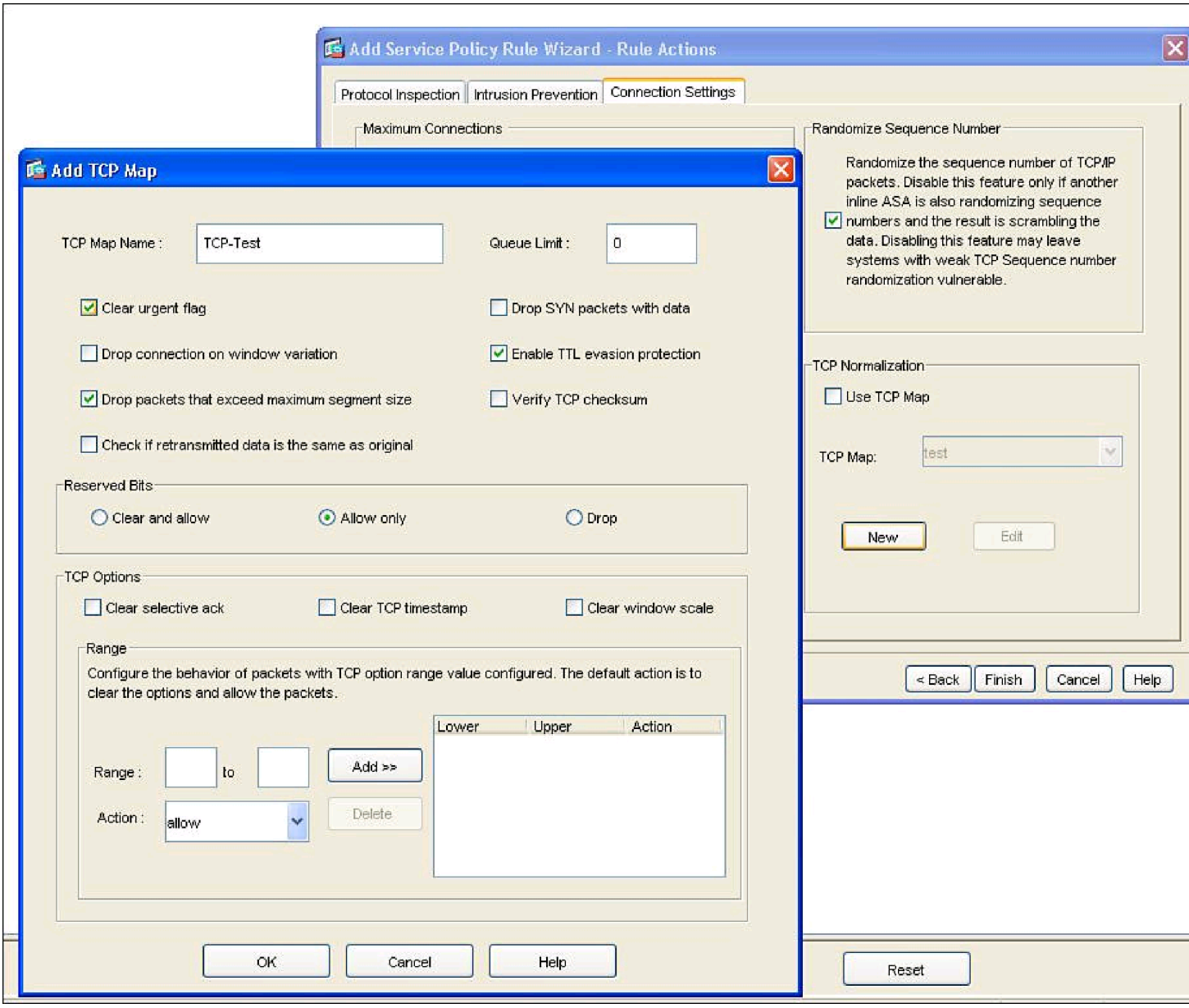

Cisco ASDM 5.2 for ASA - 172.23.62.89 | active context: admin (Preview Release)
File Rules Search Options Tools Wizards Help
Mode:
admin
Home
Configuration
Monitoring
Back
Forward
Assistant
Refresh
Save
Help
Search:
Interfaces
Security Policy
NAT
IPS
Routing
Global Objects
Properties
Configuration > Security Policy > Service Policy Rules
Access Rule
Add
Add Service Policy Rule Wizard - Service Policy
Adding a new service policy rule requires three steps:
Step 1: Configure a service policy.
Step 2: Configure the traffic classification criteria for the service policy rule.
Step 3: Configure actions on the traffic classified by the service policy rule.
Create a service policy and apply to:
Only one service policy can be configured per interface or at global level. If a service policy already exists, then you can add a new rule into the existing service policy. Otherwise, you can create a new service policy.
Interface:
dmz - (create new service policy)
Policy Name:
dmz-policy
Description:
Global - applies to all interfaces
Policy Name:
Inspect-HTTP
Description:
Inspect HTTP
< Back
Next >
Cancel
Help
Apply
Reset
Failover
<admin>
15

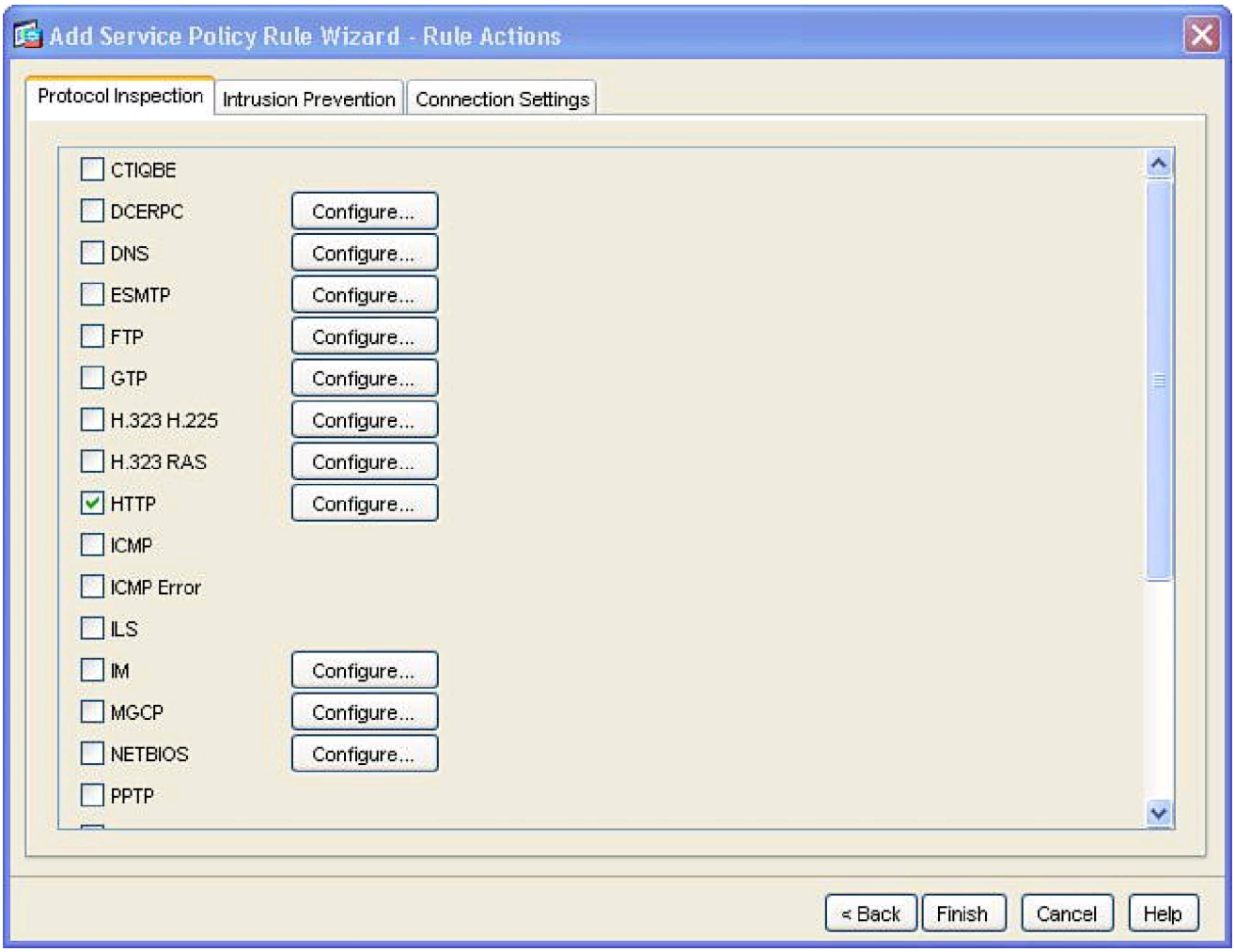

Cisco ASDM 5.2 for ASA - 172.23.62.89 | active context: admin (Preview Release)
File Rules Search Options Tools Wizards Help
Mode:
admin
Home
Configuration
Monitoring
Back
Forward
Assistant
Refresh
Save
Help
Search:
Configuration > Security Policy > Service Policy Rules
Interfaces
Security Policy
NAT
IPS
Routing
Global Objects
Properties
Access Rule
Add
Add Service Policy Rule Wizard - Traffic Classification Criteria
Create a new traffic class:
global-class
Description (optional):
Traffic match criteria
Default Inspection Traffic
Source and Destination IP Address (uses ACL)
TCP or UDP Destination Port
RTP Range
IP DiffServ CodePoints (DSCP)
IP Precedence
Any traffic
If traffic does not match a existing traffic class, then it will match the class-default traffic class. Class-default can be used in catch all situation.
Use class-default as the traffic class.
< Back
Next >
Cancel
Help
Apply
Reset
Failover
<admin>
15

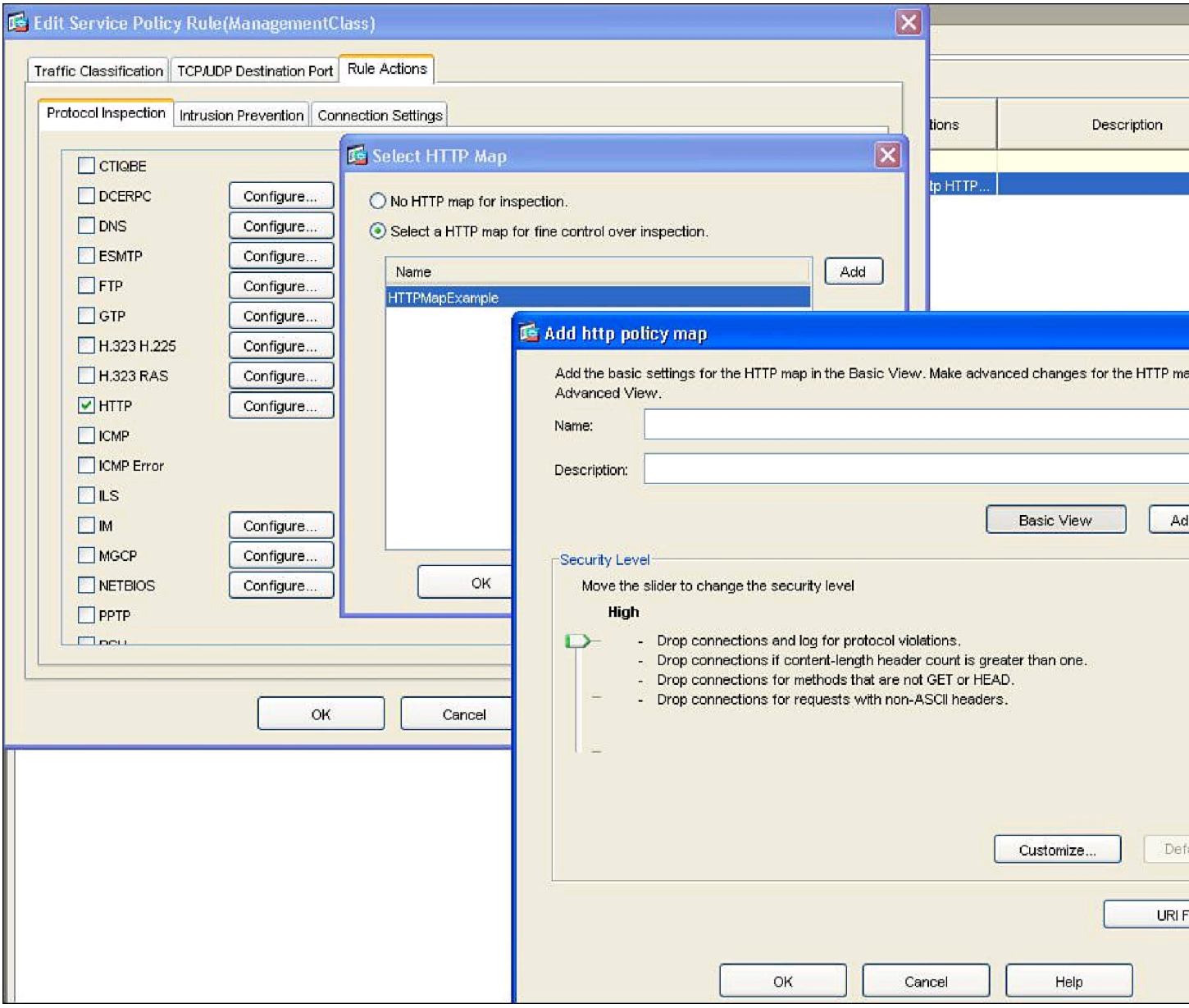

Cisco ASDM 5.2 for ASA - 172.23.62.89 | active context: admin (Preview Release)
File Rules Search Options Tools Wizards Help
Mode:
admin
Home
Configuration
Monitoring
Back
Forward
Assistant
Refresh
Save
Help
Search:
Interfaces
Security Policy
NAT
IPS
Routing
Global Objects
Properties
Configuration > Security Policy > Service Policy Rules
Access Rule
Add
Add Service Policy Rule Wizard - Traffic Match - Destination Port
Match on Destination Port
Protocol: tcp
Service: http/www
< Back
Next >
Cancel
Help
Apply
Reset
Failover
<admin>
15

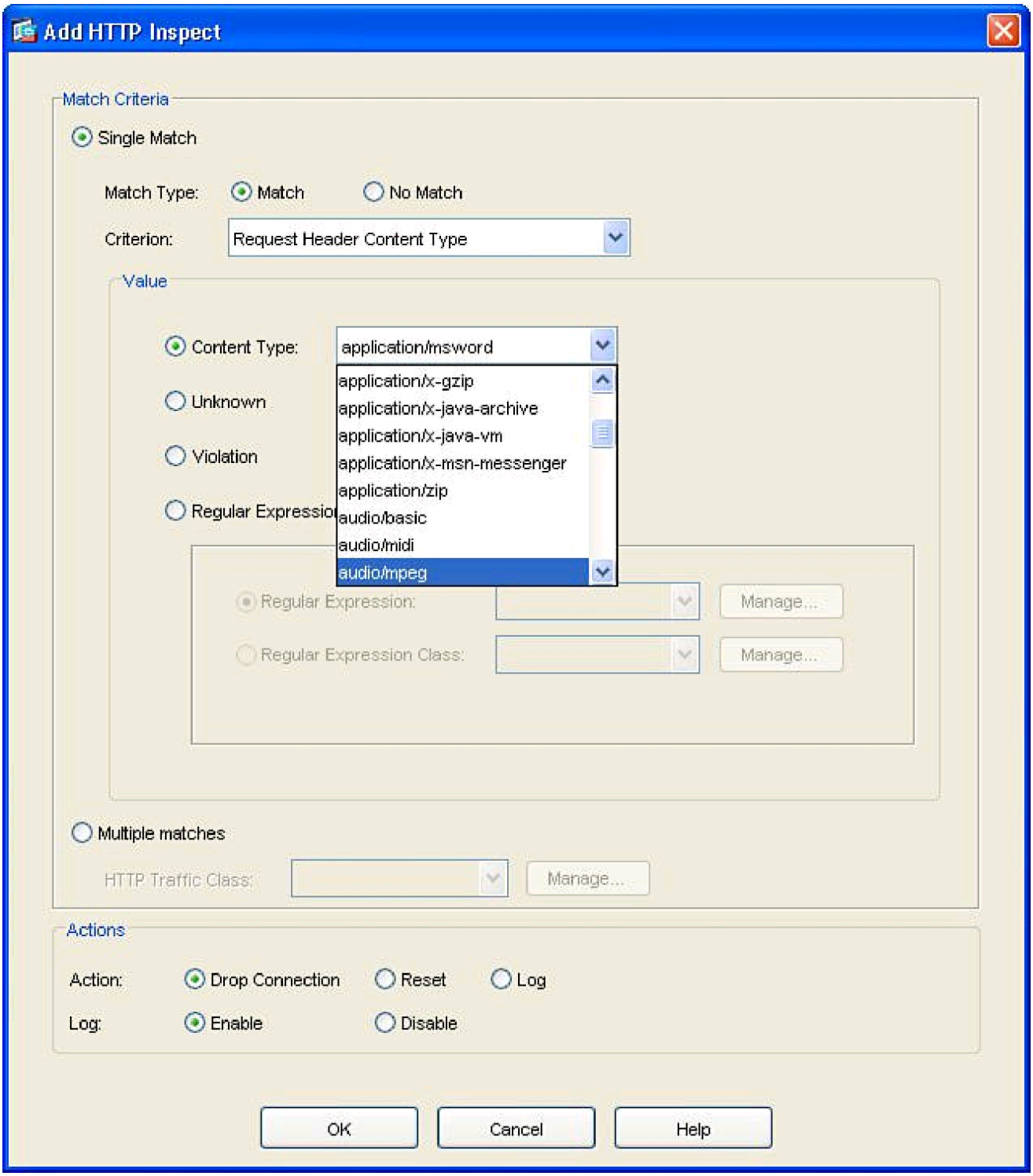

Cisco ASDM 5.2 for ASA - 172.23.62.89 | active context: admin (Preview Release)
File Rules Search Options Tools Wizards Help
Mode: admin
Home Configuration Monitoring Back Forward Assistant Refresh Save Help Search:
Configuration > Security Policy > Service Policy Rules
Interfaces
Security Policy
NAT
IPS
Routing
Global Objects
Properties
Access Rule
Add
Add Service Policy Rule Wizard - Rule Actions
Protocol Inspection
Intrusion Prevention
Connection Settings
CTIQBE
DCERPC Configure...
DNS Configure...
ESMTP Configure...
FTP Configure...
GTP Configure...
H.323 H.225 Configure...
H.323 RAS Configure...
HTTP Configure...
ICMP
ICMP Error
ILS
IM Configure...
MGCP Configure...
NETBIOS Configure...
< Back
Finish
Cancel
Help
Apply
Reset
Failover
<admin>
15

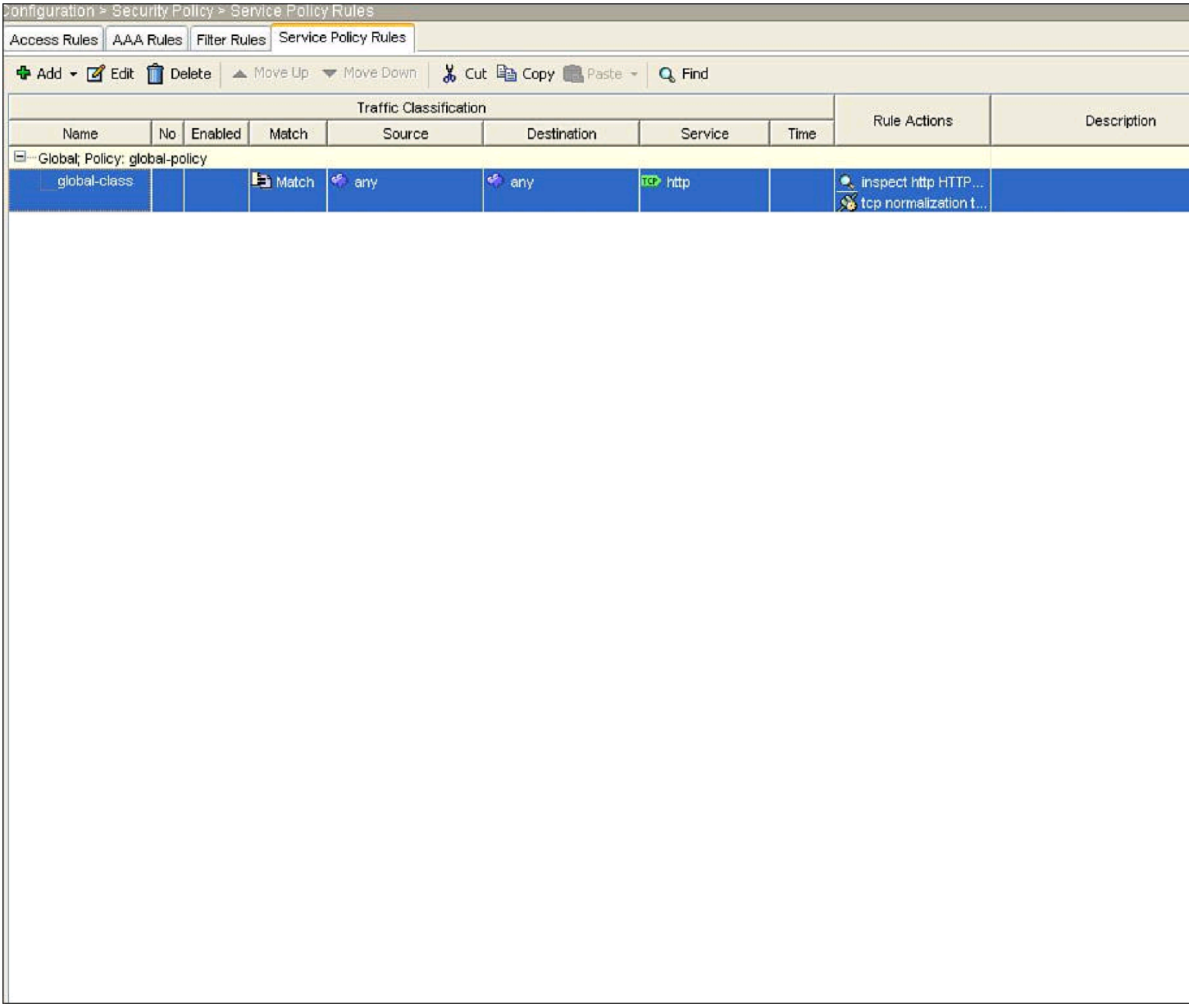

Add Service Policy Rule Wizard - Rule Actions
Protocol Inspection
Intrusion Prevention
Connection Settings
Maximum Connections
Maximum TCP & UDP Connections:
Default (0)
Maximum Embryonic Connections:
Default (0)
Randomize Sequence Number
Randomize the sequence number of TCP/IP packets. Disable this feature only if another inline ASA is also randomizing sequence numbers and the result is scrambling the data. Disabling this feature may leave systems with weak TCP Sequence number randomization vulnerable.
TCP Timeout
Embryonic Connection Timeout:
Default (0:00:20)
Half Closed Connection Timeout:
Default (0:10:00)
Connection Timeout:
Default (1:00:00)
Send reset to TCP endpoints before timeout
Dead Connection Detection:
Retries:
5
Timeout:
Default (0:15:00)
TCP Normalization
Use TCP Map
TCP Map:
test
New
Edit
< Back
Finish
Cancel
Help

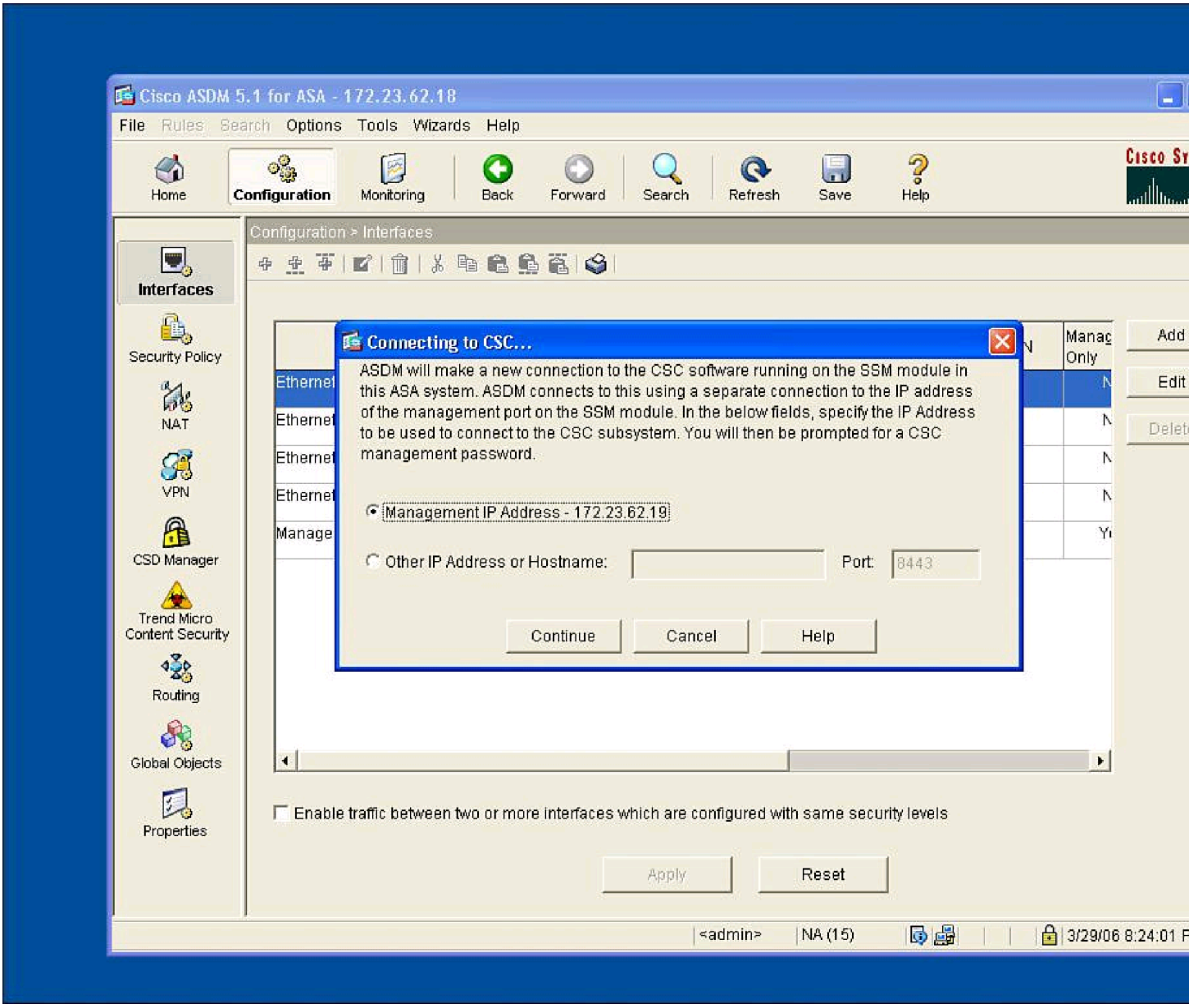

Add Service Policy Rule Wizard - Rule Actions
Protocol Inspection
Intrusion Prevention
Connection Settings
Maximum Connections
Randomize Sequence Number
Randomize the sequence number of TCP/IP packets. Disable this feature only if another inline ASA is also randomizing sequence numbers and the result is scrambling the data. Disabling this feature may leave systems with weak TCP Sequence number randomization vulnerable.
TCP Normalization
Use TCP Map
TCP Map:
test
New
Edit
< Back
Finish
Cancel
Help
Reset
Add TCP Map
TCP Map Name :
TCP-Test
Queue Limit :
0
Clear urgent flag
Drop SYN packets with data
Drop connection on window variation
Enable TTL evasion protection
Drop packets that exceed maximum segment size
Verify TCP checksum
Check if retransmitted data is the same as original
Reserved Bits
Clear and allow
Allow only
Drop
TCP Options
Clear selective ack
Clear TCP timestamp
Clear window scale
Range
Configure the behavior of packets with TCP option range value configured. The default action is to clear the options and allow the packets.
Range :
to
Action :
allow
Add >>
Delete
Lower
Upper
Action
OK
Cancel
Help

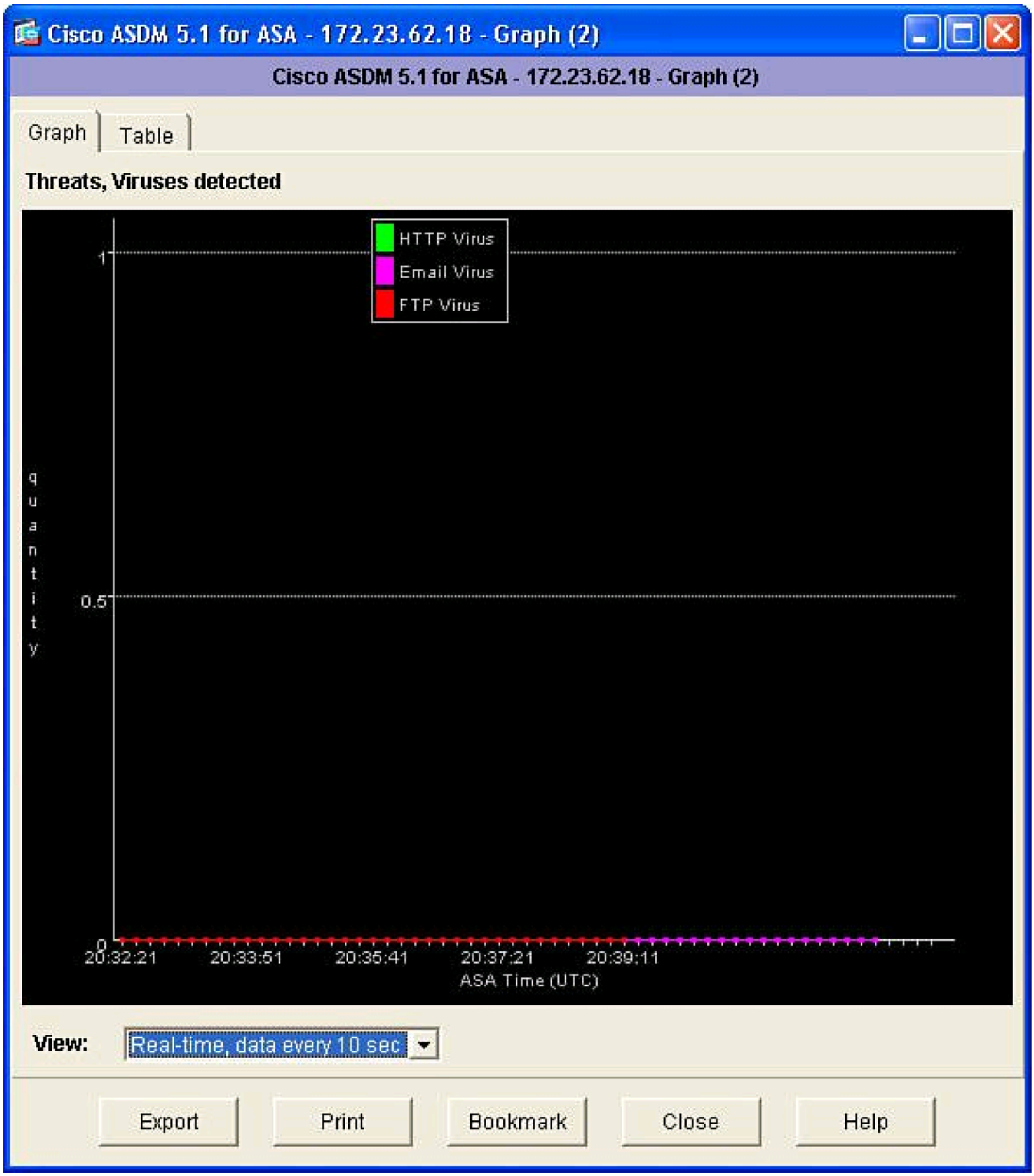

Add Service Policy Rule Wizard - Rule Actions
Protocol Inspection
Intrusion Prevention
Connection Settings
CTIQBE
DCERPC
Configure...
DNS
Configure...
ESMTP
Configure...
FTP
Configure...
GTP
Configure...
H.323 H.225
Configure...
H.323 RAS
Configure...
HTTP
Configure...
ICMP
ICMP Error
ILS
IM
Configure...
MGCP
Configure...
NETBIOS
Configure...
PPTP
< Back
Finish
Cancel
Help

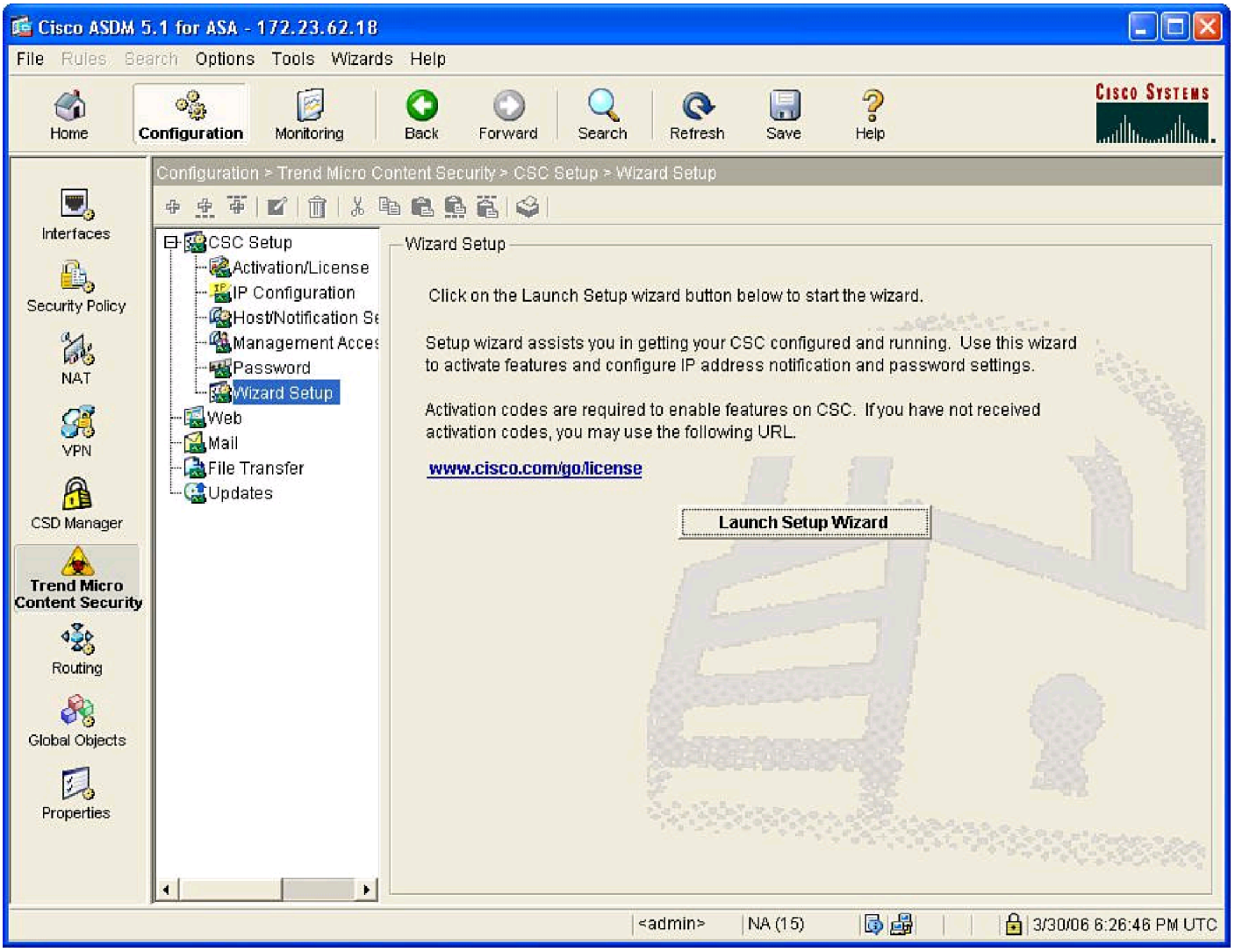

Edit Service Policy Rule(ManagementClass)
Traffic Classification
TCP/UDP Destination Port
Rule Actions
Protocol Inspection
Intrusion Prevention
Connection Settings
CTIQBE
DCERPC
DNS
ESMTP
FTP
GTP
H.323 H.225
H.323 RAS
HTTP
ICMP
ICMP Error
ILS
IM
MGCP
NETBIOS
PPTP
Configure...
OK
Cancel
Select HTTP Map
No HTTP map for inspection.
Select a HTTP map for fine control over inspection.
Name
HTTPMapExample
Add
OK
Add http policy map
Add the basic settings for the HTTP map in the Basic View. Make advanced changes for the HTTP ma
Advanced View.
Name:
Description:
Basic View
Security Level
Move the slider to change the security level
High
- Drop connections and log for protocol violations.
- Drop connections if content-length header count is greater than one.
- Drop connections for methods that are not GET or HEAD.
- Drop connections for requests with non-ASCII headers.
Customize...
OK
Cancel
Help
Description

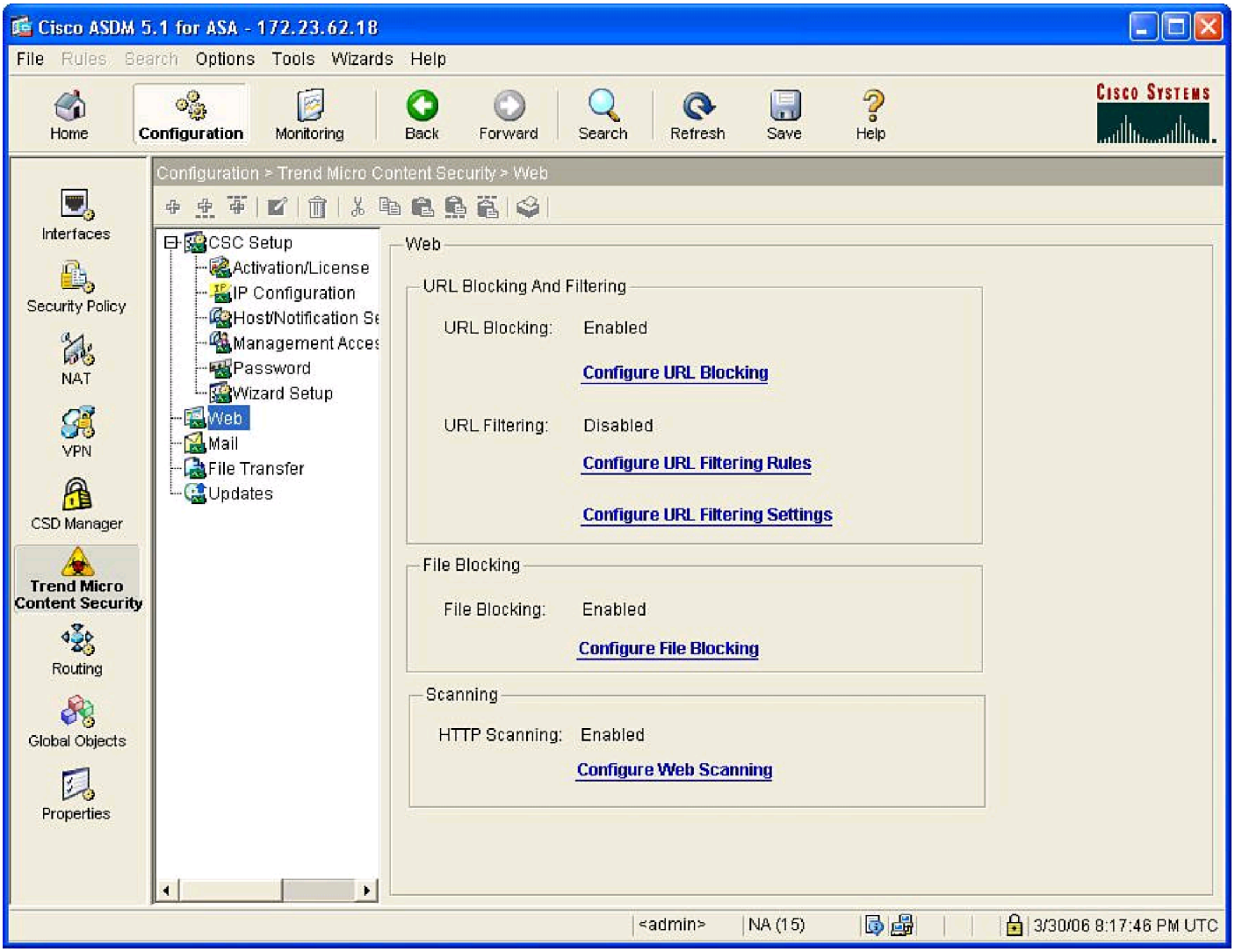

Add HTTP Inspect
Match Criteria
Single Match
Match Type:
Match
No Match
Criterion:
Request Header Content Type
Value
Content Type:
application/msword
application/x-gzip
application/x-java-archive
application/x-java-vm
application/x-msn-messenger
application/zip
audio/basic
audio/midi
audio/mpeg
Unknown
Violation
Regular Expressio
Regular Expression:
Manage...
Regular Expression Class:
Manage...
Multiple matches
HTTP Traffic Class:
Manage...
Actions
Action:
Drop Connection
Reset
Log
Log:
Enable
Disable
OK
Cancel
Help


Configuration > Security Policy > Service Policy Rules
Access Rules
AAA Rules
Filter Rules
Service Policy Rules
Add
Edit
Delete
Move Up
Move Down
Cut
Copy
Paste
Find
Traffic Classification
Name
No
Enabled
Match
Source
Destination
Service
Time
Rule Actions
Description
Global; Policy: global-policy
global-class
Match
any
any
http
inspect http HTTP...
tcp normalization t...

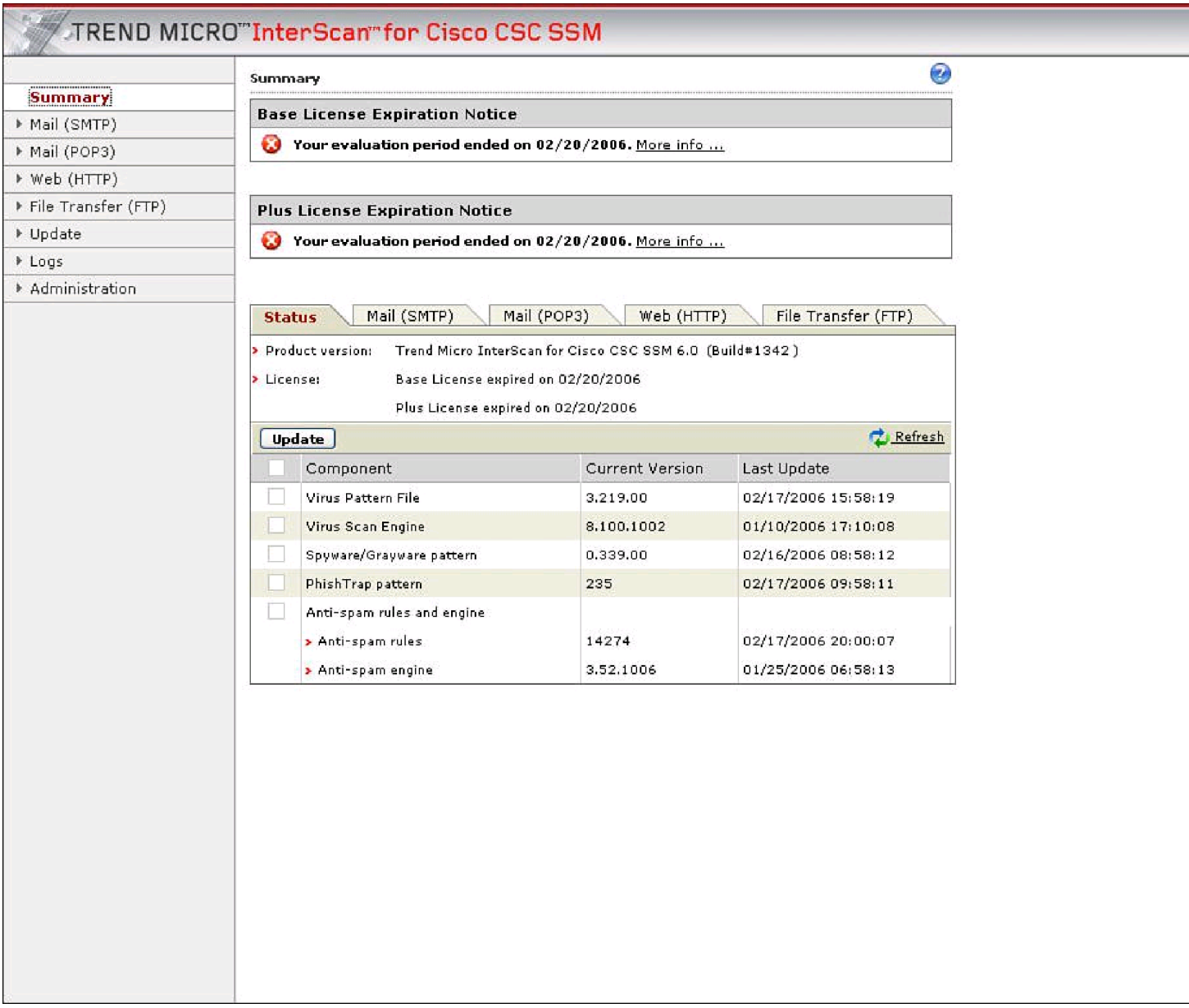

Cisco ASDM 5.1 for ASA - 172.23.62.18
File Rules Search Options Tools Wizards Help
Home
Configuration
Monitoring
Back
Forward
Search
Refresh
Save
Help
Configuration > Interfaces
Interfaces
Security Policy
NAT
VPN
CSD Manager
Trend Micro Content Security
Routing
Global Objects
Properties
Connecting to CSC...
ASDM will make a new connection to the CSC software running on the SSM module in this ASA system. ASDM connects to this using a separate connection to the IP address of the management port on the SSM module. In the below fields, specify the IP Address to be used to connect to the CSC subsystem. You will then be prompted for a CSC management password.
Management IP Address - 172.23.62.19
Other IP Address or Hostname:
Port:
8443
Continue
Cancel
Help
Add
Edit
Enable traffic between two or more interfaces which are configured with same security levels
Apply
Reset
<admin>
NA (15)
3/29/06 8:24:01

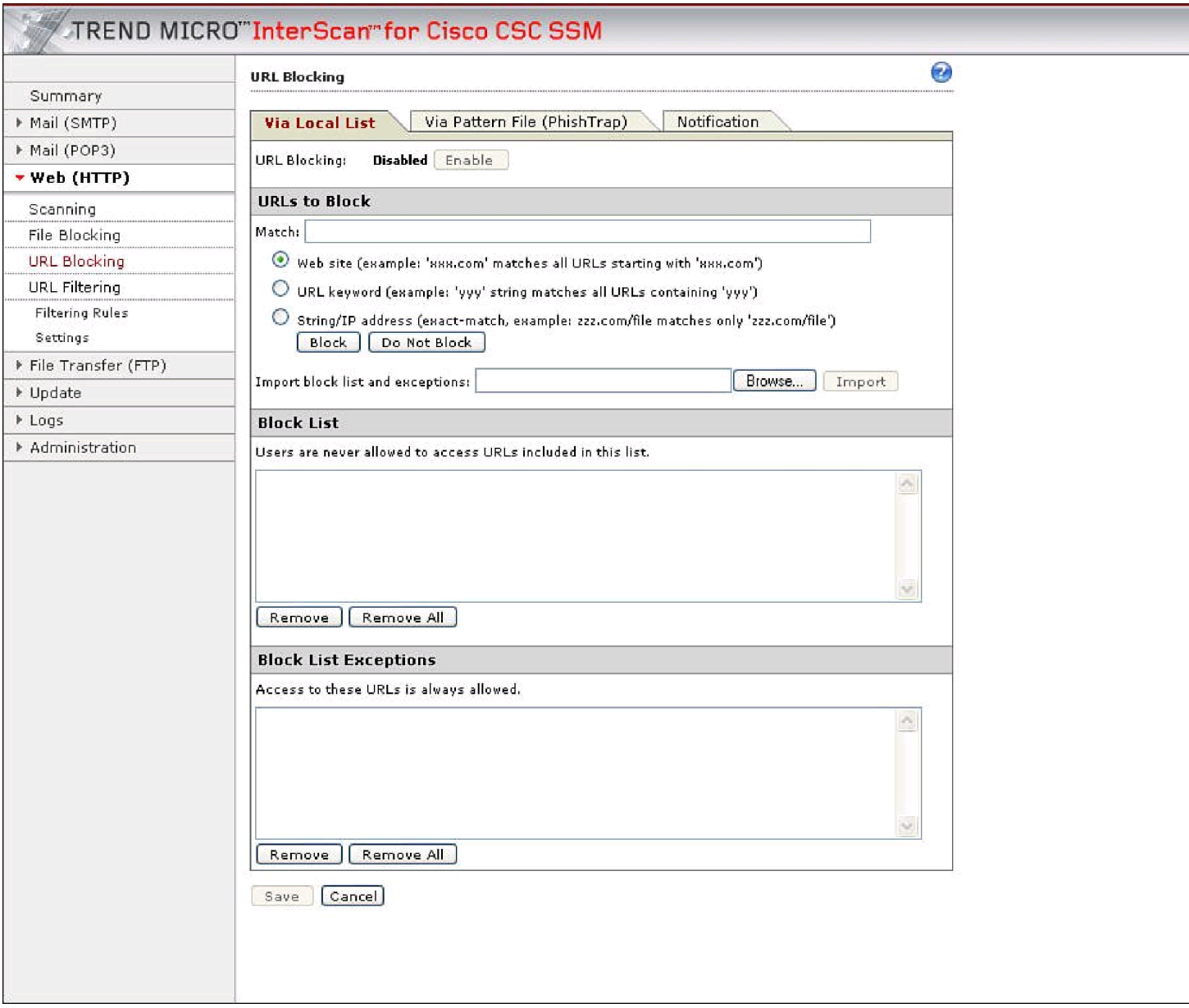

Cisco ASDM 5.1 for ASA - 172.23.62.18 - Graph (2)
Cisco ASDM 5.1 for ASA - 172.23.62.18 - Graph (2)
Graph
Table
Threats, Viruses detected
HTTP Virus
Email Virus
FTP Virus
1
0.5
0
quantity
20:32:21
20:33:51
20:35:41
20:37:21
20:39:11
ASA Time (UTC)
View:
Real-time, data every 10 sec
Export
Print
Bookmark
Close
Help

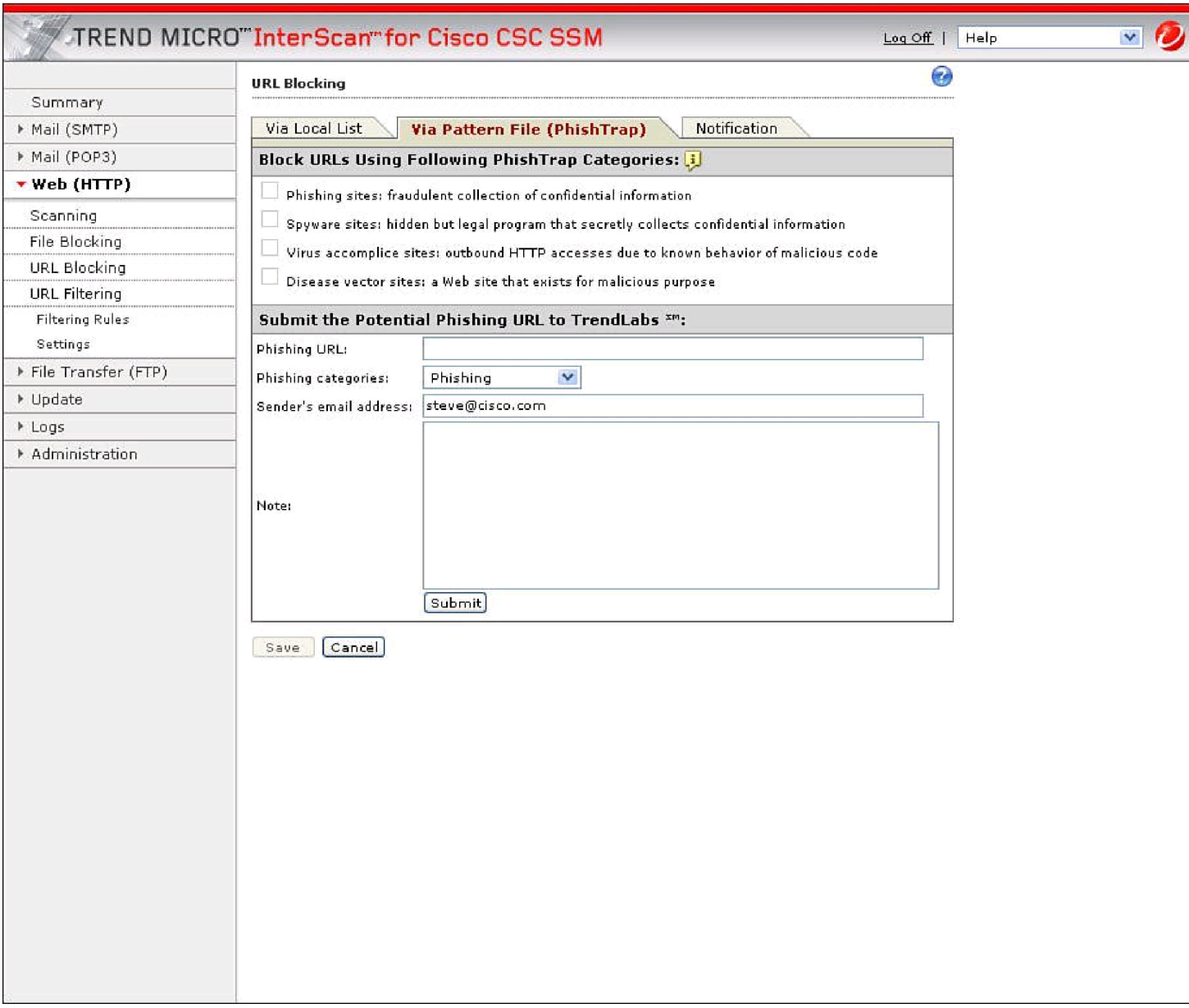

Cisco ASDM 5.1 for ASA - 172.23.62.18
File Rules Search Options Tools Wizards Help
Home
Configuration
Monitoring
Back
Forward
Search
Refresh
Save
Help
Cisco Systems
Interfaces
Security Policy
NAT
VPN
CSD Manager
Trend Micro Content Security
Routing
Global Objects
Properties
Configuration > Trend Micro Content Security > CSC Setup > Wizard Setup
CSC Setup
Activation/License
IP Configuration
Host/Notification Se
Management Acces
Password
Wizard Setup
Web
Mail
File Transfer
Updates
Wizard Setup
Click on the Launch Setup wizard button below to start the wizard.
Setup wizard assists you in getting your CSC configured and running. Use this wizard to activate features and configure IP address notification and password settings.
Activation codes are required to enable features on CSC. If you have not received activation codes, you may use the following URL.
www.cisco.com/go/license
Launch Setup Wizard
<admin>
NA (15)
3/30/06 6:26:46 PM UTC

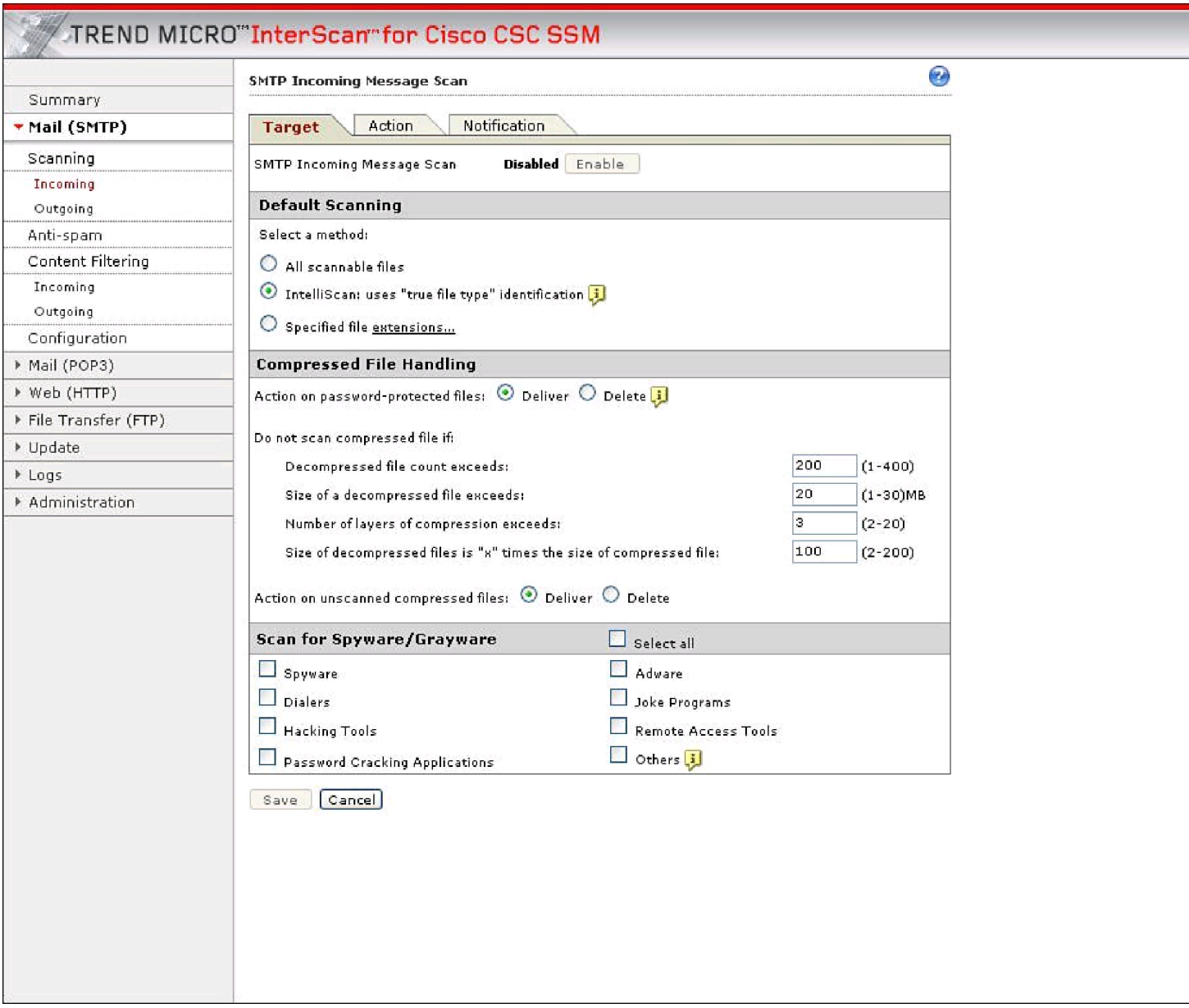

Cisco ASDM 5.1 for ASA - 172.23.62.18
File Rules Search Options Tools Wizards Help
Home
Configuration
Monitoring
Back
Forward
Search
Refresh
Save
Help
Cisco Systems
Interfaces
Security Policy
NAT
VPN
CSD Manager
Trend Micro Content Security
Routing
Global Objects
Properties
Configuration > Trend Micro Content Security > Web
CSC Setup
Activation/License
IP Configuration
Host/Notification Se
Management Acces
Password
Wizard Setup
Web
Mail
File Transfer
Updates
Web
URL Blocking And Filtering
URL Blocking: Enabled
Configure URL Blocking
URL Filtering: Disabled
Configure URL Filtering Rules
Configure URL Filtering Settings
File Blocking
File Blocking: Enabled
Configure File Blocking
Scanning
HTTP Scanning: Enabled
Configure Web Scanning
<admin>
NA (15)
3/30/06 8:17:46 PM UTC

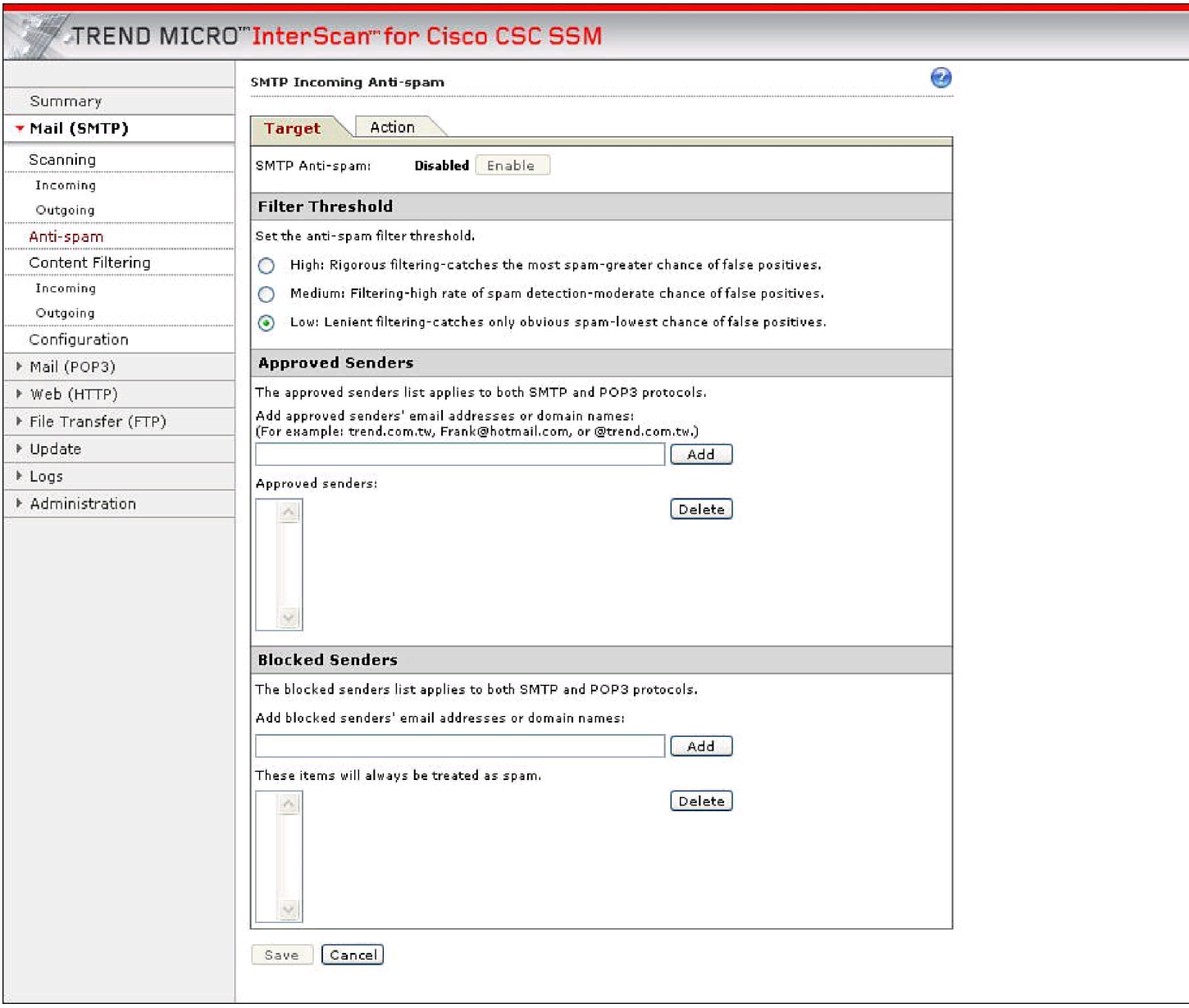

TREND MICRO™ InterScan™ for Cisco CSC SSM
TREND MICRO
InterScan for Cisco CSC SSM
Please type your password to access the product console.
Password:
Log on
© Copyright 1996-2006 Trend Micro Incorporated. All rights reserved.

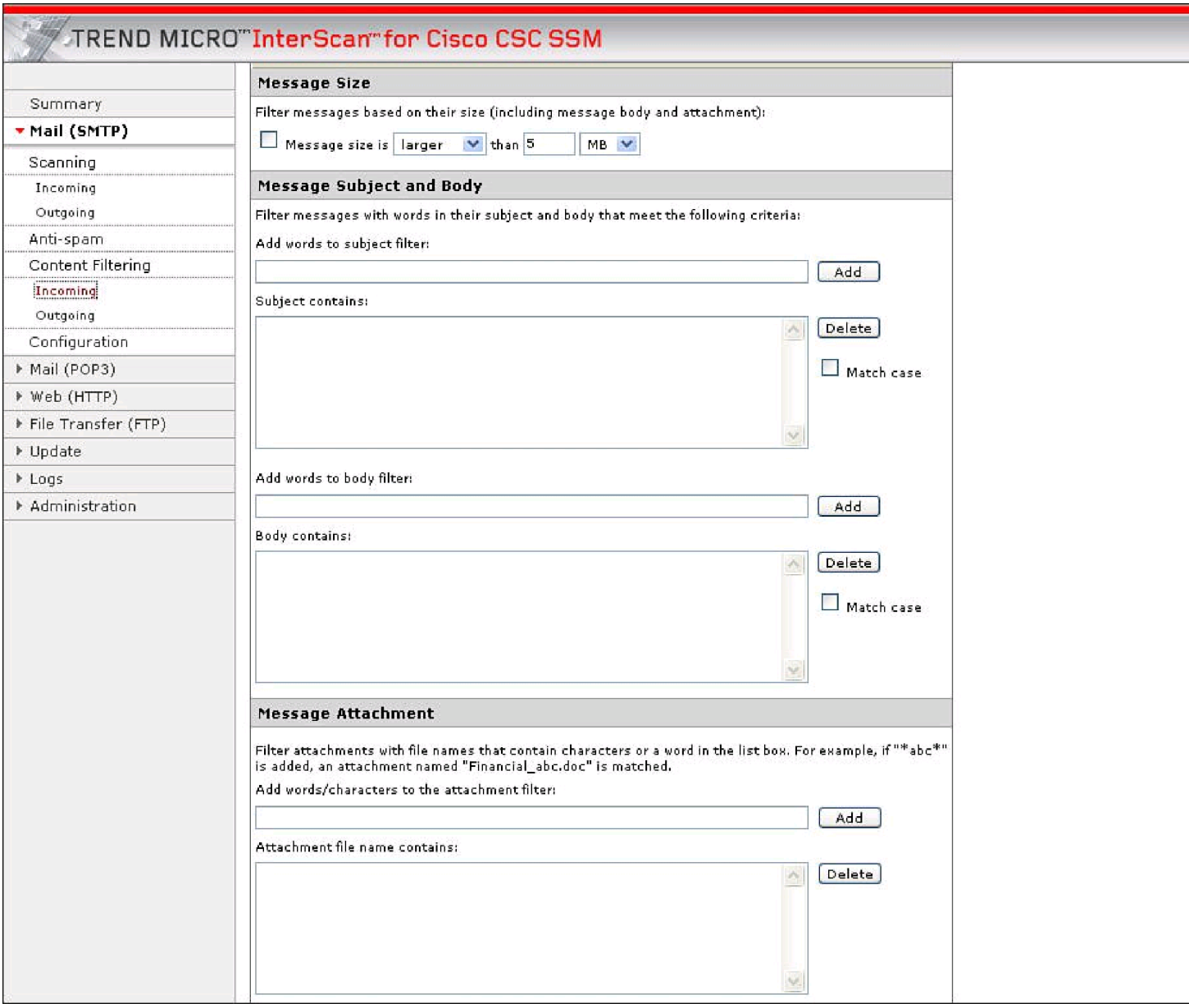

TREND MICRO™ InterScan™ for Cisco CSC SSM
Summary
Mail (SMTP)
Mail (POP3)
Web (HTTP)
File Transfer (FTP)
Update
Logs
Administration
Summary
Base License Expiration Notice
Your evaluation period ended on 02/20/2006. More info ...
Plus License Expiration Notice
Your evaluation period ended on 02/20/2006. More info ...
Status
Mail (SMTP)
Mail (POP3)
Web (HTTP)
File Transfer (FTP)
Product version: Trend Micro InterScan for Cisco CSC SSM 6.0 (Build#1342)
License: Base License expired on 02/20/2006
Plus License expired on 02/20/2006
Update
Refresh
Component
Current Version
Last Update
Virus Pattern File 3.219.00 02/17/2006 15:58:19
Virus Scan Engine 8.100.1002 01/10/2006 17:10:08
Spyware/Grayware pattern 0.339.00 02/16/2006 08:58:12
PhishTrap pattern 235 02/17/2006 09:58:11
Anti-spam rules and engine
Anti-spam rules 14274 02/17/2006 20:00:07
Anti-spam engine 3.52.1006 01/25/2006 06:58:13

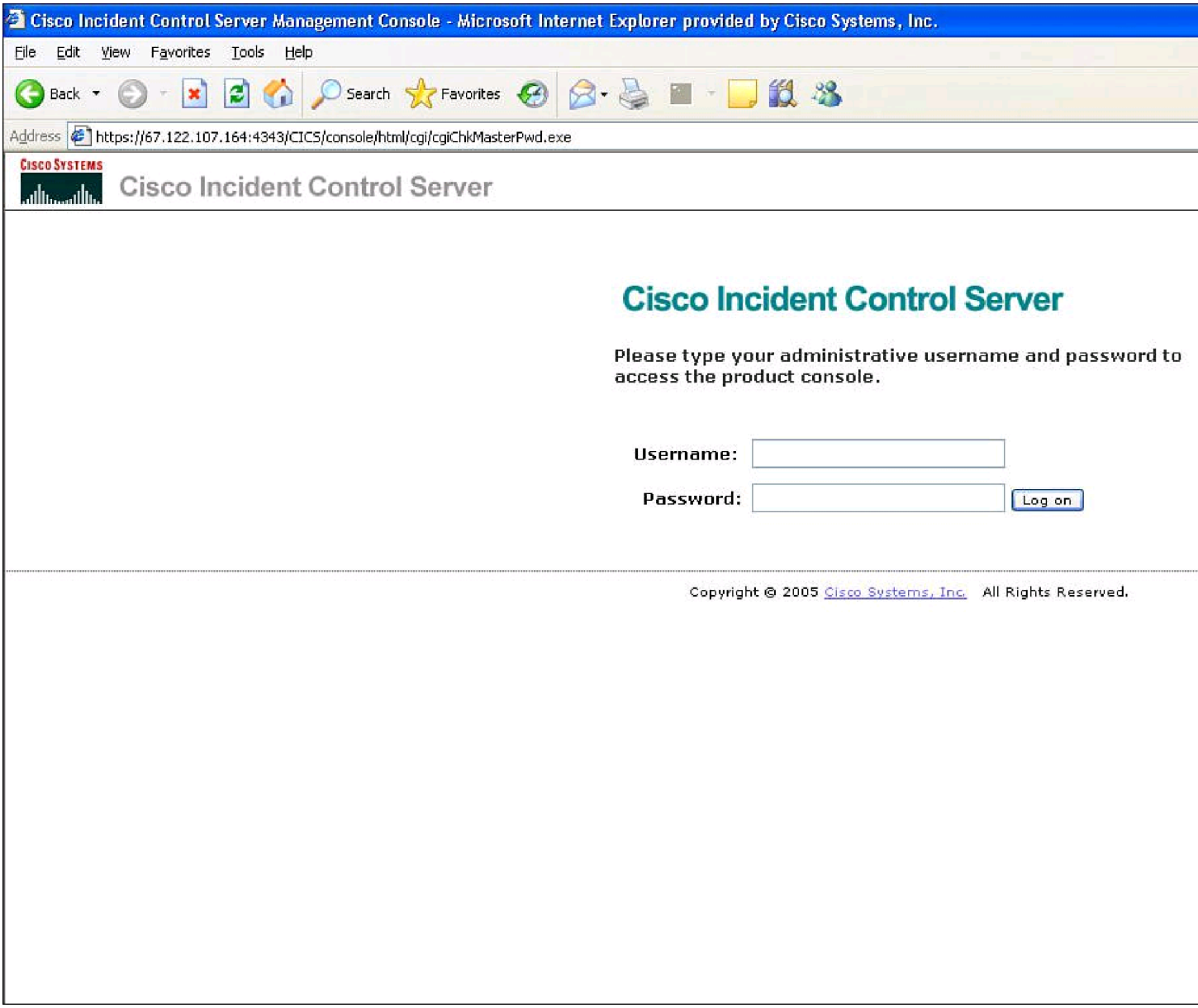

TREND MICRO™ InterScan™ for Cisco CSC SSM
Summary
Mail (SMTP)
Mail (POP3)
Web (HTTP)
Scanning
File Blocking
URL Blocking
URL Filtering
Filtering Rules
Settings
File Transfer (FTP)
Update
Logs
Administration
URL Blocking
Via Local List
Via Pattern File (PhishTrap)
Notification
URL Blocking: Disabled Enable
URLs to Block
Match:
Web site (example: 'xxx.com' matches all URLs starting with 'xxx.com')
URL keyword (example: 'yyy' string matches all URLs containing 'yyy')
String/IP address (exact-match, example: zzz.com/file matches only 'zzz.com/file')
Block
Do Not Block
Import block list and exceptions:
Browse...
Import
Block List
Users are never allowed to access URLs included in this list.
Remove
Remove All
Block List Exceptions
Access to these URLs is always allowed.
Remove
Remove All
Save
Cancel

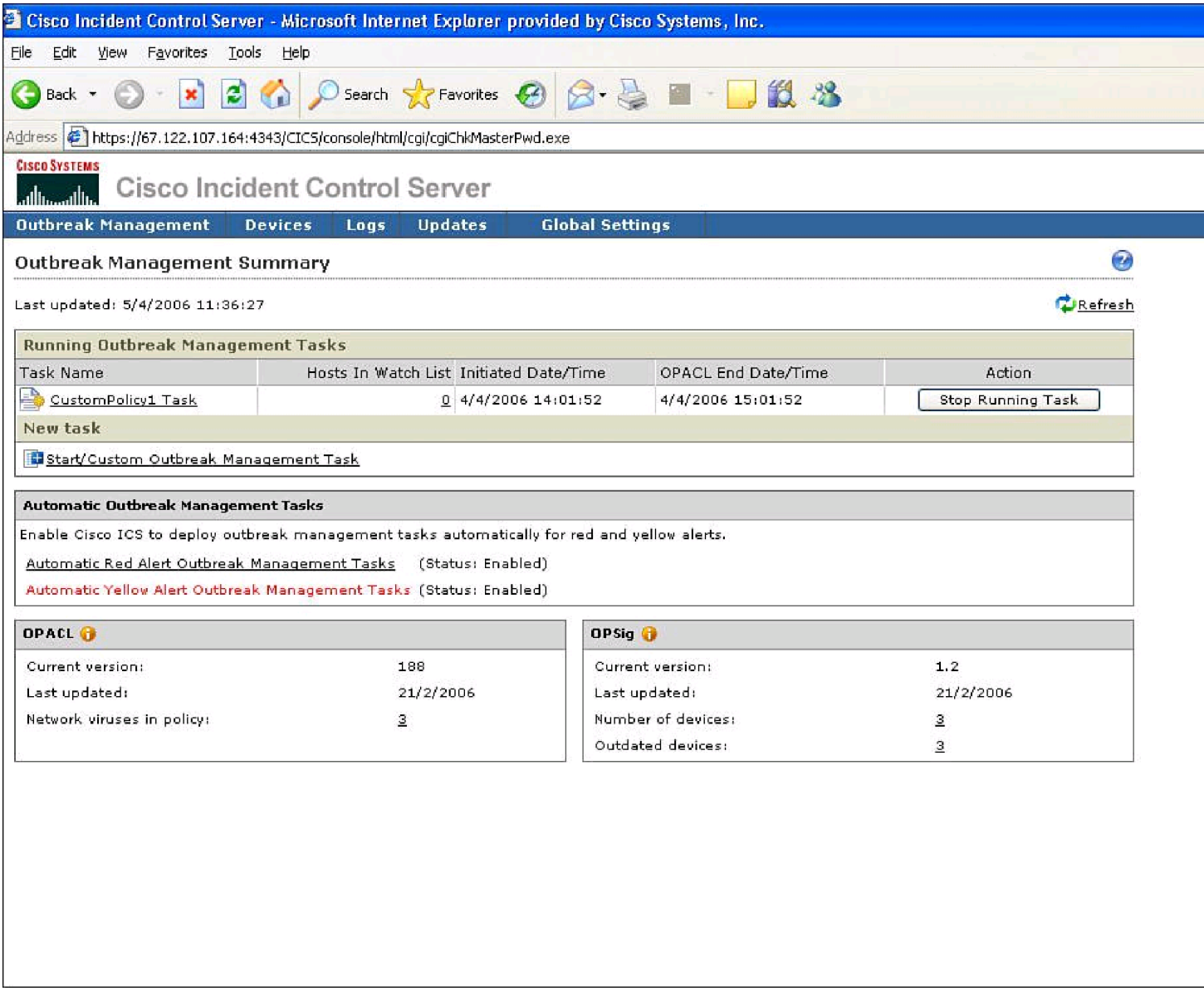

TREND MICRO™ InterScan™ for Cisco CSC SSM
Log Off | Help
Summary
Mail (SMTP)
Mail (POP3)
Web (HTTP)
Scanning
File Blocking
URL Blocking
URL Filtering
Filtering Rules
Settings
File Transfer (FTP)
Update
Logs
Administration
URL Blocking
Via Local List
Via Pattern File (PhishTrap)
Notification
Block URLs Using Following PhishTrap Categories:
Phishing sites: fraudulent collection of confidential information
Spyware sites: hidden but legal program that secretly collects confidential information
Virus accomplice sites: outbound HTTP accesses due to known behavior of malicious code
Disease vector sites: a Web site that exists for malicious purpose
Submit the Potential Phishing URL to TrendLabs SM:
Phishing URL:
Phishing categories:
Phishing
Sender's email address:
steve@cisco.com
Note:
Submit
Save
Cancel

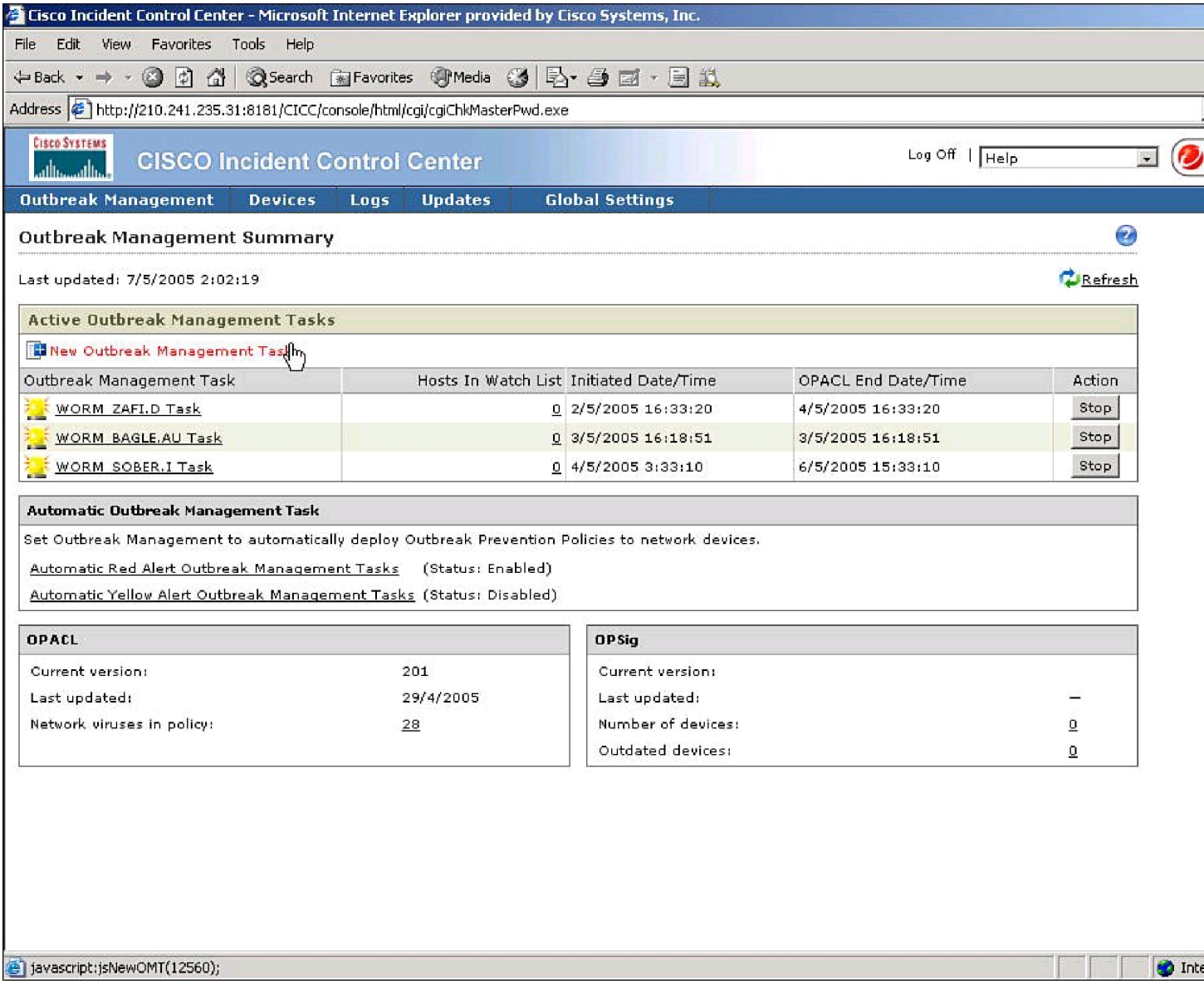

TREND MICRO™ InterScan™ for Cisco CSC SSM
Summary
Mail (SMTP)
Scanning
Incoming
Outgoing
Anti-spam
Content Filtering
Incoming
Outgoing
Configuration
Mail (POP3)
Web (HTTP)
File Transfer (FTP)
Update
Logs
Administration
SMTP Incoming Message Scan
Target
Action
Notification
SMTP Incoming Message Scan
Disabled
Enable
Default Scanning
Select a method:
All scannable files
IntelliScan: uses "true file type" identification
Specified file extensions...
Compressed File Handling
Action on password-protected files:
Deliver
Delete
Do not scan compressed file if:
Decompressed file count exceeds:
200
(1-400)
Size of a decompressed file exceeds:
20
(1-30)MB
Number of layers of compression exceeds:
3
(2-20)
Size of decompressed files is "x" times the size of compressed file:
100
(2-200)
Action on unscanned compressed files:
Deliver
Delete
Scan for Spyware/Grayware
Select all
Spyware
Adware
Dialers
Joke Programs
Hacking Tools
Remote Access Tools
Password Cracking Applications
Others
Save
Cancel

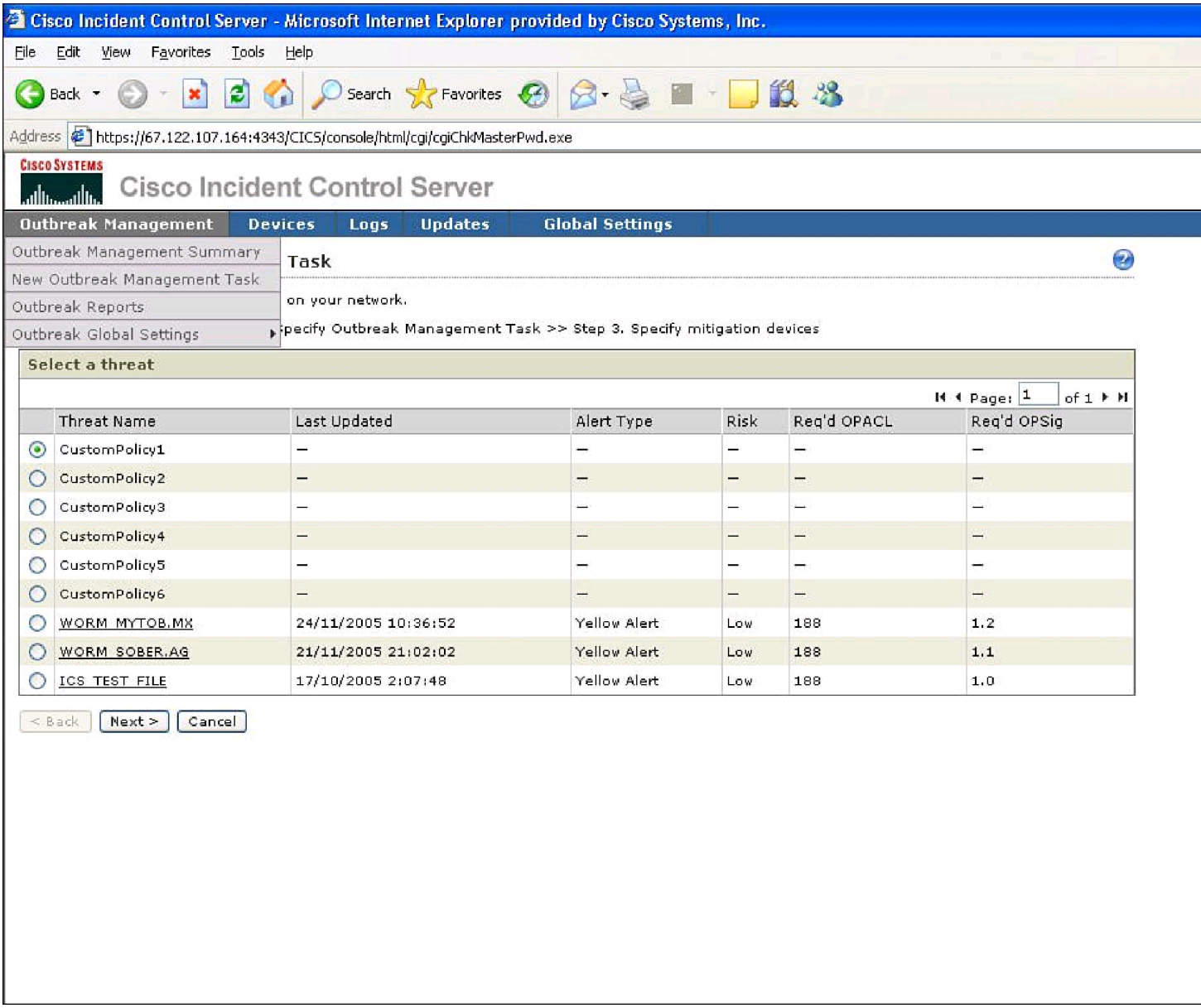

TREND MICRO™ InterScan™ for Cisco CSC SSM
Summary
Mail (SMTP)
Scanning
Incoming
Outgoing
Anti-spam
Content Filtering
Incoming
Outgoing
Configuration
Mail (POP3)
Web (HTTP)
File Transfer (FTP)
Update
Logs
Administration
SMTP Incoming Anti-spam
Target
Action
SMTP Anti-spam:
Disabled
Enable
Filter Threshold
Set the anti-spam filter threshold.
High: Rigorous filtering-catches the most spam-greater chance of false positives.
Medium: Filtering-high rate of spam detection-moderate chance of false positives.
Low: Lenient filtering-catches only obvious spam-lowest chance of false positives.
Approved Senders
The approved senders list applies to both SMTP and POP3 protocols.
Add approved senders' email addresses or domain names:
(For example: trend.com.tw, Frank@hotmail.com, or @trend.com.tw.)
Add
Approved senders:
Delete
Blocked Senders
The blocked senders list applies to both SMTP and POP3 protocols.
Add blocked senders' email addresses or domain names:
Add
These items will always be treated as spam.
Delete
Save
Cancel

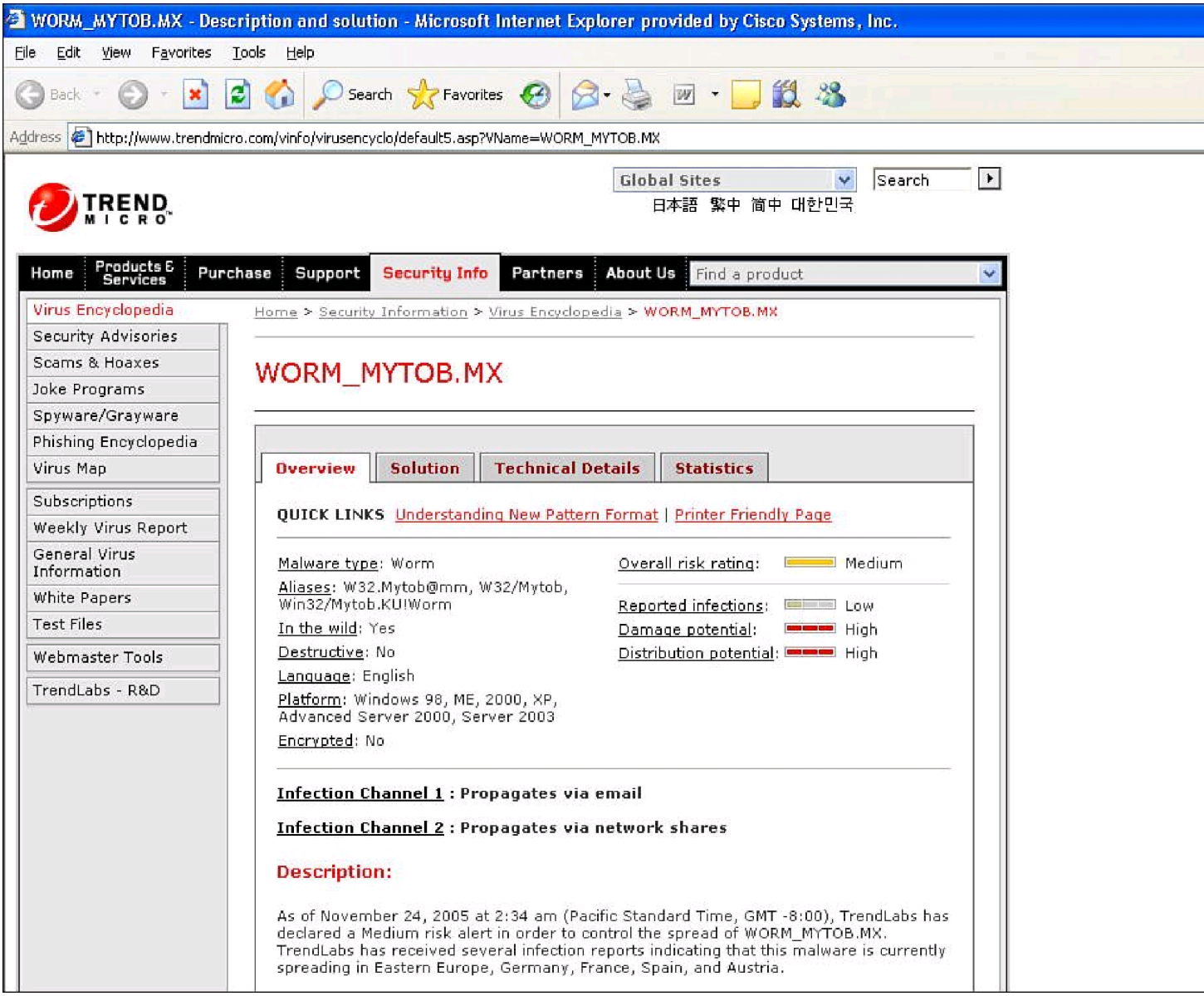

TREND MICRO™ InterScan™ for Cisco CSC SSM
Summary
Mail (SMTP)
Scanning
Incoming
Outgoing
Anti-spam
Content Filtering
Incoming
Outgoing
Configuration
Mail (POP3)
Web (HTTP)
File Transfer (FTP)
Update
Logs
Administration
Message Size
Filter messages based on their size (including message body and attachment):
Message size is larger than 5 MB
Message Subject and Body
Filter messages with words in their subject and body that meet the following criteria:
Add words to subject filter:
Add
Subject contains:
Delete
Match case
Add words to body filter:
Add
Body contains:
Delete
Match case
Message Attachment
Filter attachments with file names that contain characters or a word in the list box. For example, if "*abc*" is added, an attachment named "Financial_abc.doc" is matched.
Add words/characters to the attachment filter:
Add
Attachment file name contains:
Delete


Cisco Incident Control Server Management Console - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites
Address https://67.122.107.164:4343/CICS/console/html/cgi/cgiChkMasterPwd.exe
Cisco Systems
Cisco Incident Control Server
Cisco Incident Control Server
Please type your administrative username and password to access the product console.
Username:
Password:
Log on
Copyright © 2005 Cisco Systems, Inc. All Rights Reserved.

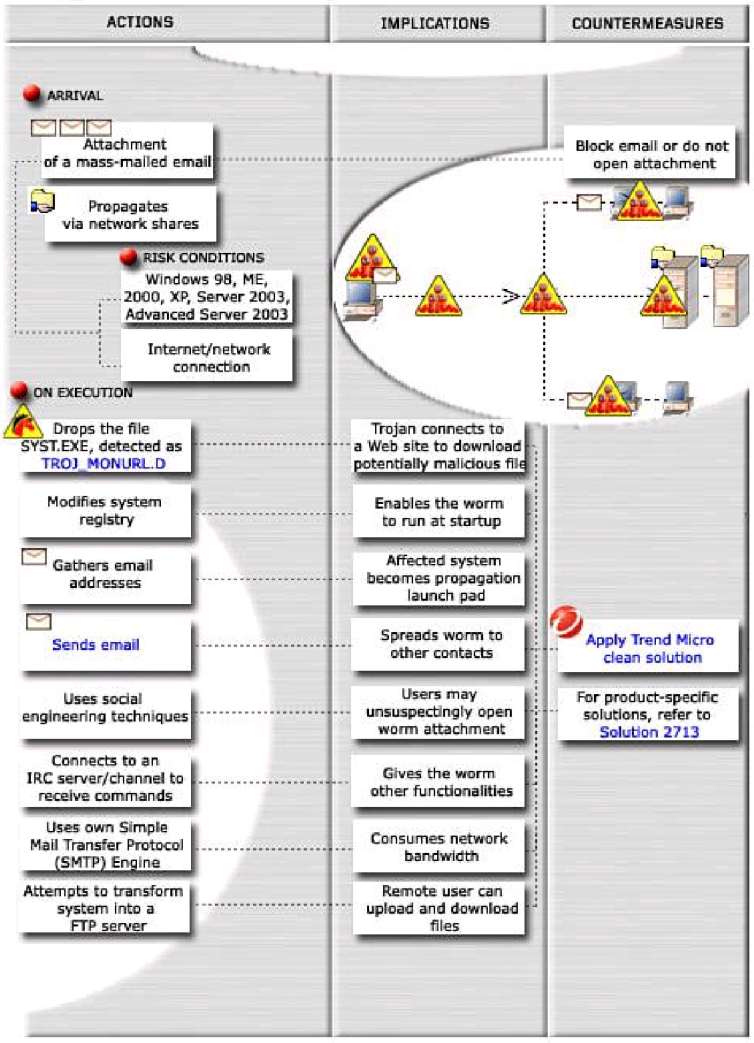

Cisco Incident Control Server - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites
Address https://67.122.107.164:4343/CICS/console/html/cgi/cgiChkMasterPwd.exe
Cisco Systems
Cisco Incident Control Server
Outbreak Management Devices Logs Updates Global Settings
Outbreak Management Summary
Last updated: 5/4/2006 11:36:27
Refresh
Running Outbreak Management Tasks
Task Name
Hosts In Watch List
Initiated Date/Time
OPACL End Date/Time
Action
CustomPolicy1 Task
0
4/4/2006 14:01:52
4/4/2006 15:01:52
Stop Running Task
New task
Start/Custom Outbreak Management Task
Automatic Outbreak Management Tasks
Enable Cisco ICS to deploy outbreak management tasks automatically for red and yellow alerts.
Automatic Red Alert Outbreak Management Tasks (Status: Enabled)
Automatic Yellow Alert Outbreak Management Tasks (Status: Enabled)
OPACL
Current version: 188
Last updated: 21/2/2006
Network viruses in policy: 3
OPSig
Current version: 1.2
Last updated: 21/2/2006
Number of devices: 3
Outdated devices: 3


Cisco Incident Control Center - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://210.241.235.31:8181/CICC/console/html/cgi/cgiChkMasterPwd.exe
CISCO Incident Control Center
Log Off | Help
Outbreak Management Devices Logs Updates Global Settings
Outbreak Management Summary
Last updated: 7/5/2005 2:02:19
Refresh
Active Outbreak Management Tasks
New Outbreak Management Task
Outbreak Management Task | Hosts In Watch List | Initiated Date/Time | OPACL End Date/Time | Action
WORM_ZAFI.D Task | 0 | 2/5/2005 16:33:20 | 4/5/2005 16:33:20 | Stop
WORM_BAGLE.AU Task | 0 | 3/5/2005 16:18:51 | 3/5/2005 16:18:51 | Stop
WORM_SOBER.I Task | 0 | 4/5/2005 3:33:10 | 6/5/2005 15:33:10 | Stop
Automatic Outbreak Management Task
Set Outbreak Management to automatically deploy Outbreak Prevention Policies to network devices.
Automatic Red Alert Outbreak Management Tasks (Status: Enabled)
Automatic Yellow Alert Outbreak Management Tasks (Status: Disabled)
OPACL
Current version: 201
Last updated: 29/4/2005
Network viruses in policy: 28
OPSig
Current version:
Last updated: –
Number of devices: 0
Outdated devices: 0
javascript:jsNewOMT(12560);


Cisco Incident Control Server - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites
Address https://67.122.107.164:4343/CICS/console/html/cgi/cgiChkMasterPwd.exe
Cisco Systems
Cisco Incident Control Server
Outbreak Management Devices Logs Updates Global Settings
Outbreak Management Summary
New Outbreak Management Task
Outbreak Reports
Outbreak Global Settings
Task
on your network.
pecify Outbreak Management Task >> Step 3. Specify mitigation devices
Select a threat
Page: 1 of 1
Threat Name | Last Updated | Alert Type | Risk | Req'd OPACL | Req'd OPSig
CustomPolicy1 | – | – | – | – | –
CustomPolicy2 | – | – | – | – | –
CustomPolicy3 | – | – | – | – | –
CustomPolicy4 | – | – | – | – | –
CustomPolicy5 | – | – | – | – | –
CustomPolicy6 | – | – | – | – | –
WORM_MYTOB.MX | 24/11/2005 10:36:52 | Yellow Alert | Low | 188 | 1.2
WORM_SOBER.AG | 21/11/2005 21:02:02 | Yellow Alert | Low | 188 | 1.1
ICS_TEST_FILE | 17/10/2005 2:07:48 | Yellow Alert | Low | 188 | 1.0
< Back Next > Cancel

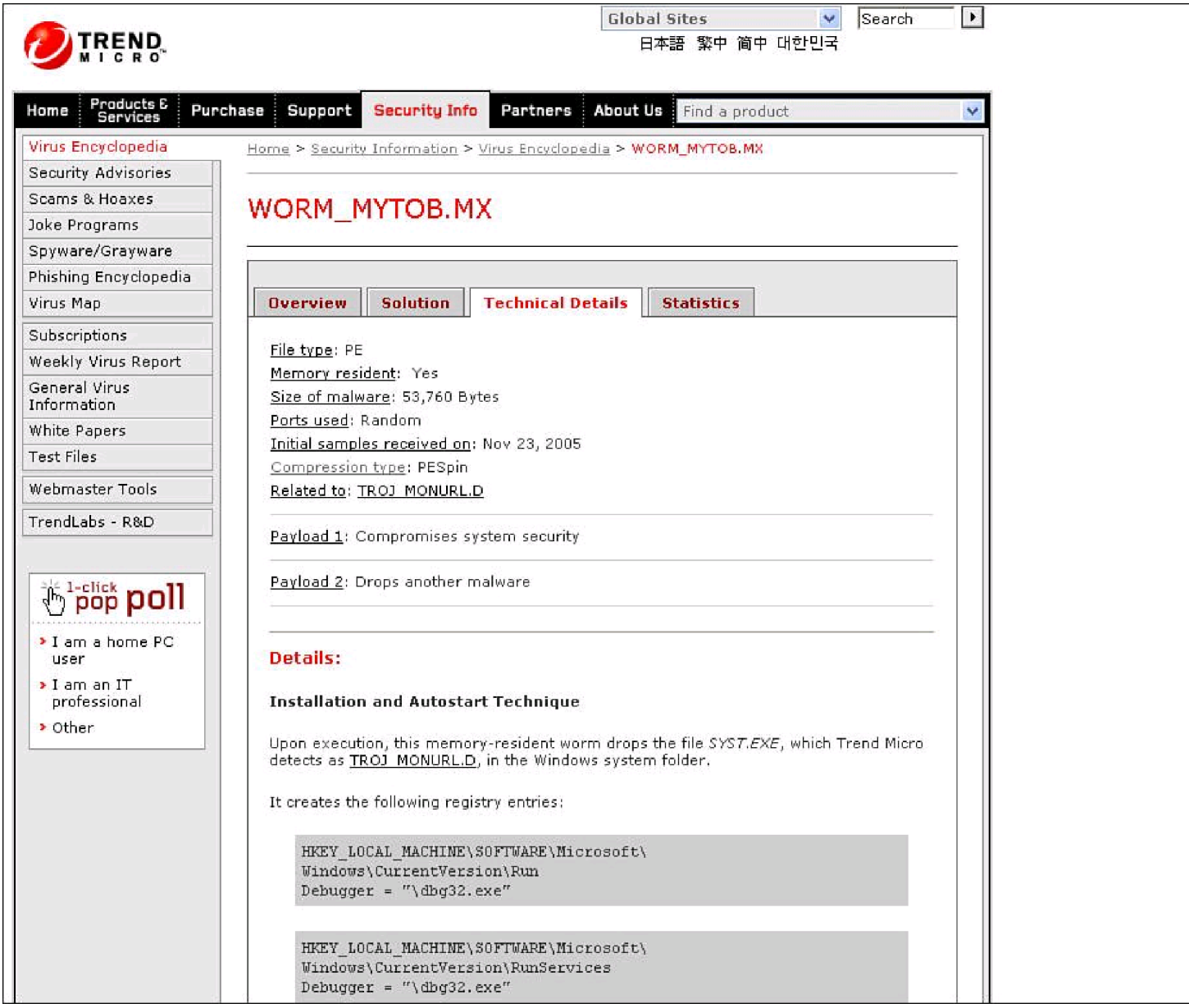

WORM_MYTOB.MX - Description and solution - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MYTOB.MX
TREND MICRO
Global Sites
Search
日本語 繁中 简中 대한민국
Home
Products & Services
Purchase
Support
Security Info
Partners
About Us
Find a product
Virus Encyclopedia
Security Advisories
Scams & Hoaxes
Joke Programs
Spyware/Grayware
Phishing Encyclopedia
Virus Map
Subscriptions
Weekly Virus Report
General Virus Information
White Papers
Test Files
Webmaster Tools
TrendLabs - R&D
Home > Security Information > Virus Encyclopedia > WORM_MYTOB.MX
WORM_MYTOB.MX
Overview
Solution
Technical Details
Statistics
QUICK LINKS Understanding New Pattern Format | Printer Friendly Page
Malware type: Worm
Aliases: W32.Mytob@mm, W32/Mytob, Win32/Mytob.KU!Worm
In the wild: Yes
Destructive: No
Language: English
Platform: Windows 98, ME, 2000, XP, Advanced Server 2000, Server 2003
Encrypted: No
Overall risk rating: Medium
Reported infections: Low
Damage potential: High
Distribution potential: High
Infection Channel 1 : Propagates via email
Infection Channel 2 : Propagates via network shares
Description:
As of November 24, 2005 at 2:34 am (Pacific Standard Time, GMT -8:00), TrendLabs has declared a Medium risk alert in order to control the spread of WORM_MYTOB.MX. TrendLabs has received several infection reports indicating that this malware is currently spreading in Eastern Europe, Germany, France, Spain, and Austria.

WORM_MYTOB.MX Behavior Diagram



Comments/Suggestions

We would like to know what you think about the Behavior Diagram, our latest Virus Encyclopedia feature. Please click here to send us your comments, suggestions, or feedbacks.



TREND MICRO

Global Sites | Search

日本語 繁中 简中 대한민국

Home | Products & Services | Purchase | Support | Security Info | Partners | About Us | Find a product

Virus Encyclopedia
Security Advisories
Scams & Hoaxes
Joke Programs
Spyware/Grayware
Phishing Encyclopedia
Virus Map
Subscriptions
Weekly Virus Report
General Virus Information
White Papers
Test Files
Webmaster Tools
TrendLabs - R&D

1-click pop poll
- I am a home PC user
- I am an IT professional
- Other

Home > Security Information > Virus Encyclopedia > WORM_MYTOB.MX

WORM_MYTOB.MX

Overview | Solution | Technical Details | Statistics

File type: PE
Memory resident: Yes
Size of malware: 53,760 Bytes
Ports used: Random
Initial samples received on: Nov 23, 2005
Compression type: PESpin
Related to: TROJ_MONURL.D

Payload 1: Compromises system security

Payload 2: Drops another malware

Details:

Installation and Autostart Technique

Upon execution, this memory-resident worm drops the file *SYST.EXE*, which Trend Micro detects as TROJ_MONURL.D, in the Windows system folder.

It creates the following registry entries:

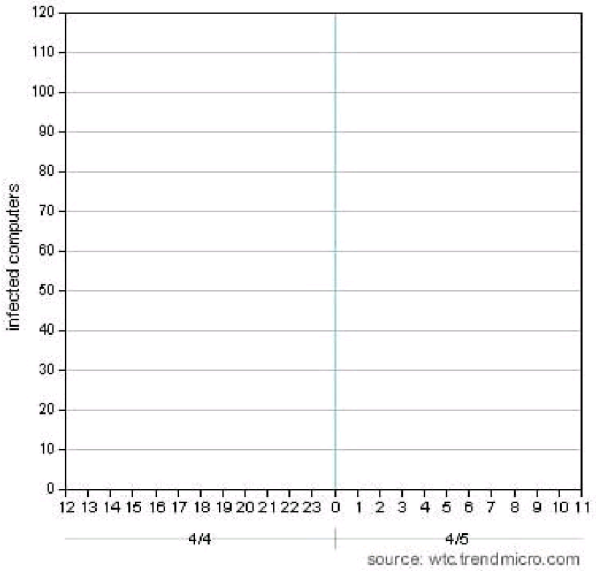
```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\Run
Debugger = "\dbg32.exe"
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\RunServices
Debugger = "\dbg32.exe"
```

WORM_MYTOB.MX

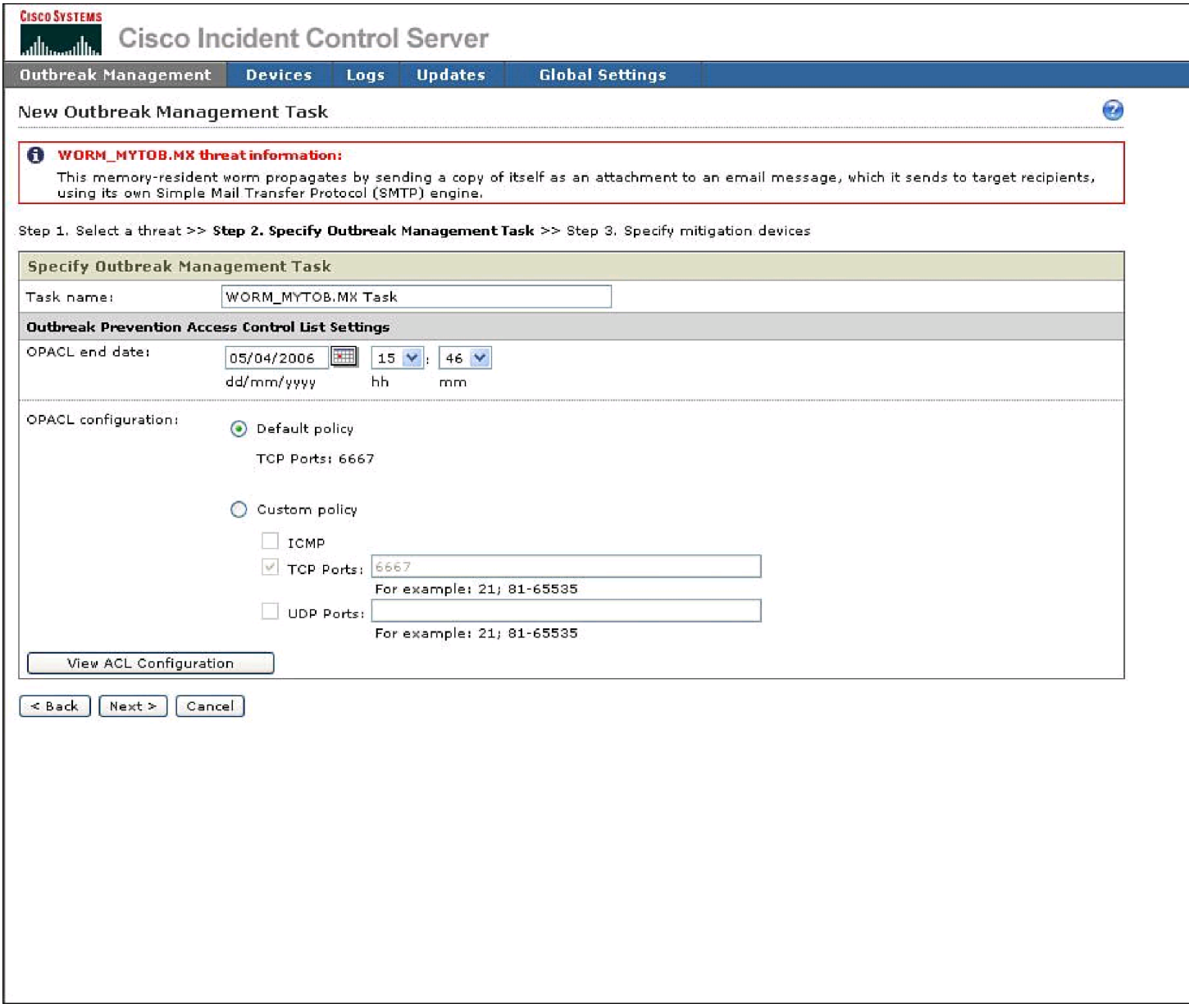
Overview | Solution | Technical Details | Statistics

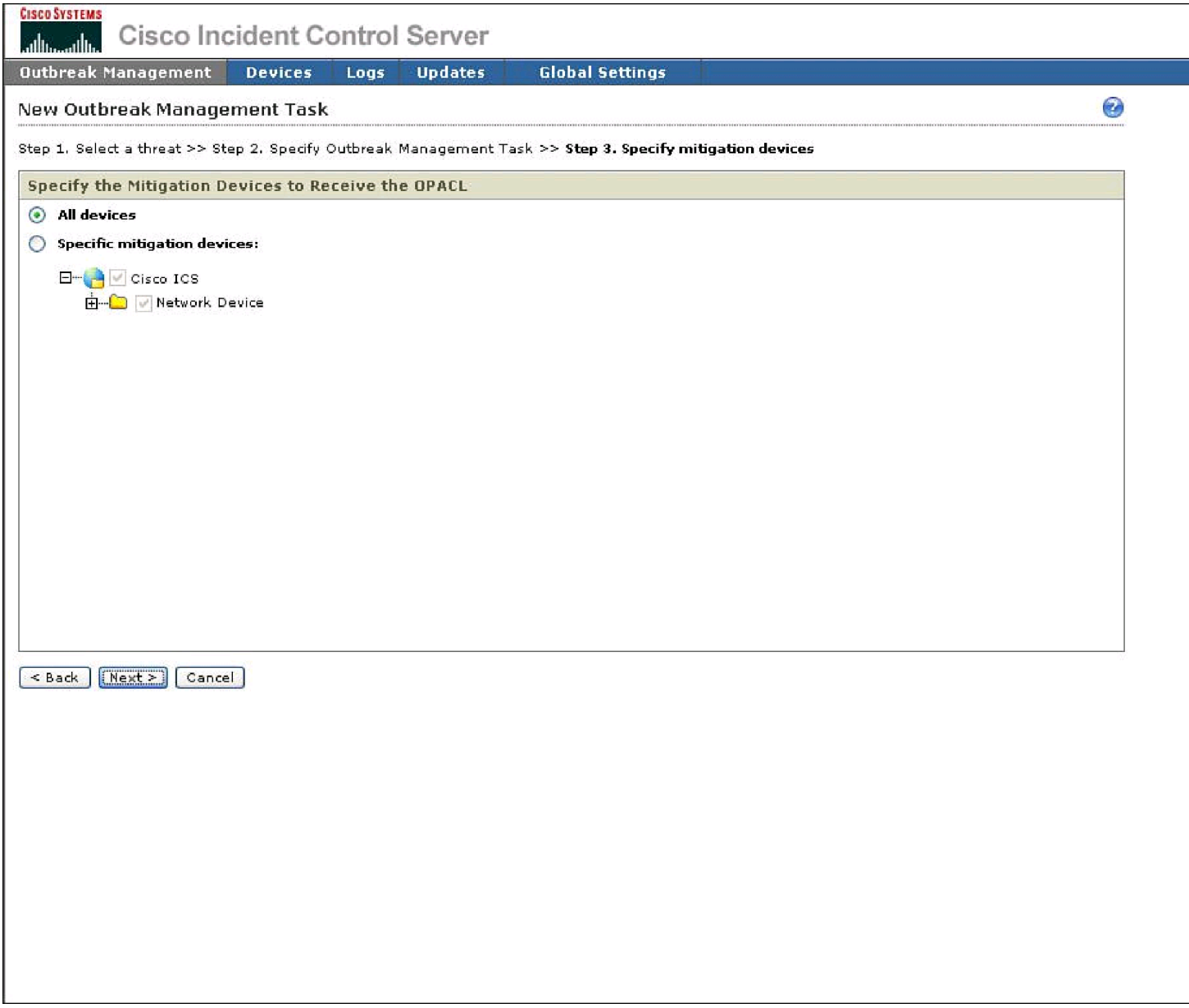
Time Period: 1d | 7d | 1m | 1y | All

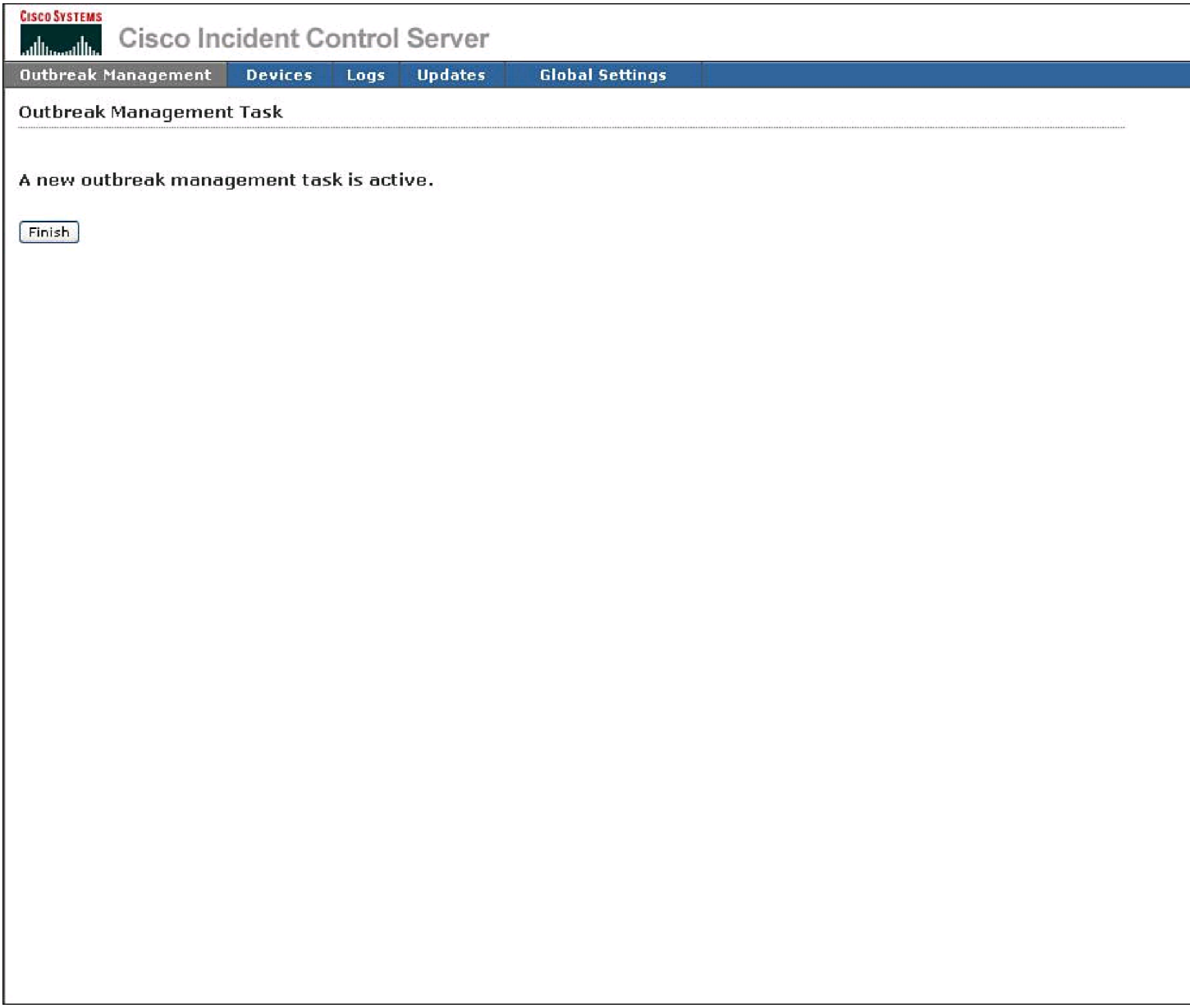


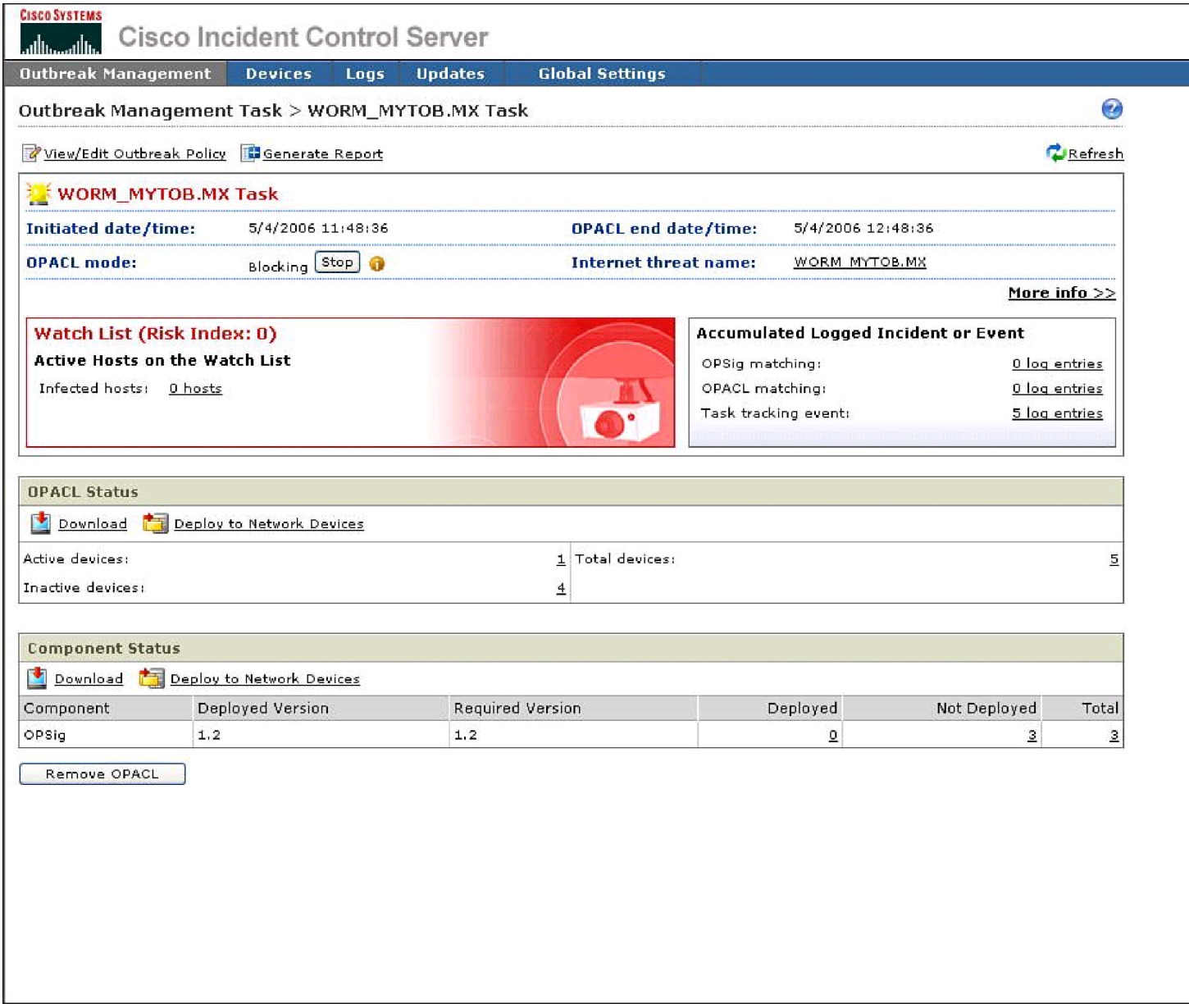
Computers infected since November 24, 2005

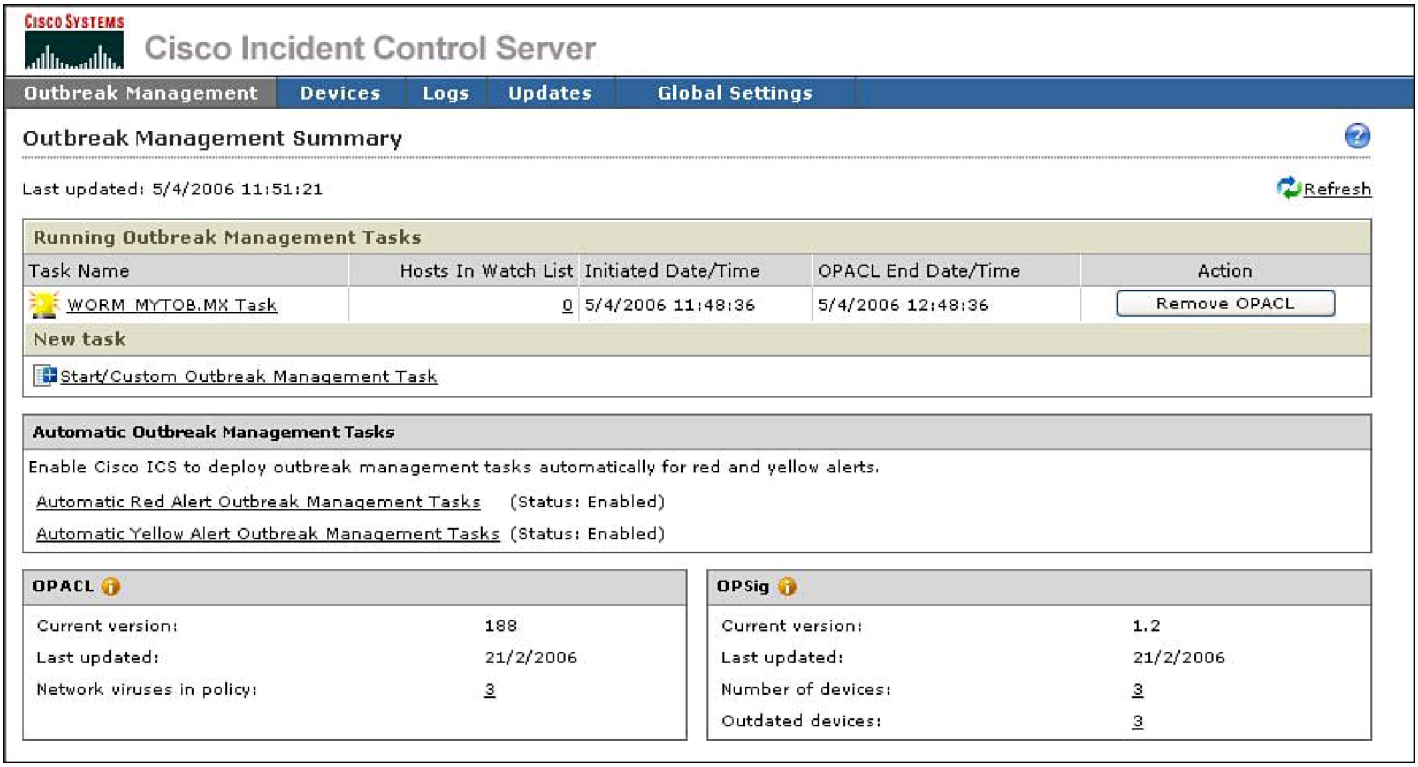
North America	1,023
Asia	301
Europe	167
Australia and New Zealand	22
Africa	6
South America	1
(unknown)	36
Total	**1,556**

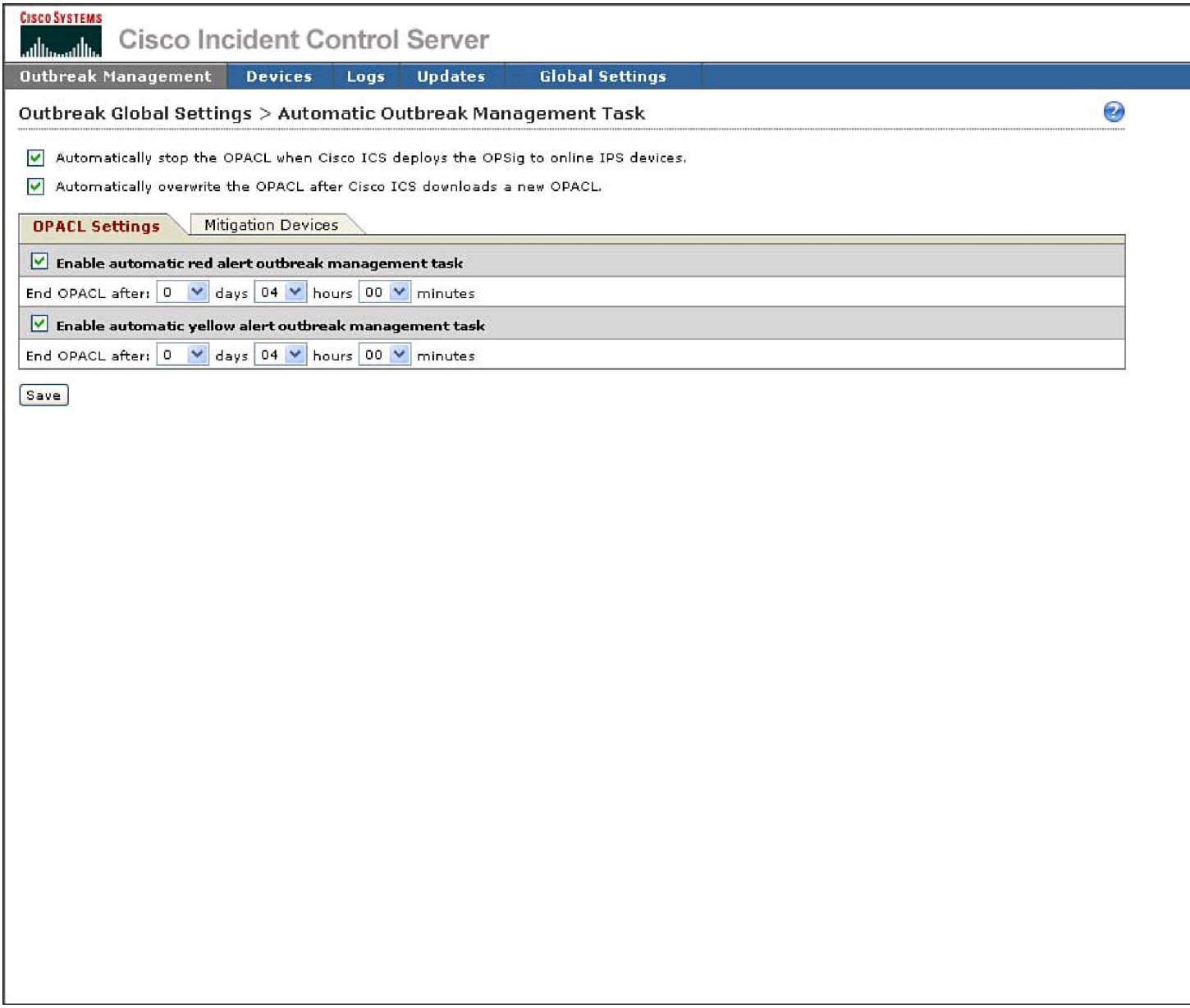

Cisco Systems
Cisco Incident Control Server
Outbreak Management
Devices
Logs
Updates
Global Settings
New Outbreak Management Task
WORM_MYTOB.MX threat information:
This memory-resident worm propagates by sending a copy of itself as an attachment to an email message, which it sends to target recipients, using its own Simple Mail Transfer Protocol (SMTP) engine.
Step 1. Select a threat >> Step 2. Specify Outbreak Management Task >> Step 3. Specify mitigation devices
Specify Outbreak Management Task
Task name:
WORM_MYTOB.MX Task
Outbreak Prevention Access Control List Settings
OPACL end date:
05/04/2006
dd/mm/yyyy
15
hh
46
mm
OPACL configuration:
Default policy
TCP Ports: 6667
Custom policy
ICMP
TCP Ports:
6667
For example: 21; 81-65535
UDP Ports:
For example: 21; 81-65535
View ACL Configuration
< Back
Next >
Cancel

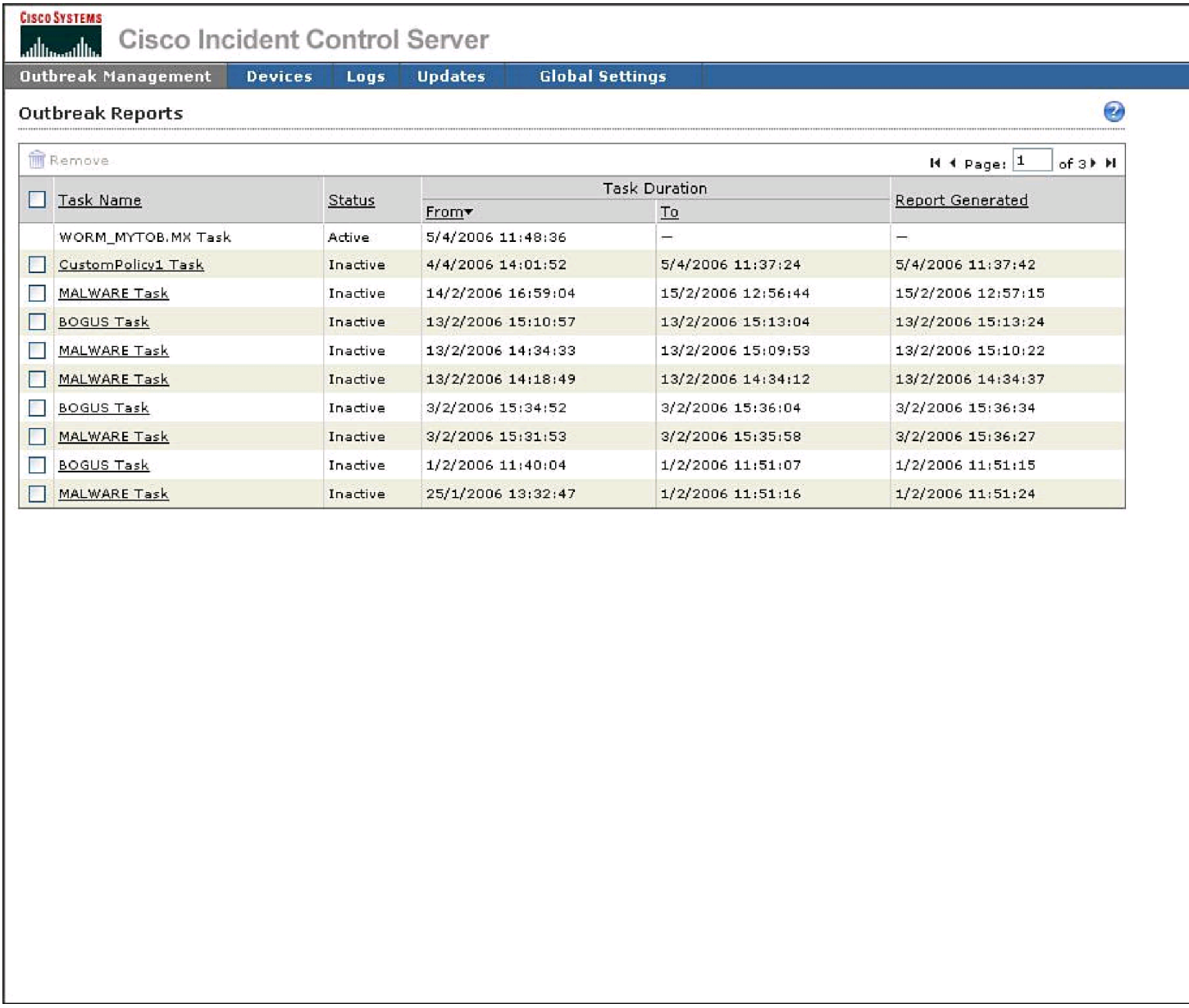

Cisco Systems
Cisco Incident Control Server
Outbreak Management
Devices
Logs
Updates
Global Settings
New Outbreak Management Task
Step 1. Select a threat >> Step 2. Specify Outbreak Management Task >> Step 3. Specify mitigation devices
Specify the Mitigation Devices to Receive the OPACL
All devices
Specific mitigation devices:
Cisco ICS
Network Device
< Back
Next >
Cancel


Cisco Systems
Cisco Incident Control Server
Outbreak Management
Devices
Logs
Updates
Global Settings
Outbreak Management Task
A new outbreak management task is active.
Finish


Cisco Systems
Cisco Incident Control Server
Outbreak Management
Devices
Logs
Updates
Global Settings
Outbreak Management Task > WORM_MYTOB.MX Task
View/Edit Outbreak Policy
Generate Report
Refresh
WORM_MYTOB.MX Task
Initiated date/time: 5/4/2006 11:48:36
OPACL end date/time: 5/4/2006 12:48:36
OPACL mode: Blocking Stop
Internet threat name: WORM_MYTOB.MX
More info >>
Watch List (Risk Index: 0)
Active Hosts on the Watch List
Infected hosts: 0 hosts
Accumulated Logged Incident or Event
OPSig matching: 0 log entries
OPACL matching: 0 log entries
Task tracking event: 5 log entries
OPACL Status
Download
Deploy to Network Devices
Active devices: 1
Total devices: 5
Inactive devices: 4
Component Status
Download
Deploy to Network Devices
Component
Deployed Version
Required Version
Deployed
Not Deployed
Total
OPSig
1.2
1.2
0
3
3
Remove OPACL


Cisco Systems
Cisco Incident Control Server
Outbreak Management
Devices
Logs
Updates
Global Settings
Outbreak Management Summary
Last updated: 5/4/2006 11:51:21
Refresh
Running Outbreak Management Tasks
Task Name
Hosts In Watch List
Initiated Date/Time
OPACL End Date/Time
Action
WORM_MYTOB.MX Task
0
5/4/2006 11:48:36
5/4/2006 12:48:36
Remove OPACL
New task
Start/Custom Outbreak Management Task
Automatic Outbreak Management Tasks
Enable Cisco ICS to deploy outbreak management tasks automatically for red and yellow alerts.
Automatic Red Alert Outbreak Management Tasks (Status: Enabled)
Automatic Yellow Alert Outbreak Management Tasks (Status: Enabled)
OPACL
Current version: 188
Last updated: 21/2/2006
Network viruses in policy: 3
OPSig
Current version: 1.2
Last updated: 21/2/2006
Number of devices: 3
Outdated devices: 3


Cisco Systems
Cisco Incident Control Server
Outbreak Management
Devices
Logs
Updates
Global Settings
Outbreak Global Settings > Automatic Outbreak Management Task
Automatically stop the OPACL when Cisco ICS deploys the OPSig to online IPS devices.
Automatically overwrite the OPACL after Cisco ICS downloads a new OPACL.
OPACL Settings
Mitigation Devices
Enable automatic red alert outbreak management task
End OPACL after: 0 days 04 hours 00 minutes
Enable automatic yellow alert outbreak management task
End OPACL after: 0 days 04 hours 00 minutes
Save



Task Name	Status	Task Duration		Report Generated
		From	To	
WORM_MYTOB.MX Task	Active	5/4/2006 11:48:36	–	–
CustomPolicy1 Task	Inactive	4/4/2006 14:01:52	5/4/2006 11:37:24	5/4/2006 11:37:42
MALWARE Task	Inactive	14/2/2006 16:59:04	15/2/2006 12:56:44	15/2/2006 12:57:15
BOGUS Task	Inactive	13/2/2006 15:10:57	13/2/2006 15:13:04	13/2/2006 15:13:24
MALWARE Task	Inactive	13/2/2006 14:34:33	13/2/2006 15:09:53	13/2/2006 15:10:22
MALWARE Task	Inactive	13/2/2006 14:18:49	13/2/2006 14:34:12	13/2/2006 14:34:37
BOGUS Task	Inactive	3/2/2006 15:34:52	3/2/2006 15:36:04	3/2/2006 15:36:34
MALWARE Task	Inactive	3/2/2006 15:31:53	3/2/2006 15:35:58	3/2/2006 15:36:27
BOGUS Task	Inactive	1/2/2006 11:40:04	1/2/2006 11:51:07	1/2/2006 11:51:15
MALWARE Task	Inactive	25/1/2006 13:32:47	1/2/2006 11:51:16	1/2/2006 11:51:24

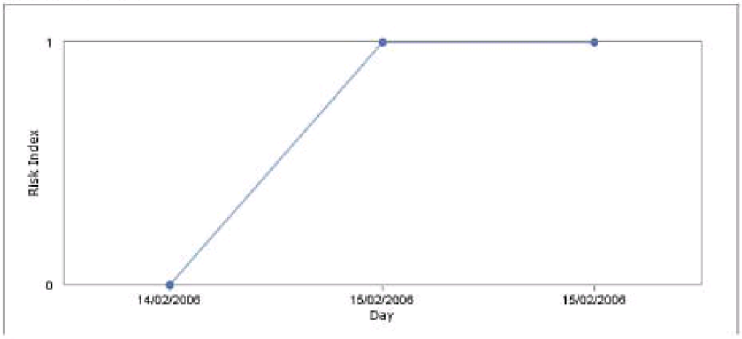
Outbreak Management Task Report

Report generation date:
15/02/2006 12:57:10

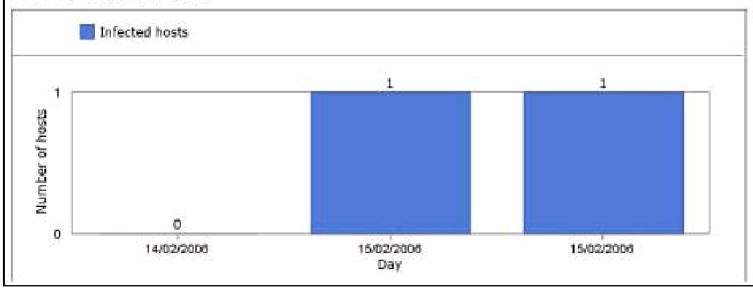
On 14/02/2006 15:59:04 Cisco Outbreak Management initiated an outbreak management task for MALWARE to monitor its influences on your network. Detailed information regarding that task is in this report.

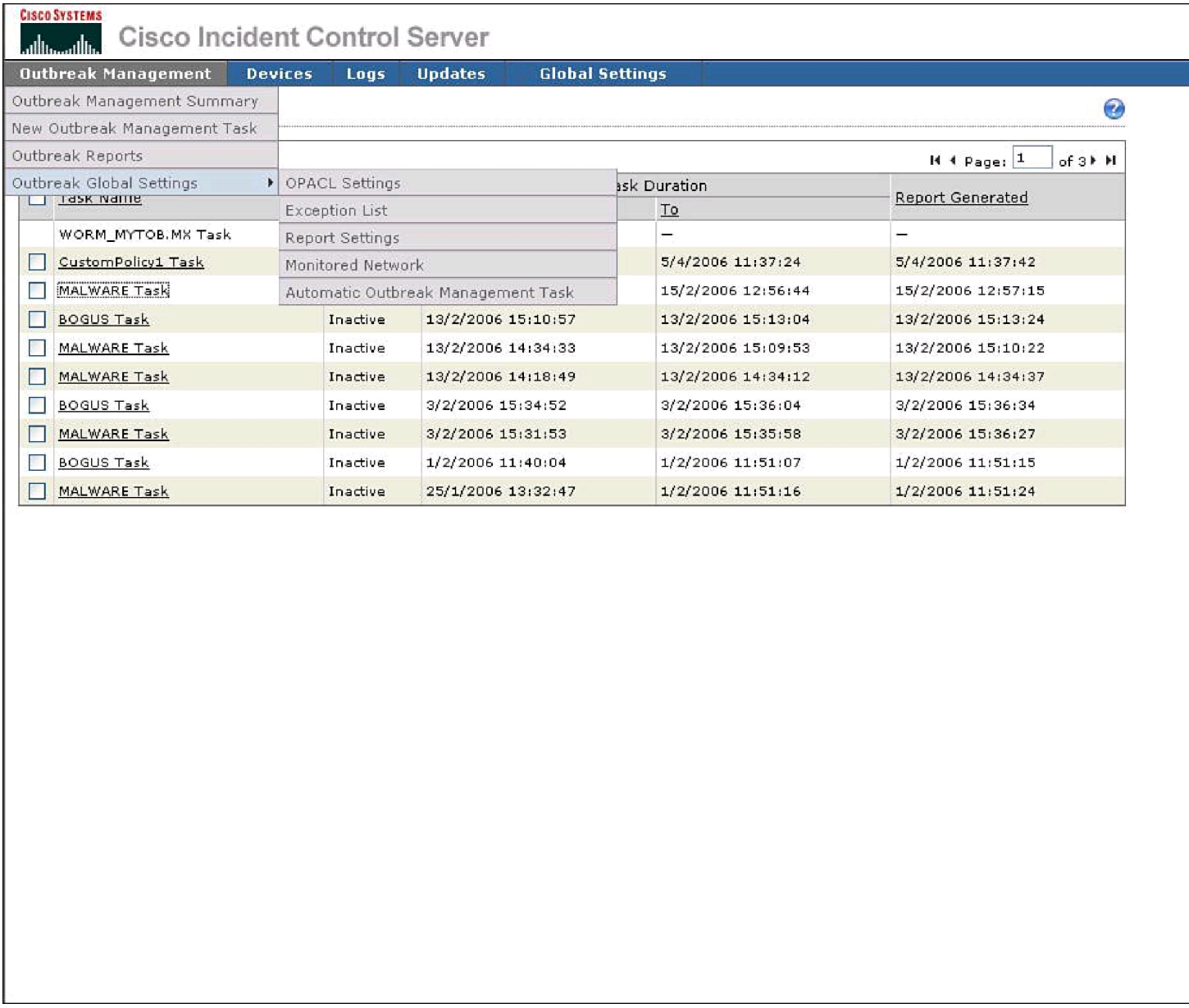
Initiated date/time:	14/02/2006 15:59:04	OPACL end date/time:	15/02/2006 11:56:43
OPACL mode:	Stopped	Internet threat name:	MALWARE
Alert type:	Yellow Alert		
Threat information:	This is a test OPAcl that would block connection to tcp port 52843.		

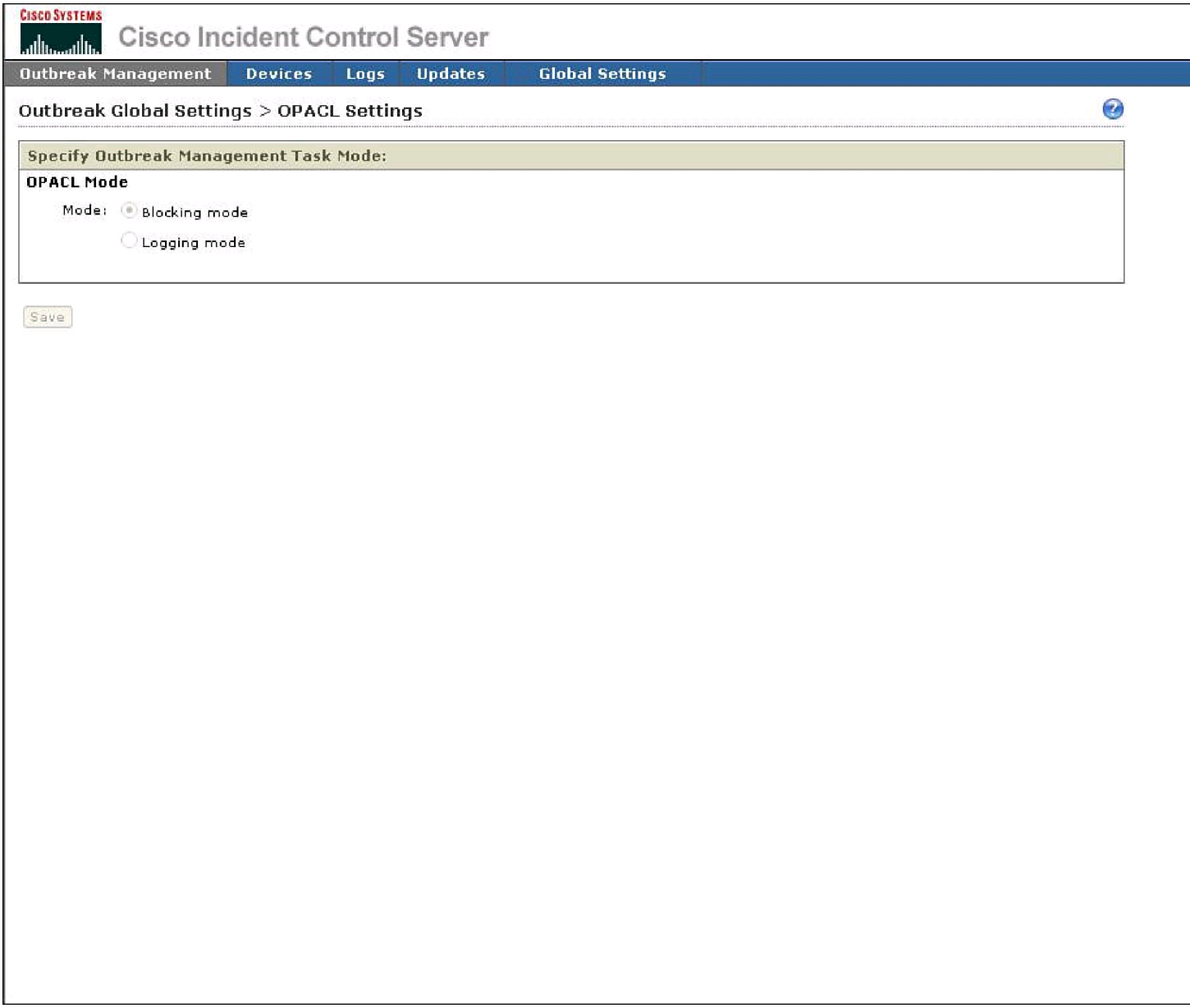
Risk Index Graph

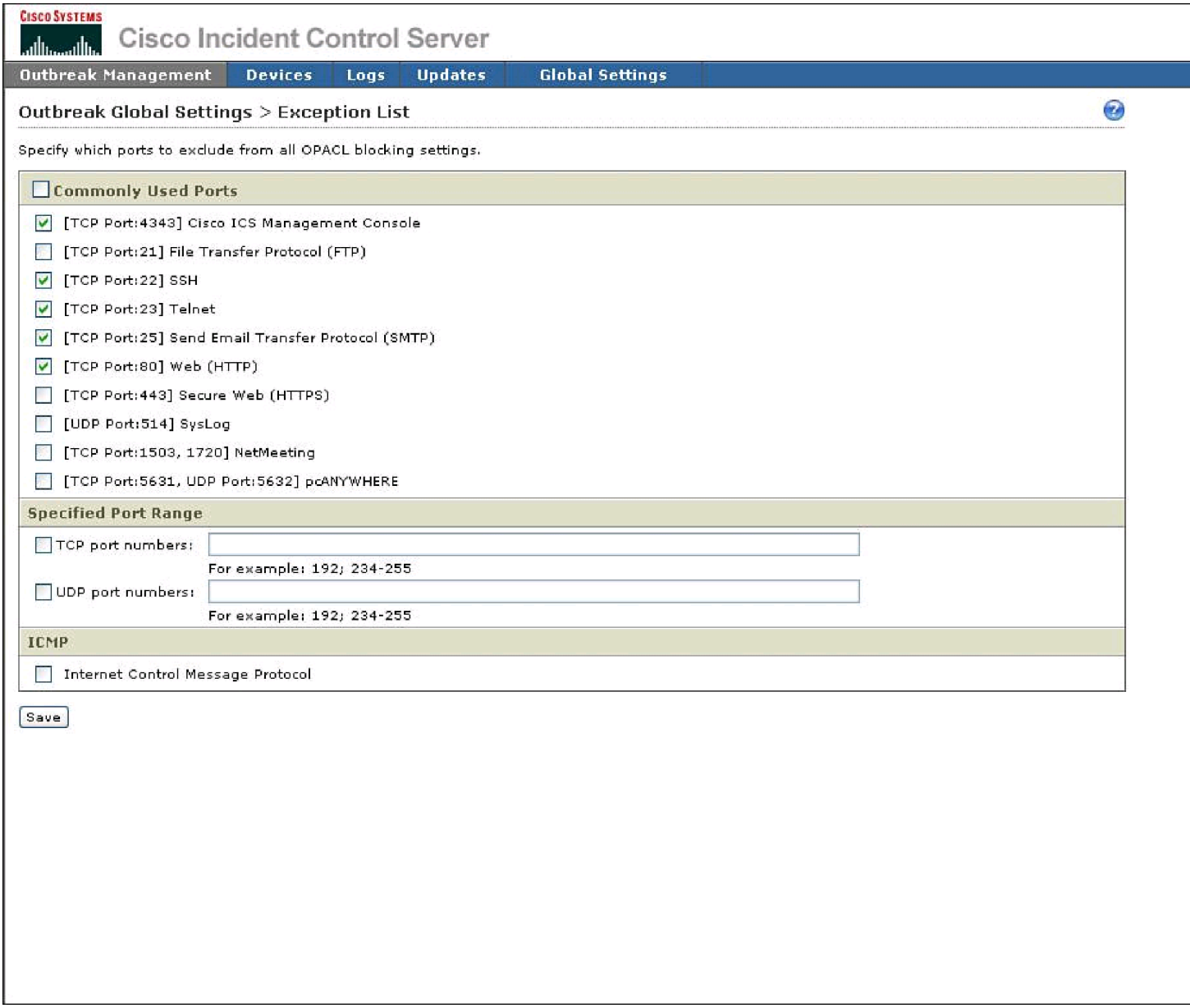


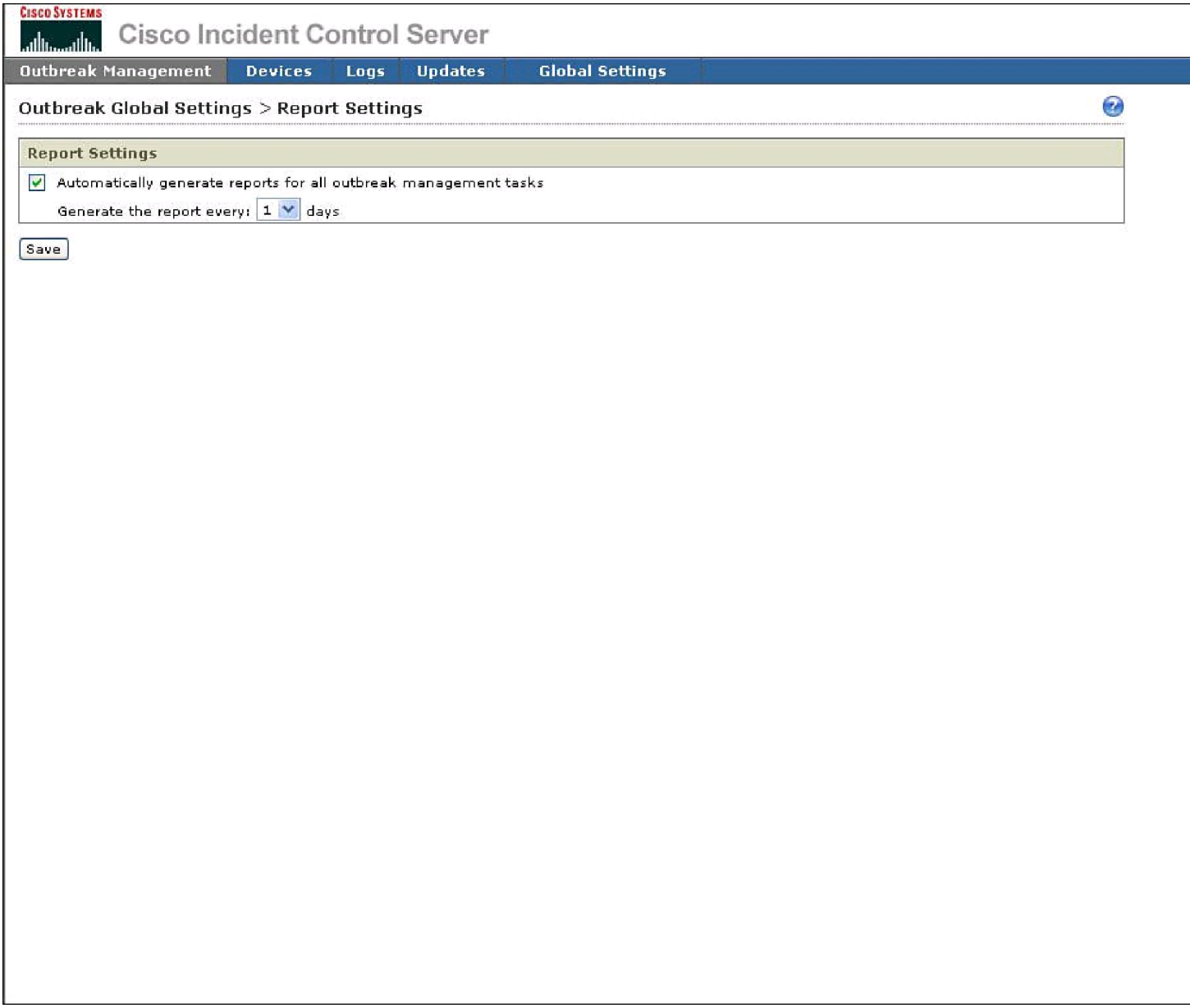
Hosts on Watch List Status

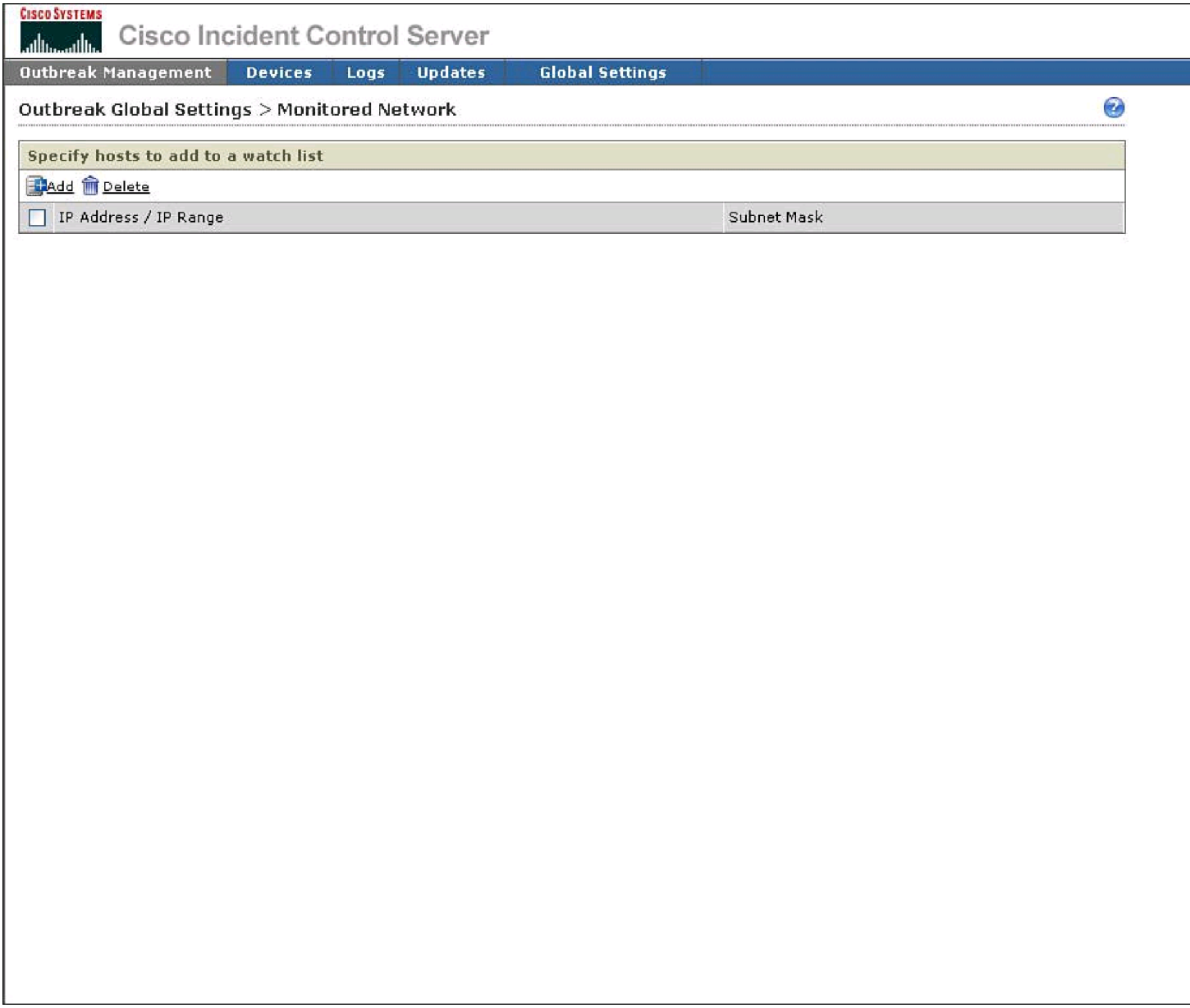


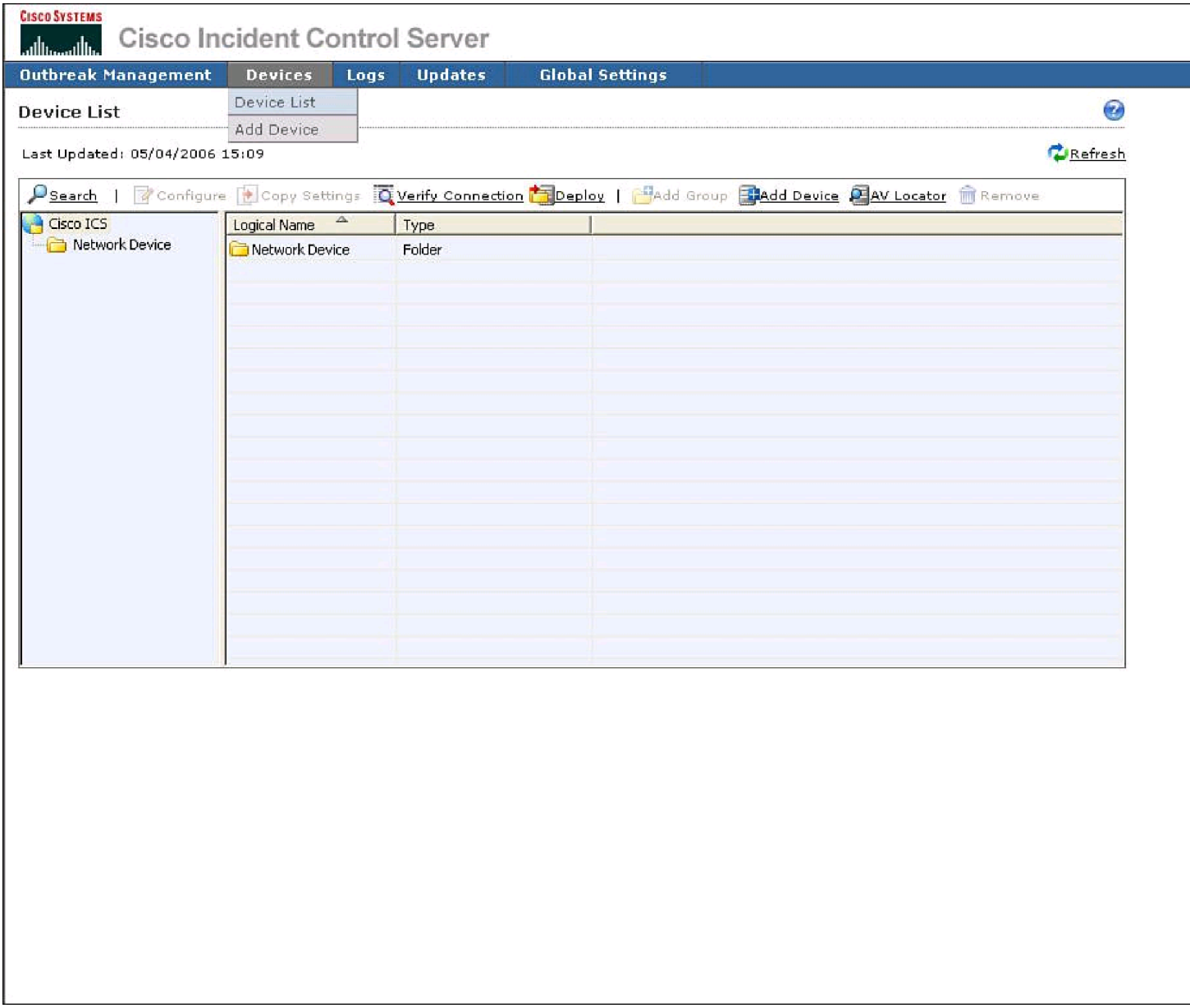

Cisco Systems
Cisco Incident Control Server
Outbreak Management
Devices
Logs
Updates
Global Settings
Outbreak Management Summary
New Outbreak Management Task
Outbreak Reports
Outbreak Global Settings
OPACL Settings
Exception List
Report Settings
Monitored Network
Automatic Outbreak Management Task
Page: 1 of 3
Task Name
Task Duration
To
Report Generated
WORM_MYTOB.MX Task
–
–
CustomPolicy1 Task
5/4/2006 11:37:24
5/4/2006 11:37:42
MALWARE Task
15/2/2006 12:56:44
15/2/2006 12:57:15
BOGUS Task
Inactive
13/2/2006 15:10:57
13/2/2006 15:13:04
13/2/2006 15:13:24
MALWARE Task
Inactive
13/2/2006 14:34:33
13/2/2006 15:09:53
13/2/2006 15:10:22
MALWARE Task
Inactive
13/2/2006 14:18:49
13/2/2006 14:34:12
13/2/2006 14:34:37
BOGUS Task
Inactive
3/2/2006 15:34:52
3/2/2006 15:36:04
3/2/2006 15:36:34
MALWARE Task
Inactive
3/2/2006 15:31:53
3/2/2006 15:35:58
3/2/2006 15:36:27
BOGUS Task
Inactive
1/2/2006 11:40:04
1/2/2006 11:51:07
1/2/2006 11:51:15
MALWARE Task
Inactive
25/1/2006 13:32:47
1/2/2006 11:51:16
1/2/2006 11:51:24

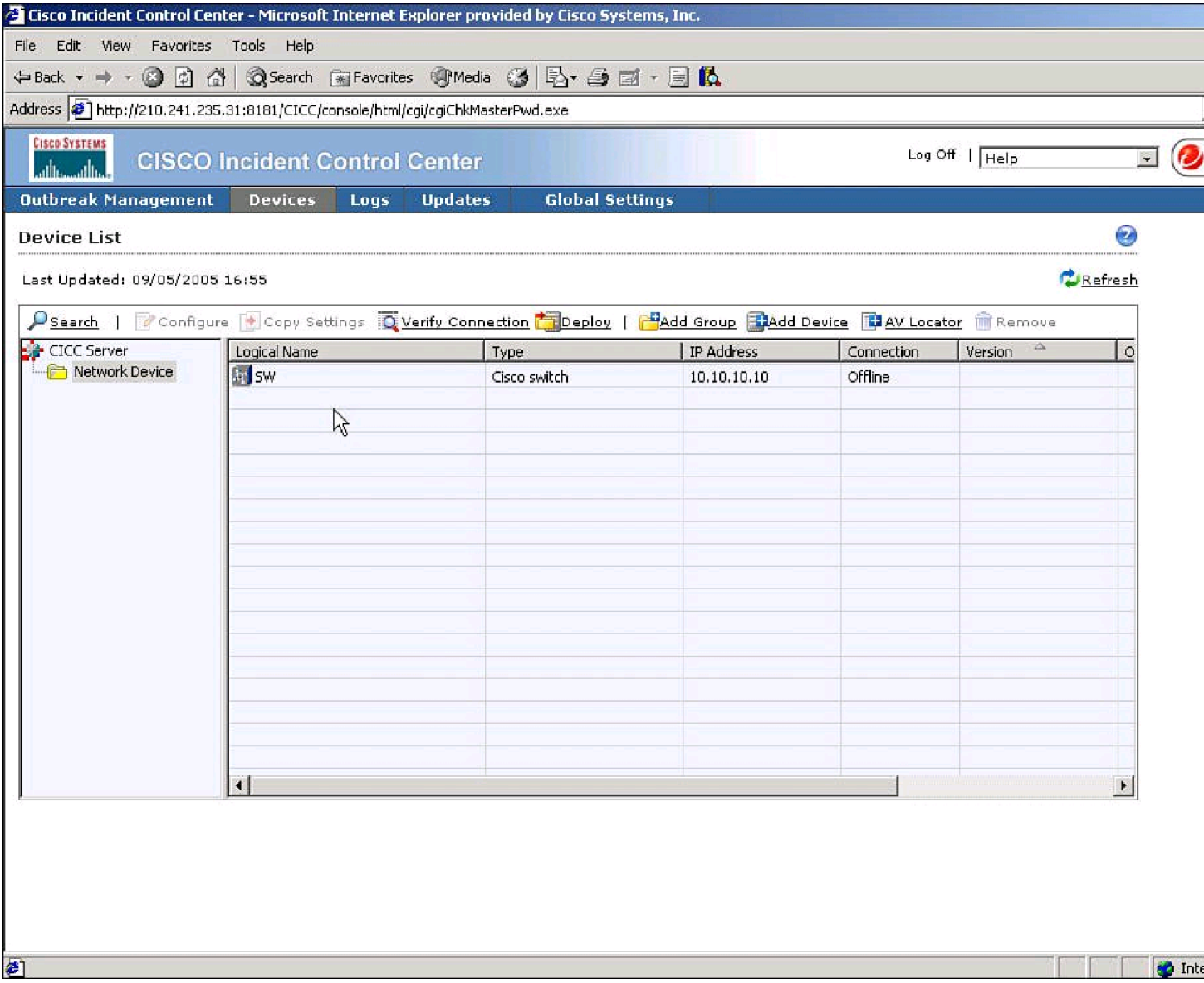

Cisco Systems
Cisco Incident Control Server
Outbreak Management
Devices
Logs
Updates
Global Settings
Outbreak Global Settings > OPACL Settings
Specify Outbreak Management Task Mode:
OPACL Mode
Mode:
Blocking mode
Logging mode
Save

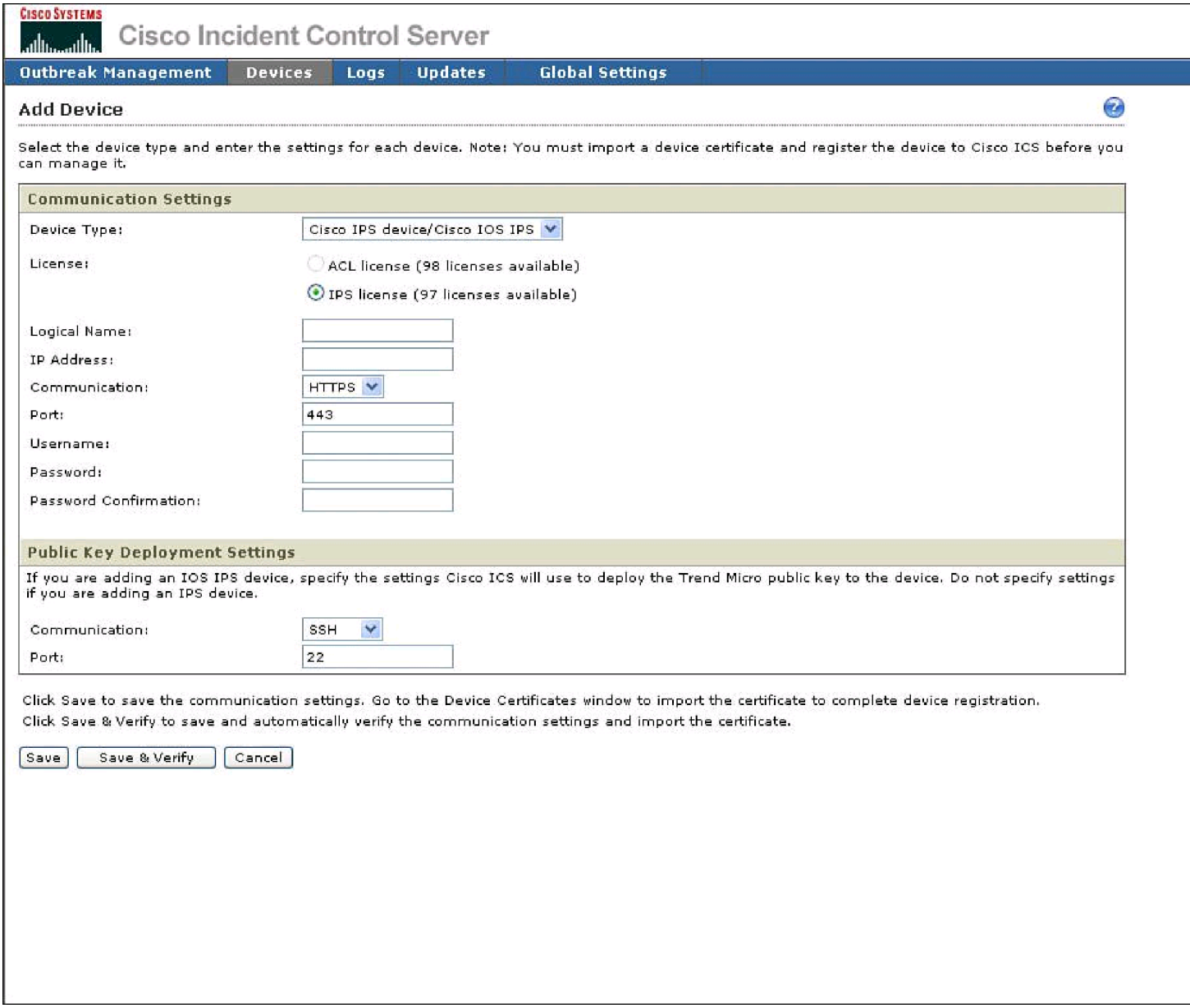

Cisco Systems
Cisco Incident Control Server
Outbreak Management
Devices
Logs
Updates
Global Settings
Outbreak Global Settings > Exception List
Specify which ports to exclude from all OPACL blocking settings.
Commonly Used Ports
[TCP Port:4343] Cisco ICS Management Console
[TCP Port:21] File Transfer Protocol (FTP)
[TCP Port:22] SSH
[TCP Port:23] Telnet
[TCP Port:25] Send Email Transfer Protocol (SMTP)
[TCP Port:80] Web (HTTP)
[TCP Port:443] Secure Web (HTTPS)
[UDP Port:514] SysLog
[TCP Port:1503, 1720] NetMeeting
[TCP Port:5631, UDP Port:5632] pcANYWHERE
Specified Port Range
TCP port numbers:
For example: 192; 234-255
UDP port numbers:
For example: 192; 234-255
ICMP
Internet Control Message Protocol
Save

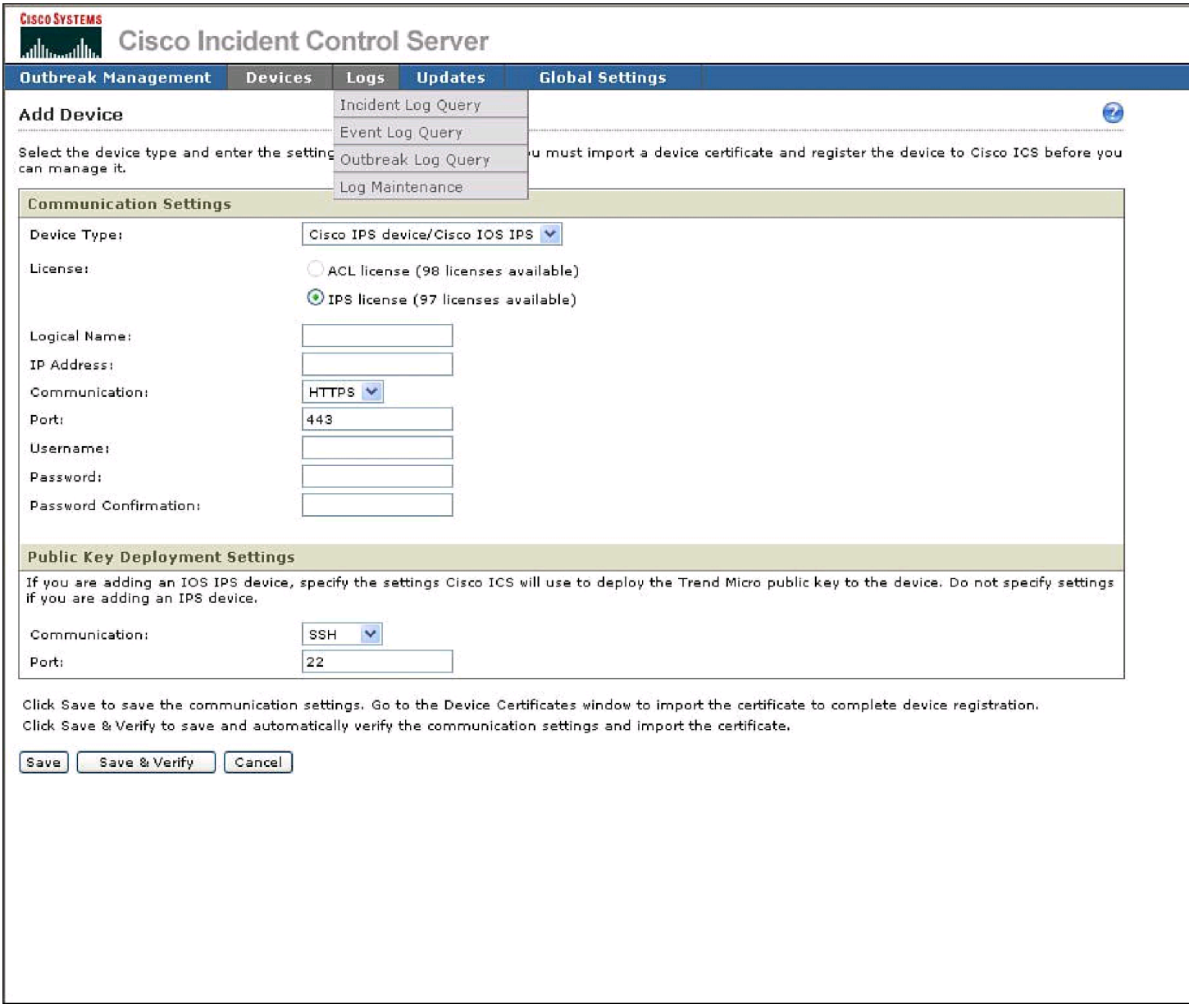

Cisco Systems
Cisco Incident Control Server
Outbreak Management
Devices
Logs
Updates
Global Settings
Outbreak Global Settings > Report Settings
Report Settings
Automatically generate reports for all outbreak management tasks
Generate the report every: 1 days
Save

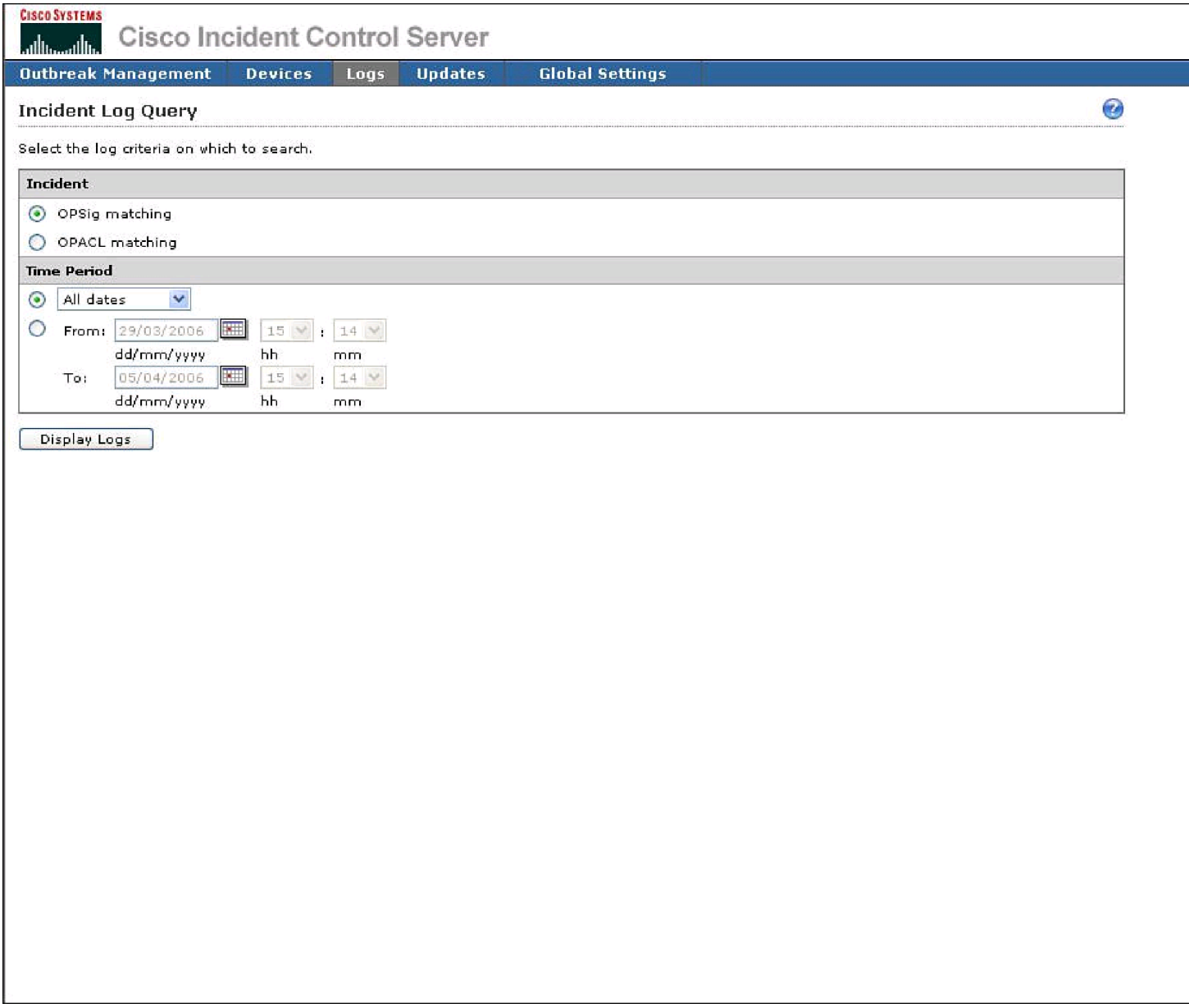

Cisco Systems
Cisco Incident Control Server
Outbreak Management
Devices
Logs
Updates
Global Settings
Outbreak Global Settings > Monitored Network
Specify hosts to add to a watch list
Add
Delete
IP Address / IP Range
Subnet Mask


Cisco Systems
Cisco Incident Control Server
Outbreak Management
Devices
Logs
Updates
Global Settings
Device List
Add Device
Device List
Last Updated: 05/04/2006 15:09
Refresh
Search
Configure
Copy Settings
Verify Connection
Deploy
Add Group
Add Device
AV Locator
Remove
Cisco ICS
Network Device
Logical Name
Type
Network Device
Folder


Cisco Incident Control Center - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://210.241.235.31:8181/CICC/console/html/cgi/cgiChkMasterPwd.exe
CISCO Incident Control Center
Log Off | Help
Outbreak Management Devices Logs Updates Global Settings
Device List
Last Updated: 09/05/2005 16:55
Refresh
Search | Configure Copy Settings Verify Connection Deploy | Add Group Add Device AV Locator Remove
CICC Server
Network Device
Logical Name Type IP Address Connection Version
SW Cisco switch 10.10.10.10 Offline


Cisco Systems
Cisco Incident Control Server
Outbreak Management
Devices
Logs
Updates
Global Settings
Add Device
Select the device type and enter the settings for each device. Note: You must import a device certificate and register the device to Cisco ICS before you can manage it.
Communication Settings
Device Type:
Cisco IPS device/Cisco IOS IPS
License:
ACL license (98 licenses available)
IPS license (97 licenses available)
Logical Name:
IP Address:
Communication:
HTTPS
Port:
443
Username:
Password:
Password Confirmation:
Public Key Deployment Settings
If you are adding an IOS IPS device, specify the settings Cisco ICS will use to deploy the Trend Micro public key to the device. Do not specify settings if you are adding an IPS device.
Communication:
SSH
Port:
22
Click Save to save the communication settings. Go to the Device Certificates window to import the certificate to complete device registration.
Click Save & Verify to save and automatically verify the communication settings and import the certificate.
Save
Save & Verify
Cancel


Cisco Systems
Cisco Incident Control Server
Outbreak Management
Devices
Logs
Updates
Global Settings
Incident Log Query
Event Log Query
Outbreak Log Query
Log Maintenance
Add Device
Select the device type and enter the setting
u must import a device certificate and register the device to Cisco ICS before you can manage it.
Communication Settings
Device Type:
Cisco IPS device/Cisco IOS IPS
License:
ACL license (98 licenses available)
IPS license (97 licenses available)
Logical Name:
IP Address:
Communication:
HTTPS
Port:
443
Username:
Password:
Password Confirmation:
Public Key Deployment Settings
If you are adding an IOS IPS device, specify the settings Cisco ICS will use to deploy the Trend Micro public key to the device. Do not specify settings if you are adding an IPS device.
Communication:
SSH
Port:
22
Click Save to save the communication settings. Go to the Device Certificates window to import the certificate to complete device registration.
Click Save & Verify to save and automatically verify the communication settings and import the certificate.
Save
Save & Verify
Cancel


Cisco Systems
Cisco Incident Control Server
Outbreak Management
Devices
Logs
Updates
Global Settings
Incident Log Query
Select the log criteria on which to search.
Incident
OPSig matching
OPACL matching
Time Period
All dates
From:
29/03/2006
dd/mm/yyyy
15
hh
14
mm
To:
05/04/2006
dd/mm/yyyy
15
hh
14
mm
Display Logs

Cisco Incident Control Server

Outbreak Management | Devices | Logs | Updates | Global Settings

Event Log Query > All Events

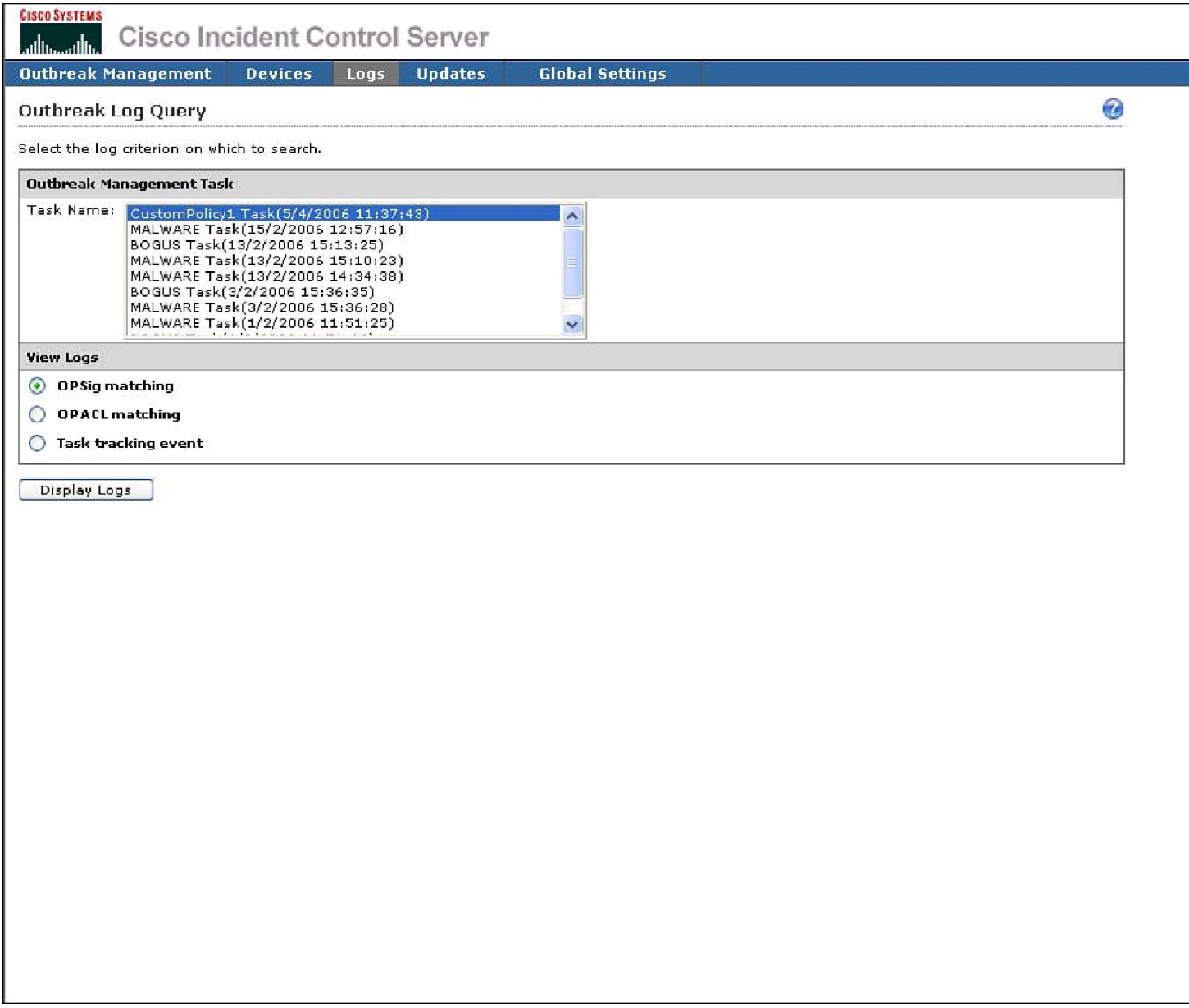
Results from 15/12/2005 12:23:50 **to** 5/4/2006 12:08:25

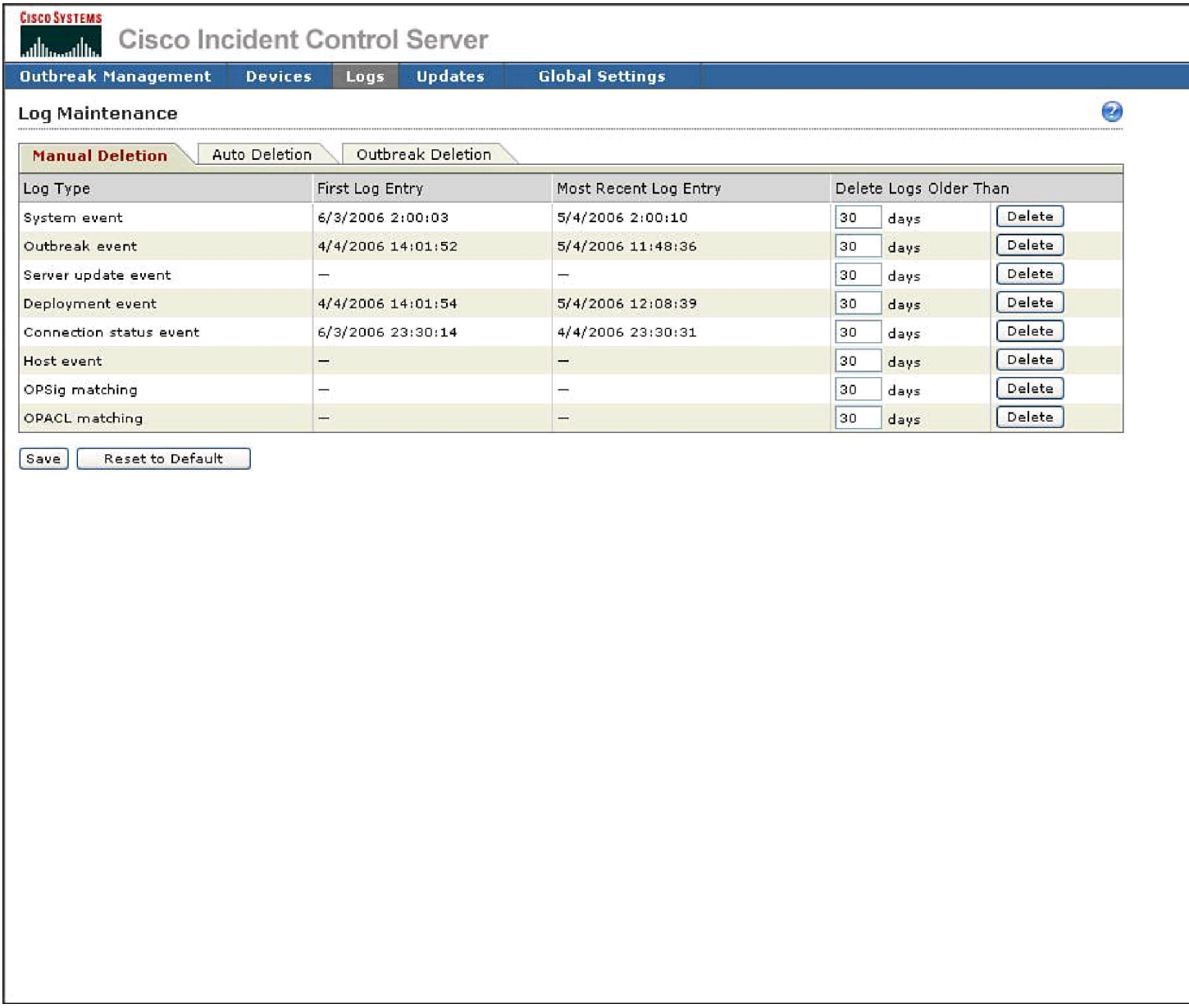
Export to CSV

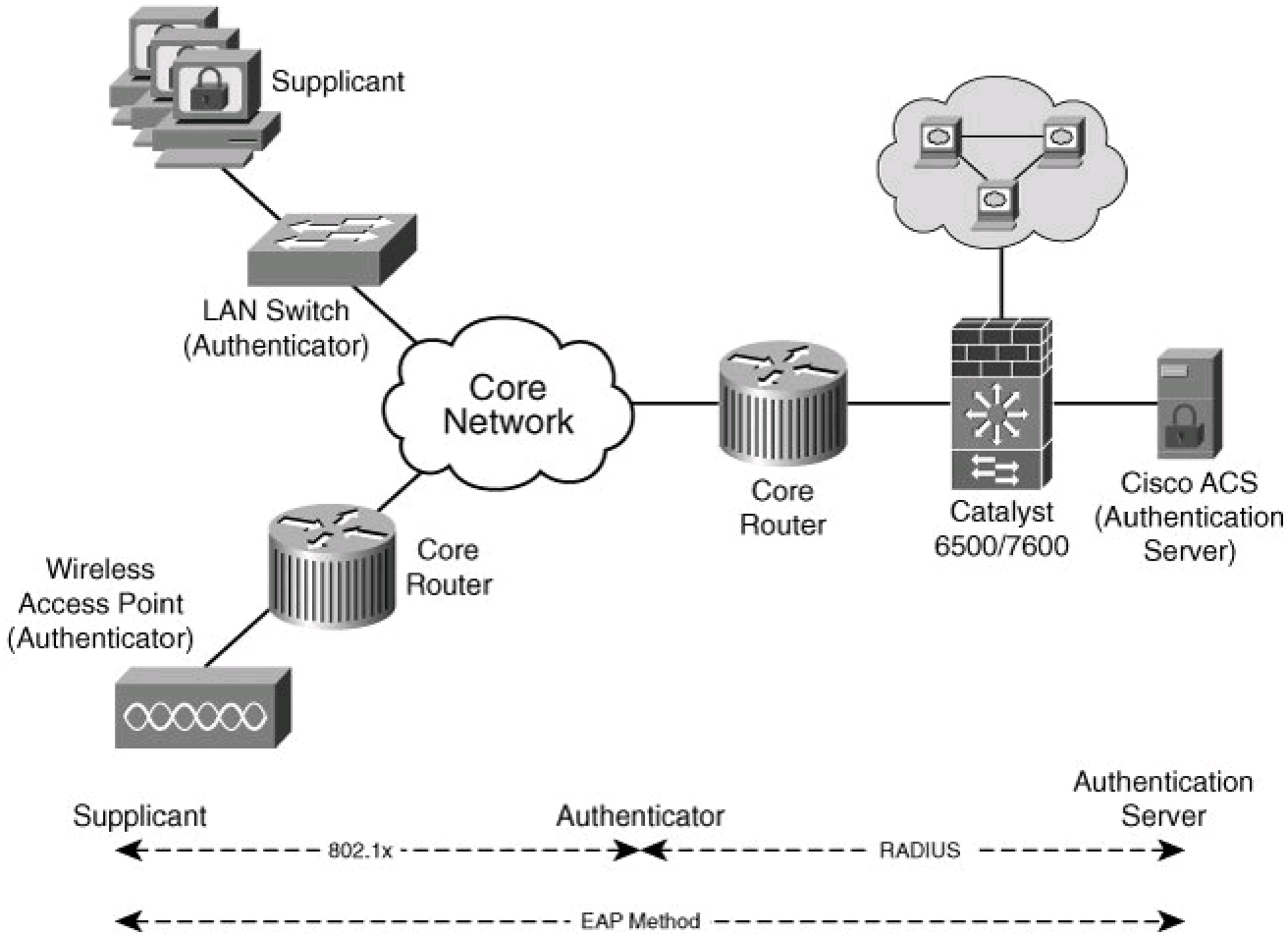
total : 423 logs | Page: 1 of 43 | 10 logs per page

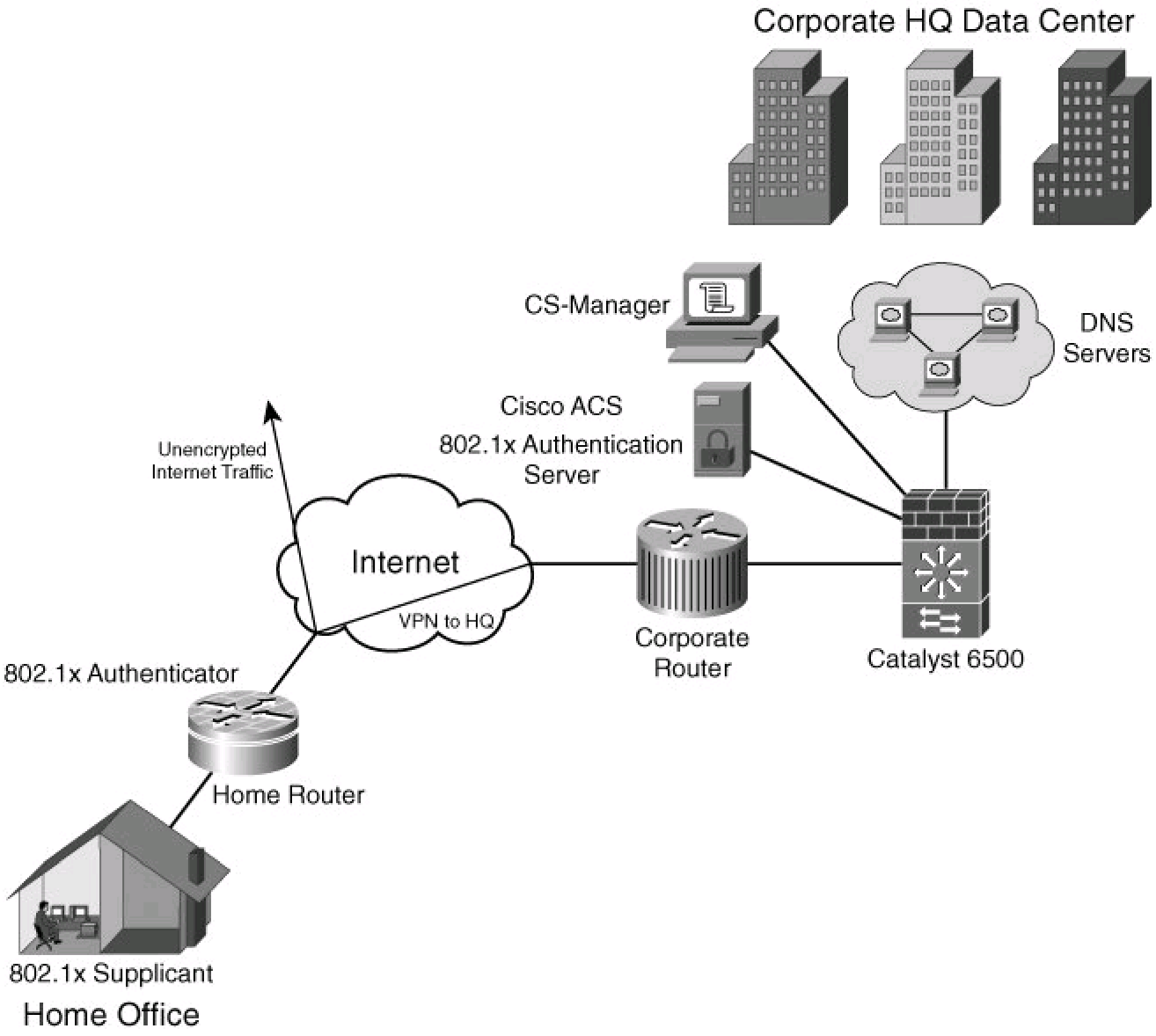
Date/Time	Severity	Event Type	Task Name	Event Details	Account	Device Logical Name	Device IP	Result
5/4/2006 11:48:46	Info	Deployment	—	Deployed OPACL update to an individual device for a new or modified task.	System initiated	HEADEND	10.10.20.10	Successful
5/4/2006 11:48:37	Notice	Deployment	—	Deployed OPACL update to an individual device for a new or modified task.	System initiated	SWITCH	192.168.201.40	Device receiving deployment is offline.
5/4/2006 11:48:37	Notice	Deployment	—	Deployed OPACL update to an individual device for a new or modified task.	System initiated	OPS1751	192.168.201.40	Device receiving deployment is offline.
5/4/2006 11:48:37	Notice	Deployment	—	Deployed OPACL update to an individual device for a new or modified task.	System initiated	BRANCH	192.168.201.40	Device receiving deployment is offline.
5/4/2006 11:48:36	Notice	Outbreak	WORM_MYTOB.MX Task	Outbreak Management Task started. OPACL will be deployed.	cics	—	—	Successful
5/4/2006 11:37:42	Notice	Outbreak	CustomPolicy1 Task	Report generated.	System initiated	—	—	Successful
5/4/2006 11:37:32	Info	Deployment	—	Deployed OPACL update to an individual device for a new or modified task.	System initiated	HEADEND	10.10.20.10	Successful
5/4/2006 11:37:26	Info	Deployment	—	Deployed OPACL update to an individual device for a new or modified task.	System initiated	SENSOR	10.10.20.20	Successful
5/4/2006 11:37:25	Notice	Deployment	—	Deployed OPACL update to an individual device for a new or modified task.	System initiated	SWITCH	192.168.201.40	Device receiving deployment is offline.
5/4/2006 11:37:25	Notice	Deployment	—	Deployed OPACL update to an individual device for a new or modified task.	System initiated	OPS1751	192.168.201.40	Device receiving deployment is offline.

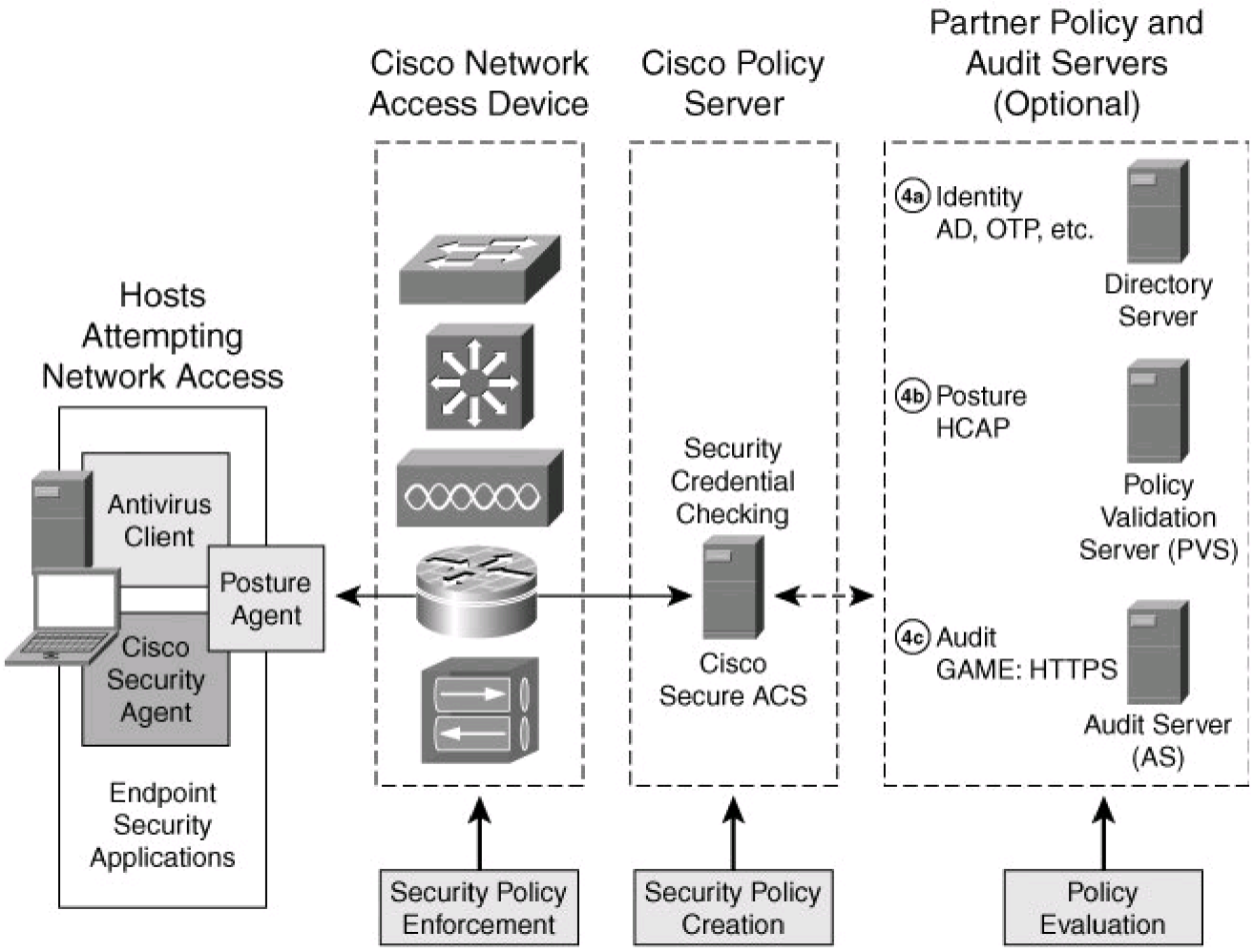
< Back

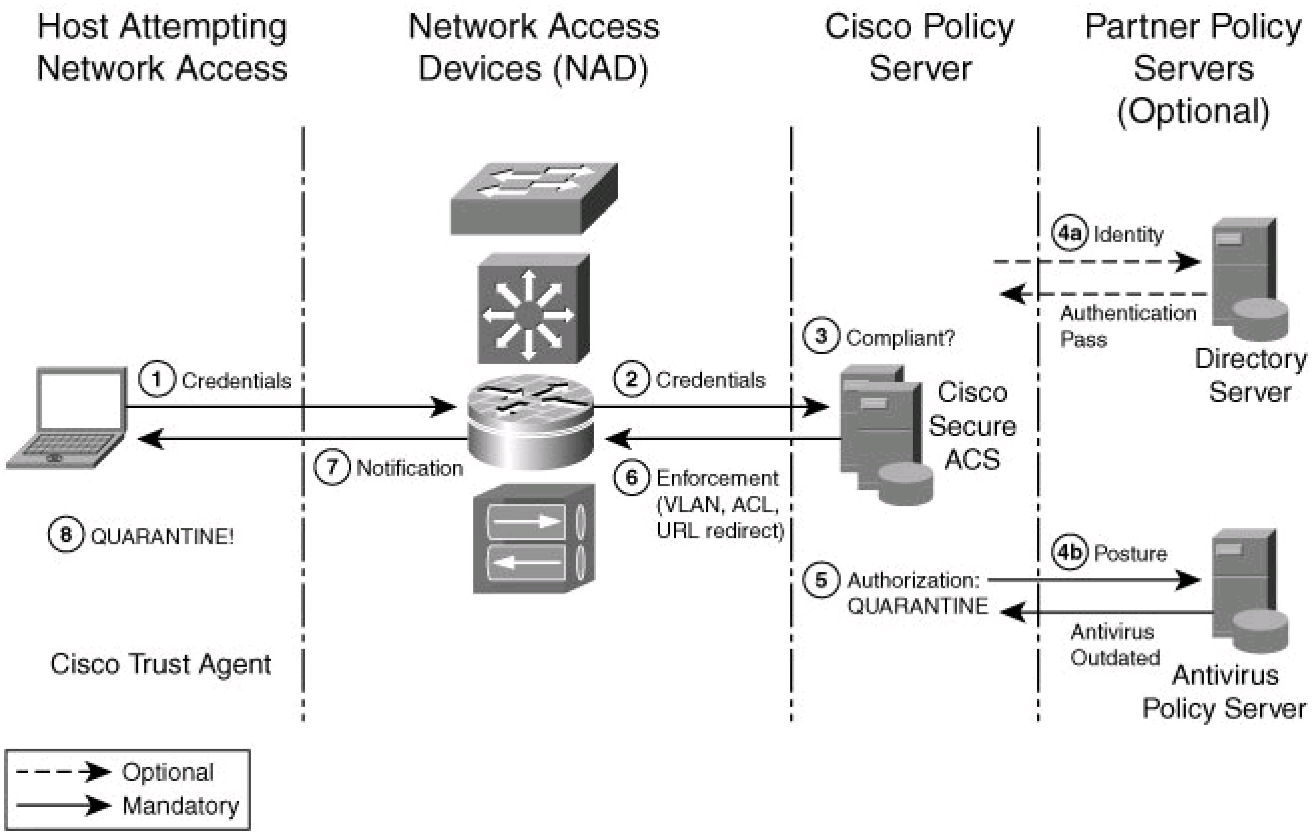

Cisco Systems
Cisco Incident Control Server
Outbreak Management
Devices
Logs
Updates
Global Settings
Outbreak Log Query
Select the log criterion on which to search.
Outbreak Management Task
Task Name:
CustomPolicy1 Task(5/4/2006 11:37:43)
MALWARE Task(15/2/2006 12:57:16)
BOGUS Task(13/2/2006 15:13:25)
MALWARE Task(13/2/2006 15:10:23)
MALWARE Task(13/2/2006 14:34:38)
BOGUS Task(3/2/2006 15:36:35)
MALWARE Task(3/2/2006 15:36:28)
MALWARE Task(1/2/2006 11:51:25)
View Logs
OPSig matching
OPACL matching
Task tracking event
Display Logs

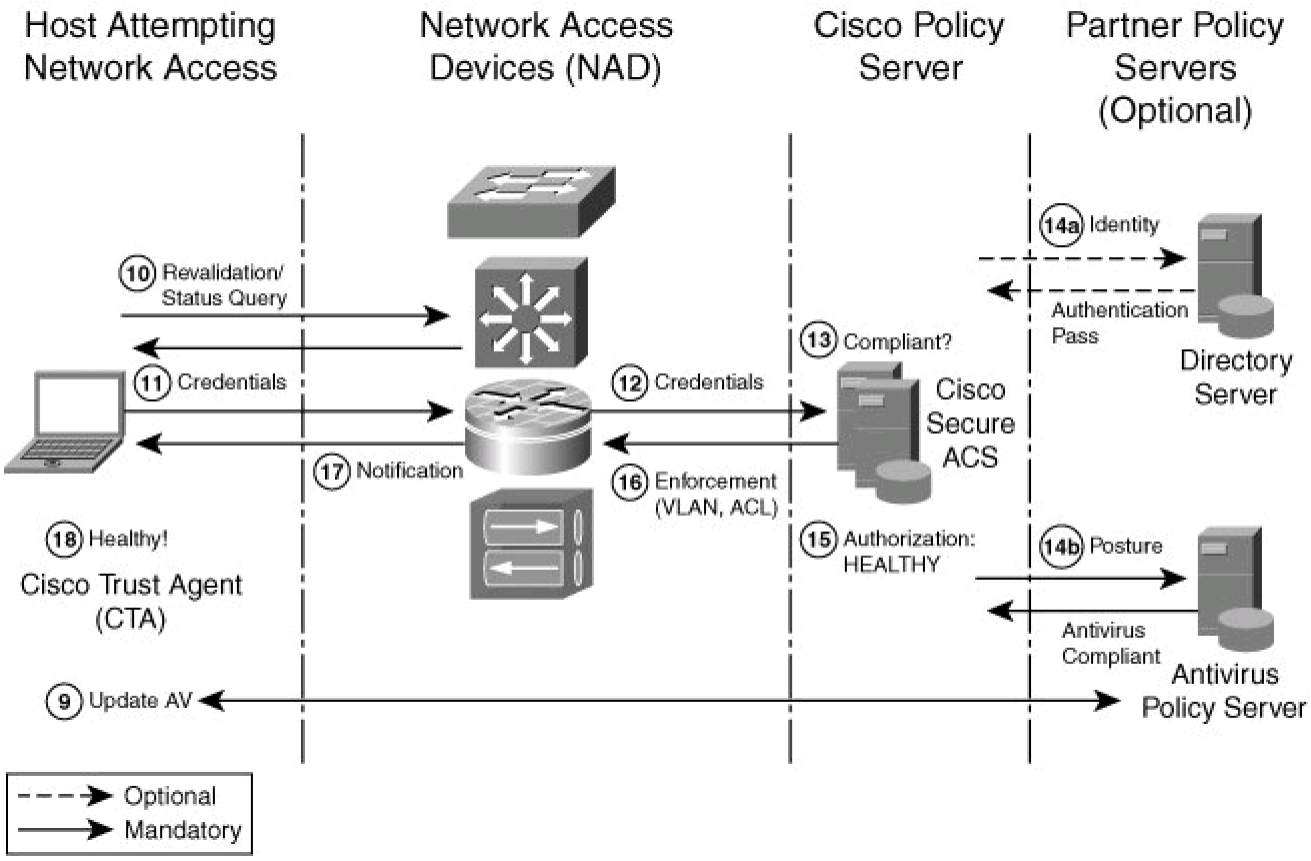

Cisco Systems
Cisco Incident Control Server
Outbreak Management
Devices
Logs
Updates
Global Settings
Log Maintenance
Manual Deletion
Auto Deletion
Outbreak Deletion
Log Type
First Log Entry
Most Recent Log Entry
Delete Logs Older Than
System event
6/3/2006 2:00:03
5/4/2006 2:00:10
30 days
Delete
Outbreak event
4/4/2006 14:01:52
5/4/2006 11:48:36
30 days
Delete
Server update event
–
–
30 days
Delete
Deployment event
4/4/2006 14:01:54
5/4/2006 12:08:39
30 days
Delete
Connection status event
6/3/2006 23:30:14
4/4/2006 23:30:31
30 days
Delete
Host event
–
–
30 days
Delete
OPSig matching
–
–
30 days
Delete
OPACL matching
–
–
30 days
Delete
Save
Reset to Default

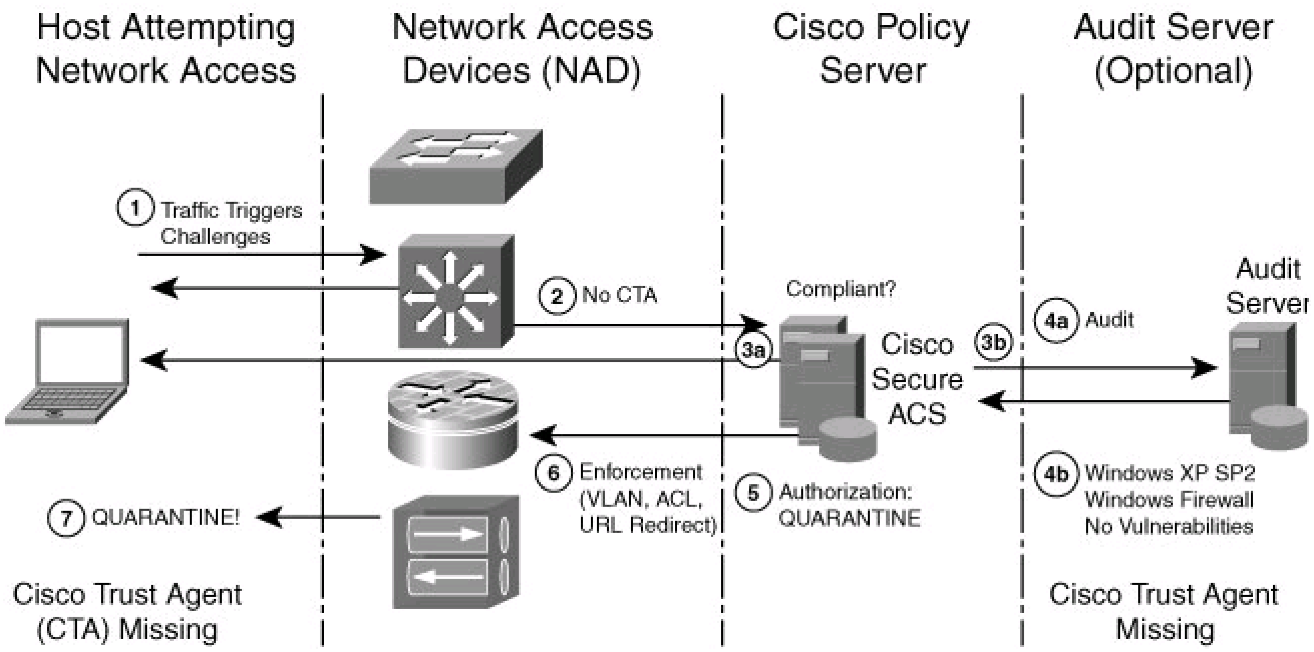

Supplicant
LAN Switch
(Authenticator)
Core
Network
Core
Router
Wireless
Access Point
(Authenticator)
Core
Router
Catalyst
6500/7600
Cisco ACS
(Authentication
Server)
Supplicant
Authenticator
Authentication
Server
802.1x
RADIUS
EAP Method

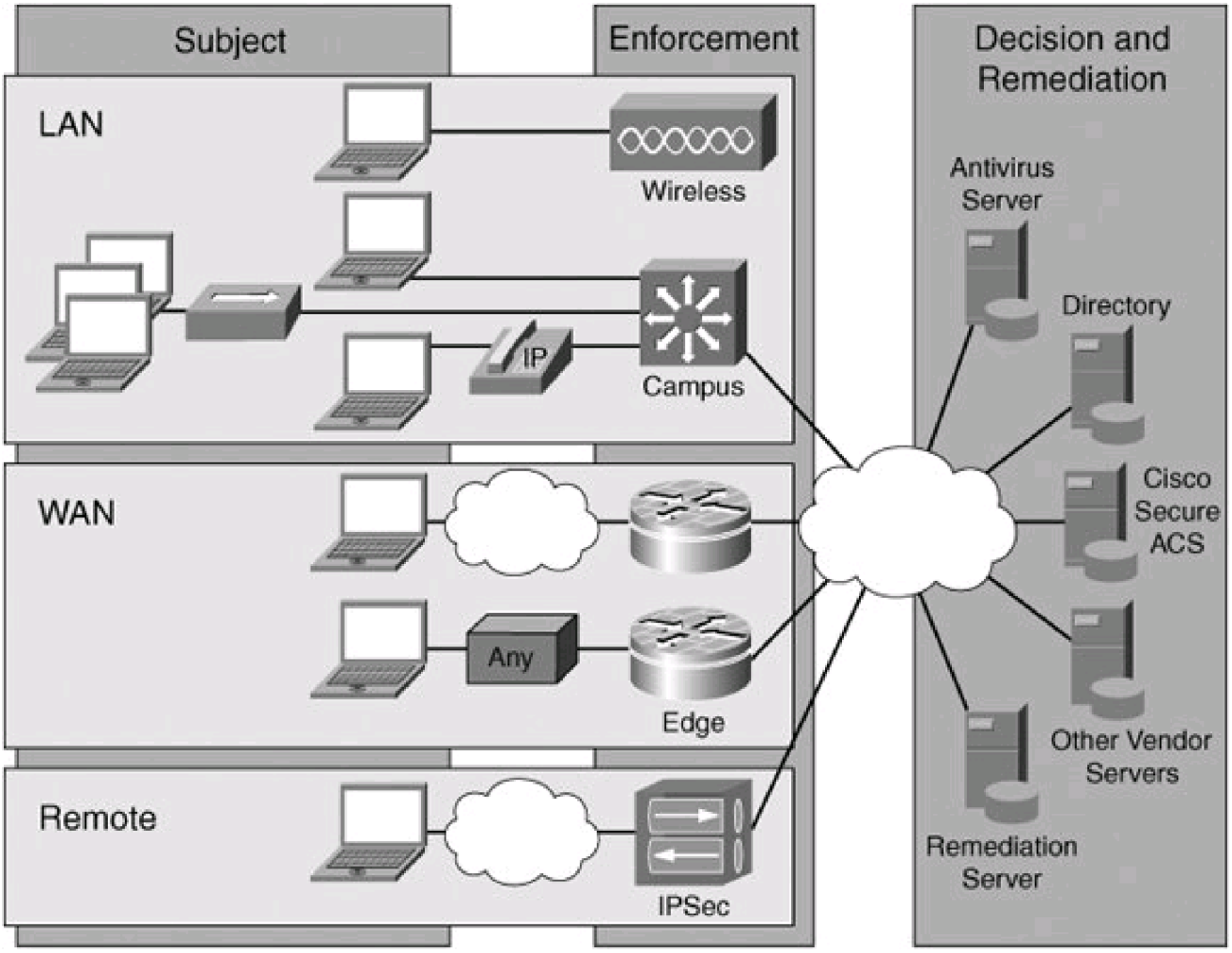

Corporate HQ Data Center
CS-Manager
DNS
Servers
Cisco ACS
802.1x Authentication
Server
Unencrypted
Internet Traffic
Internet
VPN to HQ
Corporate
Router
Catalyst 6500
802.1x Authenticator
Home Router
802.1x Supplicant
Home Office


Cisco Network Access Device
Cisco Policy Server
Partner Policy and Audit Servers (Optional)
Hosts Attempting Network Access
Antivirus Client
Posture Agent
Cisco Security Agent
Endpoint Security Applications
Security Credential Checking
Cisco Secure ACS
4a Identity
AD, OTP, etc.
Directory Server
4b Posture
HCAP
Policy Validation Server (PVS)
4c Audit
GAME: HTTPS
Audit Server (AS)
Security Policy Enforcement
Security Policy Creation
Policy Evaluation


Host Attempting Network Access
Network Access Devices (NAD)
Cisco Policy Server
Partner Policy Servers (Optional)
4a Identity
Authentication Pass
Directory Server
3 Compliant?
1 Credentials
2 Credentials
Cisco Secure ACS
7 Notification
6 Enforcement (VLAN, ACL, URL redirect)
8 QUARANTINE!
4b Posture
5 Authorization: QUARANTINE
Antivirus Outdated
Antivirus Policy Server
Cisco Trust Agent
Optional
Mandatory


Host Attempting Network Access
Network Access Devices (NAD)
Cisco Policy Server
Partner Policy Servers (Optional)
10 Revalidation/ Status Query
11 Credentials
12 Credentials
13 Compliant?
14a Identity
Authentication Pass
Directory Server
Cisco Secure ACS
17 Notification
16 Enforcement (VLAN, ACL)
18 Healthy!
Cisco Trust Agent (CTA)
15 Authorization: HEALTHY
14b Posture
Antivirus Compliant
Antivirus Policy Server
9 Update AV
Optional
Mandatory


Host Attempting Network Access
Network Access Devices (NAD)
Cisco Policy Server
Audit Server (Optional)
1 Traffic Triggers Challenges
2 No CTA
Compliant?
3a
Cisco Secure ACS
3b
4a Audit
Audit Server
4b Windows XP SP2
Windows Firewall
No Vulnerabilities
5 Authorization: QUARANTINE
6 Enforcement (VLAN, ACL, URL Redirect)
7 QUARANTINE!
Cisco Trust Agent (CTA) Missing
Cisco Trust Agent Missing


Subject
Enforcement
Decision and Remediation
LAN
Wireless
IP
Campus
WAN
Any
Edge
Remote
IPSec
Antivirus Server
Directory
Cisco Secure ACS
Other Vendor Servers
Remediation Server

Cisco Clean Access Man

Monitoring > Summary

Device Management
- CCA Servers
- Filters
- Roaming
- Clean Access

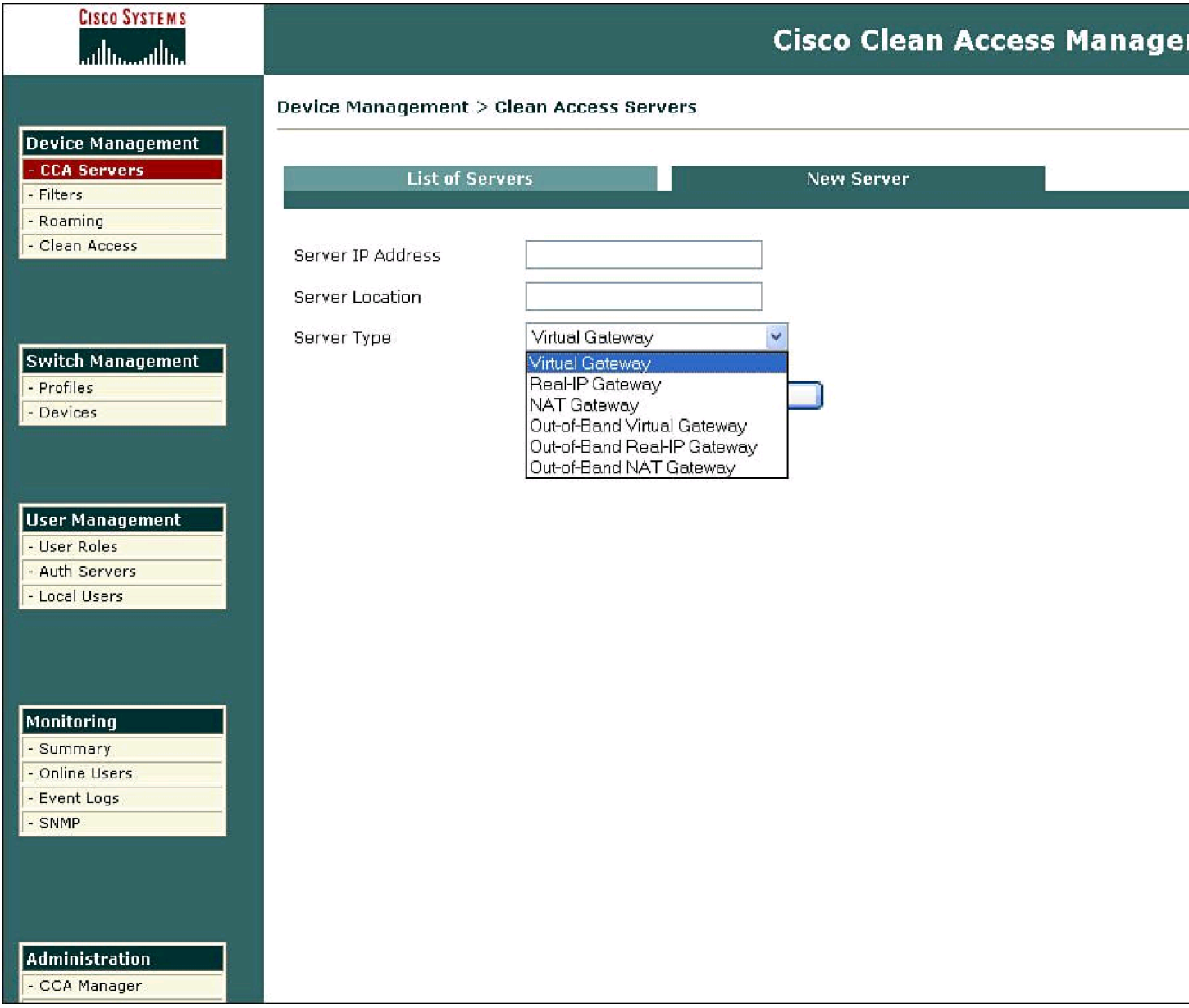
Switch Management
- Profiles
- Devices

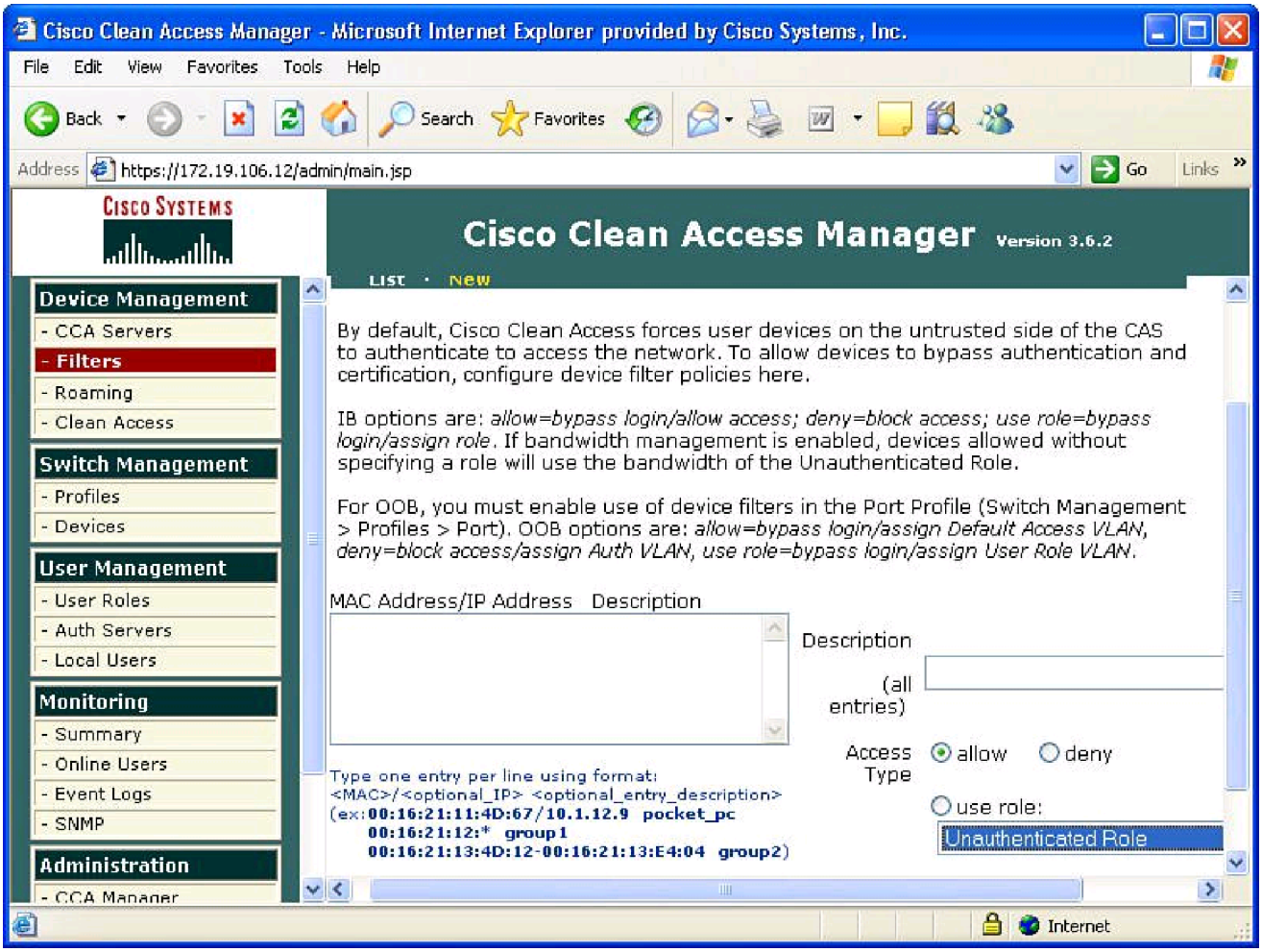
User Management
- User Roles
- Auth Servers
- Local Users

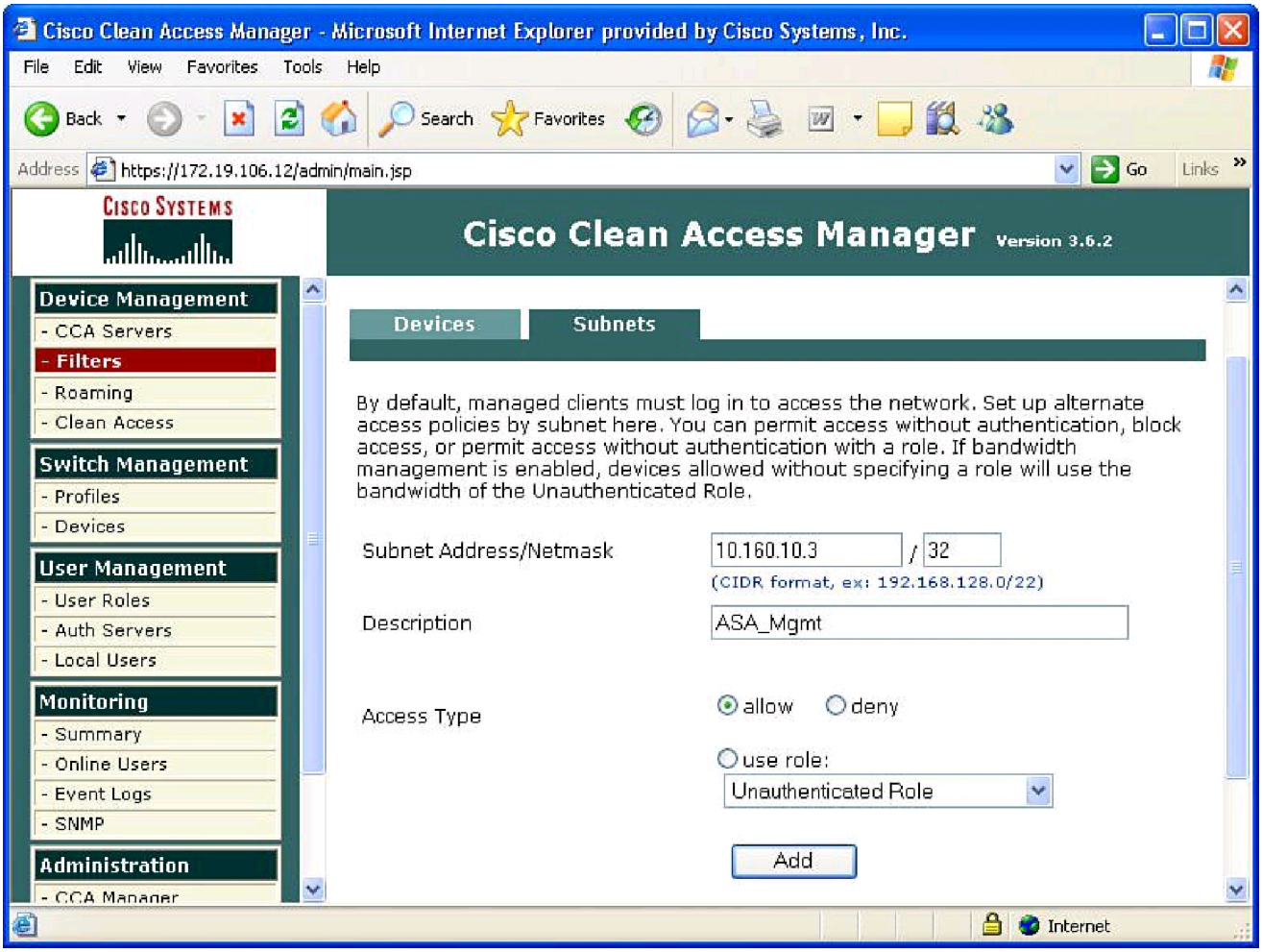
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP

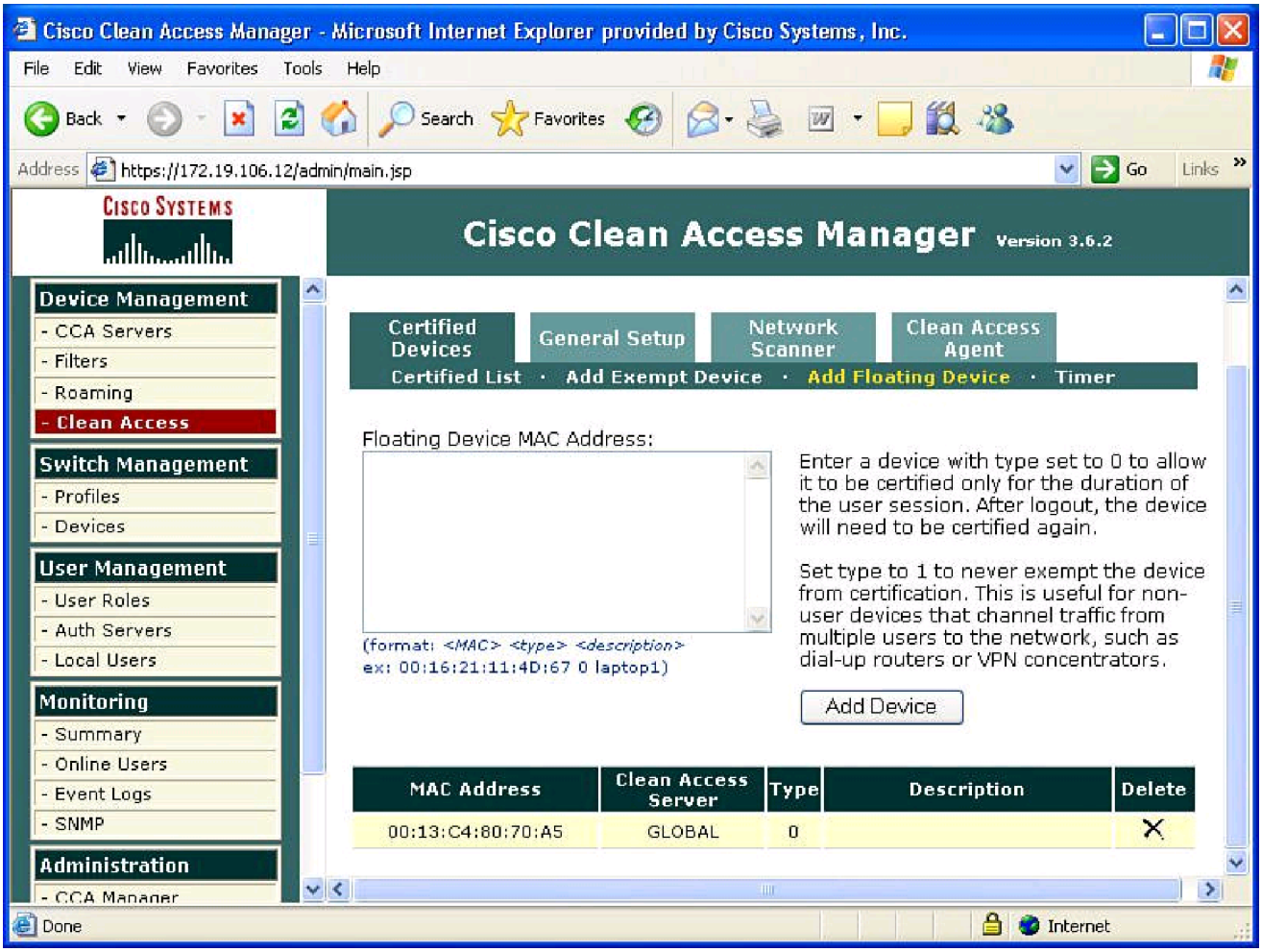
Administration

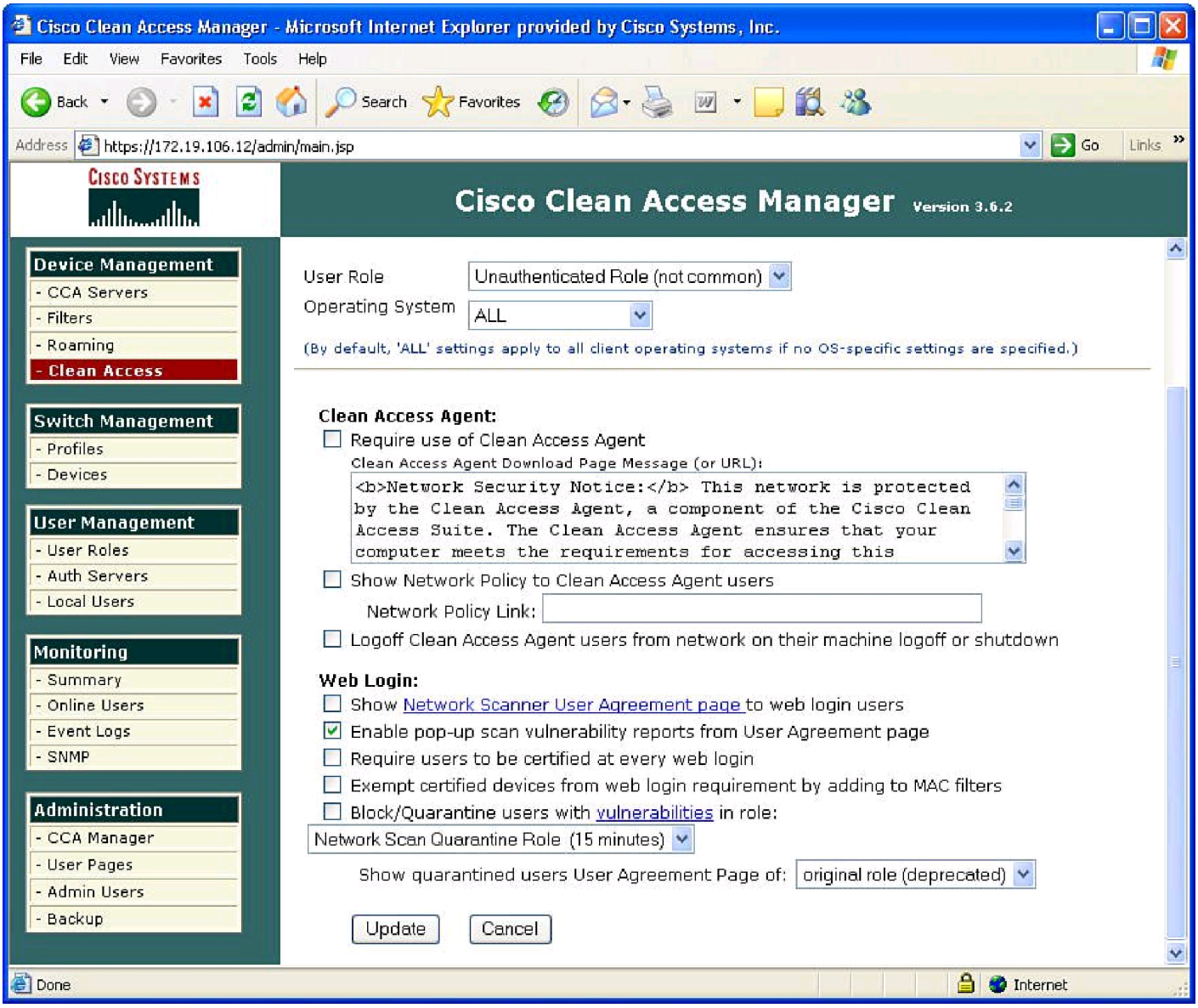
Current Clean Access Agent Version:	**3.6.1.0**	
Current Clean Access Agent Patch Version:	**3.6.2.0**	
Clean Access Servers configured:	**1**	
Global MAC addresses configured:	**0**	
Global subnets configured:	**0**	
Online users:	*(In-Band*	*/ Out-of-Band)*
Total:	**0**	**0**
Unique online users' names:	**0**	**0**
Unique online users' MAC addresses:	**0**	**0**
Online users in Unauthenticated Role:	**0**	**0**
Online users in Agent Quarantine Role:	**0**	**0**
Online users in Network Scan Quarantine Role:	**0**	**0**
Online users in Allow All:	**0**	**0**
Online users in Guest:	**0**	**0**
Online users in Consultant:	**0**	**0**
Online users in ScanTest:	**0**	**0**
Online users in TAC:	**0**	**0**
Online users in Dormitory Student:	**0**	**0**
Online users in printer:	**0**	**0**
Online users in Chicago_users:	**0**	**0**
Online users in Nowhere:	**0**	**0**
Online users in alok:	**0**	**0**
Online users in San_Jose_Users:	**0**	**0**

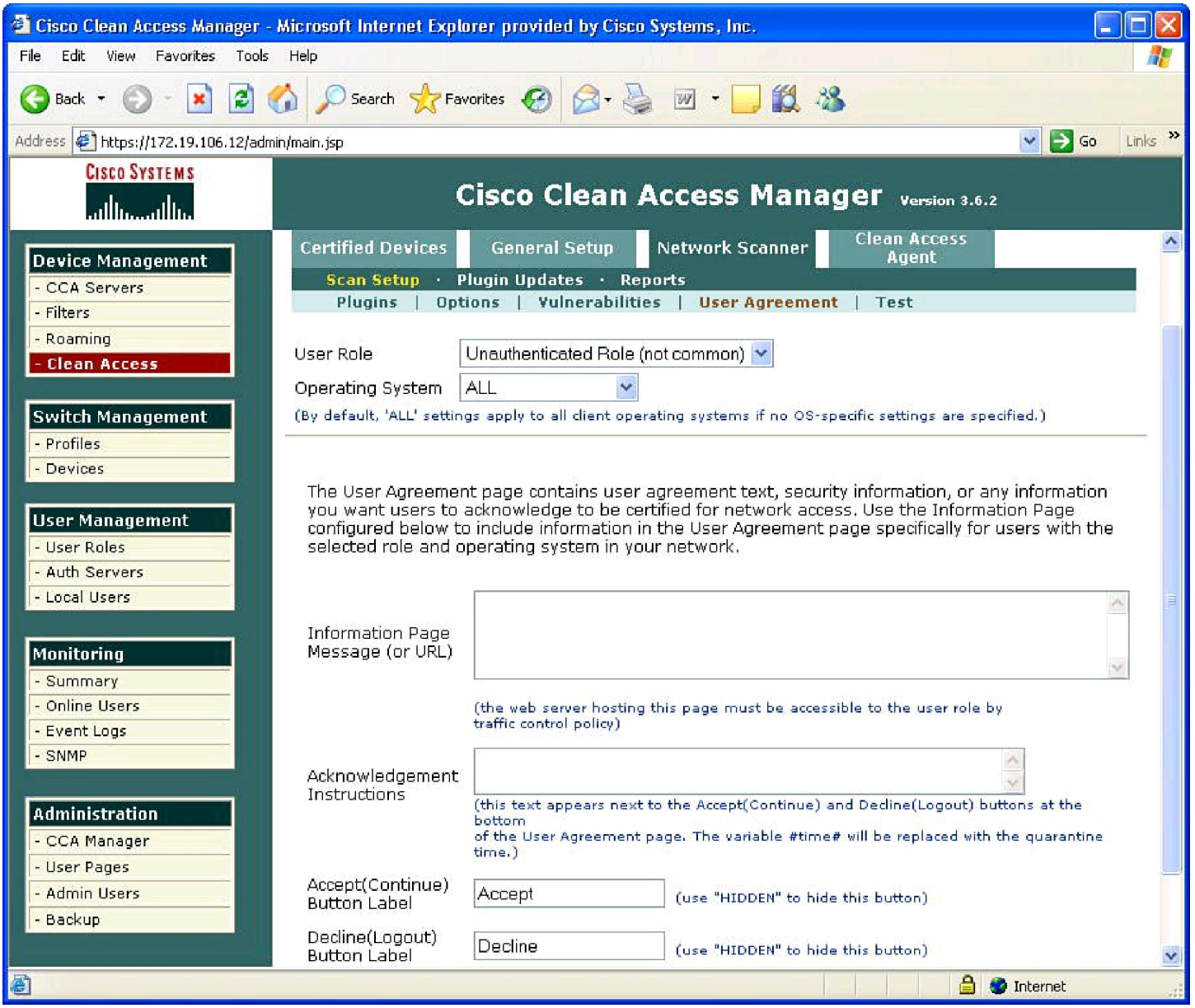

Cisco Systems
Cisco Clean Access Manager
Device Management > Clean Access Servers
Device Management
- CCA Servers
- Filters
- Roaming
- Clean Access
Switch Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
List of Servers
New Server
Server IP Address
Server Location
Server Type
Virtual Gateway
Virtual Gateway
Real-IP Gateway
NAT Gateway
Out-of-Band Virtual Gateway
Out-of-Band Real-IP Gateway
Out-of-Band NAT Gateway

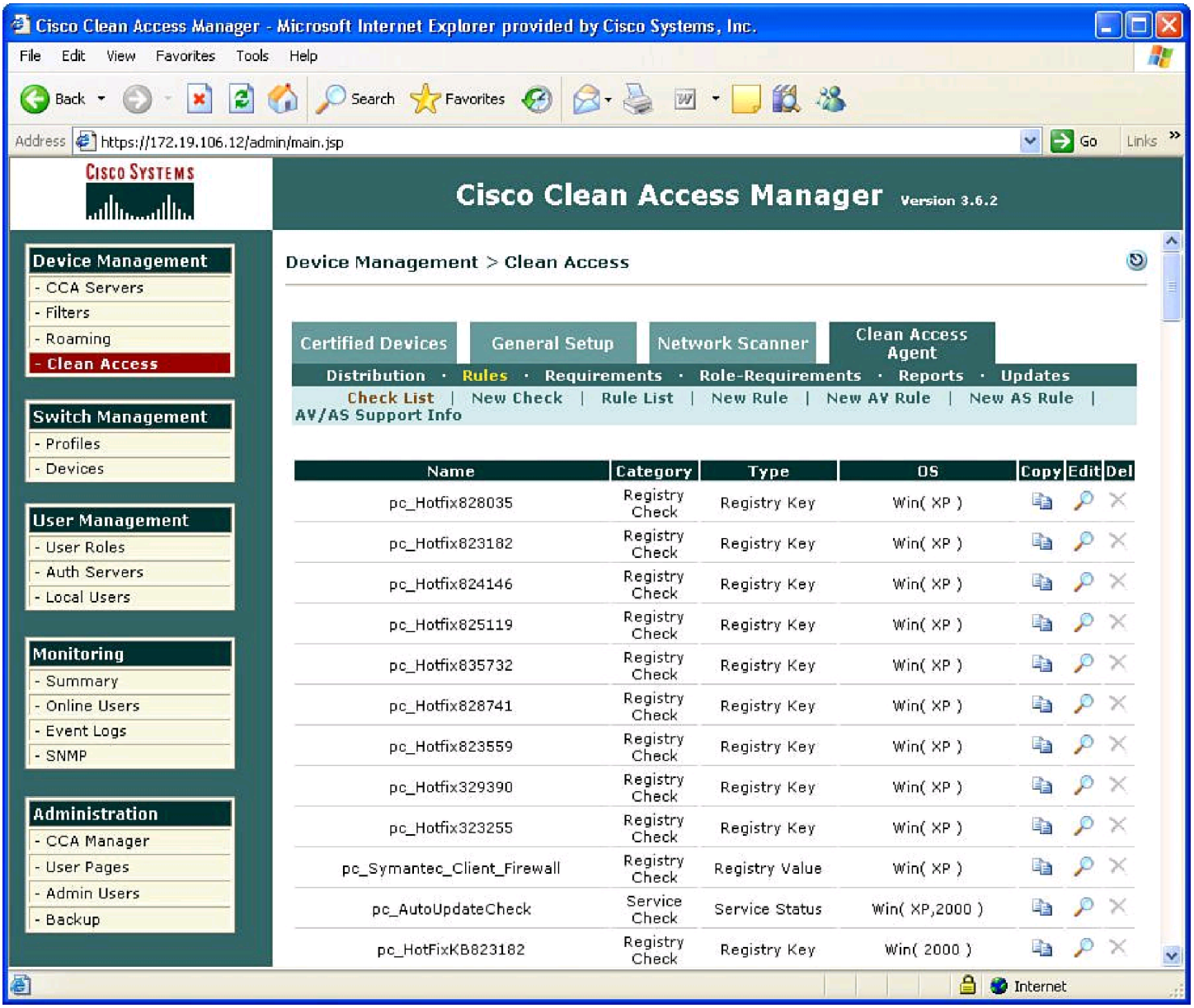

Cisco Clean Access Manager - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.19.106.12/admin/main.jsp
Go Links
Cisco Systems
Cisco Clean Access Manager Version 3.6.2
List · New
Device Management
- CCA Servers
- Filters
- Roaming
- Clean Access
Switch Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
By default, Cisco Clean Access forces user devices on the untrusted side of the CAS to authenticate to access the network. To allow devices to bypass authentication and certification, configure device filter policies here.
IB options are: allow=bypass login/allow access; deny=block access; use role=bypass login/assign role. If bandwidth management is enabled, devices allowed without specifying a role will use the bandwidth of the Unauthenticated Role.
For OOB, you must enable use of device filters in the Port Profile (Switch Management > Profiles > Port). OOB options are: allow=bypass login/assign Default Access VLAN, deny=block access/assign Auth VLAN, use role=bypass login/assign User Role VLAN.
MAC Address/IP Address Description
Type one entry per line using format:
<MAC>/<optional_IP> <optional_entry_description>
(ex:00:16:21:11:4D:67/10.1.12.9 pocket_pc
00:16:21:12:* group1
00:16:21:13:4D:12-00:16:21:13:E4:04 group2)
Description (all entries)
Access Type
allow
deny
use role:
Unauthenticated Role
Internet

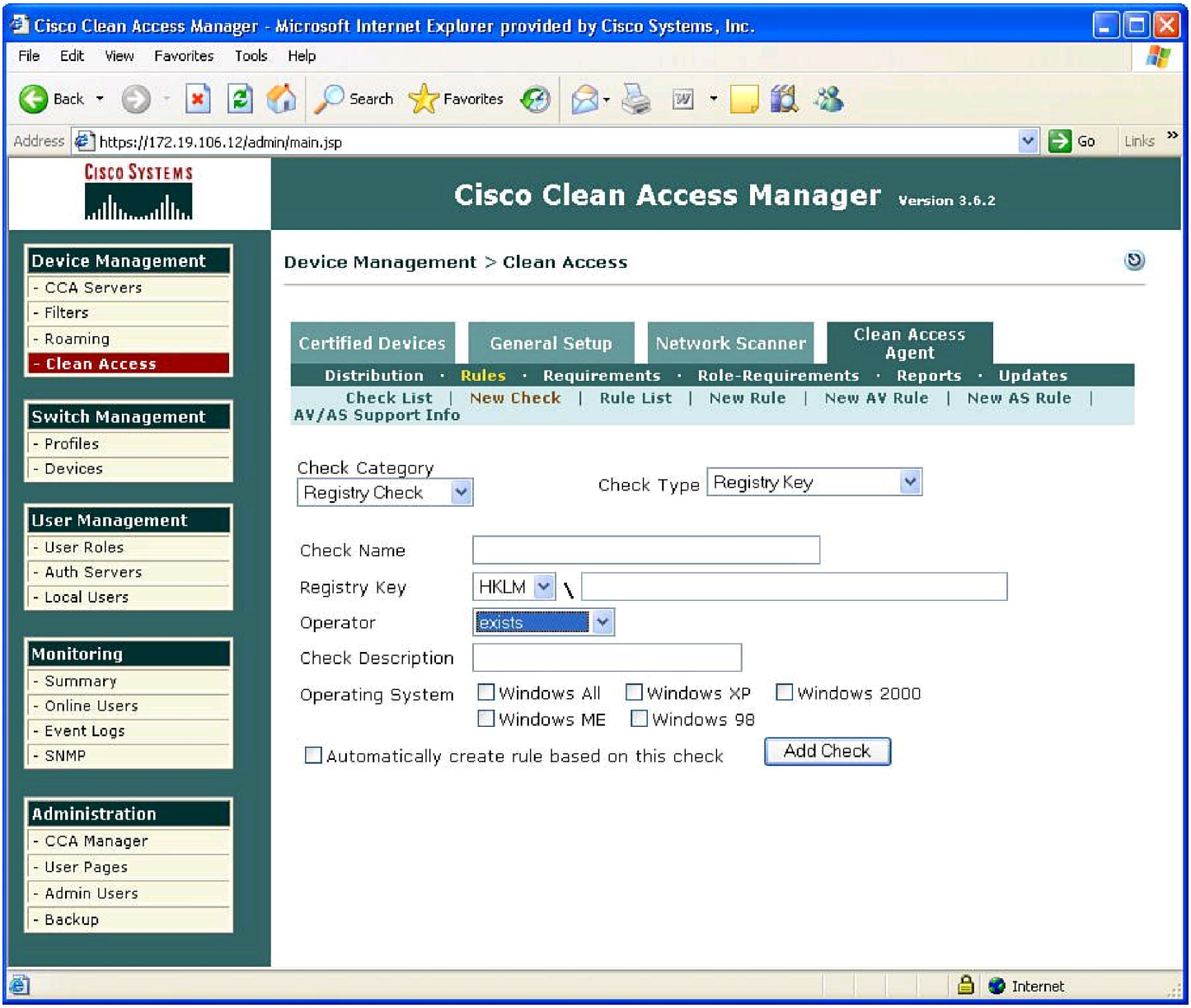

Cisco Clean Access Manager - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.19.106.12/admin/main.jsp
Go Links
Cisco Systems
Cisco Clean Access Manager Version 3.6.2
Device Management
- CCA Servers
- Filters
- Roaming
- Clean Access
Switch Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
Devices
Subnets
By default, managed clients must log in to access the network. Set up alternate access policies by subnet here. You can permit access without authentication, block access, or permit access without authentication with a role. If bandwidth management is enabled, devices allowed without specifying a role will use the bandwidth of the Unauthenticated Role.
Subnet Address/Netmask
10.160.10.3 / 32
(CIDR format, ex: 192.168.128.0/22)
Description
ASA_Mgmt
Access Type
allow
deny
use role:
Unauthenticated Role
Add
Internet

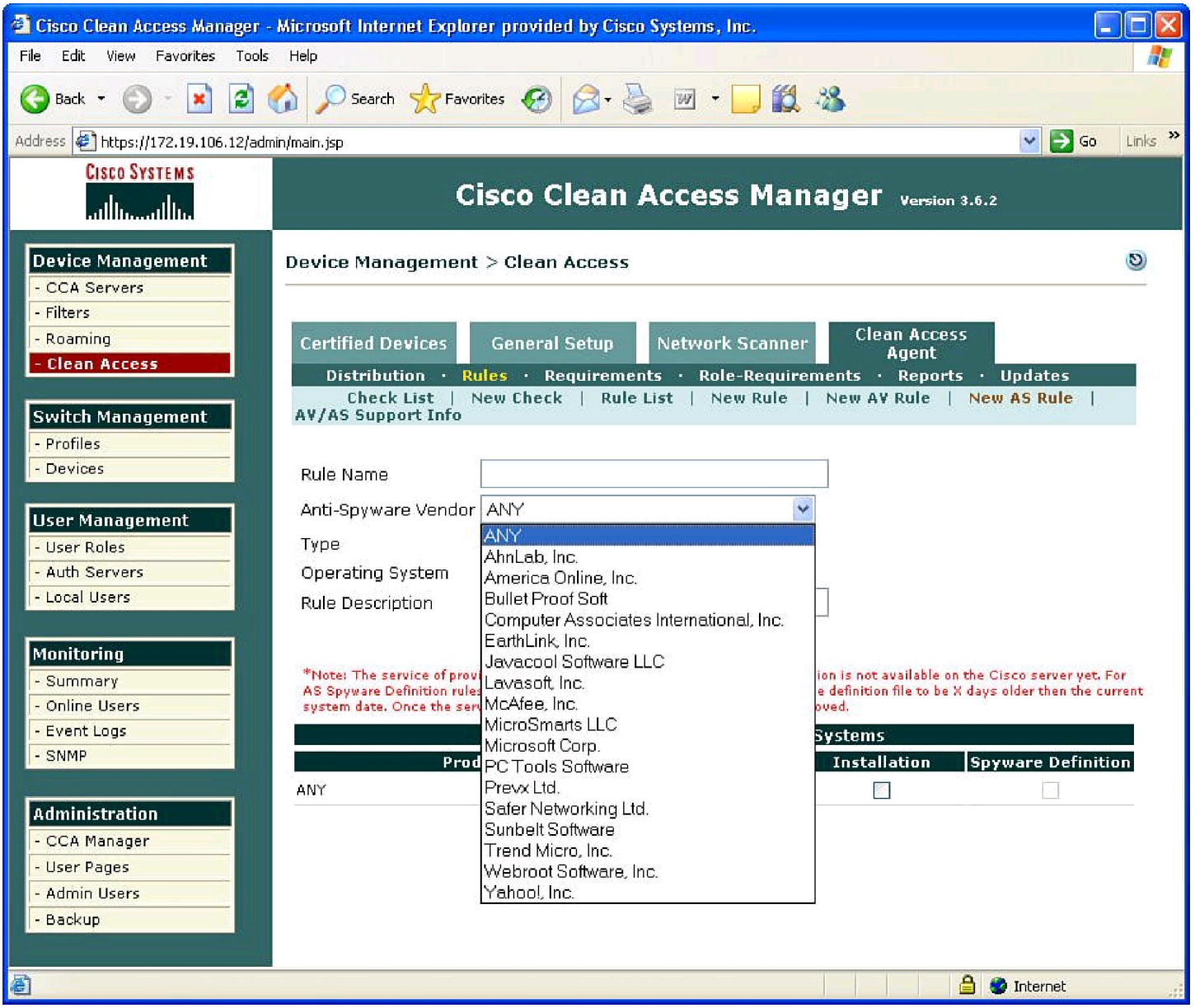

Cisco Clean Access Manager - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.19.106.12/admin/main.jsp
Go Links
Cisco Systems
Cisco Clean Access Manager Version 3.6.2
Device Management
- CCA Servers
- Filters
- Roaming
- Clean Access
Switch Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Certified List · Add Exempt Device · Add Floating Device · Timer
Floating Device MAC Address:
(format: <MAC> <type> <description>
ex: 00:16:21:11:4D:67 0 laptop1)
Enter a device with type set to 0 to allow it to be certified only for the duration of the user session. After logout, the device will need to be certified again.
Set type to 1 to never exempt the device from certification. This is useful for non-user devices that channel traffic from multiple users to the network, such as dial-up routers or VPN concentrators.
Add Device
MAC Address
Clean Access Server
Type
Description
Delete
00:13:C4:80:70:A5
GLOBAL
0
Done
Internet

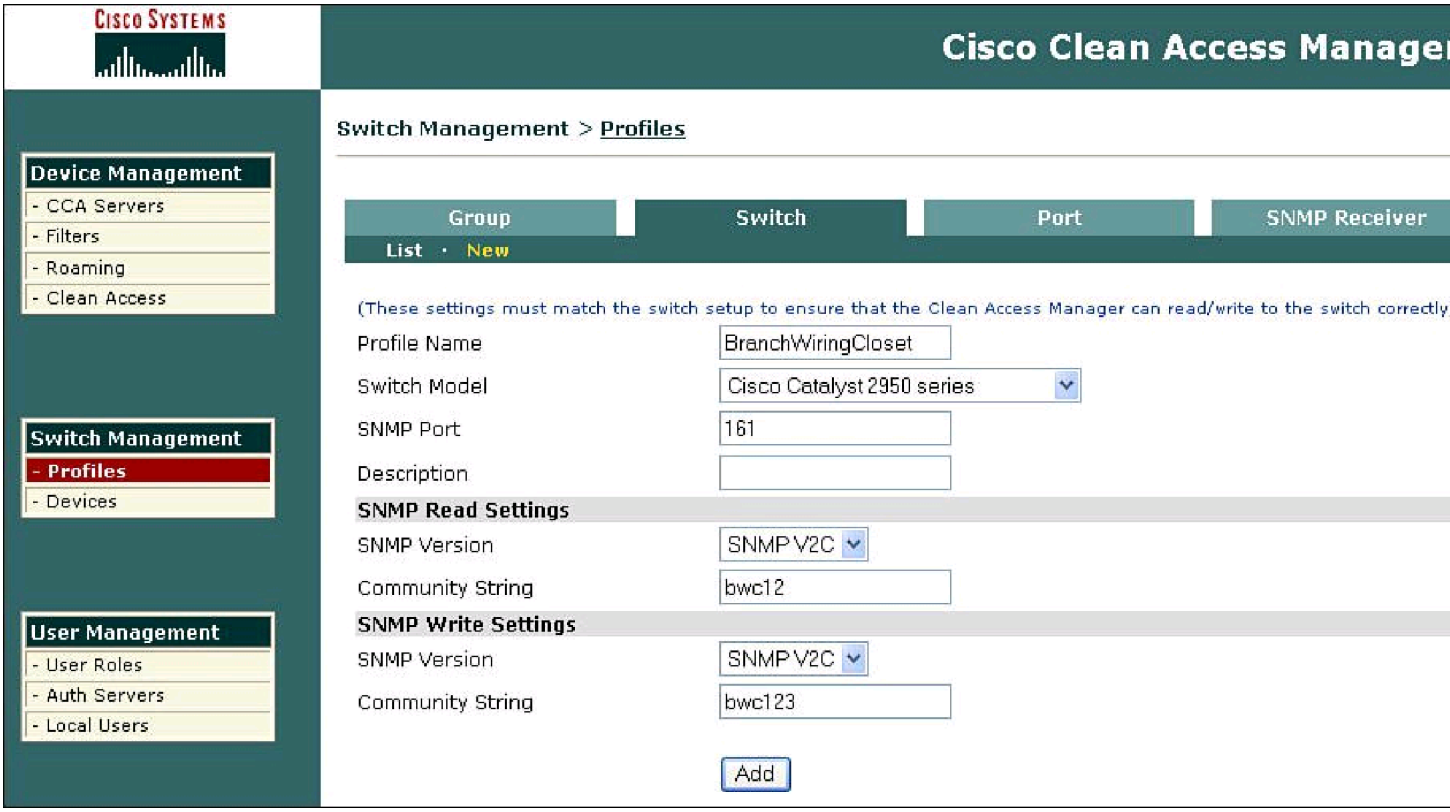

Cisco Clean Access Manager - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.19.106.12/admin/main.jsp
Go Links
Cisco Systems
Cisco Clean Access Manager Version 3.6.2
Device Management
- CCA Servers
- Filters
- Roaming
- Clean Access
Switch Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
- User Pages
- Admin Users
- Backup
User Role
Unauthenticated Role (not common)
Operating System
ALL
(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)
Clean Access Agent:
Require use of Clean Access Agent
Clean Access Agent Download Page Message (or URL):
Network Security Notice: This network is protected by the Clean Access Agent, a component of the Cisco Clean Access Suite. The Clean Access Agent ensures that your computer meets the requirements for accessing this
Show Network Policy to Clean Access Agent users
Network Policy Link:
Logoff Clean Access Agent users from network on their machine logoff or shutdown
Web Login:
Show Network Scanner User Agreement page to web login users
Enable pop-up scan vulnerability reports from User Agreement page
Require users to be certified at every web login
Exempt certified devices from web login requirement by adding to MAC filters
Block/Quarantine users with vulnerabilities in role:
Network Scan Quarantine Role (15 minutes)
Show quarantined users User Agreement Page of:
original role (deprecated)
Update
Cancel
Done
Internet


Cisco Clean Access Manager - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.19.106.12/admin/main.jsp
Go Links
Cisco Systems
Cisco Clean Access Manager Version 3.6.2
Device Management
- CCA Servers
- Filters
- Roaming
- Clean Access
Switch Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
- User Pages
- Admin Users
- Backup
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Scan Setup · Plugin Updates · Reports
Plugins | Options | Vulnerabilities | User Agreement | Test
User Role
Unauthenticated Role (not common)
Operating System
ALL
(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)
The User Agreement page contains user agreement text, security information, or any information you want users to acknowledge to be certified for network access. Use the Information Page configured below to include information in the User Agreement page specifically for users with the selected role and operating system in your network.
Information Page Message (or URL)
(the web server hosting this page must be accessible to the user role by traffic control policy)
Acknowledgement Instructions
(this text appears next to the Accept(Continue) and Decline(Logout) buttons at the bottom of the User Agreement page. The variable #time# will be replaced with the quarantine time.)
Accept(Continue) Button Label
Accept
(use "HIDDEN" to hide this button)
Decline(Logout) Button Label
Decline
(use "HIDDEN" to hide this button)
Internet


Cisco Clean Access Manager - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.19.106.12/admin/main.jsp
Go Links
Cisco Systems
Cisco Clean Access Manager Version 3.6.2
Device Management
- CCA Servers
- Filters
- Roaming
- Clean Access
Switch Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
- User Pages
- Admin Users
- Backup
Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
Check List | New Check | Rule List | New Rule | New AV Rule | New AS Rule | AV/AS Support Info
Name Category Type OS Copy Edit Del
pc_Hotfix828035 Registry Check Registry Key Win(XP)
pc_Hotfix823182 Registry Check Registry Key Win(XP)
pc_Hotfix824146 Registry Check Registry Key Win(XP)
pc_Hotfix825119 Registry Check Registry Key Win(XP)
pc_Hotfix835732 Registry Check Registry Key Win(XP)
pc_Hotfix828741 Registry Check Registry Key Win(XP)
pc_Hotfix823559 Registry Check Registry Key Win(XP)
pc_Hotfix329390 Registry Check Registry Key Win(XP)
pc_Hotfix323255 Registry Check Registry Key Win(XP)
pc_Symantec_Client_Firewall Registry Check Registry Value Win(XP)
pc_AutoUpdateCheck Service Check Service Status Win(XP,2000)
pc_HotFixKB823182 Registry Check Registry Key Win(2000)
Internet


Cisco Clean Access Manager - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.19.106.12/admin/main.jsp
Go Links
Cisco Systems
Cisco Clean Access Manager Version 3.6.2
Device Management
- CCA Servers
- Filters
- Roaming
- Clean Access
Switch Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
- User Pages
- Admin Users
- Backup
Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
Check List | New Check | Rule List | New Rule | New AV Rule | New AS Rule | AV/AS Support Info
Check Category
Registry Check
Check Type
Registry Key
Check Name
Registry Key
HKLM
\
Operator
exists
Check Description
Operating System
Windows All
Windows XP
Windows 2000
Windows ME
Windows 98
Automatically create rule based on this check
Add Check
Internet

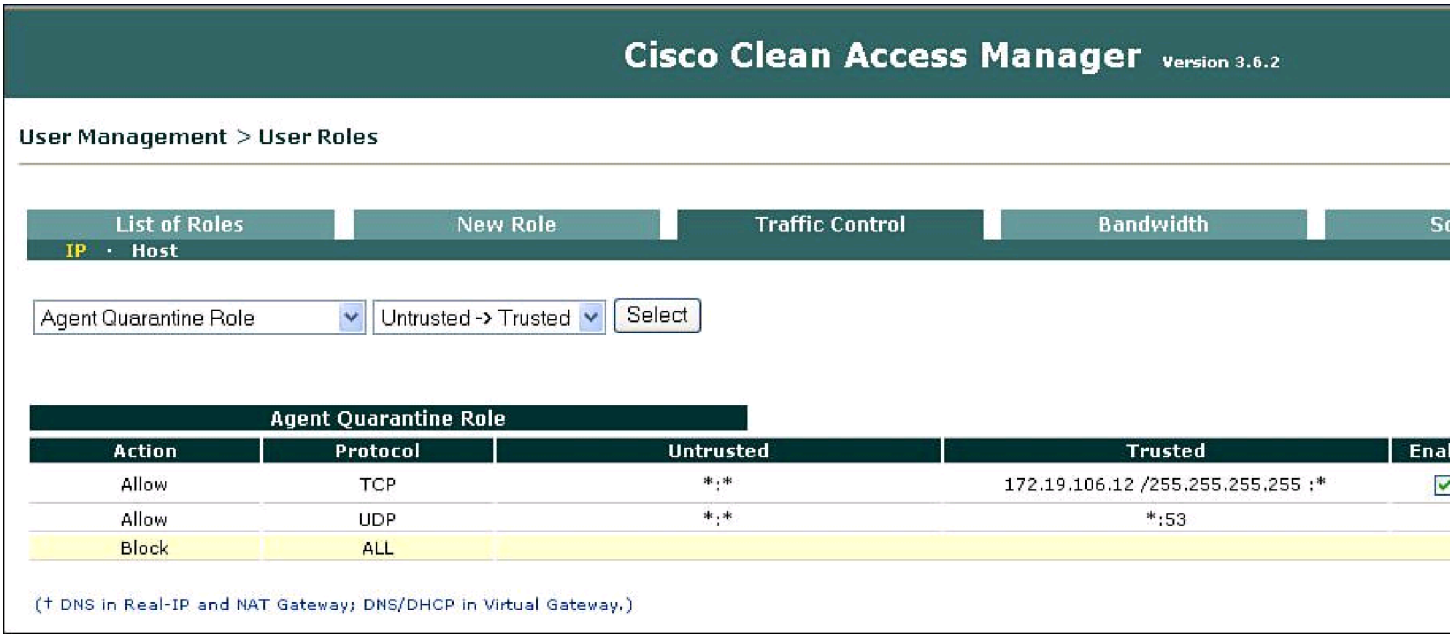

Cisco Clean Access Manager - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.19.106.12/admin/main.jsp
Go Links
Cisco Systems
Cisco Clean Access Manager Version 3.6.2
Device Management
- CCA Servers
- Filters
- Roaming
- Clean Access
Switch Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
- User Pages
- Admin Users
- Backup
Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Distribution · Rules · Requirements · Role-Requirements · Reports · Updates
Check List | New Check | Rule List | New Rule | New AV Rule | New AS Rule | AV/AS Support Info
Rule Name
Anti-Spyware Vendor
ANY
Type
Operating System
Rule Description
ANY
AhnLab, Inc.
America Online, Inc.
Bullet Proof Soft
Computer Associates International, Inc.
EarthLink, Inc.
Javacool Software LLC
Lavasoft, Inc.
McAfee, Inc.
MicroSmarts LLC
Microsoft Corp.
PC Tools Software
Prevx Ltd.
Safer Networking Ltd.
Sunbelt Software
Trend Micro, Inc.
Webroot Software, Inc.
Yahoo!, Inc.
Installation
Spyware Definition
ANY
Internet

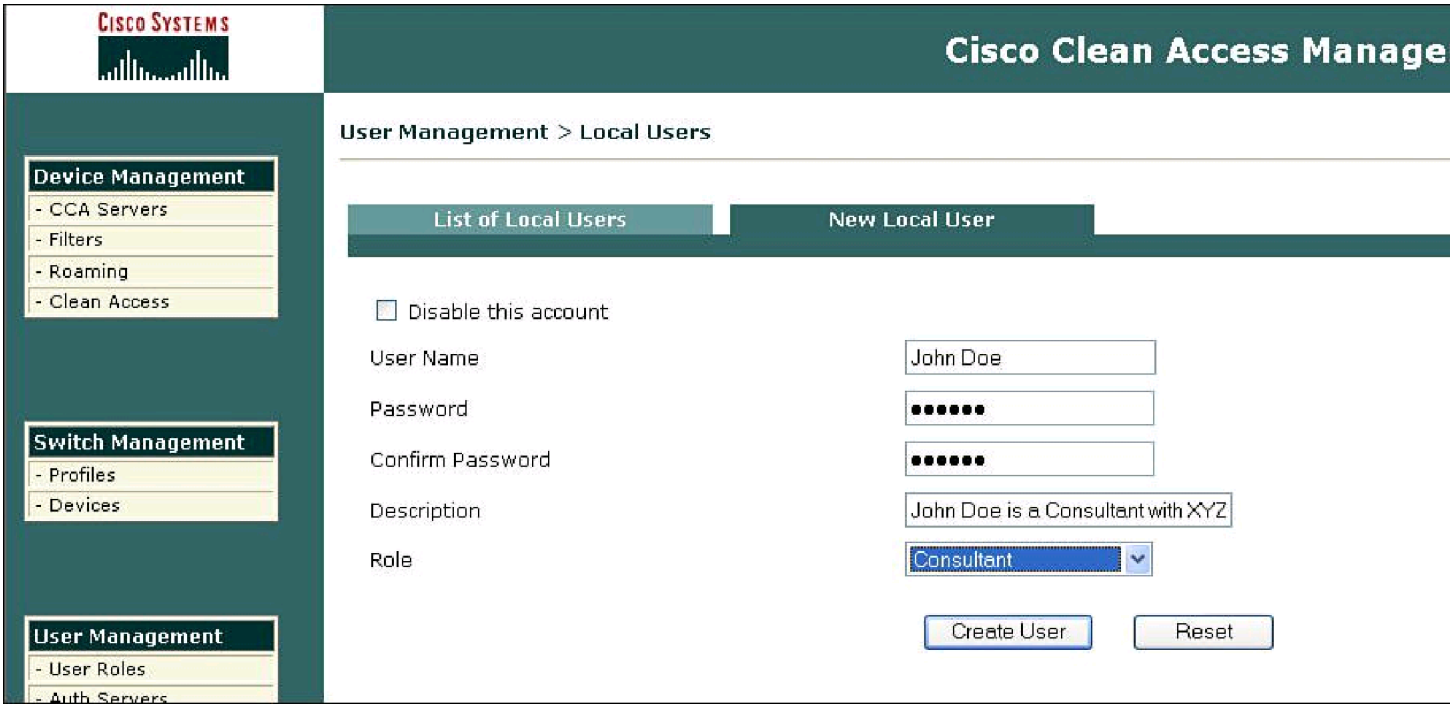

Cisco Systems
Cisco Clean Access Manage
Device Management
- CCA Servers
- Filters
- Roaming
- Clean Access
Switch Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Switch Management > Profiles
Group
Switch
Port
SNMP Receiver
List · New
(These settings must match the switch setup to ensure that the Clean Access Manager can read/write to the switch correctly
Profile Name
BranchWiringCloset
Switch Model
Cisco Catalyst 2950 series
SNMP Port
161
Description
SNMP Read Settings
SNMP Version
SNMP V2C
Community String
bwc12
SNMP Write Settings
SNMP Version
SNMP V2C
Community String
bwc123
Add

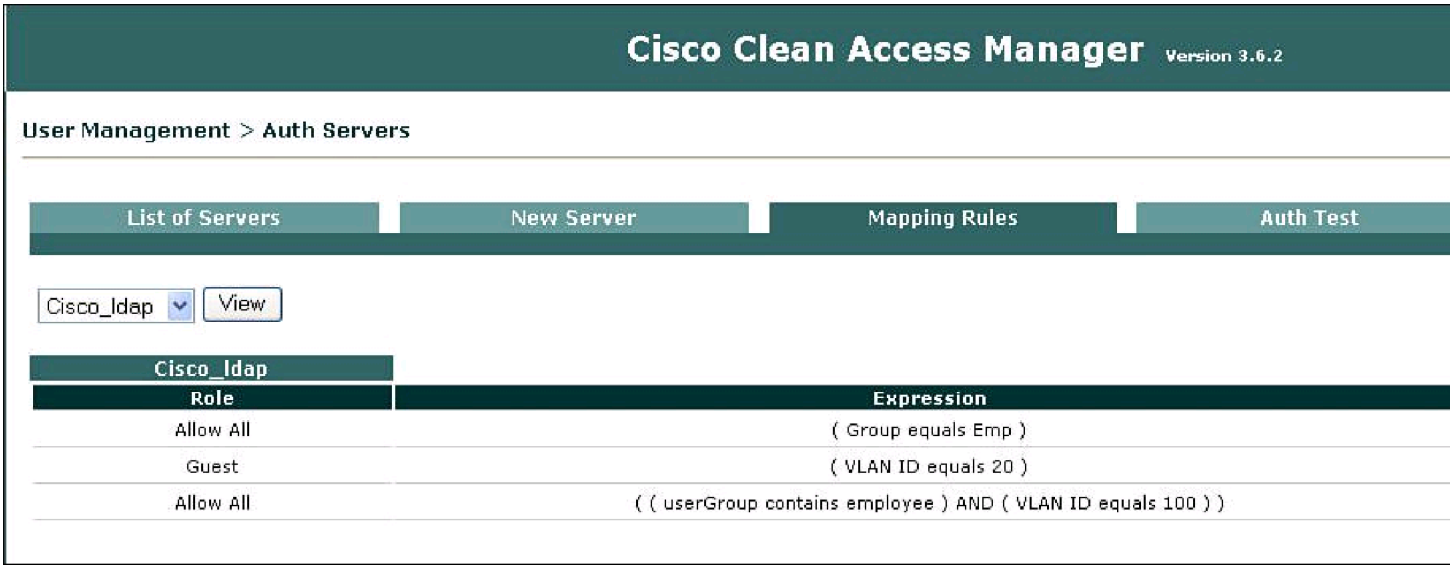
User Management > User Roles

List of Roles | New Role | Traffic Control | Bandwidth | Sc

Role Name	IPSec	Roam	VLAN	Description	F
Unauthenticated Role	deny	deny		Role for unauthenticated users	
Agent Quarantine Role	deny	deny		Role for users to download requirements	
Network Scan Quarantine Role	deny	deny		Role for quarantined users	
Allow All	deny	deny		Allow All	
Guest	deny	deny		Guest	
Consultant	deny	deny		Consultant	
ScanTest	deny	deny		Test role for network scanner	
TAC	deny	deny		TAC Access	
Dormitory Student	deny	deny		Dorm	
printer	deny	deny			
Chicago_users	deny	deny		chicago	
Nowhere	deny	deny			
alok	deny	deny			
San_Jose_Users	deny	deny		San Jose	


Cisco Clean Access Manager Version 3.6.2
User Management > User Roles
List of Roles
New Role
Traffic Control
Bandwidth
IP · Host
Agent Quarantine Role
Untrusted -> Trusted
Select
Agent Quarantine Role
Action
Protocol
Untrusted
Trusted
Allow
TCP
:
172.19.106.12 /255.255.255.255 :*
Allow
UDP
:
*:53
Block
ALL
(† DNS in Real-IP and NAT Gateway; DNS/DHCP in Virtual Gateway.)

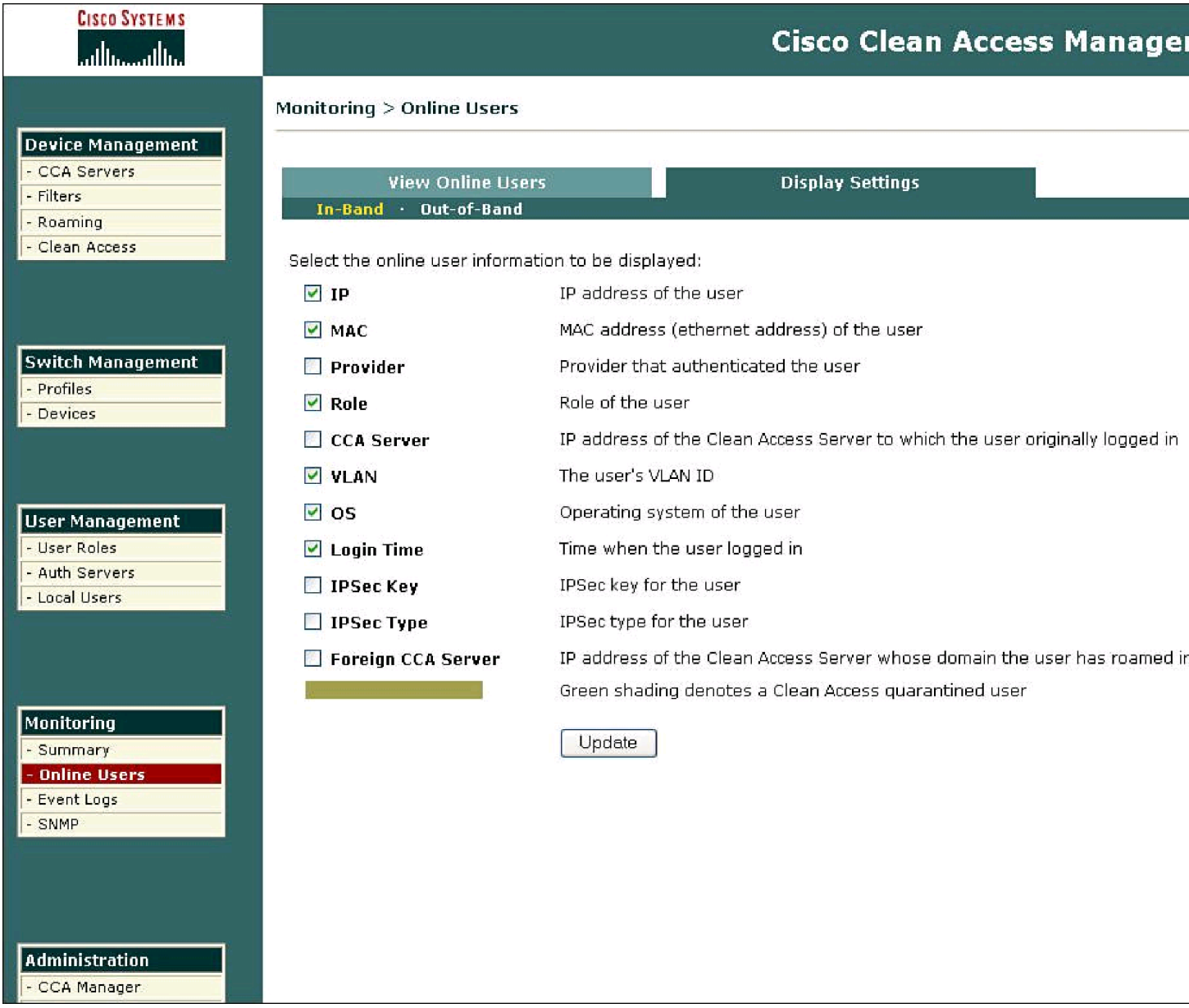

Cisco Systems
Cisco Clean Access Manage
Device Management
- CCA Servers
- Filters
- Roaming
- Clean Access
Switch Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
User Management > Local Users
List of Local Users
New Local User
Disable this account
User Name
John Doe
Password
Confirm Password
Description
John Doe is a Consultant with XYZ
Role
Consultant
Create User
Reset

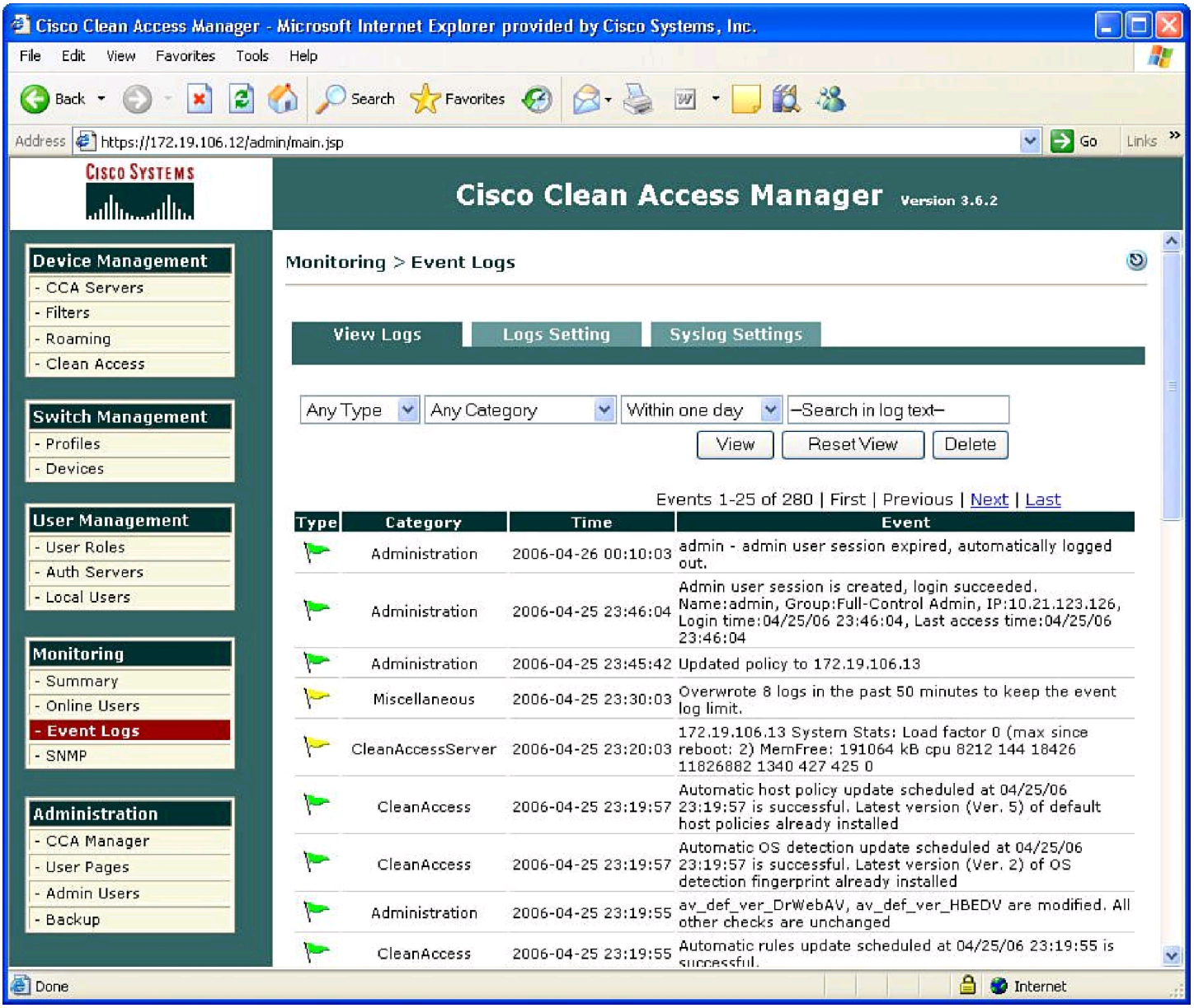

Cisco Clean Access Manager Version 3.6.2
User Management > Auth Servers
List of Servers
New Server
Mapping Rules
Auth Test
Cisco_ldap
View
Cisco_ldap
Role
Expression
Allow All
(Group equals Emp)
Guest
(VLAN ID equals 20)
Allow All
((userGroup contains employee) AND (VLAN ID equals 100))

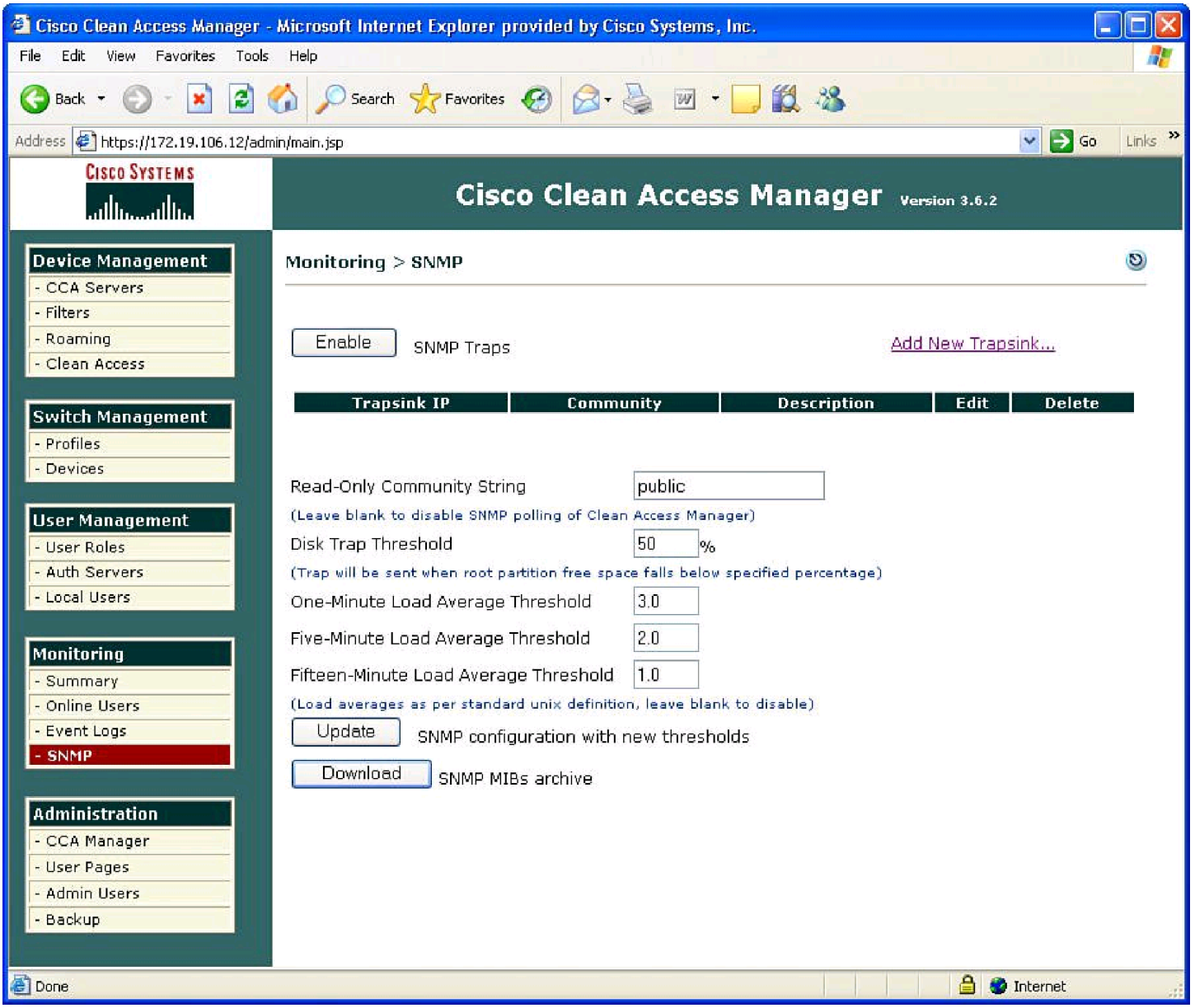
Cisco Clean Access Manager Version 3.6.2

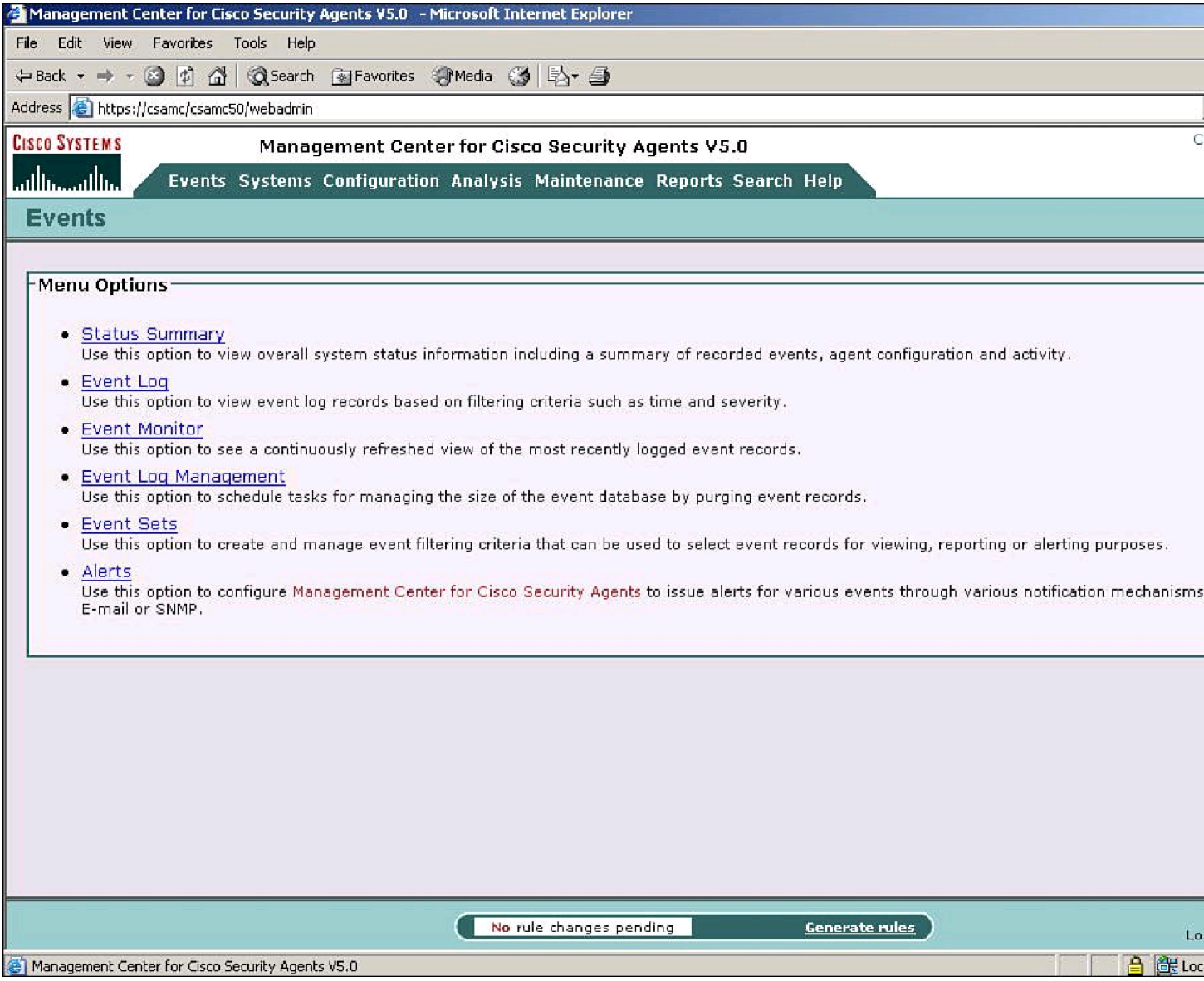
Monitoring > Summary

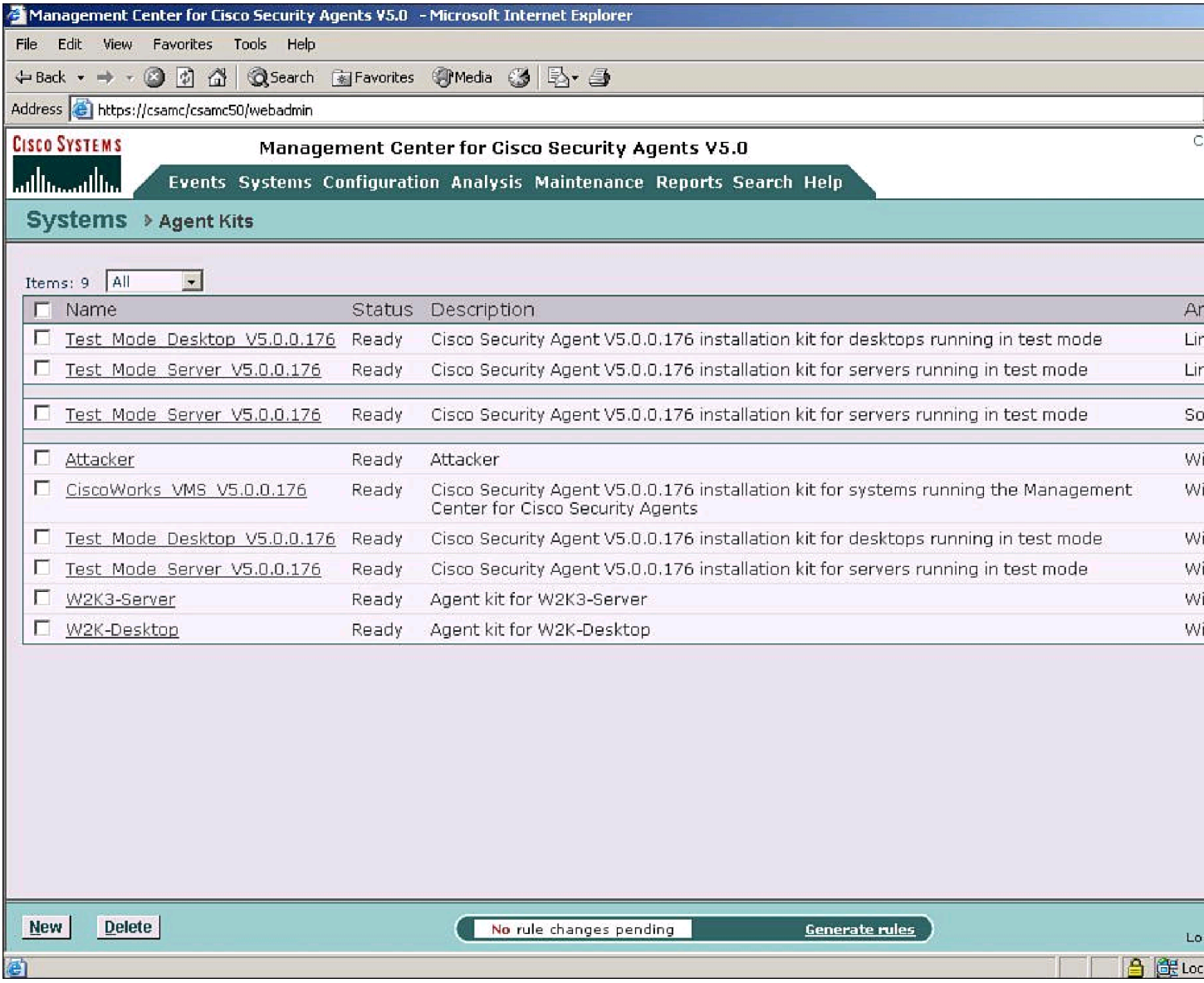
Current Clean Access Agent Version:	**3.6.1.0**	
Current Clean Access Agent Patch Version:	**3.6.2.0**	
Clean Access Servers configured:	**1**	
Global MAC addresses configured:	**0**	
Global subnets configured:	**2**	
Online users:	*(In-Band* /	*Out-of-Band)*
Total:	**0**	**0**
Unique online users' names:	**0**	**0**
Unique online users' MAC addresses:	**0**	**0**
Online users in Unauthenticated Role:	**0**	**0**
Online users in Agent Quarantine Role:	**0**	**0**
Online users in Network Scan Quarantine Role:	**0**	**0**
Online users in Allow All:	**0**	**0**
Online users in Guest:	**0**	**0**
Online users in Consultant:	**0**	**0**
Online users in ScanTest:	**0**	**0**
Online users in TAC:	**0**	**0**
Online users in Dormitory Student:	**0**	**0**
Online users in printer:	**0**	**0**
Online users in Chicago_users:	**0**	**0**
Online users in Nowhere:	**0**	**0**
Online users in alok:	**0**	**0**
Online users in San_Jose_Users:	**0**	**0**

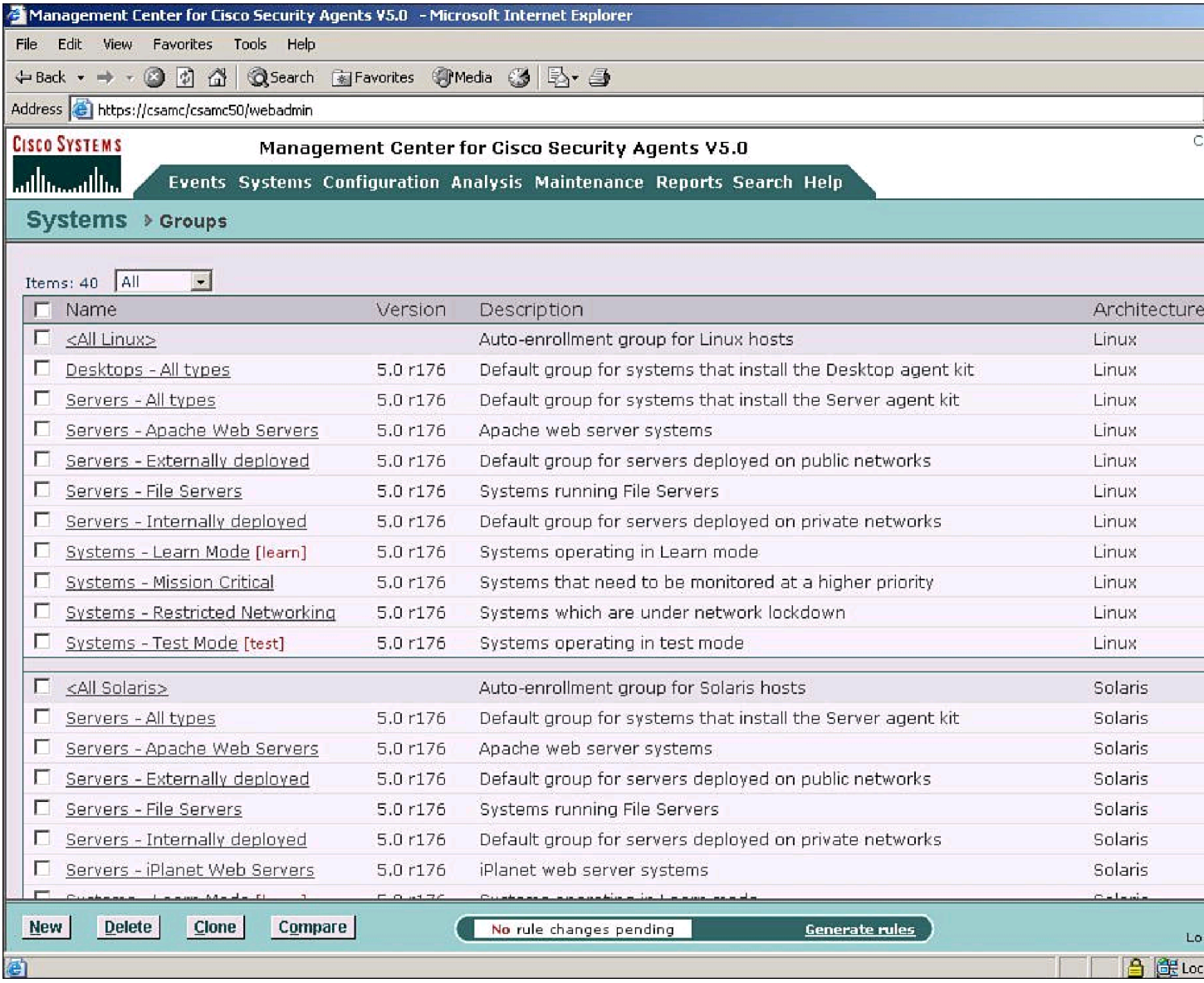

Cisco Systems
Cisco Clean Access Manager
Monitoring > Online Users
Device Management
- CCA Servers
- Filters
- Roaming
- Clean Access
Switch Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
View Online Users
Display Settings
In-Band · Out-of-Band
Select the online user information to be displayed:
IP
IP address of the user
MAC
MAC address (ethernet address) of the user
Provider
Provider that authenticated the user
Role
Role of the user
CCA Server
IP address of the Clean Access Server to which the user originally logged in
VLAN
The user's VLAN ID
OS
Operating system of the user
Login Time
Time when the user logged in
IPSec Key
IPSec key for the user
IPSec Type
IPSec type for the user
Foreign CCA Server
IP address of the Clean Access Server whose domain the user has roamed in
Green shading denotes a Clean Access quarantined user
Update

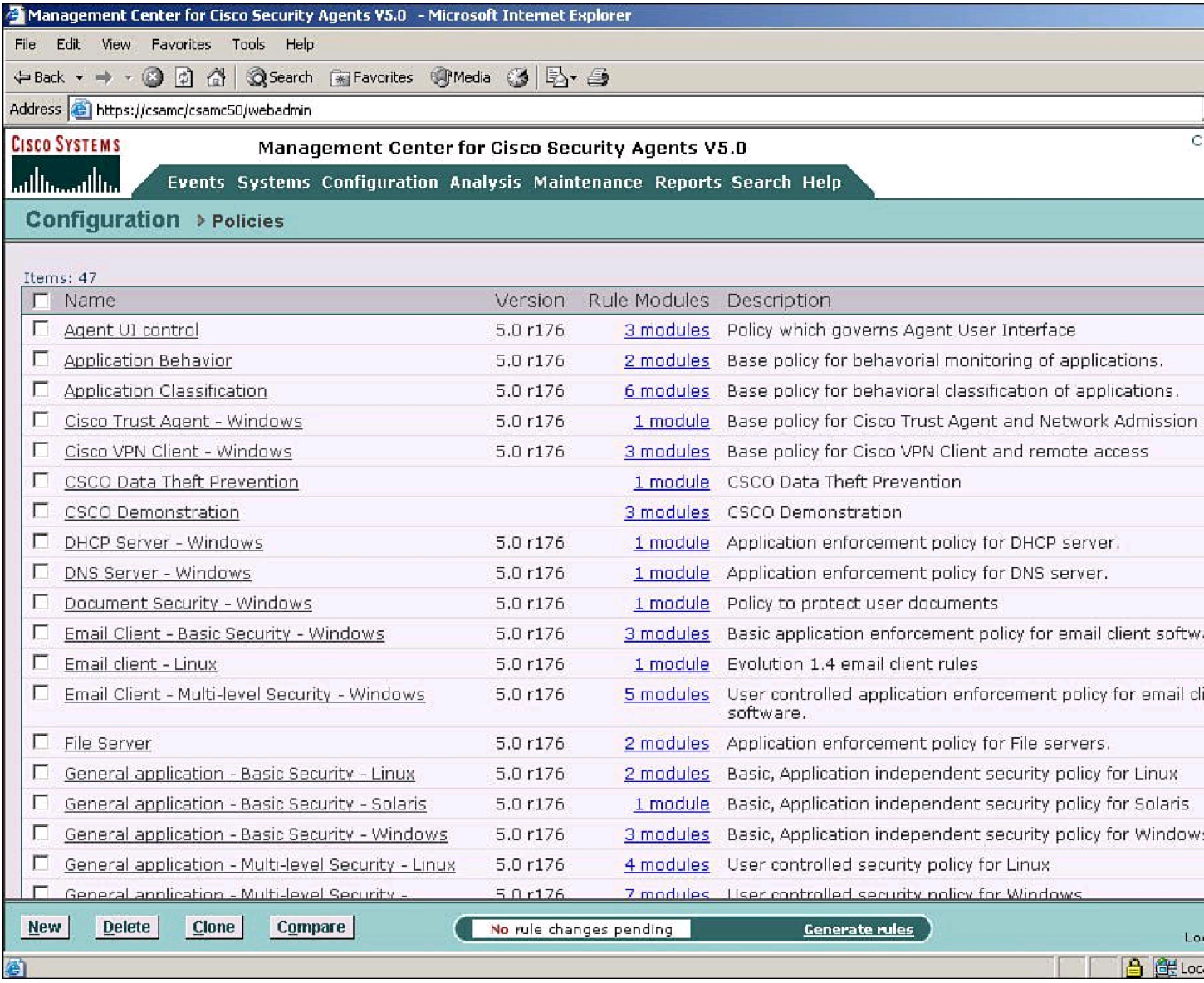

Cisco Clean Access Manager - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.19.106.12/admin/main.jsp
Go Links
Cisco Systems
Cisco Clean Access Manager Version 3.6.2
Device Management
- CCA Servers
- Filters
- Roaming
- Clean Access
Switch Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
- User Pages
- Admin Users
- Backup
Monitoring > Event Logs
View Logs
Logs Setting
Syslog Settings
Any Type
Any Category
Within one day
–Search in log text–
View
Reset View
Delete
Events 1-25 of 280 | First | Previous | Next | Last
Type
Category
Time
Event
Administration
2006-04-26 00:10:03
admin - admin user session expired, automatically logged out.
Administration
2006-04-25 23:46:04
Admin user session is created, login succeeded. Name:admin, Group:Full-Control Admin, IP:10.21.123.126, Login time:04/25/06 23:46:04, Last access time:04/25/06 23:46:04
Administration
2006-04-25 23:45:42
Updated policy to 172.19.106.13
Miscellaneous
2006-04-25 23:30:03
Overwrote 8 logs in the past 50 minutes to keep the event log limit.
CleanAccessServer
2006-04-25 23:20:03
172.19.106.13 System Stats: Load factor 0 (max since reboot: 2) MemFree: 191064 kB cpu 8212 144 18426 11826882 1340 427 425 0
CleanAccess
2006-04-25 23:19:57
Automatic host policy update scheduled at 04/25/06 23:19:57 is successful. Latest version (Ver. 5) of default host policies already installed
CleanAccess
2006-04-25 23:19:57
Automatic OS detection update scheduled at 04/25/06 23:19:57 is successful. Latest version (Ver. 2) of OS detection fingerprint already installed
Administration
2006-04-25 23:19:55
av_def_ver_DrWebAV, av_def_ver_HBEDV are modified. All other checks are unchanged
CleanAccess
2006-04-25 23:19:55
Automatic rules update scheduled at 04/25/06 23:19:55 is successful.
Done
Internet

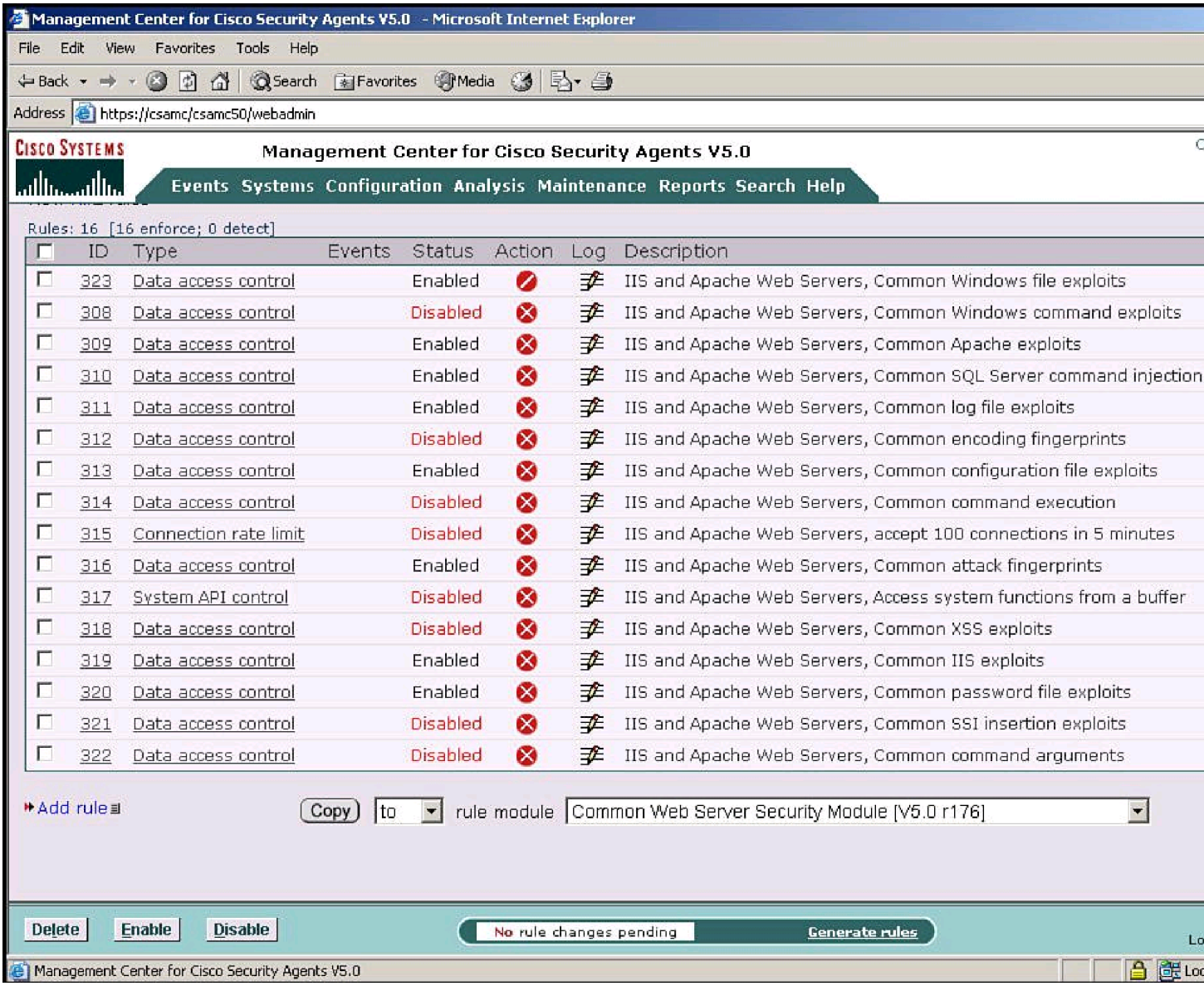

Cisco Clean Access Manager - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.19.106.12/admin/main.jsp
Go Links
Cisco Systems
Cisco Clean Access Manager Version 3.6.2
Device Management
- CCA Servers
- Filters
- Roaming
- Clean Access
Switch Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
- User Pages
- Admin Users
- Backup
Monitoring > SNMP
Enable
SNMP Traps
Add New Trapsink...
Trapsink IP
Community
Description
Edit
Delete
Read-Only Community String
public
(Leave blank to disable SNMP polling of Clean Access Manager)
Disk Trap Threshold
50
%
(Trap will be sent when root partition free space falls below specified percentage)
One-Minute Load Average Threshold
3.0
Five-Minute Load Average Threshold
2.0
Fifteen-Minute Load Average Threshold
1.0
(Load averages as per standard unix definition, leave blank to disable)
Update
SNMP configuration with new thresholds
Download
SNMP MIBs archive
Done
Internet

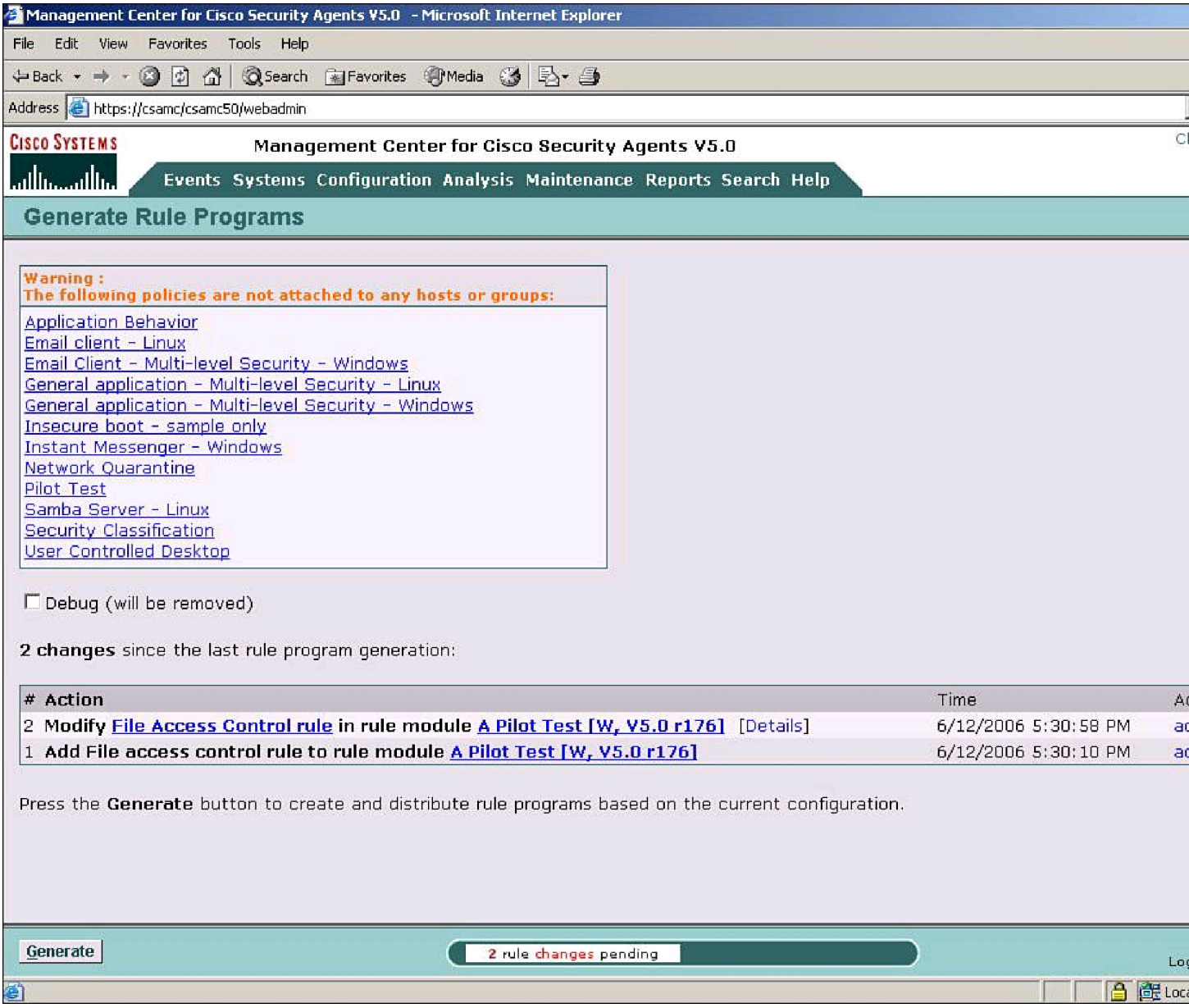

Management Center for Cisco Security Agents V5.0 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://csamc/csamc50/webadmin
Cisco Systems
Management Center for Cisco Security Agents V5.0
Events Systems Configuration Analysis Maintenance Reports Search Help
Events
Menu Options
Status Summary
Use this option to view overall system status information including a summary of recorded events, agent configuration and activity.
Event Log
Use this option to view event log records based on filtering criteria such as time and severity.
Event Monitor
Use this option to see a continuously refreshed view of the most recently logged event records.
Event Log Management
Use this option to schedule tasks for managing the size of the event database by purging event records.
Event Sets
Use this option to create and manage event filtering criteria that can be used to select event records for viewing, reporting or alerting purposes.
Alerts
Use this option to configure Management Center for Cisco Security Agents to issue alerts for various events through various notification mechanisms
E-mail or SNMP.
No rule changes pending
Generate rules
Management Center for Cisco Security Agents V5.0

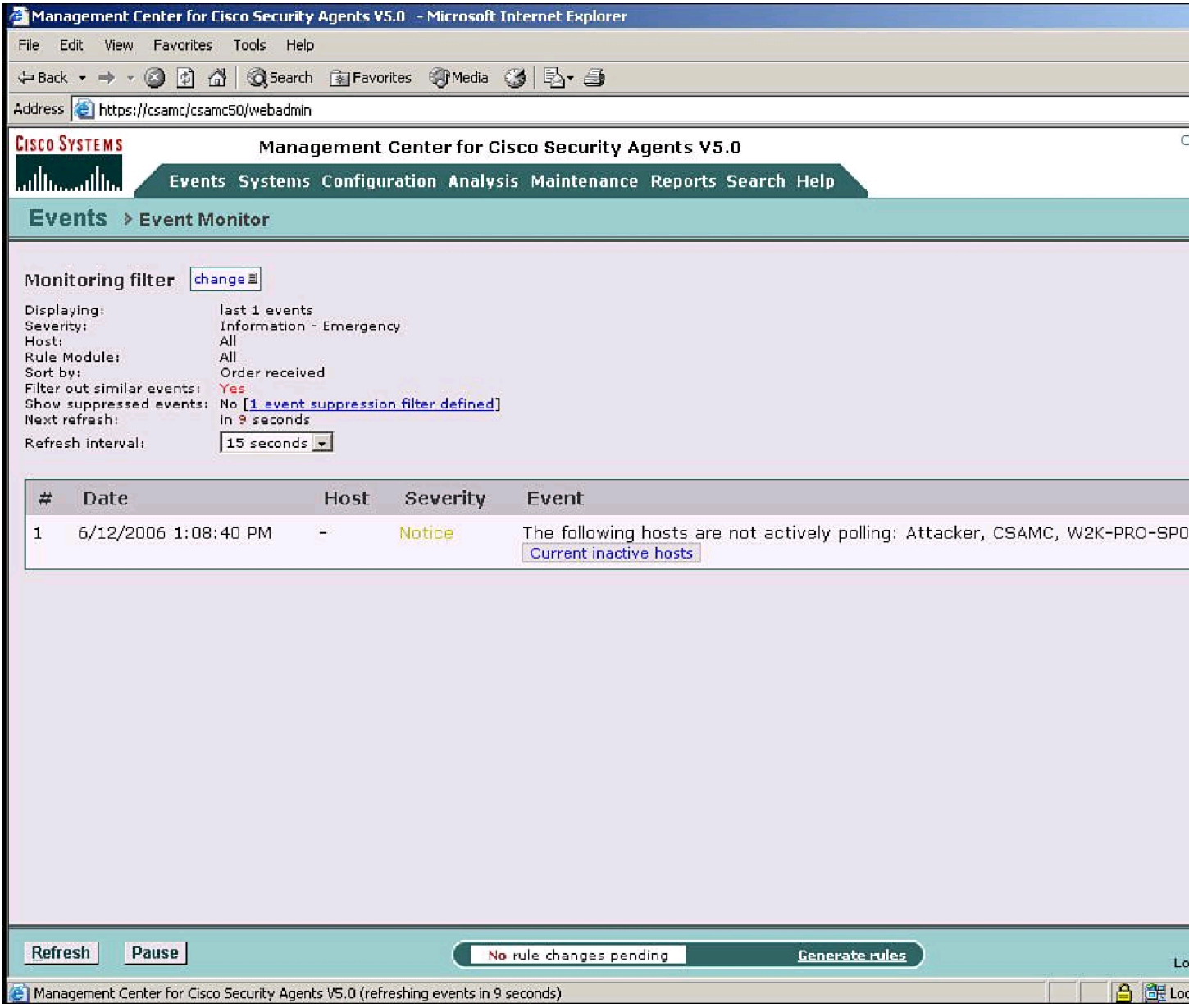

Management Center for Cisco Security Agents V5.0 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://csamc/csamc50/webadmin
Cisco Systems
Management Center for Cisco Security Agents V5.0
Events Systems Configuration Analysis Maintenance Reports Search Help
Systems › Agent Kits
Items: 9 All
Name Status Description
Test_Mode_Desktop_V5.0.0.176 Ready Cisco Security Agent V5.0.0.176 installation kit for desktops running in test mode
Test_Mode_Server_V5.0.0.176 Ready Cisco Security Agent V5.0.0.176 installation kit for servers running in test mode
Test_Mode_Server_V5.0.0.176 Ready Cisco Security Agent V5.0.0.176 installation kit for servers running in test mode
Attacker Ready Attacker
CiscoWorks_VMS_V5.0.0.176 Ready Cisco Security Agent V5.0.0.176 installation kit for systems running the Management Center for Cisco Security Agents
Test_Mode_Desktop_V5.0.0.176 Ready Cisco Security Agent V5.0.0.176 installation kit for desktops running in test mode
Test_Mode_Server_V5.0.0.176 Ready Cisco Security Agent V5.0.0.176 installation kit for servers running in test mode
W2K3-Server Ready Agent kit for W2K3-Server
W2K-Desktop Ready Agent kit for W2K-Desktop
New
Delete
No rule changes pending
Generate rules

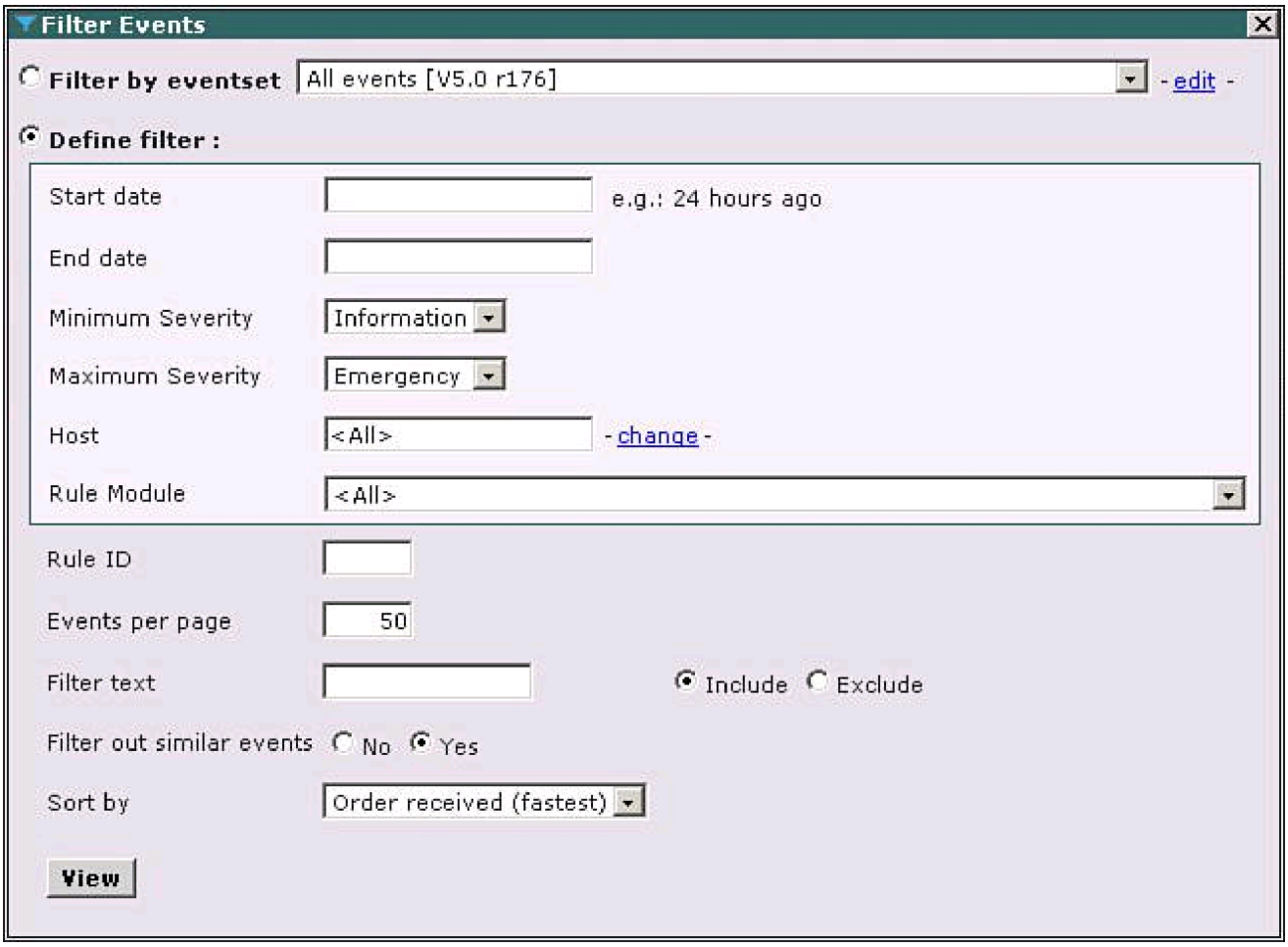

Management Center for Cisco Security Agents V5.0 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://csamc/csamc50/webadmin
Cisco Systems
Management Center for Cisco Security Agents V5.0
Events Systems Configuration Analysis Maintenance Reports Search Help
Systems Groups
Items: 40 All
Name Version Description Architecture
<All Linux> Auto-enrollment group for Linux hosts Linux
Desktops - All types 5.0 r176 Default group for systems that install the Desktop agent kit Linux
Servers - All types 5.0 r176 Default group for systems that install the Server agent kit Linux
Servers - Apache Web Servers 5.0 r176 Apache web server systems Linux
Servers - Externally deployed 5.0 r176 Default group for servers deployed on public networks Linux
Servers - File Servers 5.0 r176 Systems running File Servers Linux
Servers - Internally deployed 5.0 r176 Default group for servers deployed on private networks Linux
Systems - Learn Mode [learn] 5.0 r176 Systems operating in Learn mode Linux
Systems - Mission Critical 5.0 r176 Systems that need to be monitored at a higher priority Linux
Systems - Restricted Networking 5.0 r176 Systems which are under network lockdown Linux
Systems - Test Mode [test] 5.0 r176 Systems operating in test mode Linux
<All Solaris> Auto-enrollment group for Solaris hosts Solaris
Servers - All types 5.0 r176 Default group for systems that install the Server agent kit Solaris
Servers - Apache Web Servers 5.0 r176 Apache web server systems Solaris
Servers - Externally deployed 5.0 r176 Default group for servers deployed on public networks Solaris
Servers - File Servers 5.0 r176 Systems running File Servers Solaris
Servers - Internally deployed 5.0 r176 Default group for servers deployed on private networks Solaris
Servers - iPlanet Web Servers 5.0 r176 iPlanet web server systems Solaris
New Delete Clone Compare
No rule changes pending
Generate rules

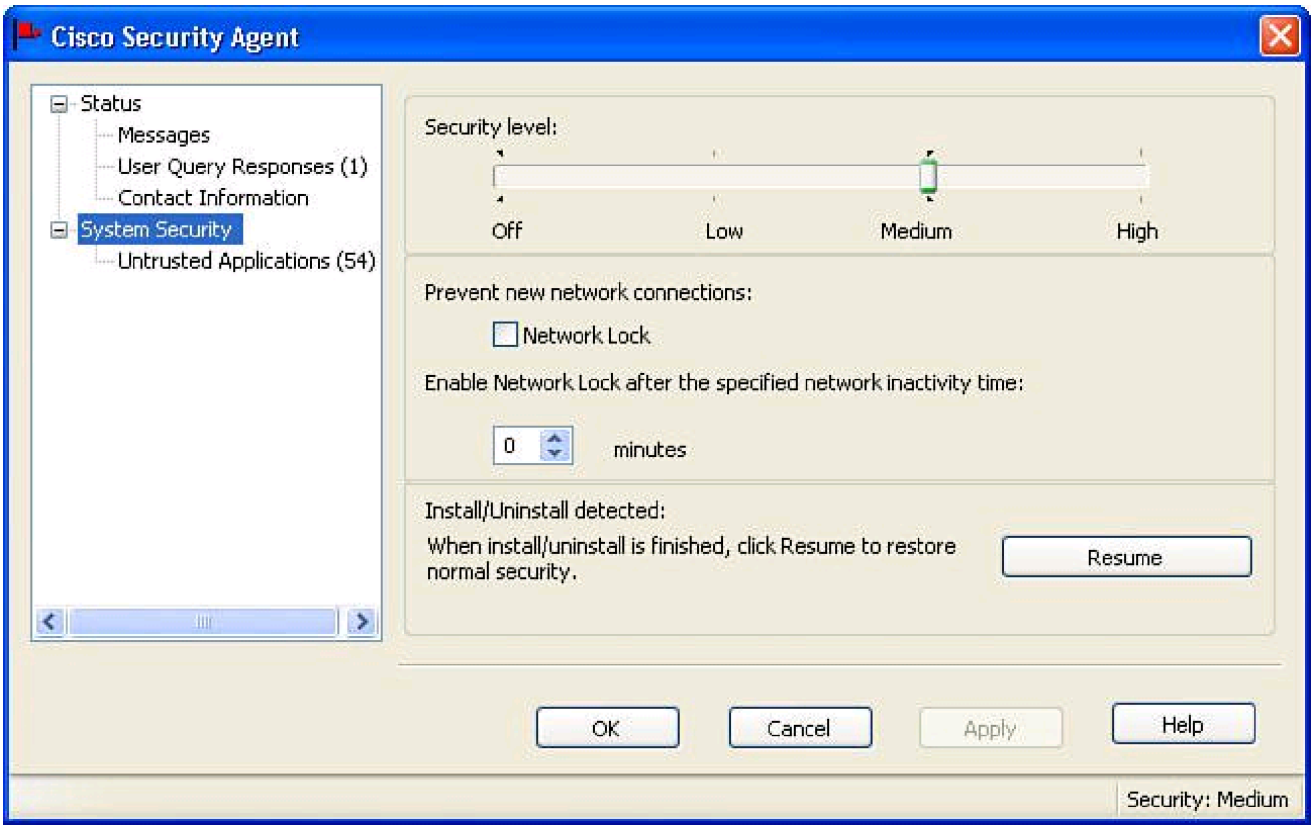

Management Center for Cisco Security Agents V5.0 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://csamc/csamc50/webadmin
Cisco Systems
Management Center for Cisco Security Agents V5.0
Events Systems Configuration Analysis Maintenance Reports Search Help
Configuration › Policies
Items: 47
Name Version Rule Modules Description
Agent UI control 5.0 r176 3 modules Policy which governs Agent User Interface
Application Behavior 5.0 r176 2 modules Base policy for behavorial monitoring of applications.
Application Classification 5.0 r176 6 modules Base policy for behavioral classification of applications.
Cisco Trust Agent - Windows 5.0 r176 1 module Base policy for Cisco Trust Agent and Network Admission
Cisco VPN Client - Windows 5.0 r176 3 modules Base policy for Cisco VPN Client and remote access
CSCO Data Theft Prevention 1 module CSCO Data Theft Prevention
CSCO Demonstration 3 modules CSCO Demonstration
DHCP Server - Windows 5.0 r176 1 module Application enforcement policy for DHCP server.
DNS Server - Windows 5.0 r176 1 module Application enforcement policy for DNS server.
Document Security - Windows 5.0 r176 1 module Policy to protect user documents
Email Client - Basic Security - Windows 5.0 r176 3 modules Basic application enforcement policy for email client softw
Email client - Linux 5.0 r176 1 module Evolution 1.4 email client rules
Email Client - Multi-level Security - Windows 5.0 r176 5 modules User controlled application enforcement policy for email cl software.
File Server 5.0 r176 2 modules Application enforcement policy for File servers.
General application - Basic Security - Linux 5.0 r176 2 modules Basic, Application independent security policy for Linux
General application - Basic Security - Solaris 5.0 r176 1 module Basic, Application independent security policy for Solaris
General application - Basic Security - Windows 5.0 r176 3 modules Basic, Application independent security policy for Windows
General application - Multi-level Security - Linux 5.0 r176 4 modules User controlled security policy for Linux
New Delete Clone Compare
No rule changes pending
Generate rules

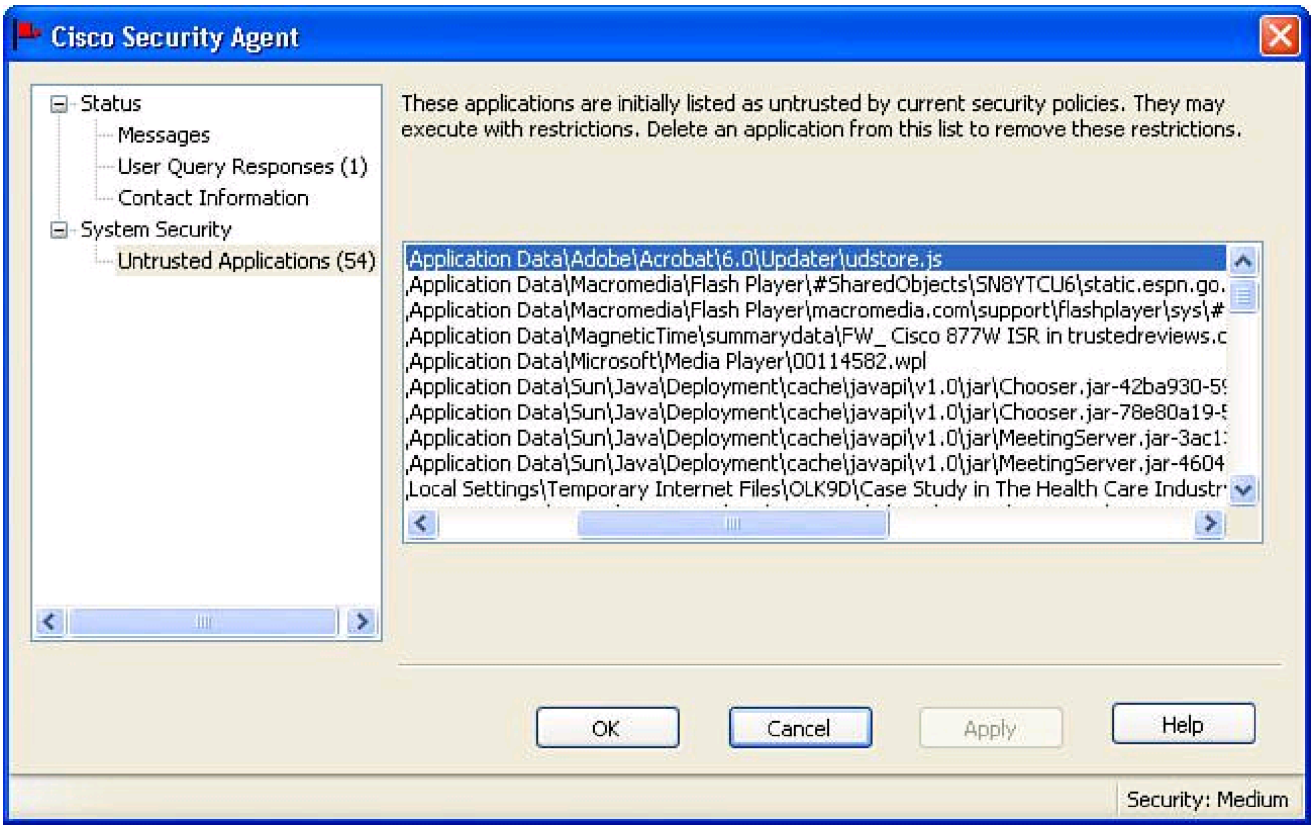

Management Center for Cisco Security Agents V5.0 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://csamc/csamc50/webadmin
Cisco Systems
Management Center for Cisco Security Agents V5.0
Events Systems Configuration Analysis Maintenance Reports Search Help
Rules: 16 [16 enforce; 0 detect]
ID Type Events Status Action Log Description
323 Data access control Enabled IIS and Apache Web Servers, Common Windows file exploits
308 Data access control Disabled IIS and Apache Web Servers, Common Windows command exploits
309 Data access control Enabled IIS and Apache Web Servers, Common Apache exploits
310 Data access control Enabled IIS and Apache Web Servers, Common SQL Server command injection
311 Data access control Enabled IIS and Apache Web Servers, Common log file exploits
312 Data access control Disabled IIS and Apache Web Servers, Common encoding fingerprints
313 Data access control Enabled IIS and Apache Web Servers, Common configuration file exploits
314 Data access control Disabled IIS and Apache Web Servers, Common command execution
315 Connection rate limit Disabled IIS and Apache Web Servers, accept 100 connections in 5 minutes
316 Data access control Enabled IIS and Apache Web Servers, Common attack fingerprints
317 System API control Disabled IIS and Apache Web Servers, Access system functions from a buffer
318 Data access control Disabled IIS and Apache Web Servers, Common XSS exploits
319 Data access control Enabled IIS and Apache Web Servers, Common IIS exploits
320 Data access control Enabled IIS and Apache Web Servers, Common password file exploits
321 Data access control Disabled IIS and Apache Web Servers, Common SSI insertion exploits
322 Data access control Disabled IIS and Apache Web Servers, Common command arguments
Add rule
Copy to rule module Common Web Server Security Module [V5.0 r176]
Delete Enable Disable
No rule changes pending Generate rules
Management Center for Cisco Security Agents V5.0

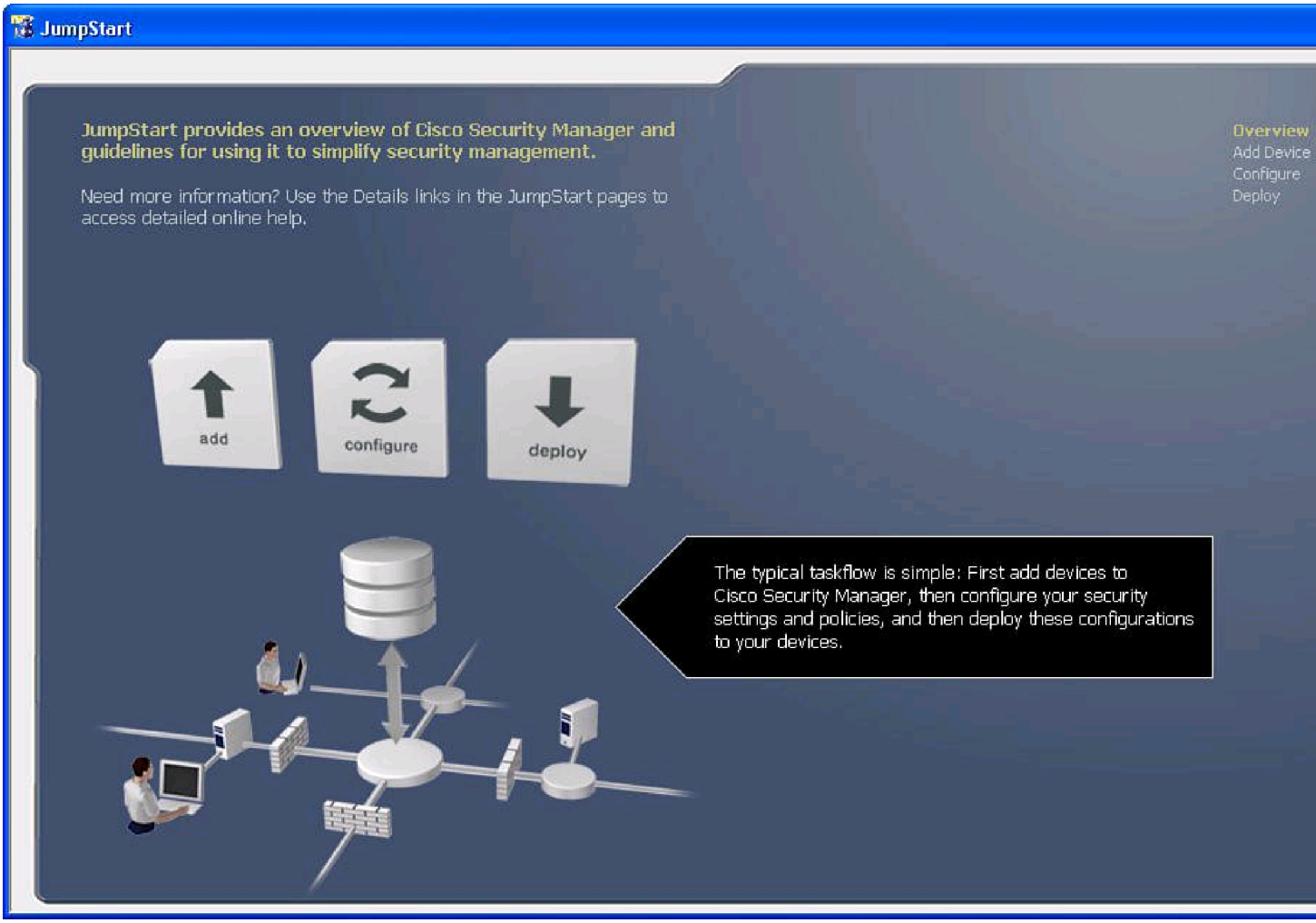

Management Center for Cisco Security Agents V5.0 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://csamc/csamc50/webadmin
Cisco Systems
Management Center for Cisco Security Agents V5.0
Events Systems Configuration Analysis Maintenance Reports Search Help
Generate Rule Programs
Warning :
The following policies are not attached to any hosts or groups:
Application Behavior
Email client - Linux
Email Client - Multi-level Security - Windows
General application - Multi-level Security - Linux
General application - Multi-level Security - Windows
Insecure boot - sample only
Instant Messenger - Windows
Network Quarantine
Pilot Test
Samba Server - Linux
Security Classification
User Controlled Desktop
Debug (will be removed)
2 changes since the last rule program generation:
Action
Time
2 Modify File Access Control rule in rule module A Pilot Test [W, V5.0 r176] [Details]
6/12/2006 5:30:58 PM
1 Add File access control rule to rule module A Pilot Test [W, V5.0 r176]
6/12/2006 5:30:10 PM
Press the Generate button to create and distribute rule programs based on the current configuration.
Generate
2 rule changes pending

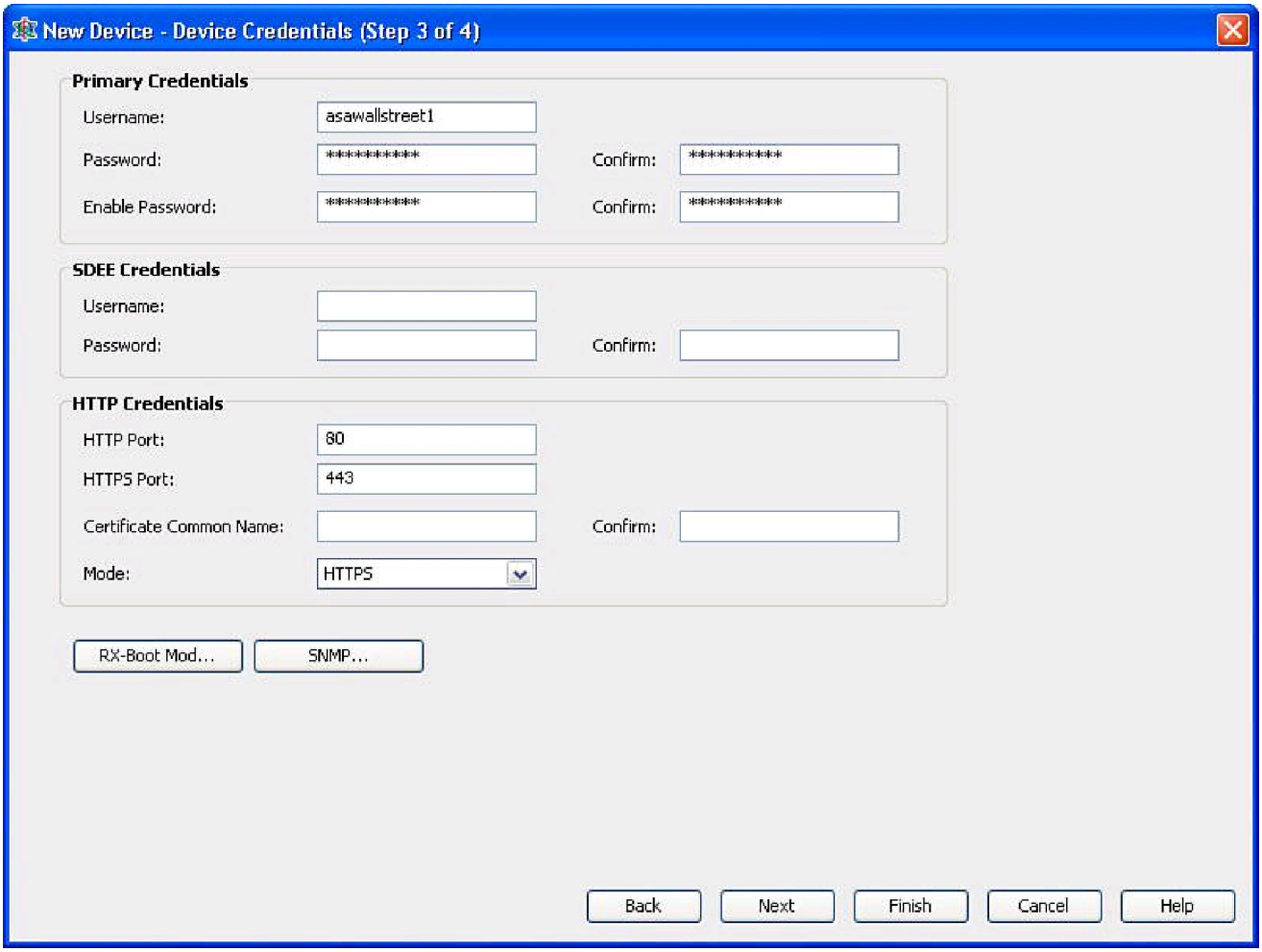

Management Center for Cisco Security Agents V5.0 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://csamc/csamc50/webadmin
Cisco Systems
Management Center for Cisco Security Agents V5.0
Events Systems Configuration Analysis Maintenance Reports Search Help
Events › Event Monitor
Monitoring filter change
Displaying: last 1 events
Severity: Information - Emergency
Host: All
Rule Module: All
Sort by: Order received
Filter out similar events: Yes
Show suppressed events: No [1 event suppression filter defined]
Next refresh: in 9 seconds
Refresh interval: 15 seconds
Date Host Severity Event
1 6/12/2006 1:08:40 PM - Notice The following hosts are not actively polling: Attacker, CSAMC, W2K-PRO-SP0
Current inactive hosts
Refresh Pause
No rule changes pending Generate rules
Management Center for Cisco Security Agents V5.0 (refreshing events in 9 seconds)

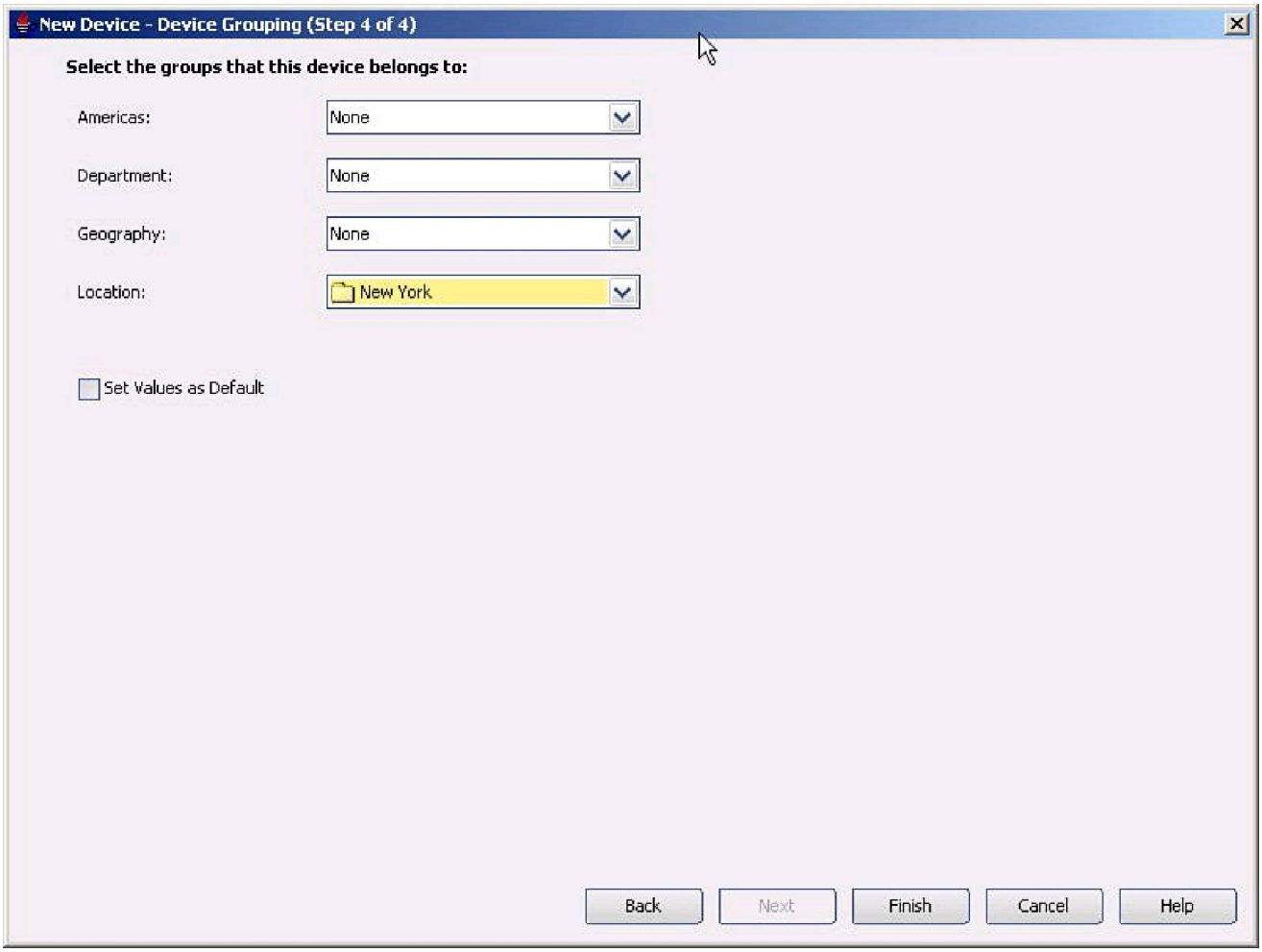

Filter Events
Filter by eventset
All events [V5.0 r176]
- edit -
Define filter :
Start date
e.g.: 24 hours ago
End date
Minimum Severity
Information
Maximum Severity
Emergency
Host
<All>
- change -
Rule Module
<All>
Rule ID
Events per page
50
Filter text
Include
Exclude
Filter out similar events
No
Yes
Sort by
Order received (fastest)
View

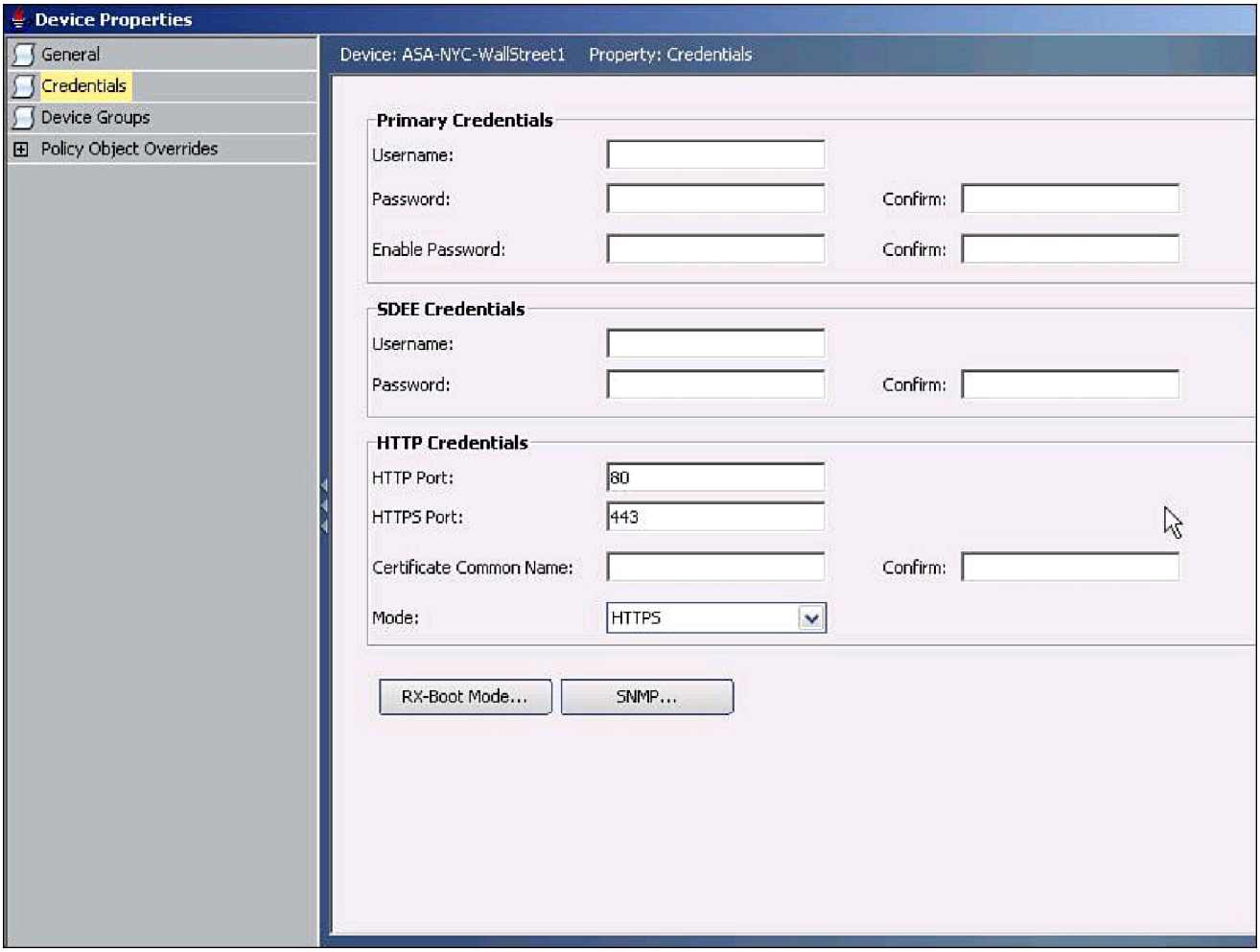

Cisco Security Agent
Status
Messages
User Query Responses (1)
Contact Information
System Security
Untrusted Applications (54)
Security level:
Off
Low
Medium
High
Prevent new network connections:
Network Lock
Enable Network Lock after the specified network inactivity time:
0
minutes
Install/Uninstall detected:
When install/uninstall is finished, click Resume to restore normal security.
Resume
OK
Cancel
Apply
Help
Security: Medium

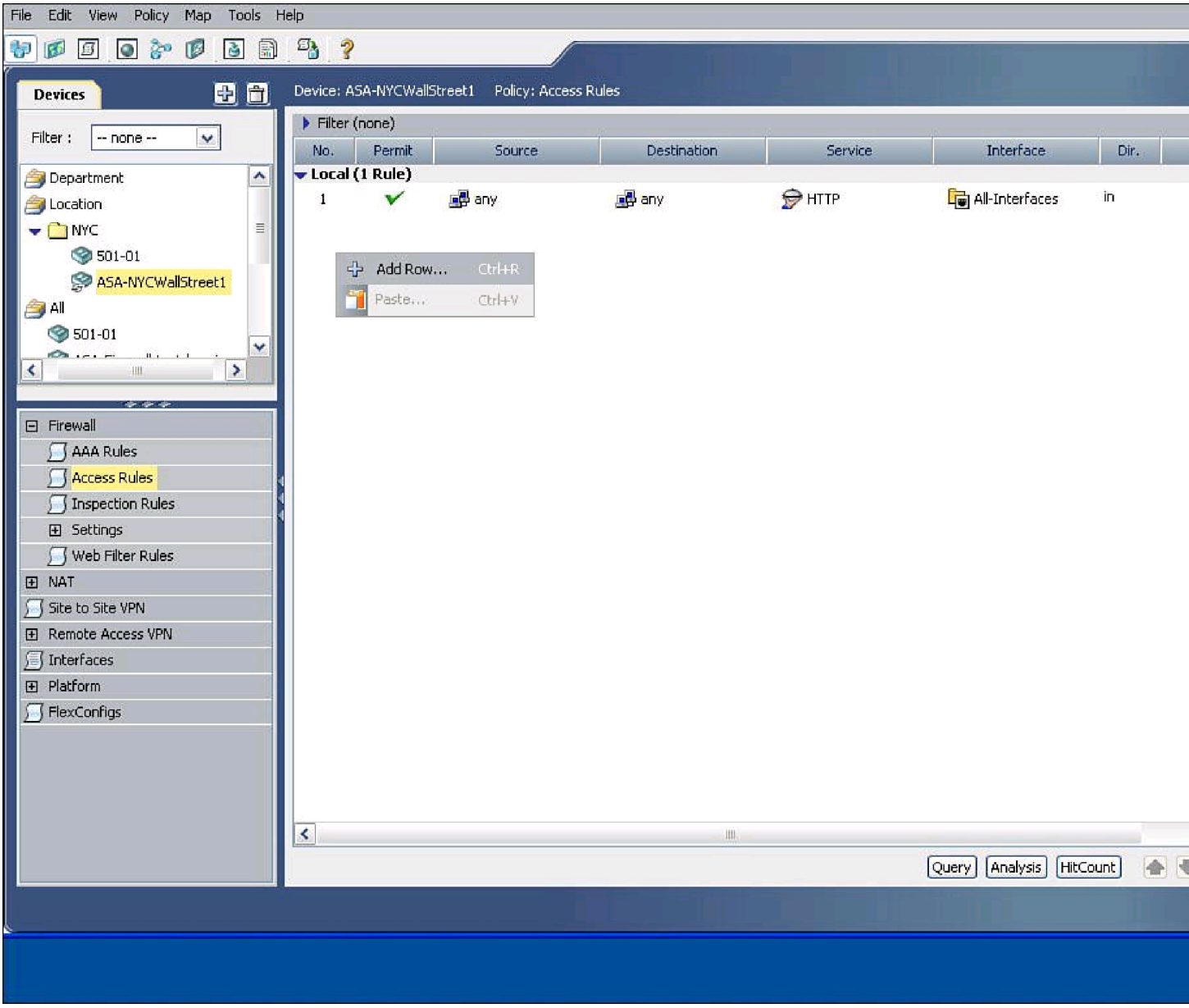

Cisco Security Agent
Status
Messages
User Query Responses (1)
Contact Information
System Security
Untrusted Applications (54)
These applications are initially listed as untrusted by current security policies. They may execute with restrictions. Delete an application from this list to remove these restrictions.
Application Data\Adobe\Acrobat\6.0\Updater\udstore.js
,Application Data\Macromedia\Flash Player\#SharedObjects\SN8YTCU6\static.espn.go.
,Application Data\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys\#
,Application Data\MagneticTime\summarydata\FW_ Cisco 877W ISR in trustedreviews.c
,Application Data\Microsoft\Media Player\00114582.wpl
,Application Data\Sun\Java\Deployment\cache\javapi\v1.0\jar\Chooser.jar-42ba930-5
,Application Data\Sun\Java\Deployment\cache\javapi\v1.0\jar\Chooser.jar-78e80a19-5
,Application Data\Sun\Java\Deployment\cache\javapi\v1.0\jar\MeetingServer.jar-3ac1
,Application Data\Sun\Java\Deployment\cache\javapi\v1.0\jar\MeetingServer.jar-4604
,Local Settings\Temporary Internet Files\OLK9D\Case Study in The Health Care Industr
OK
Cancel
Apply
Help
Security: Medium

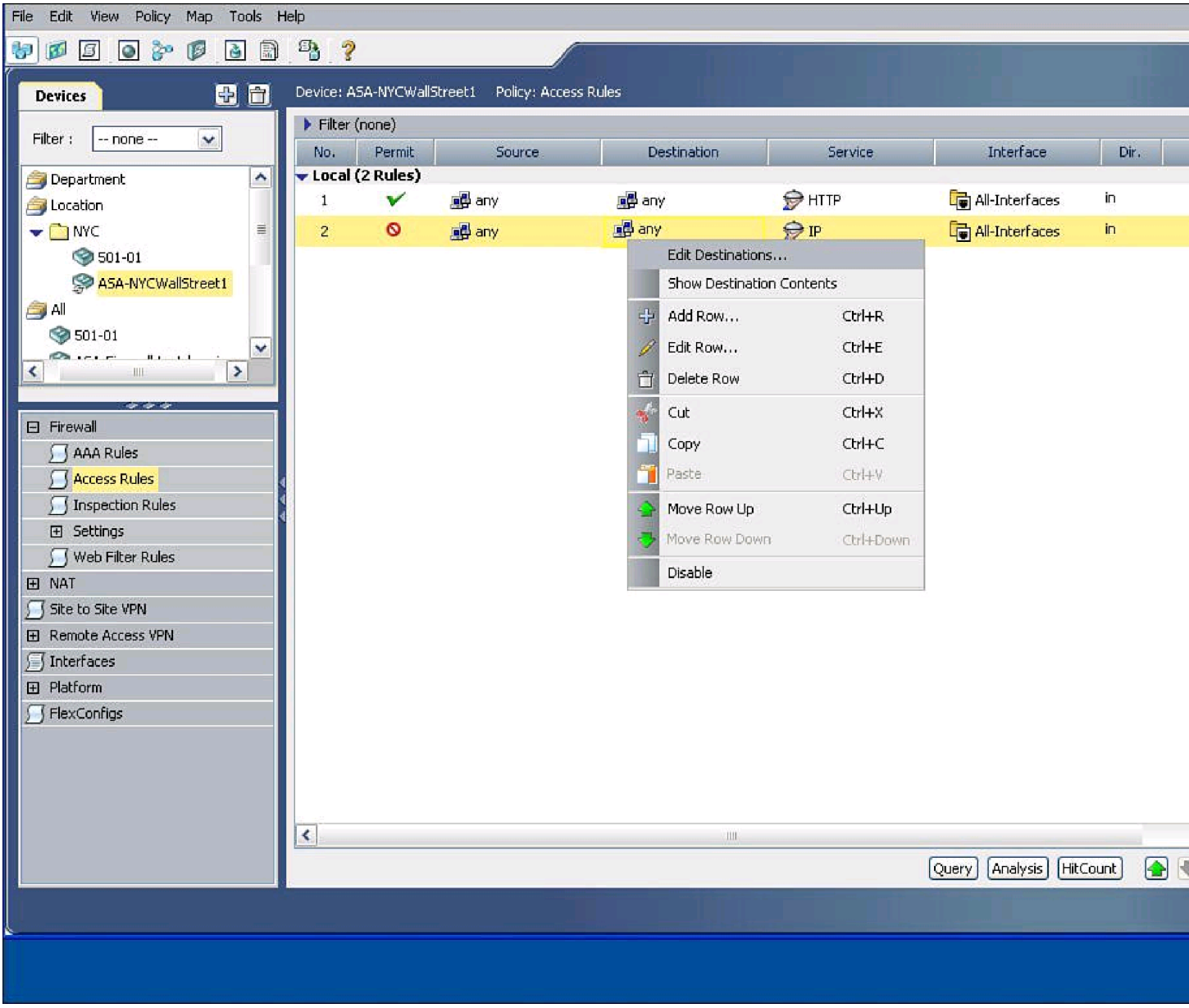

JumpStart
JumpStart provides an overview of Cisco Security Manager and guidelines for using it to simplify security management.
Need more information? Use the Details links in the JumpStart pages to access detailed online help.
Overview
Add Device
Configure
Deploy
add
configure
deploy
The typical taskflow is simple: First add devices to Cisco Security Manager, then configure your security settings and policies, and then deploy these configurations to your devices.

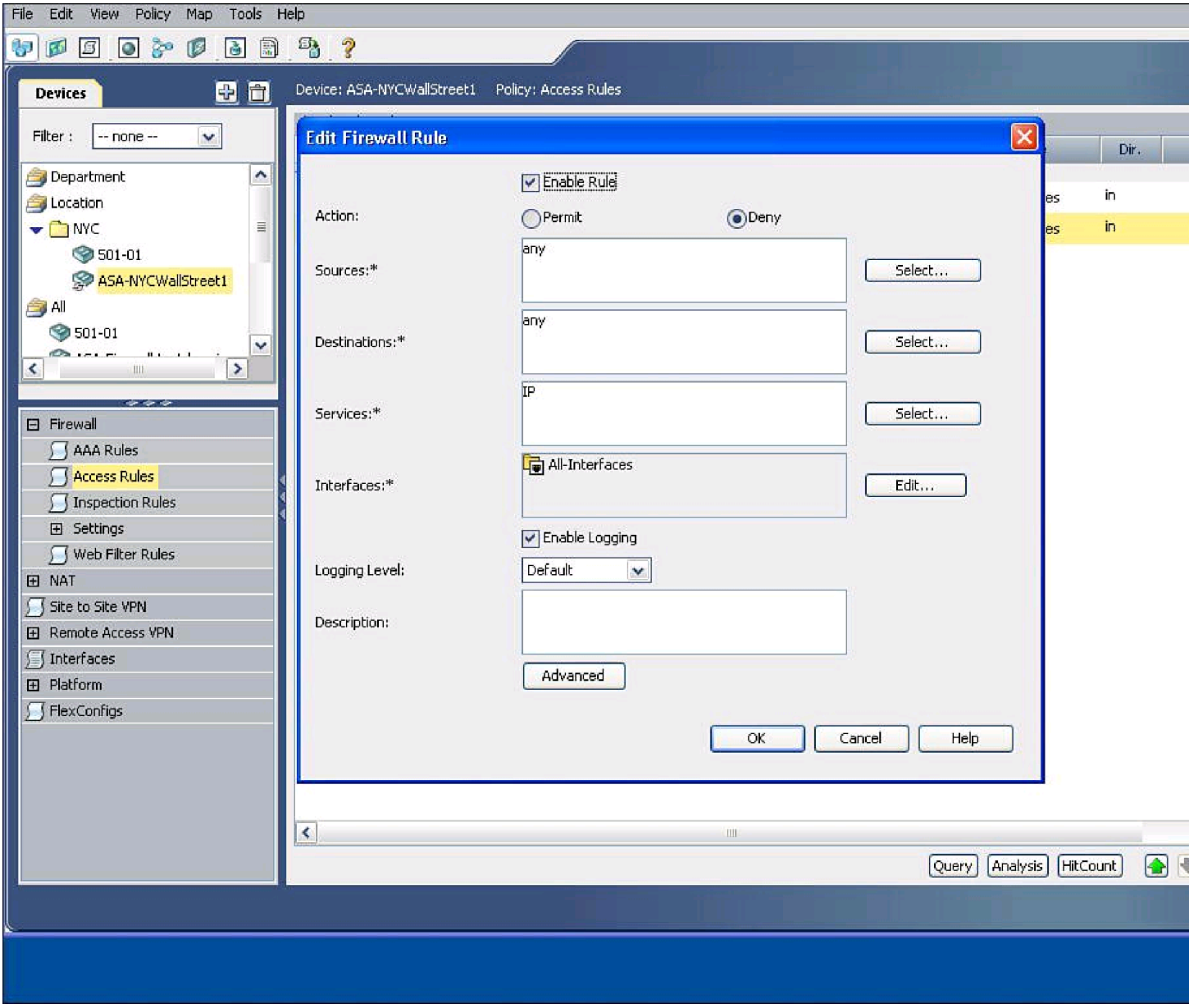

New Device - Device Credentials (Step 3 of 4)
Primary Credentials
Username:
asawallstreet1
Password:
Confirm:
Enable Password:
Confirm:
SDEE Credentials
Username:
Password:
Confirm:
HTTP Credentials
HTTP Port:
80
HTTPS Port:
443
Certificate Common Name:
Confirm:
Mode:
HTTPS
RX-Boot Mod...
SNMP...
Back
Next
Finish
Cancel
Help

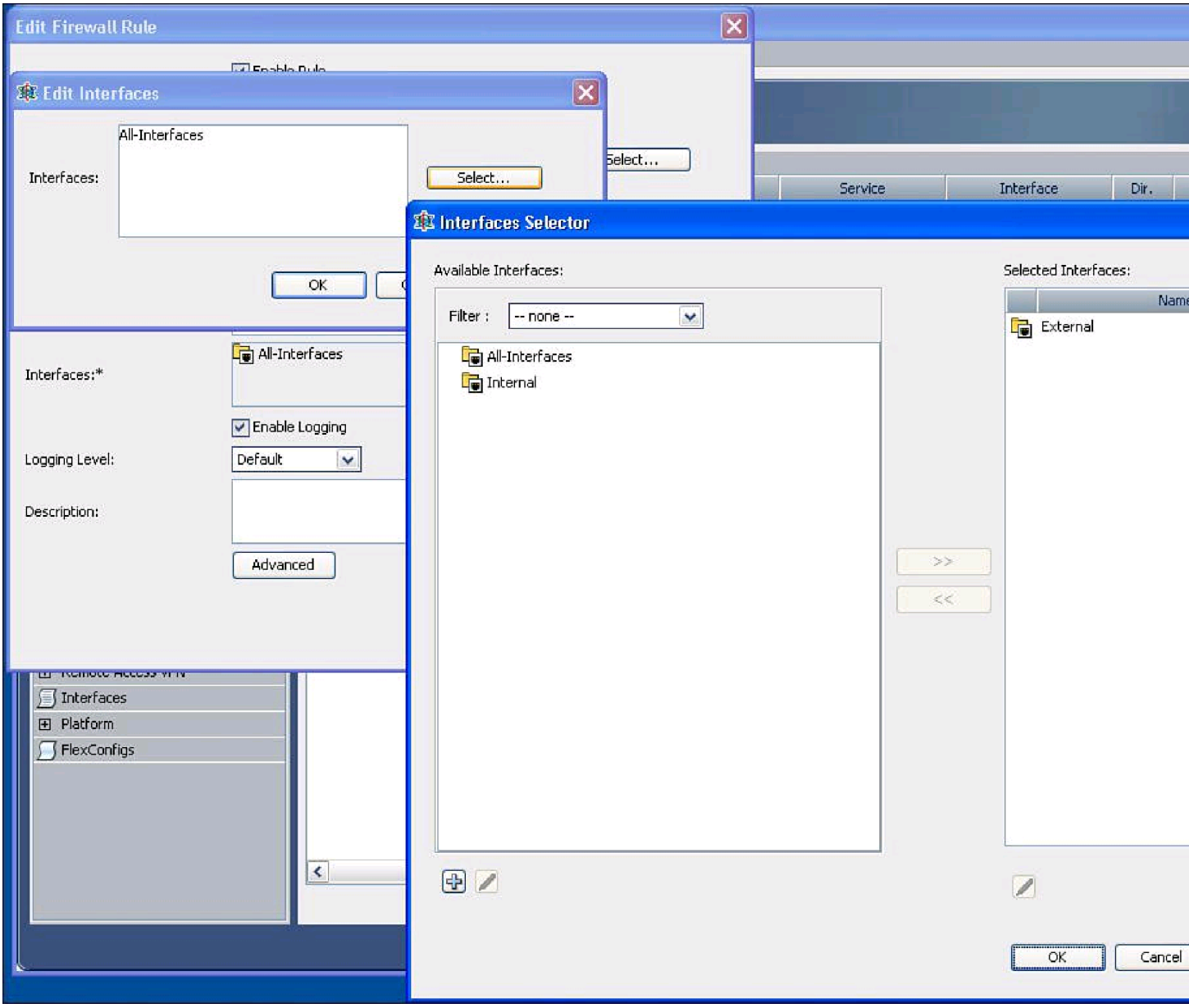

New Device - Device Grouping (Step 4 of 4)
Select the groups that this device belongs to:
Americas:
None
Department:
None
Geography:
None
Location:
New York
Set Values as Default
Back
Next
Finish
Cancel
Help

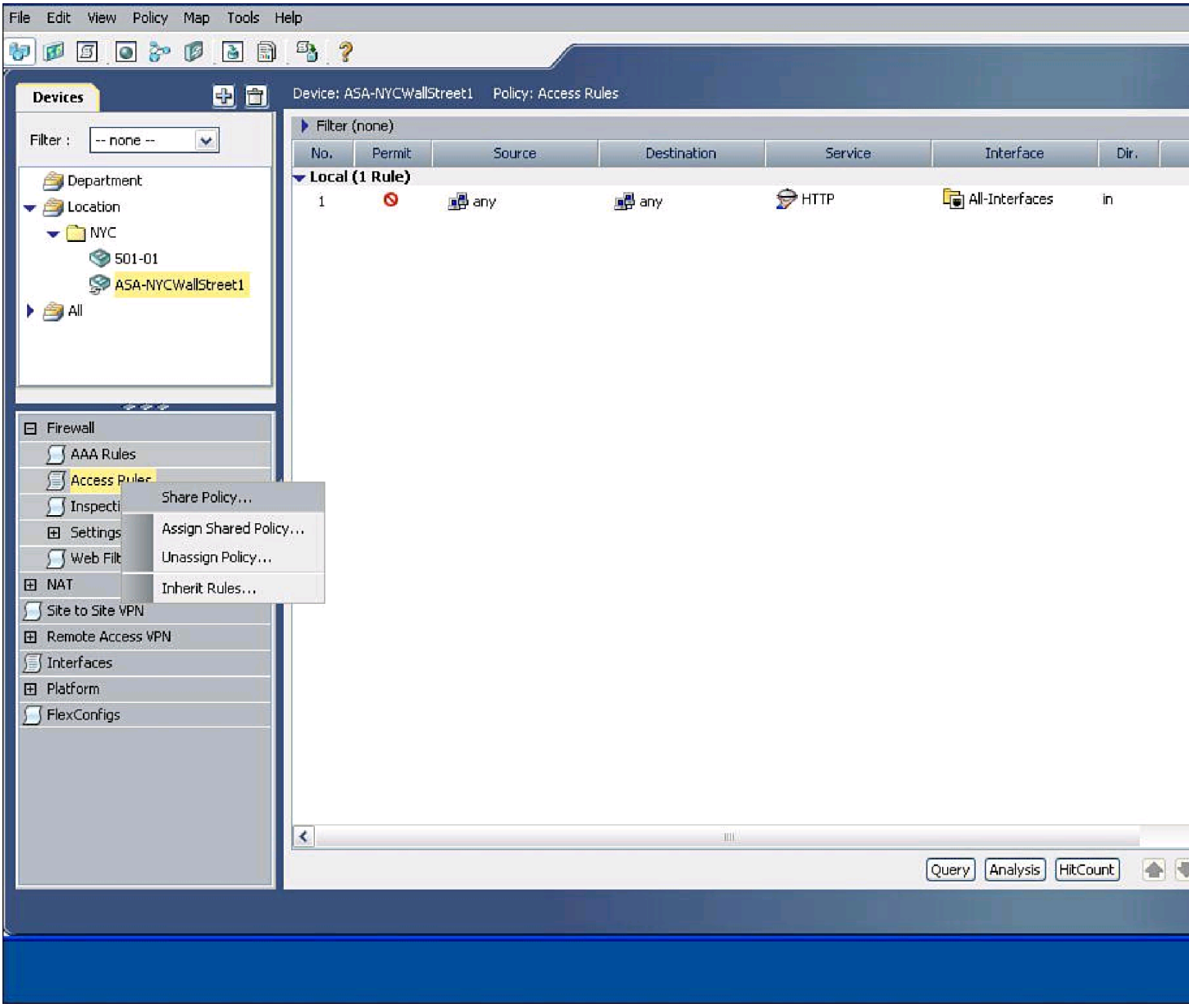

Device Properties
General
Credentials
Device Groups
Policy Object Overrides
Device: ASA-NYC-WallStreet1 Property: Credentials
Primary Credentials
Username:
Password:
Confirm:
Enable Password:
Confirm:
SDEE Credentials
Username:
Password:
Confirm:
HTTP Credentials
HTTP Port:
80
HTTPS Port:
443
Certificate Common Name:
Confirm:
Mode:
HTTPS
RX-Boot Mode...
SNMP...

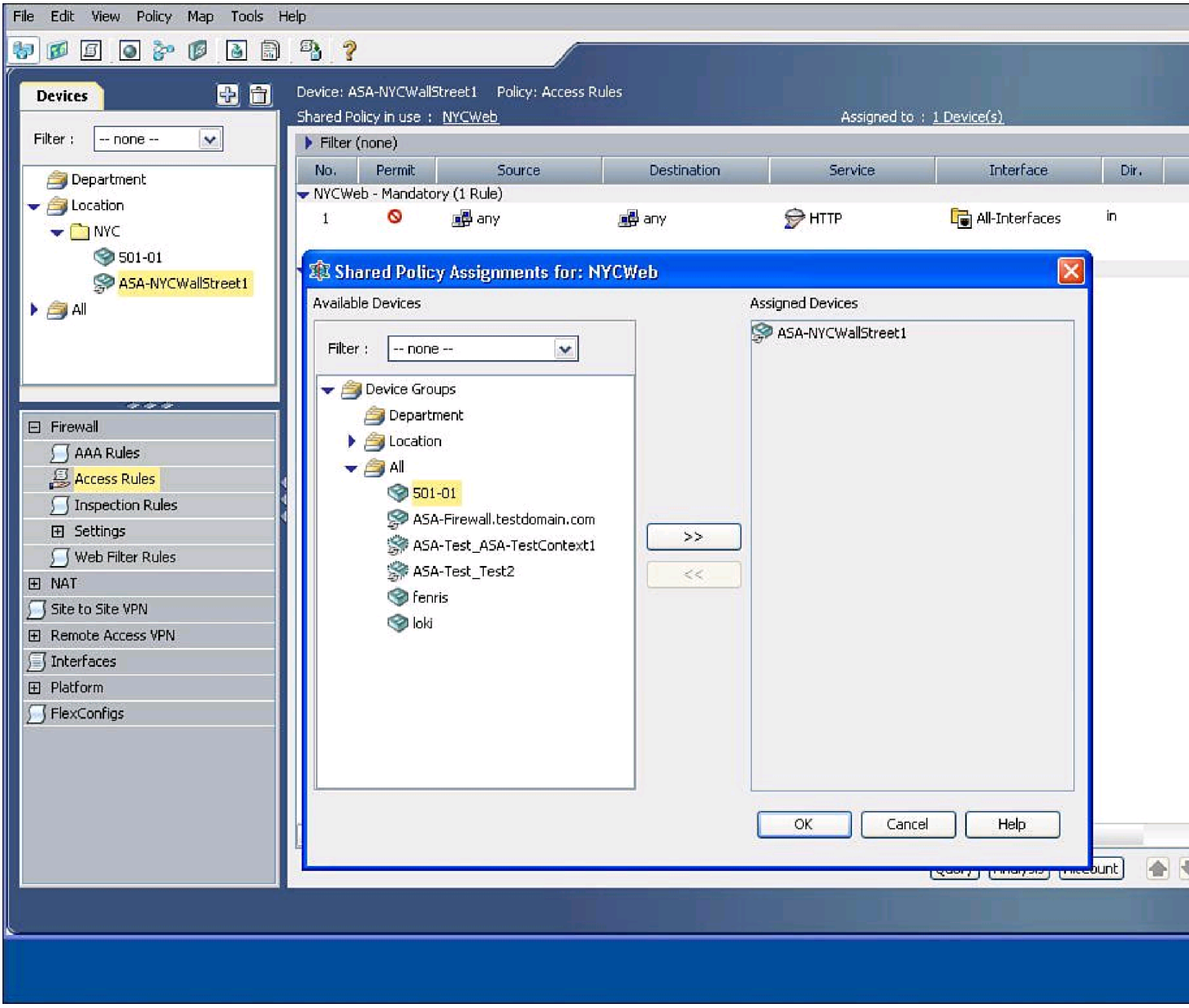

File Edit View Policy Map Tools Help
Devices
Filter : -- none --
Department
Location
NYC
501-01
ASA-NYCWallStreet1
All
501-01
Device: ASA-NYCWallStreet1 Policy: Access Rules
Filter (none)
No. Permit Source Destination Service Interface Dir.
Local (1 Rule)
1 any any HTTP All-Interfaces in
Add Row... Ctrl+R
Paste... Ctrl+V
Firewall
AAA Rules
Access Rules
Inspection Rules
Settings
Web Filter Rules
NAT
Site to Site VPN
Remote Access VPN
Interfaces
Platform
FlexConfigs
Query
Analysis
HitCount

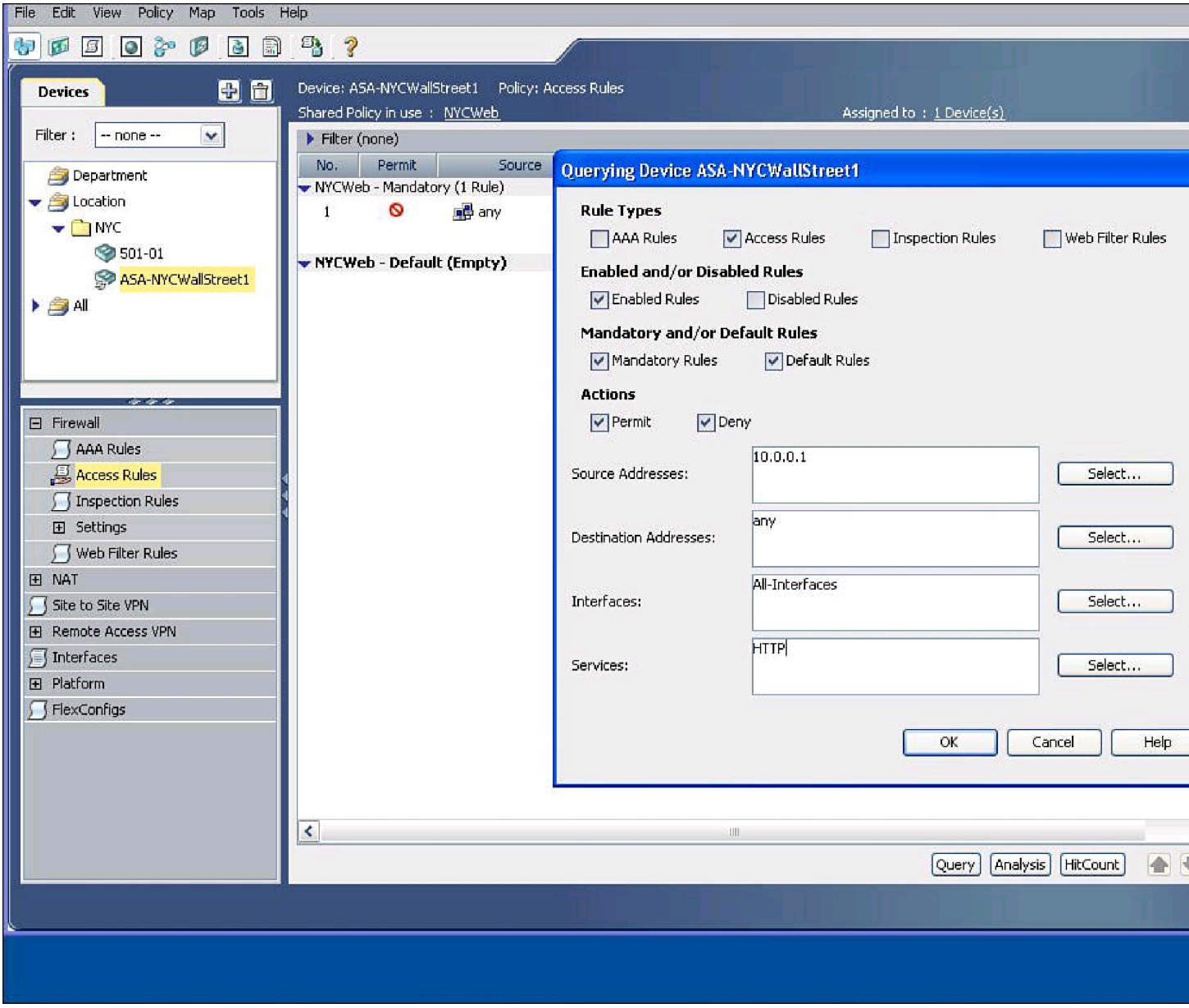

File Edit View Policy Map Tools Help
Devices
Filter : -- none --
Department
Location
NYC
501-01
ASA-NYCWallStreet1
All
501-01
Firewall
AAA Rules
Access Rules
Inspection Rules
Settings
Web Filter Rules
NAT
Site to Site VPN
Remote Access VPN
Interfaces
Platform
FlexConfigs
Device: ASA-NYCWallStreet1 Policy: Access Rules
Filter (none)
No. Permit Source Destination Service Interface Dir.
Local (2 Rules)
1 any any HTTP All-Interfaces in
2 any any IP All-Interfaces in
Edit Destinations...
Show Destination Contents
Add Row... Ctrl+R
Edit Row... Ctrl+E
Delete Row Ctrl+D
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Move Row Up Ctrl+Up
Move Row Down Ctrl+Down
Disable
Query
Analysis
HitCount

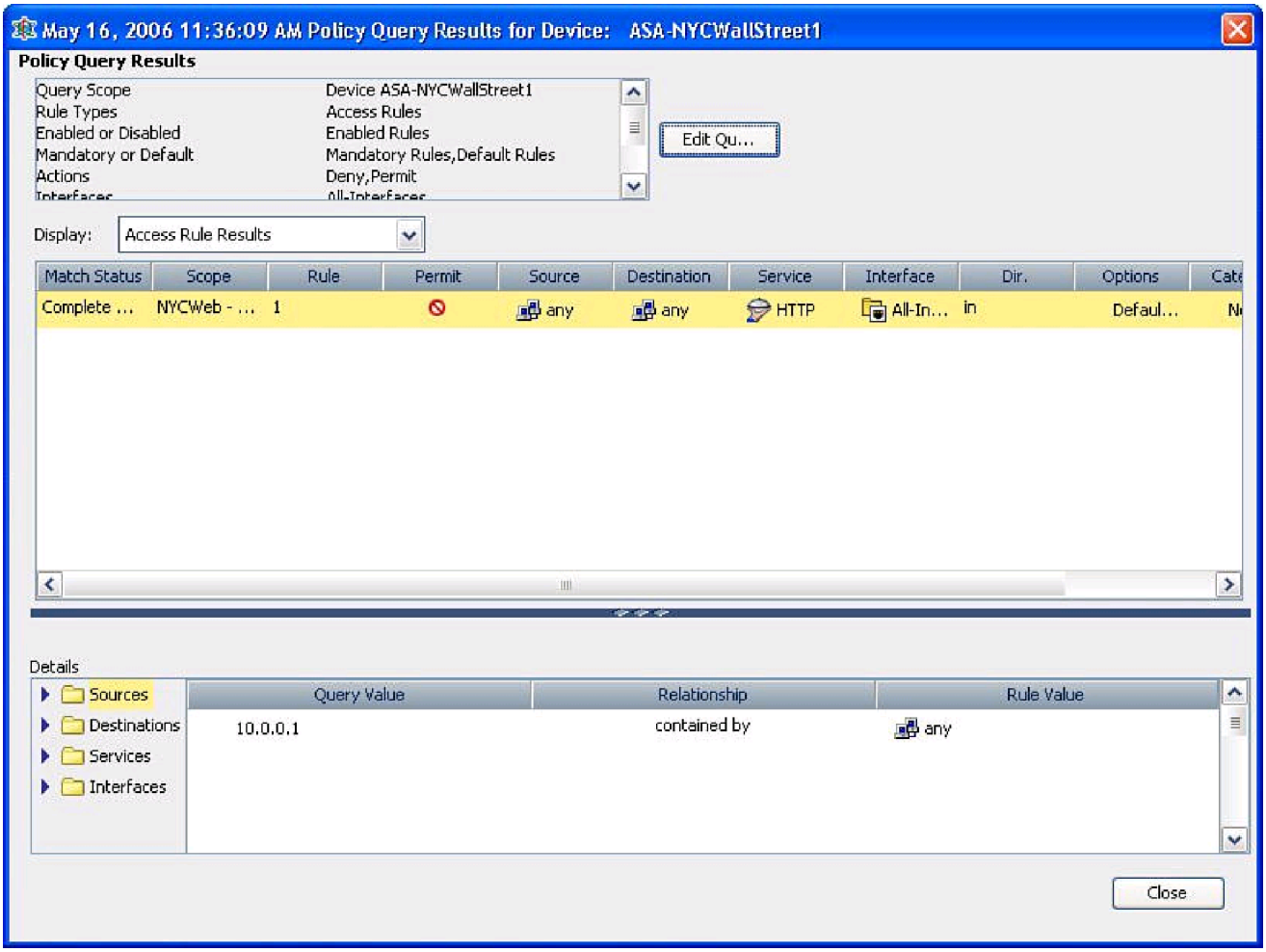

File Edit View Policy Map Tools Help
Devices
Filter : -- none --
Department
Location
NYC
501-01
ASA-NYCWallStreet1
All
501-01
Device: ASA-NYCWallStreet1 Policy: Access Rules
Firewall
AAA Rules
Access Rules
Inspection Rules
Settings
Web Filter Rules
NAT
Site to Site VPN
Remote Access VPN
Interfaces
Platform
FlexConfigs
Edit Firewall Rule
Enable Rule
Action:
Permit
Deny
Sources:*
any
Select...
Destinations:*
any
Select...
Services:*
IP
Select...
Interfaces:*
All-Interfaces
Edit...
Enable Logging
Logging Level:
Default
Description:
Advanced
OK
Cancel
Help
Dir.
in
in
Query
Analysis
HitCount

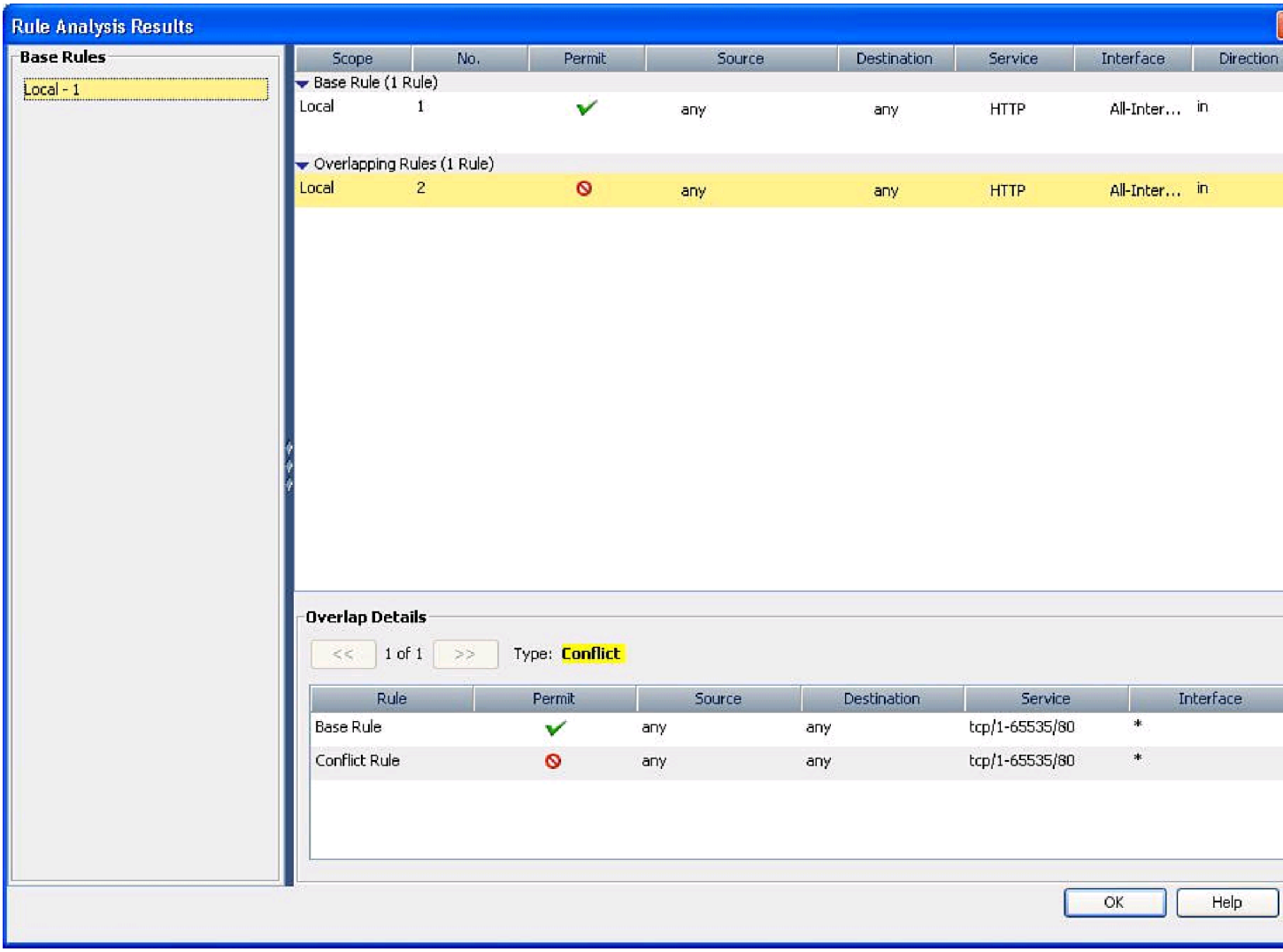

Edit Firewall Rule
Edit Interfaces
All-Interfaces
Interfaces:
Select...
OK
Service
Interface
Dir.
Interfaces Selector
Available Interfaces:
Selected Interfaces:
Filter :
-- none --
All-Interfaces
Internal
External
Interfaces:*
Enable Logging
Logging Level:
Default
Description:
Advanced
>>
<<
Interfaces
Platform
FlexConfigs
OK
Cancel

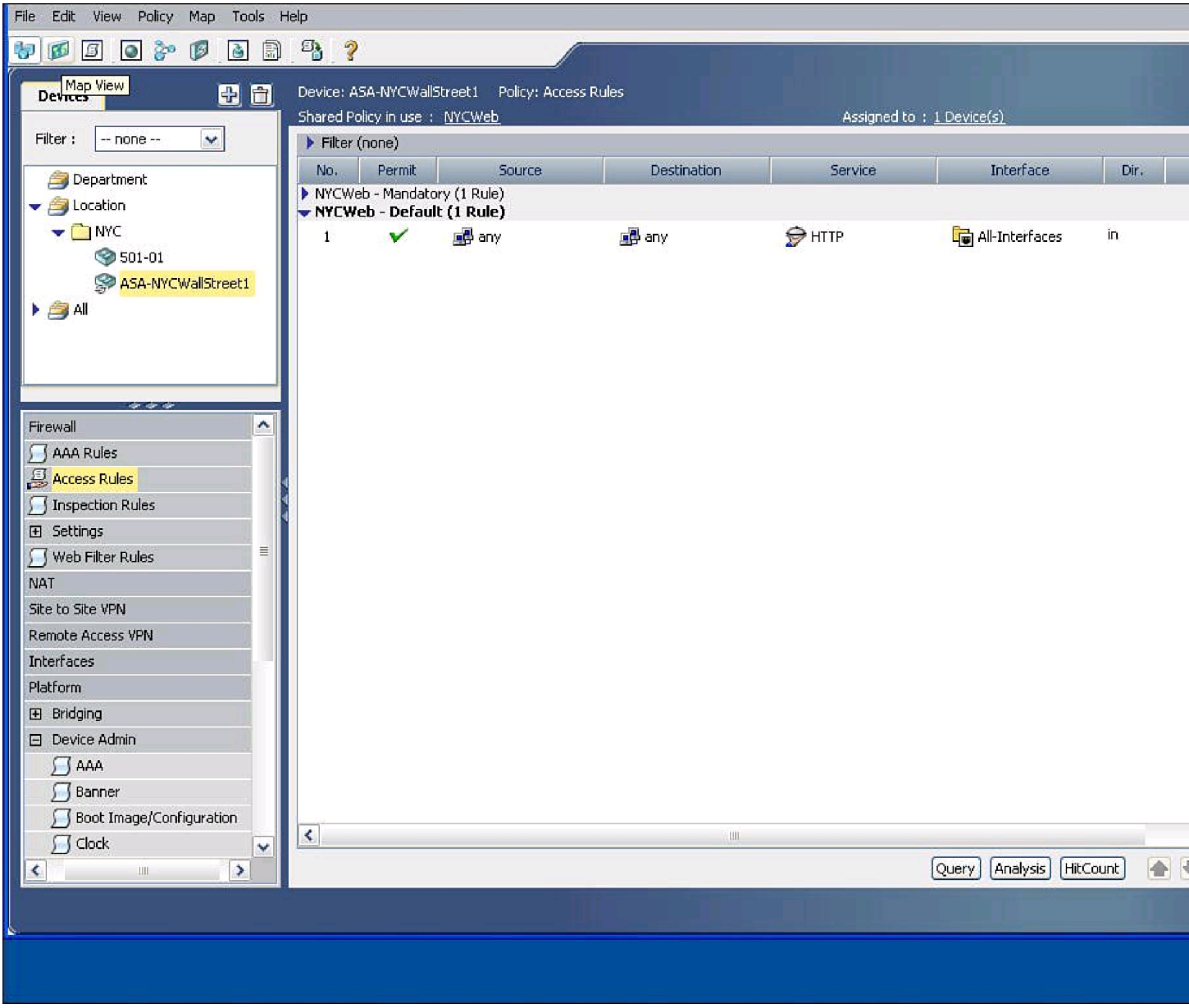

File Edit View Policy Map Tools Help
Devices
Device: ASA-NYCWallStreet1 Policy: Access Rules
Filter : -- none --
Department
Location
NYC
501-01
ASA-NYCWallStreet1
All
Filter (none)
No. Permit Source Destination Service Interface Dir.
Local (1 Rule)
1 any any HTTP All-Interfaces in
Firewall
AAA Rules
Access Rules
Inspecti
Settings
Web Filt
NAT
Site to Site VPN
Remote Access VPN
Interfaces
Platform
FlexConfigs
Share Policy...
Assign Shared Policy...
Unassign Policy...
Inherit Rules...
Query
Analysis
HitCount

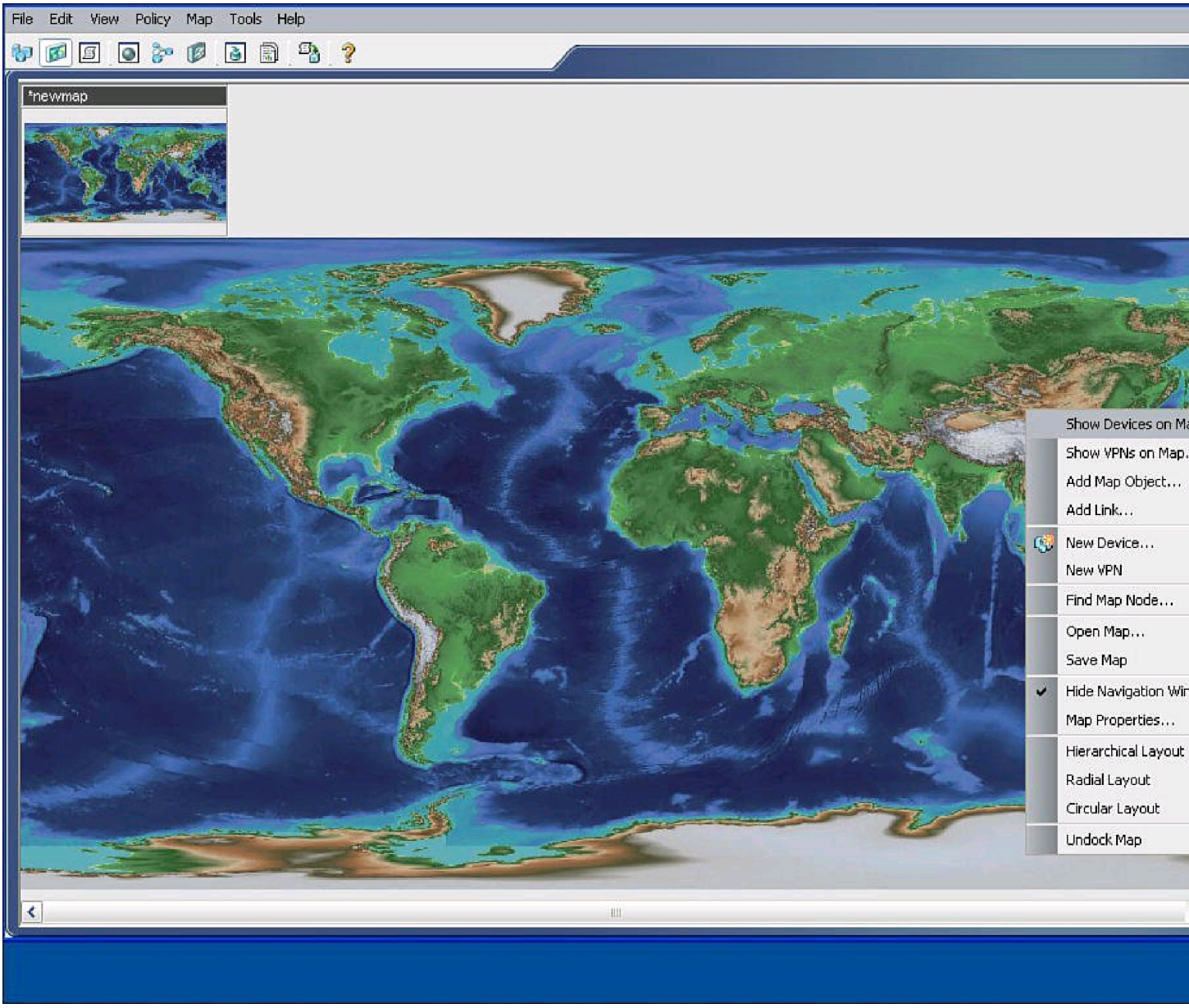

File Edit View Policy Map Tools Help
Devices
Filter : -- none --
Department
Location
NYC
501-01
ASA-NYCWallStreet1
All
Firewall
AAA Rules
Access Rules
Inspection Rules
Settings
Web Filter Rules
NAT
Site to Site VPN
Remote Access VPN
Interfaces
Platform
FlexConfigs
Device: ASA-NYCWallStreet1 Policy: Access Rules
Shared Policy in use : NYCWeb
Assigned to : 1 Device(s)
Filter (none)
No. Permit Source Destination Service Interface Dir.
NYCWeb - Mandatory (1 Rule)
1 any any HTTP All-Interfaces in
Shared Policy Assignments for: NYCWeb
Available Devices
Filter : -- none --
Device Groups
Department
Location
All
501-01
ASA-Firewall.testdomain.com
ASA-Test_ASA-TestContext1
ASA-Test_Test2
fenris
loki
>>
<<
Assigned Devices
ASA-NYCWallStreet1
OK
Cancel
Help

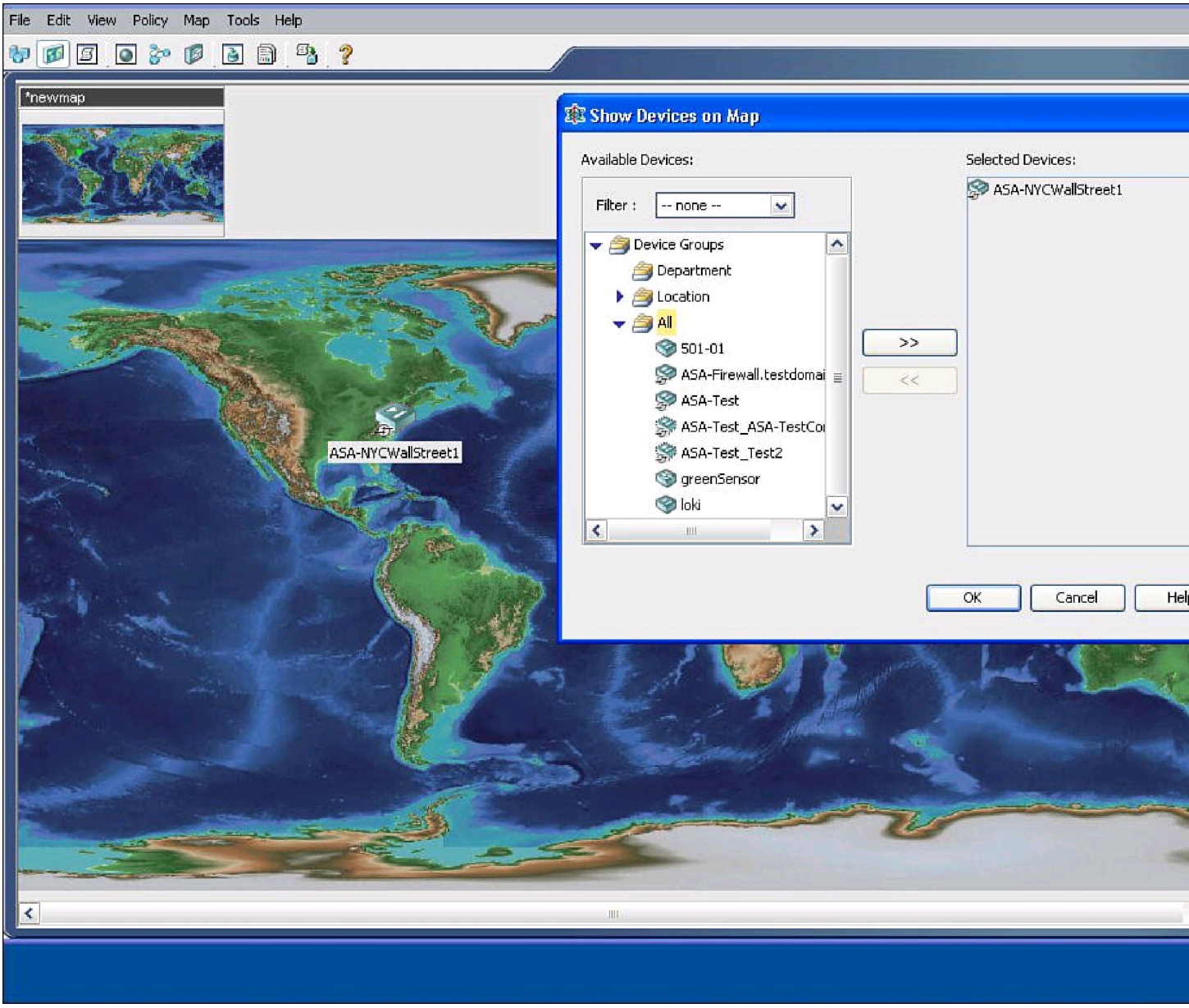

File Edit View Policy Map Tools Help
Devices
Filter : -- none --
Department
Location
NYC
501-01
ASA-NYCWallStreet1
All
Firewall
AAA Rules
Access Rules
Inspection Rules
Settings
Web Filter Rules
NAT
Site to Site VPN
Remote Access VPN
Interfaces
Platform
FlexConfigs
Device: ASA-NYCWallStreet1 Policy: Access Rules
Shared Policy in use : NYCWeb
Assigned to : 1 Device(s)
Filter (none)
No. Permit Source
NYCWeb - Mandatory (1 Rule)
1 any
NYCWeb - Default (Empty)
Querying Device ASA-NYCWallStreet1
Rule Types
AAA Rules
Access Rules
Inspection Rules
Web Filter Rules
Enabled and/or Disabled Rules
Enabled Rules
Disabled Rules
Mandatory and/or Default Rules
Mandatory Rules
Default Rules
Actions
Permit
Deny
Source Addresses:
10.0.0.1
Select...
Destination Addresses:
any
Select...
Interfaces:
All-Interfaces
Select...
Services:
HTTP
Select...
OK
Cancel
Help
Query
Analysis
HitCount

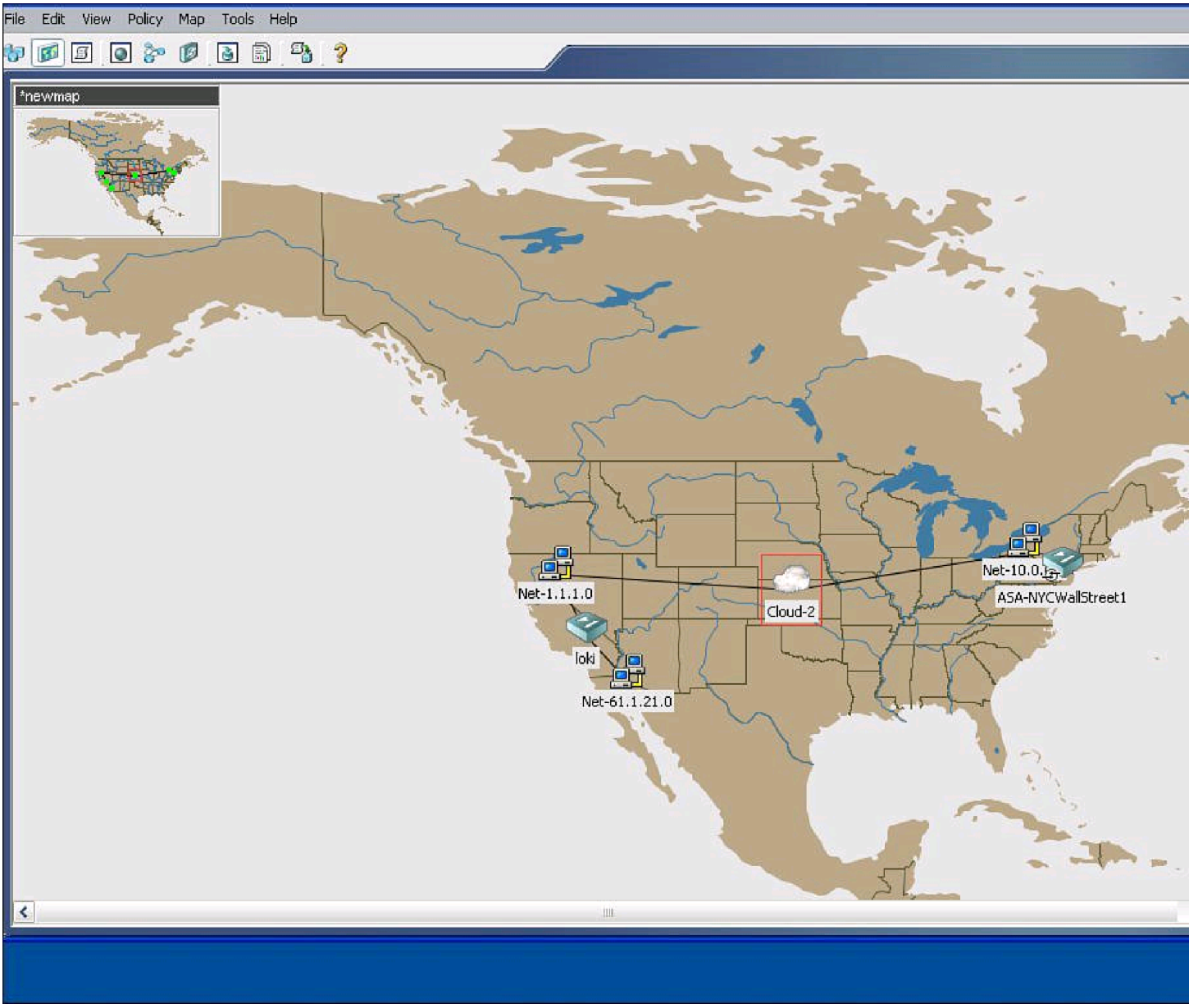

May 16, 2006 11:36:09 AM Policy Query Results for Device: ASA-NYCWallStreet1
Policy Query Results
Query Scope
Device ASA-NYCWallStreet1
Rule Types
Access Rules
Enabled or Disabled
Enabled Rules
Mandatory or Default
Mandatory Rules,Default Rules
Actions
Deny,Permit
Edit Qu...
Display:
Access Rule Results
Match Status
Scope
Rule
Permit
Source
Destination
Service
Interface
Dir.
Options
Complete ...
NYCWeb - ...
1
any
any
HTTP
All-In...
in
Defaul...
Details
Sources
Destinations
Services
Interfaces
Query Value
Relationship
Rule Value
10.0.0.1
contained by
any
Close

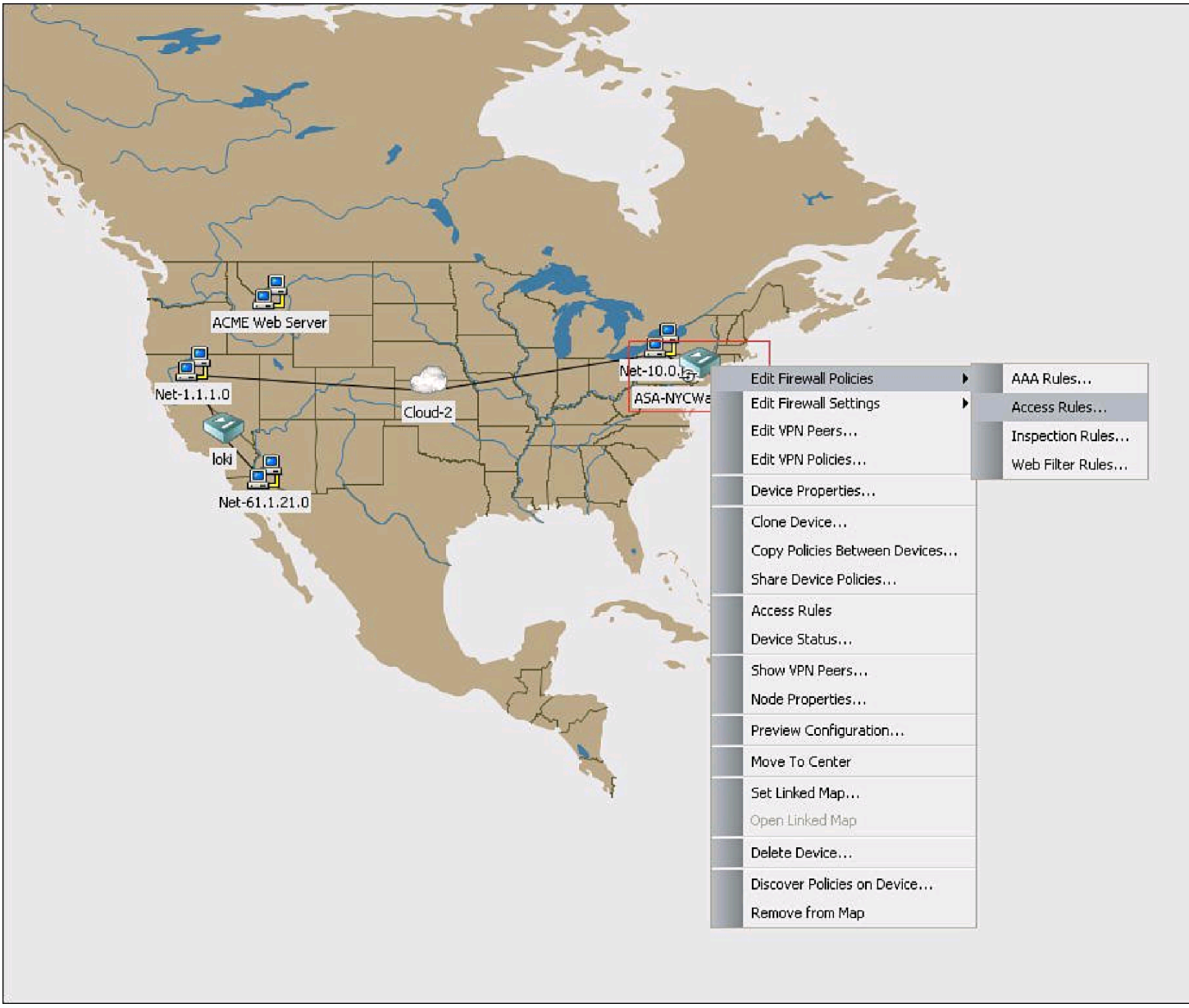

Rule Analysis Results
Base Rules
Local - 1
Scope
No.
Permit
Source
Destination
Service
Interface
Direction
Base Rule (1 Rule)
Local
1
any
any
HTTP
All-Inter...
in
Overlapping Rules (1 Rule)
Local
2
any
any
HTTP
All-Inter...
in
Overlap Details
<<
1 of 1
>>
Type: Conflict
Rule
Permit
Source
Destination
Service
Interface
Base Rule
any
any
tcp/1-65535/80
*
Conflict Rule
any
any
tcp/1-65535/80
*
OK
Help

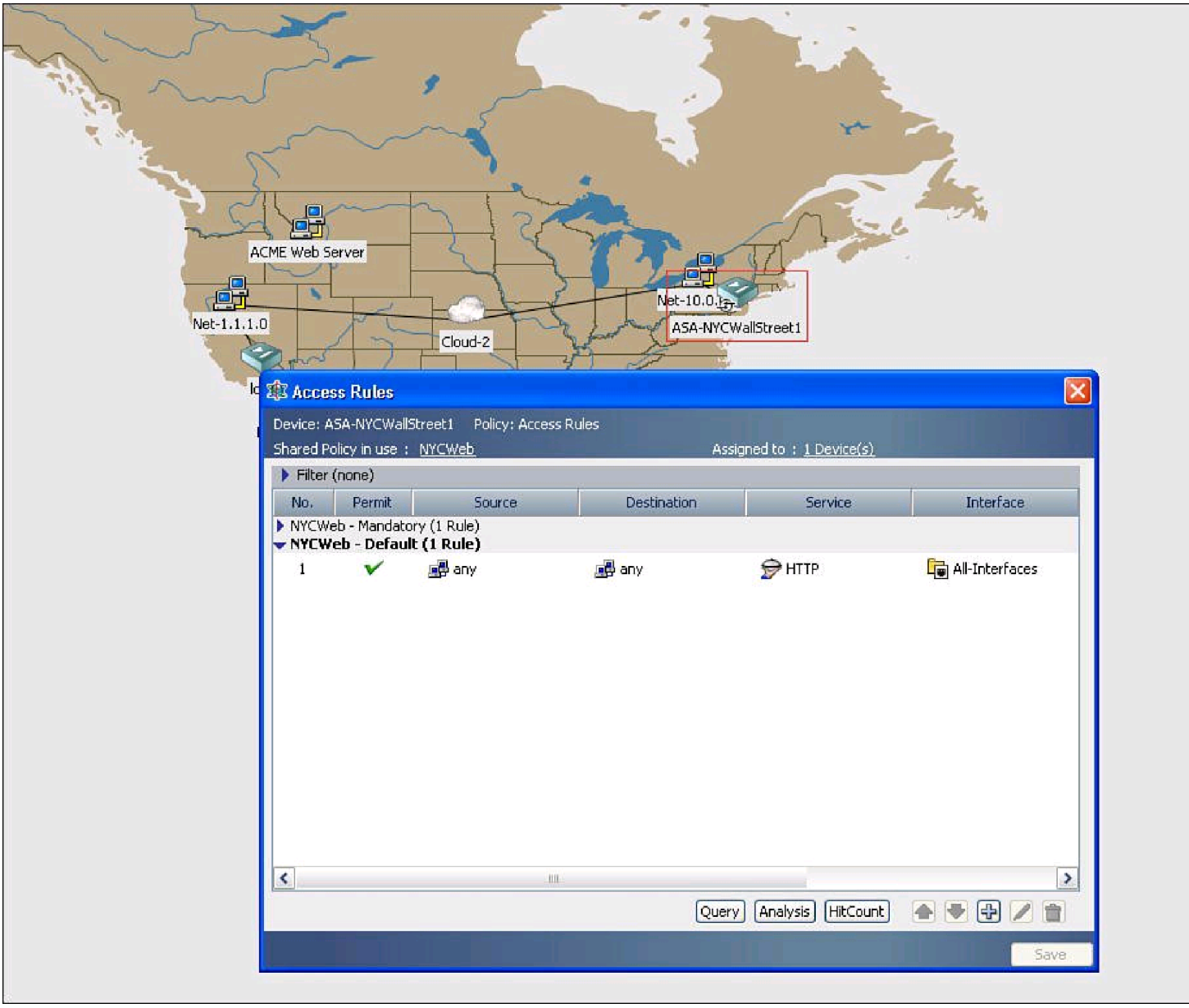

File Edit View Policy Map Tools Help
Map View
Devices
Filter : -- none --
Department
Location
NYC
501-01
ASA-NYCWallStreet1
All
Firewall
AAA Rules
Access Rules
Inspection Rules
Settings
Web Filter Rules
NAT
Site to Site VPN
Remote Access VPN
Interfaces
Platform
Bridging
Device Admin
AAA
Banner
Boot Image/Configuration
Clock
Device: ASA-NYCWallStreet1 Policy: Access Rules
Shared Policy in use : NYCWeb
Assigned to : 1 Device(s)
Filter (none)
No. Permit Source Destination Service Interface Dir.
NYCWeb - Mandatory (1 Rule)
NYCWeb - Default (1 Rule)
1 any any HTTP All-Interfaces in
Query Analysis HitCount

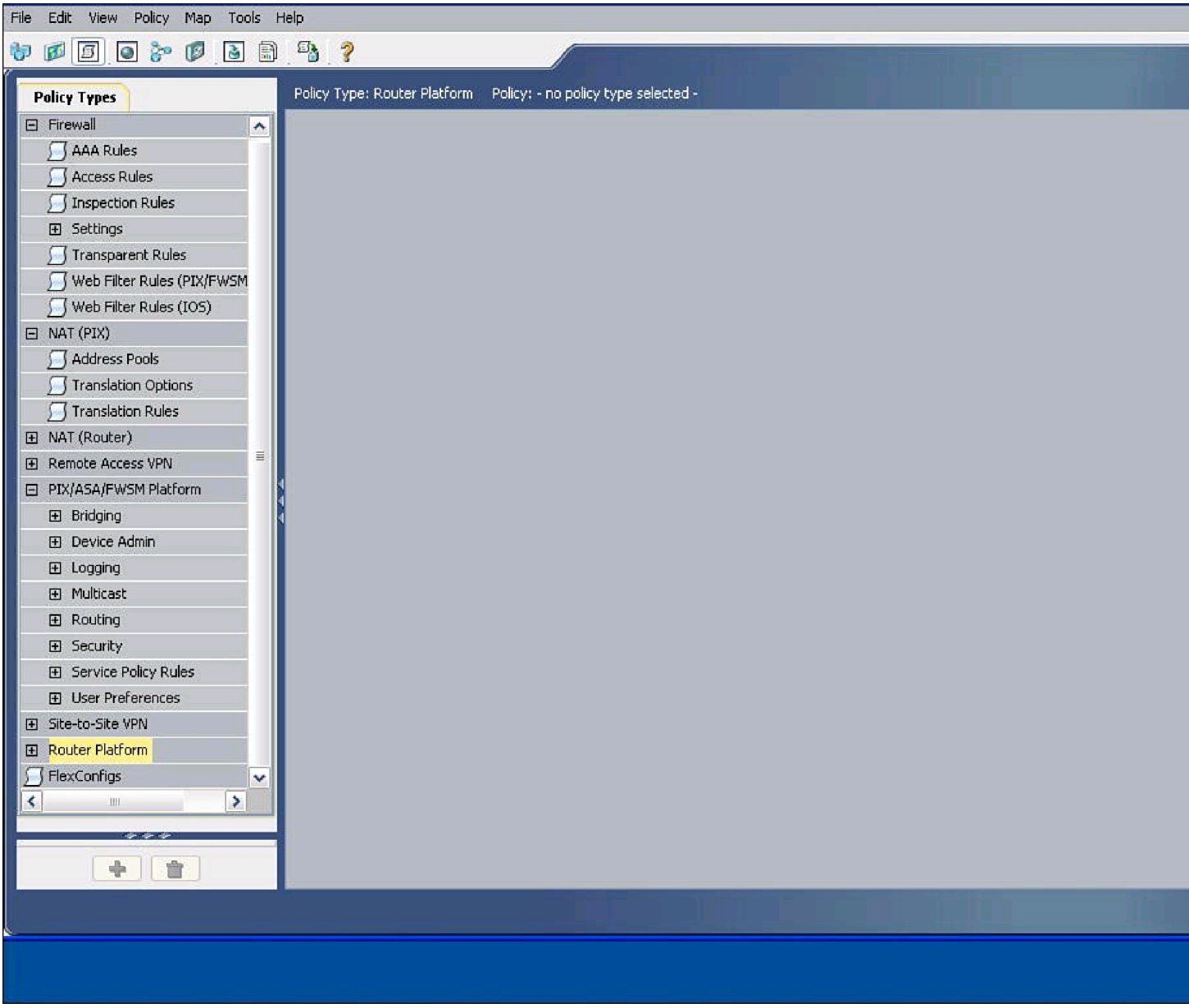

File
Edit
View
Policy
Map
Tools
Help
*newmap
Show Devices on Ma
Show VPNs on Map
Add Map Object...
Add Link...
New Device...
New VPN
Find Map Node...
Open Map...
Save Map
Hide Navigation Win
Map Properties...
Hierarchical Layout
Radial Layout
Circular Layout
Undock Map

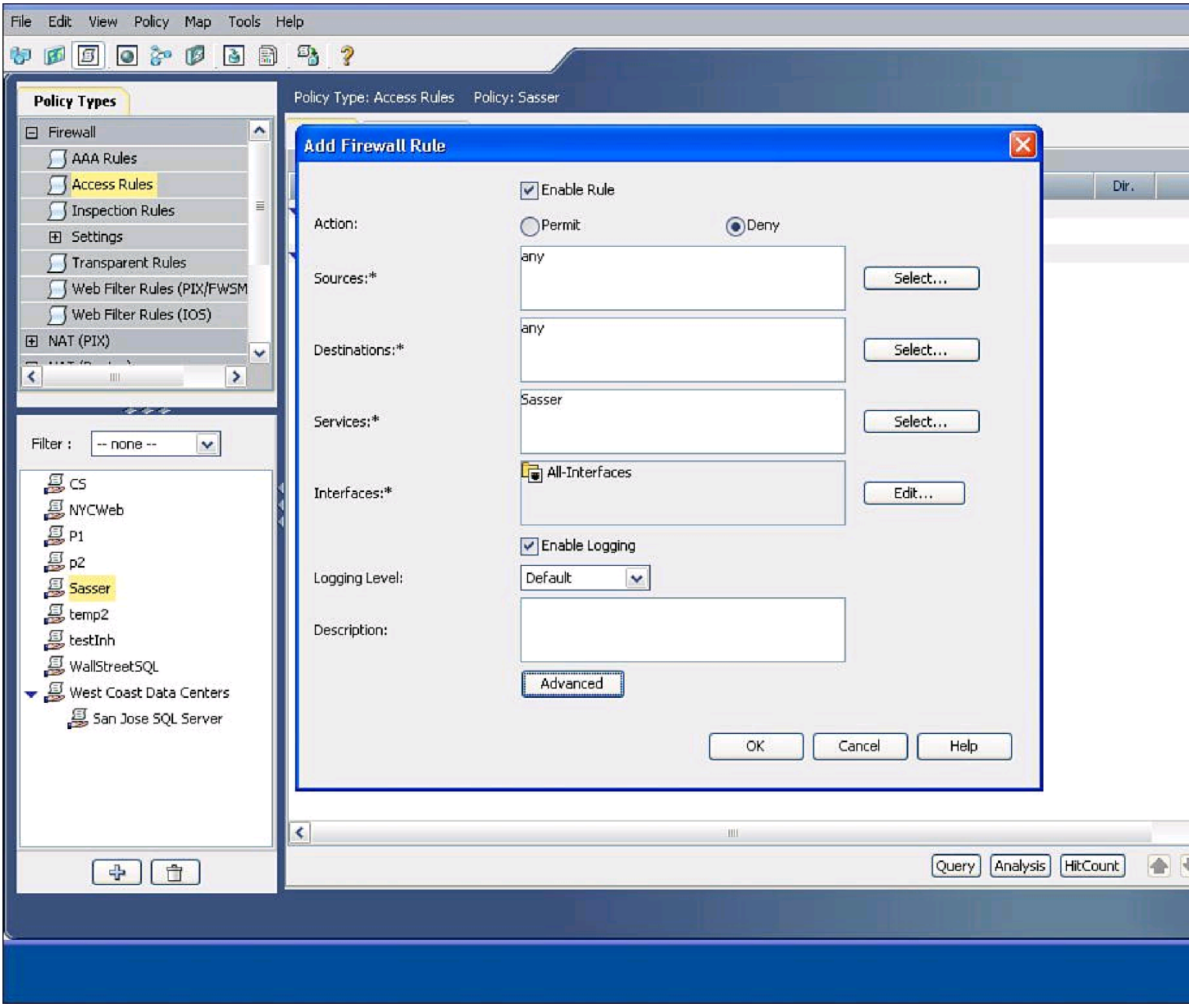

File
Edit
View
Policy
Map
Tools
Help
*newmap
ASA-NYCWallStreet1
Show Devices on Map
Available Devices:
Filter :
-- none --
Device Groups
Department
Location
All
501-01
ASA-Firewall.testdomai
ASA-Test
ASA-Test_ASA-TestCo
ASA-Test_Test2
greenSensor
loki
>>
<<
Selected Devices:
ASA-NYCWallStreet1
OK
Cancel

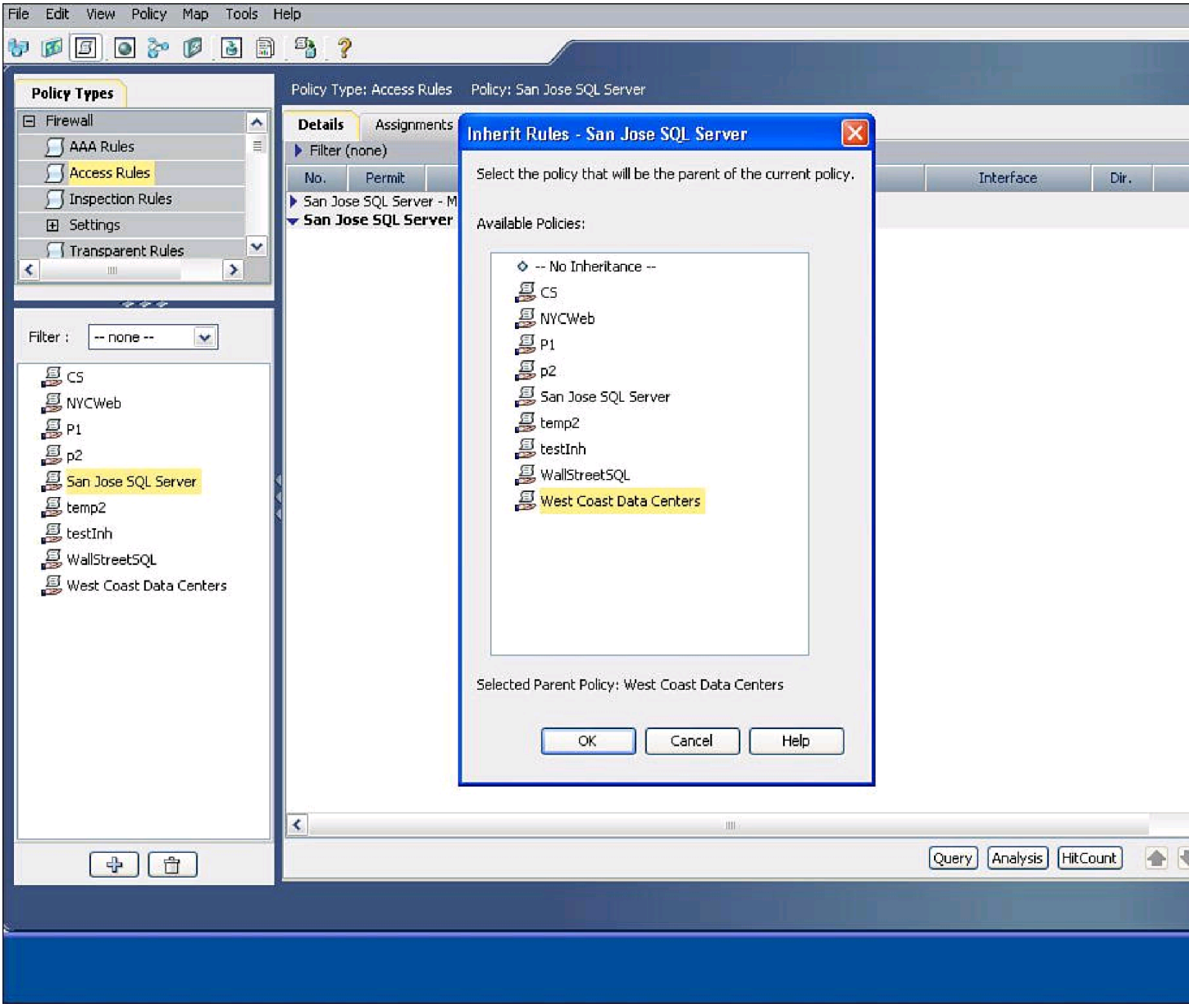

File Edit View Policy Map Tools Help
*newmap
Net-1.1.1.0
Cloud-2
Net-10.0.1.0
ASA-NYCWallStreet1
loki
Net-61.1.21.0

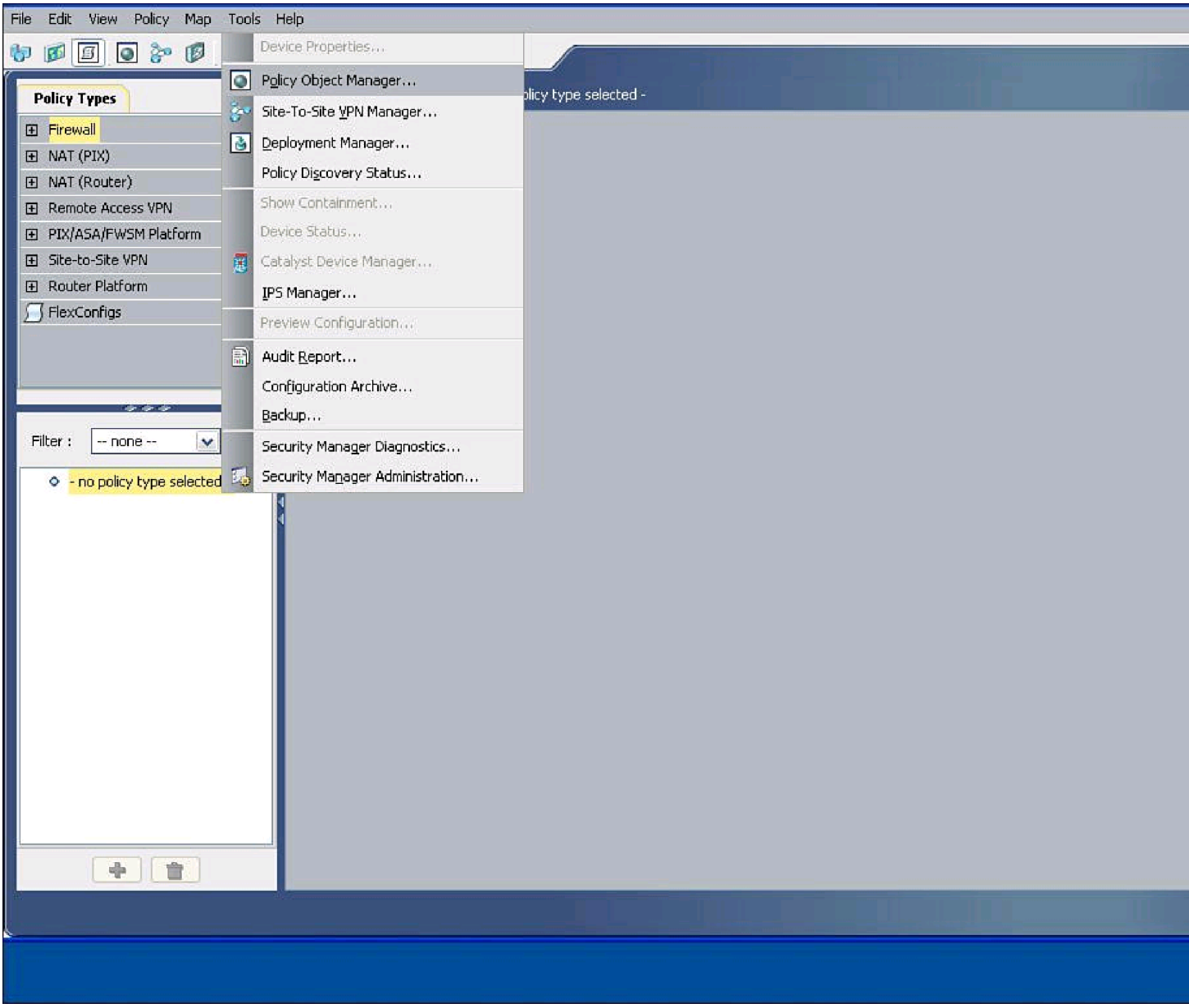

ACME Web Server
Net-1.1.1.0
Cloud-2
loki
Net-61.1.21.0
Net-10.0.1
ASA-NYCWa
Edit Firewall Policies
Edit Firewall Settings
Edit VPN Peers...
Edit VPN Policies...
Device Properties...
Clone Device...
Copy Policies Between Devices...
Share Device Policies...
Access Rules
Device Status...
Show VPN Peers...
Node Properties...
Preview Configuration...
Move To Center
Set Linked Map...
Open Linked Map
Delete Device...
Discover Policies on Device...
Remove from Map
AAA Rules...
Access Rules...
Inspection Rules...
Web Filter Rules...

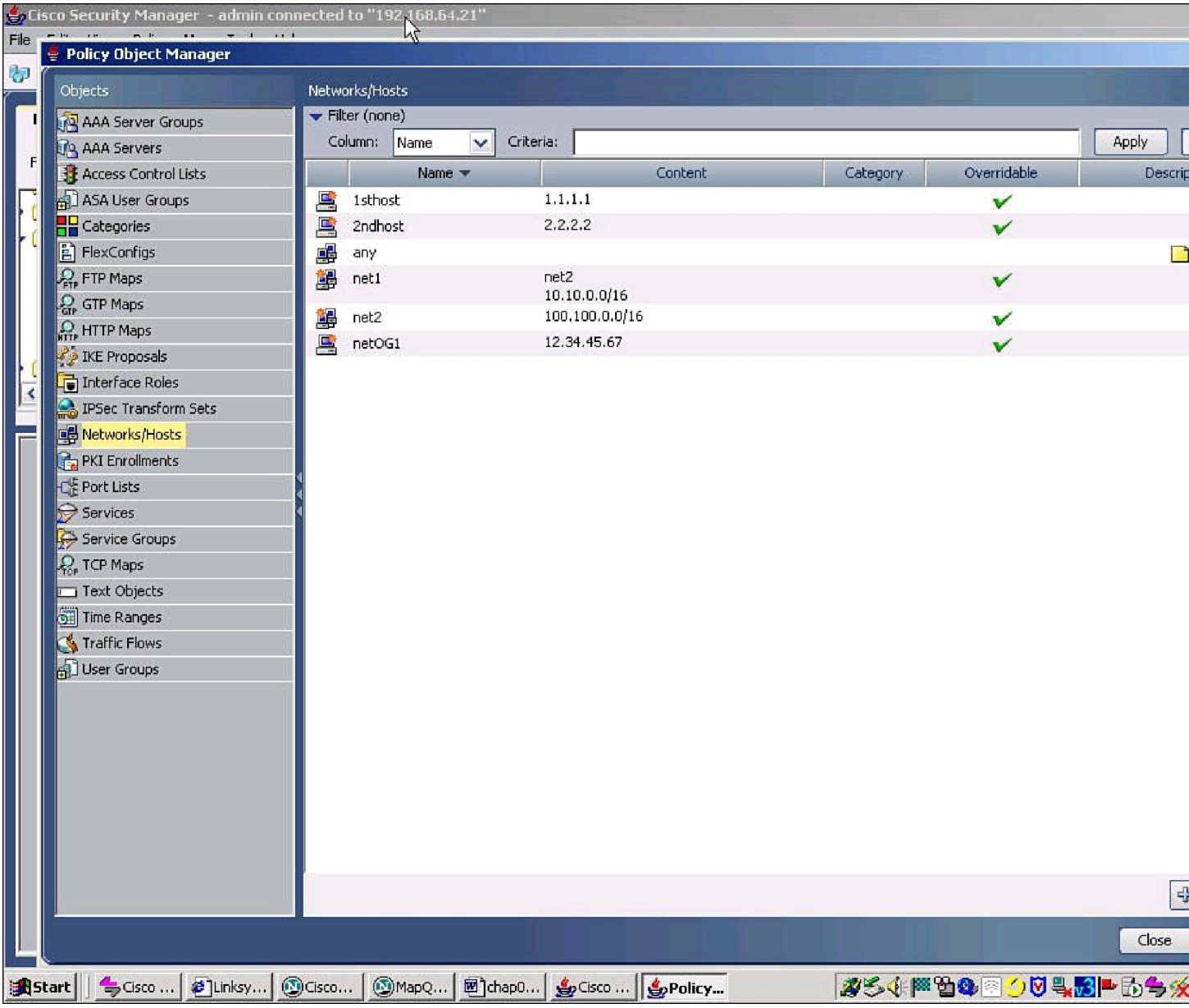

ACME Web Server
Net-1.1.1.0
Cloud-2
Net-10.0.1.0
ASA-NYCWallStreet1
Access Rules
Device: ASA-NYCWallStreet1 Policy: Access Rules
Shared Policy in use : NYCWeb
Assigned to : 1 Device(s)
Filter (none)
No.
Permit
Source
Destination
Service
Interface
NYCWeb - Mandatory (1 Rule)
NYCWeb - Default (1 Rule)
1
any
any
HTTP
All-Interfaces
Query
Analysis
HitCount
Save

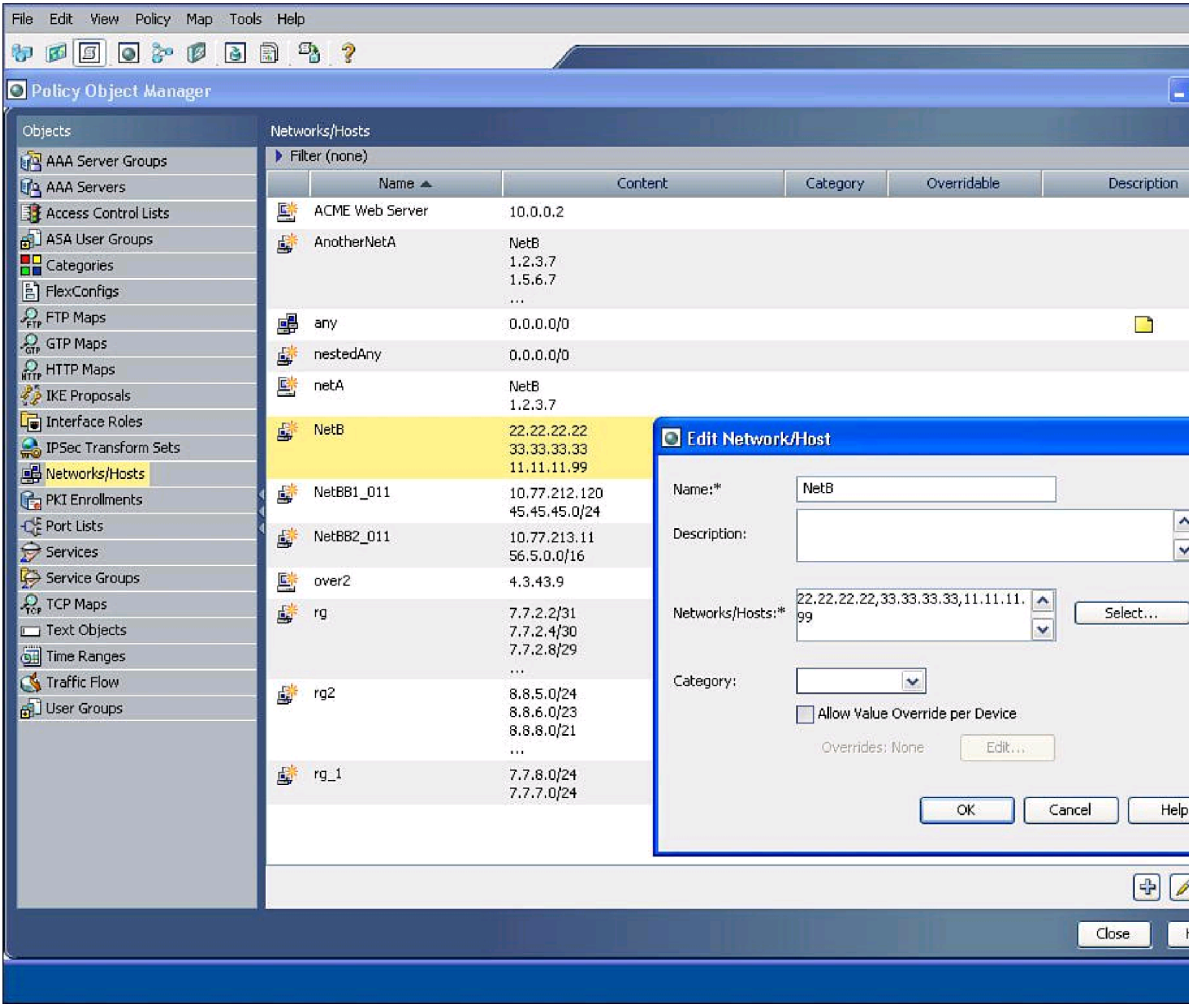

File
Edit
View
Policy
Map
Tools
Help
Policy Types
Firewall
AAA Rules
Access Rules
Inspection Rules
Settings
Transparent Rules
Web Filter Rules (PIX/FWSM
Web Filter Rules (IOS)
NAT (PIX)
Address Pools
Translation Options
Translation Rules
NAT (Router)
Remote Access VPN
PIX/ASA/FWSM Platform
Bridging
Device Admin
Logging
Multicast
Routing
Security
Service Policy Rules
User Preferences
Site-to-Site VPN
Router Platform
FlexConfigs
Policy Type: Router Platform
Policy: - no policy type selected -

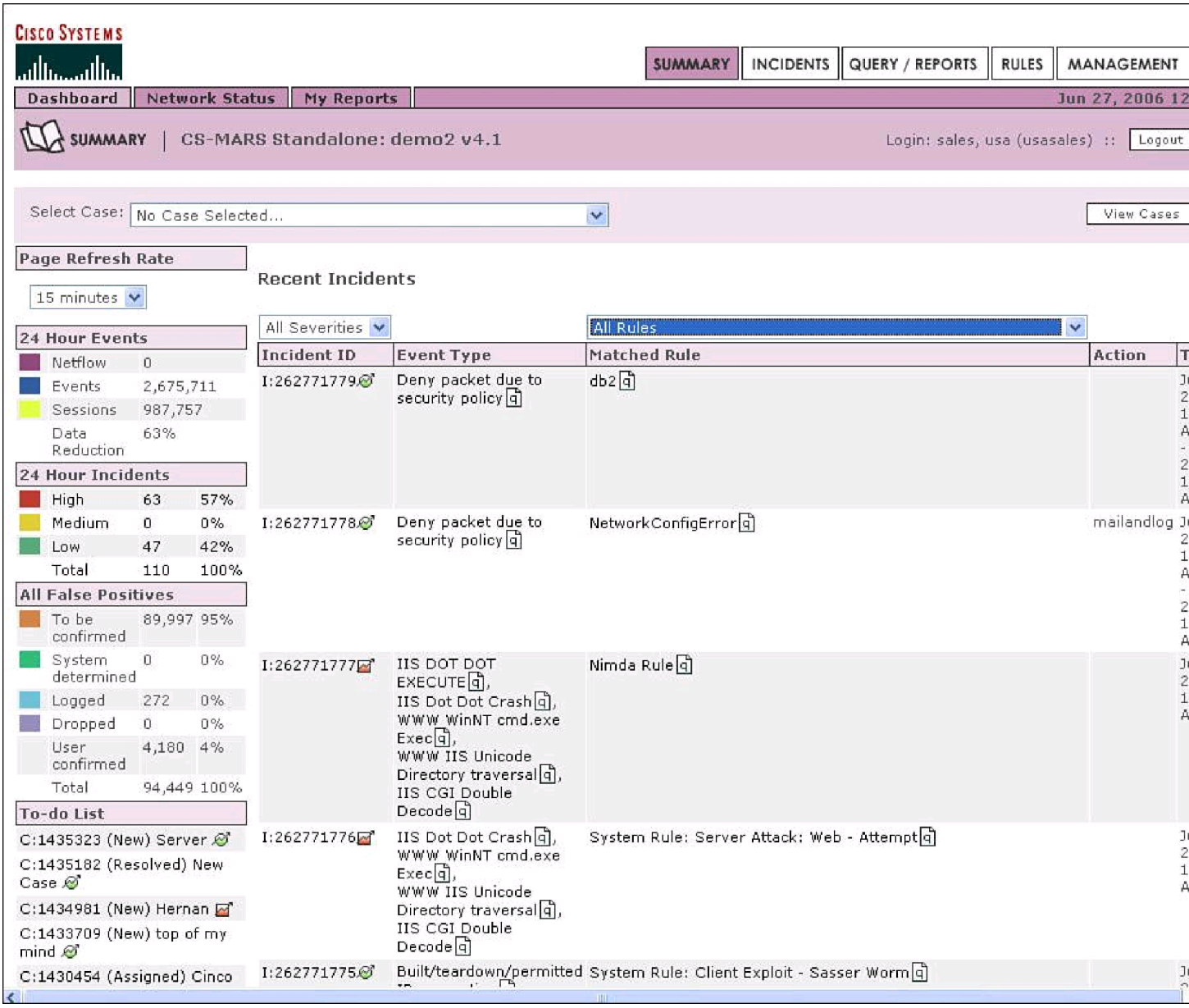

File Edit View Policy Map Tools Help
Policy Types
Firewall
AAA Rules
Access Rules
Inspection Rules
Settings
Transparent Rules
Web Filter Rules (PIX/FWSM
Web Filter Rules (IOS)
NAT (PIX)
Filter :
-- none --
CS
NYCWeb
P1
p2
Sasser
temp2
testInh
WallStreetSQL
West Coast Data Centers
San Jose SQL Server
Policy Type: Access Rules
Policy: Sasser
Add Firewall Rule
Enable Rule
Action:
Permit
Deny
Sources:*
any
Select...
Destinations:*
any
Select...
Services:*
Sasser
Select...
Interfaces:*
All-Interfaces
Edit...
Enable Logging
Logging Level:
Default
Description:
Advanced
OK
Cancel
Help
Dir.
Query
Analysis
HitCount


File Edit View Policy Map Tools Help
Policy Types
Firewall
AAA Rules
Access Rules
Inspection Rules
Settings
Transparent Rules
Filter : -- none --
CS
NYCWeb
P1
p2
San Jose SQL Server
temp2
testInh
WallStreetSQL
West Coast Data Centers
Policy Type: Access Rules
Policy: San Jose SQL Server
Details
Assignments
Filter (none)
No.
Permit
Interface
Dir.
San Jose SQL Server - M
San Jose SQL Server
Inherit Rules - San Jose SQL Server
Select the policy that will be the parent of the current policy.
Available Policies:
-- No Inheritance --
CS
NYCWeb
P1
p2
San Jose SQL Server
temp2
testInh
WallStreetSQL
West Coast Data Centers
Selected Parent Policy: West Coast Data Centers
OK
Cancel
Help
Query
Analysis
HitCount


File
Edit
View
Policy
Map
Tools
Help
Device Properties...
Policy Object Manager...
Site-To-Site VPN Manager...
Deployment Manager...
Policy Discovery Status...
Show Containment...
Device Status...
Catalyst Device Manager...
IPS Manager...
Preview Configuration...
Audit Report...
Configuration Archive...
Backup...
Security Manager Diagnostics...
Security Manager Administration...
Policy Types
Firewall
NAT (PIX)
NAT (Router)
Remote Access VPN
PIX/ASA/FWSM Platform
Site-to-Site VPN
Router Platform
FlexConfigs
Filter :
-- none --
- no policy type selected
licy type selected -


Cisco Security Manager - admin connected to "192.168.64.21"
File
Policy Object Manager
Objects
AAA Server Groups
AAA Servers
Access Control Lists
ASA User Groups
Categories
FlexConfigs
FTP Maps
GTP Maps
HTTP Maps
IKE Proposals
Interface Roles
IPSec Transform Sets
Networks/Hosts
PKI Enrollments
Port Lists
Services
Service Groups
TCP Maps
Text Objects
Time Ranges
Traffic Flows
User Groups
Networks/Hosts
Filter (none)
Column:
Name
Criteria:
Apply
Name
Content
Category
Overridable
Descrip
1sthost
1.1.1.1
2ndhost
2.2.2.2
any
net1
net2
10.10.0.0/16
net2
100.100.0.0/16
netOG1
12.34.45.67
Close
Start
Cisco ...
Linksy...
Cisco...
MapQ...
chap0...
Cisco ...
Policy...


File Edit View Policy Map Tools Help
Policy Object Manager
Objects
AAA Server Groups
AAA Servers
Access Control Lists
ASA User Groups
Categories
FlexConfigs
FTP Maps
GTP Maps
HTTP Maps
IKE Proposals
Interface Roles
IPSec Transform Sets
Networks/Hosts
PKI Enrollments
Port Lists
Services
Service Groups
TCP Maps
Text Objects
Time Ranges
Traffic Flow
User Groups
Networks/Hosts
Filter (none)
Name
Content
Category
Overridable
Description
ACME Web Server 10.0.0.2
AnotherNetA NetB 1.2.3.7 1.5.6.7 ...
any 0.0.0.0/0
nestedAny 0.0.0.0/0
netA NetB 1.2.3.7
NetB 22.22.22.22 33.33.33.33 11.11.11.99
NetBB1_011 10.77.212.120 45.45.45.0/24
NetBB2_011 10.77.213.11 56.5.0.0/16
over2 4.3.43.9
rg 7.7.2.2/31 7.7.2.4/30 7.7.2.8/29 ...
rg2 8.8.5.0/24 8.8.6.0/23 8.8.8.0/21 ...
rg_1 7.7.8.0/24 7.7.7.0/24
Edit Network/Host
Name:*
NetB
Description:
Networks/Hosts:*
22.22.22.22,33.33.33.33,11.11.11.99
Select...
Category:
Allow Value Override per Device
Overrides: None
Edit...
OK
Cancel
Help
Close


Cisco Systems
SUMMARY
INCIDENTS
QUERY / REPORTS
RULES
MANAGEMENT
Dashboard
Network Status
My Reports
Jun 27, 2006 12
SUMMARY | CS-MARS Standalone: demo2 v4.1
Login: sales, usa (usasales) ::
Logout
Select Case:
No Case Selected...
View Cases
Page Refresh Rate
15 minutes
24 Hour Events
Netflow 0
Events 2,675,711
Sessions 987,757
Data Reduction 63%
24 Hour Incidents
High 63 57%
Medium 0 0%
Low 47 42%
Total 110 100%
All False Positives
To be confirmed 89,997 95%
System determined 0 0%
Logged 272 0%
Dropped 0 0%
User confirmed 4,180 4%
Total 94,449 100%
To-do List
C:1435323 (New) Server
C:1435182 (Resolved) New Case
C:1434981 (New) Hernan
C:1433709 (New) top of my mind
C:1430454 (Assigned) Cinco
Recent Incidents
All Severities
All Rules
Incident ID
Event Type
Matched Rule
Action
I:262771779
Deny packet due to security policy
db2
I:262771778
Deny packet due to security policy
NetworkConfigError
mailandlog
I:262771777
IIS DOT DOT EXECUTE, IIS Dot Dot Crash, WWW WinNT cmd.exe Exec, WWW IIS Unicode Directory traversal, IIS CGI Double Decode
Nimda Rule
I:262771776
IIS Dot Dot Crash, WWW WinNT cmd.exe Exec, WWW IIS Unicode Directory traversal, IIS CGI Double Decode
System Rule: Server Attack: Web - Attempt
I:262771775
Built/teardown/permitted
System Rule: Client Exploit - Sasser Worm

Netflow	0	
Events	2,675,711	
Sessions	987,757	
Data Reduction	63%	

24 Hour Incidents

High	63	57%
Medium	0	0%
Low	47	42%
Total	110	100%

All False Positives

To be confirmed	89,997	95%
System determined	0	0%
Logged	272	0%
Dropped	0	0%
User confirmed	4,180	4%
Total	94,449	100%

To-do List

- C:1435323 (New) Server
- C:1435182 (Resolved) New Case
- C:1434981 (New) Hernan
- C:1433709 (New) top of my mind
- C:1430454 (Assigned) Cinco de Mayo
- C:1430119 (New) USA-TEST 2 139248695
- C:1429473 (Assigned) New Case
- C:1429125 (New) We Like mars case
- C:1428705 (Assigned) Todays case
- C:1427331 (Assigned) man another case
- C:1426881 (Assigned) Escalation de Privil...

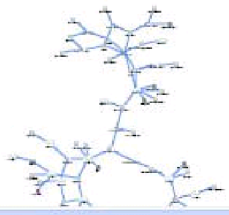
My Reports

Activity: All - Top Event

Incident ID	Event Type	Matched Rule	Action	T
I:262771779	Deny packet due to security policy	db2		Ju 20 11 A - 20 11 A
I:262771778	Deny packet due to security policy	NetworkConfigError	mailandlog	Ju 20 11 A - 20 11 A
I:262771777	IIS DOT DOT EXECUTE, IIS Dot Dot Crash, WWW WinNT cmd.exe Exec, WWW IIS Unicode Directory traversal, IIS CGI Double Decode	Nimda Rule		Ju 20 11 A
I:262771776	IIS Dot Dot Crash, WWW WinNT cmd.exe Exec, WWW IIS Unicode Directory traversal, IIS CGI Double Decode	System Rule: Server Attack: Web - Attempt		Ju 20 11 A
I:262771775	Built/teardown/permitted IP connection	System Rule: Client Exploit - Sasser Worm		Ju 20 11 A

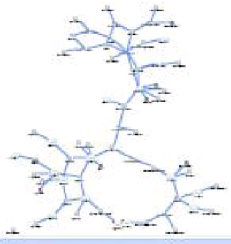
HotSpot Graph

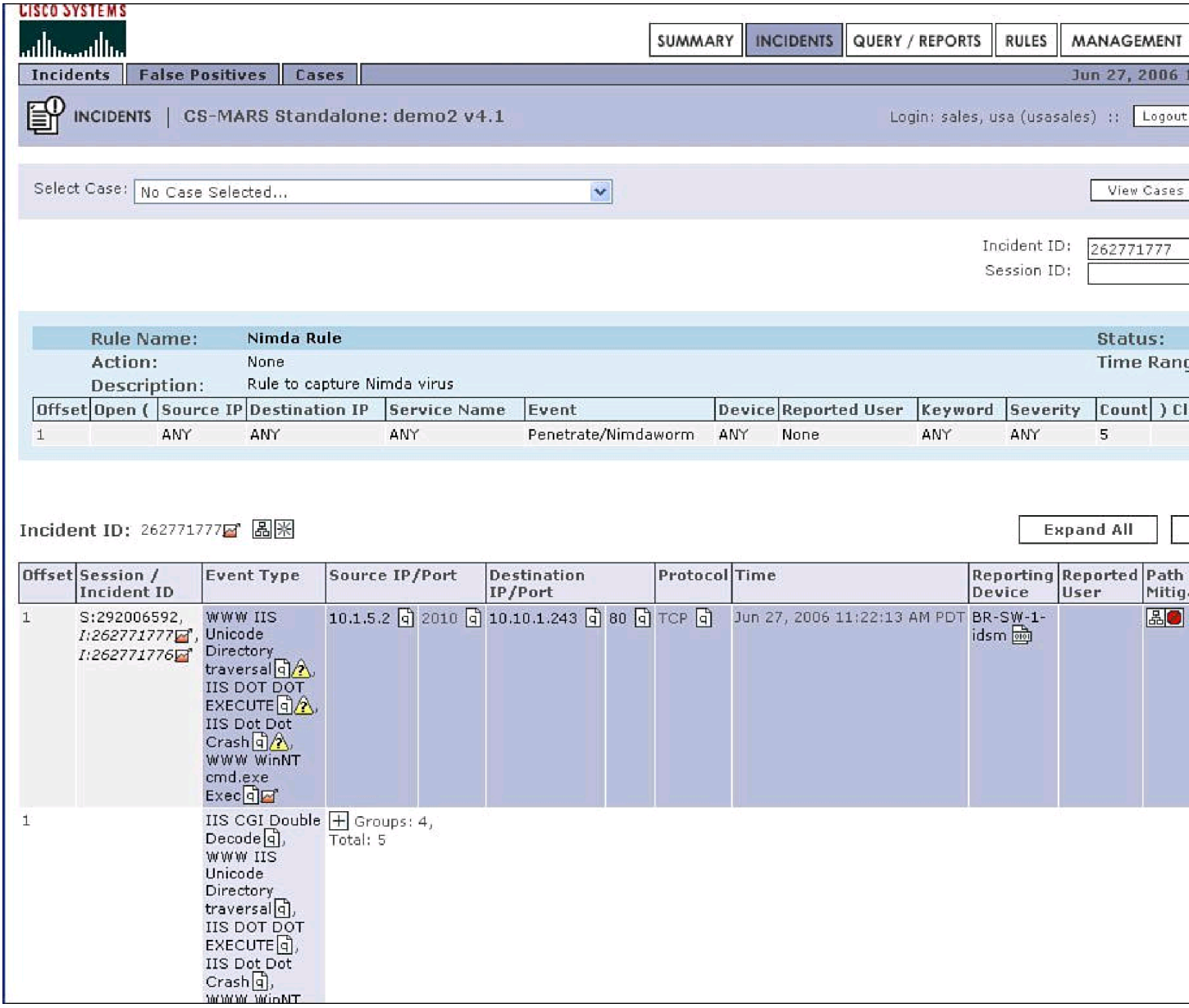
Full Topo Graph | Large Graph | Help



Attack Diagram

Large



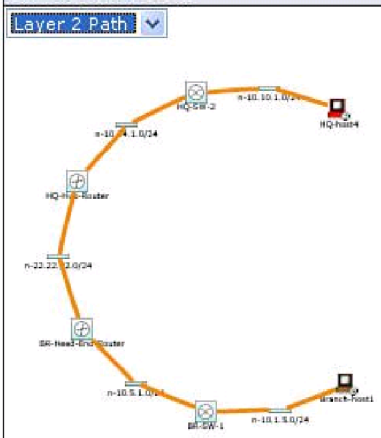

CISCO SYSTEMS
SUMMARY
INCIDENTS
QUERY / REPORTS
RULES
MANAGEMENT
Incidents
False Positives
Cases
Jun 27, 2006
INCIDENTS | CS-MARS Standalone: demo2 v4.1
Login: sales, usa (usasales) ::
Logout
Select Case:
No Case Selected...
View Cases
Incident ID:
262771777
Session ID:
Rule Name:
Nimda Rule
Status:
Action:
None
Time Rang
Description:
Rule to capture Nimda virus
Offset
Open (
Source IP
Destination IP
Service Name
Event
Device
Reported User
Keyword
Severity
Count
) Cl
1
ANY
ANY
ANY
Penetrate/Nimdaworm
ANY
None
ANY
ANY
5
Incident ID: 262771777
Expand All
Offset
Session / Incident ID
Event Type
Source IP/Port
Destination IP/Port
Protocol
Time
Reporting Device
Reported User
Path Mitig
1
S:292006592,
I:262771777,
I:262771776
WWW IIS Unicode Directory traversal,
IIS DOT DOT EXECUTE,
IIS Dot Dot Crash,
WWW WinNT cmd.exe Exec
10.1.5.2
2010
10.10.1.243
80
TCP
Jun 27, 2006 11:22:13 AM PDT
BR-SW-1-idsm
1
IIS CGI Double Decode,
WWW IIS Unicode Directory traversal,
IIS DOT DOT EXECUTE,
IIS Dot Dot Crash,
Groups: 4,
Total: 5

Jun 28, 2006 12:20:3

Standalone: demo2 v4.1 Login: sales, usa (usasales)

Static information utilizes discovered Layer 3 and 2 network topology information to determine the optimal mitigation point.

Static Info | **Dynamic Info**

Enforcement Devices	S:294841851 Path
Suggested BR-SW-1 **Alternate** BR-Head-End-Router HQ-Hub-Router HQ-SW-2	Layer 2 Path 

Enforcement Device: BR-SW-1, Suggested

Default gateway: 10.4.1.1

L3 Enforcement Device Information

Device	Type	Manager	Children	Log To	Collects From
BR-SW-1	Cisco Switch-IOS 12.2	PN-MARS on demo2	Cisco IDS 3.1 on BR-SW-1-idsm	PN-MARS on demo2	

Enforcement Device: BR-SW-1, Suggested

Default gateway: 10.4.1.1

L3 Enforcement Device Information

Device	Type	Manager	Children	Log To	Collects From
BR-SW-1	Cisco Switch-IOS 12.2	PN-MARS on demo2	Cisco IDS 3.1 on BR-SW-1-idsm	PN-MARS on demo2	

Interface Information

Direction	Interface Name	MAC Address	MAC Update Time
Inbound	FastEthernet2/0	N/A	N/A
Outbound	FastEthernet1/0	N/A	N/A

Recommended L3 Policies/Commands

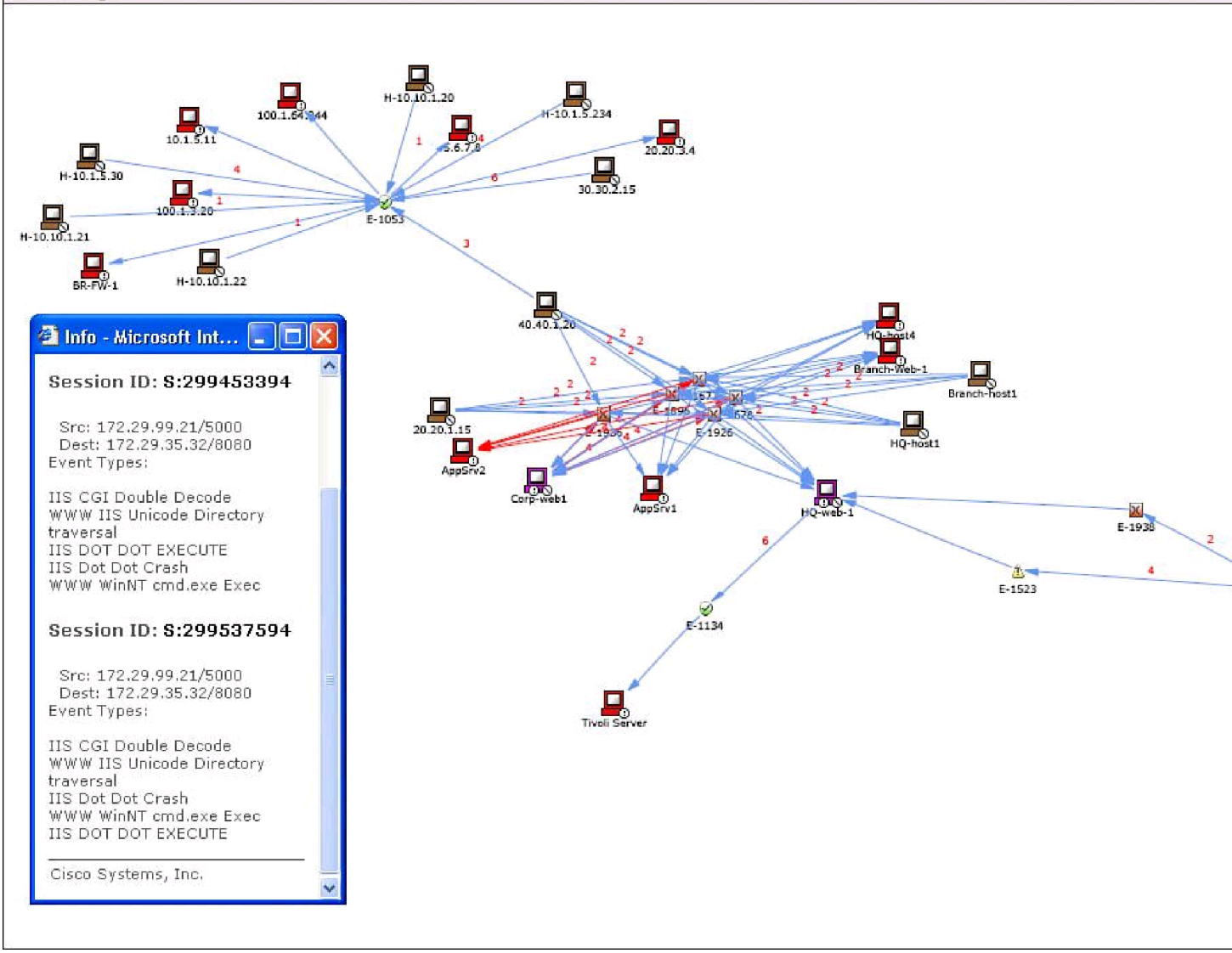
```
ip access-list extended CSM-acl-FastEthernet2/0
  deny tcp host 10.1.5.2 host 10.10.1.243 eq 80
```

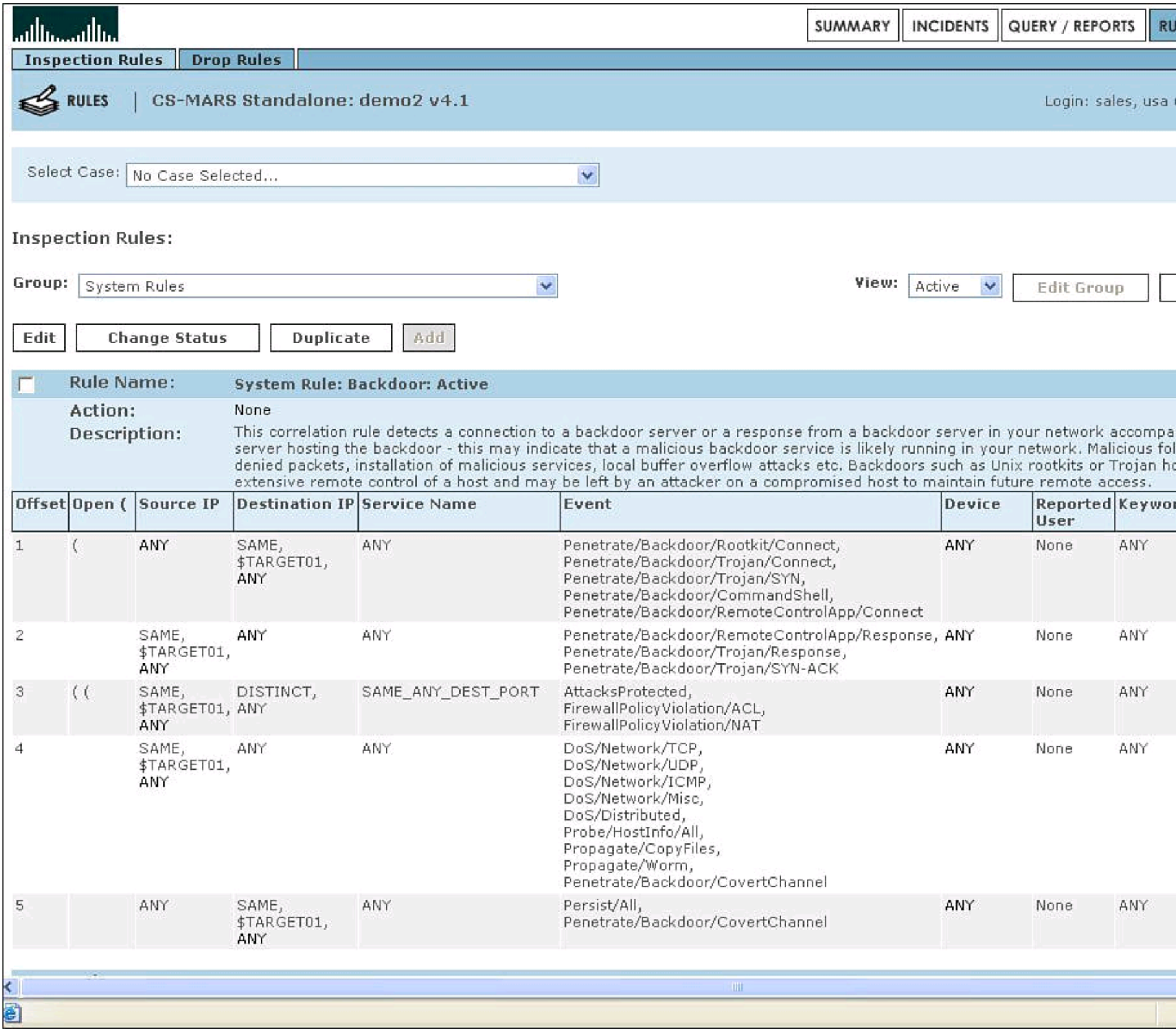
Or

```
ip access-list extended CSM-acl-FastEthernet2/0
  deny tcp host 10.1.5.2 any
```

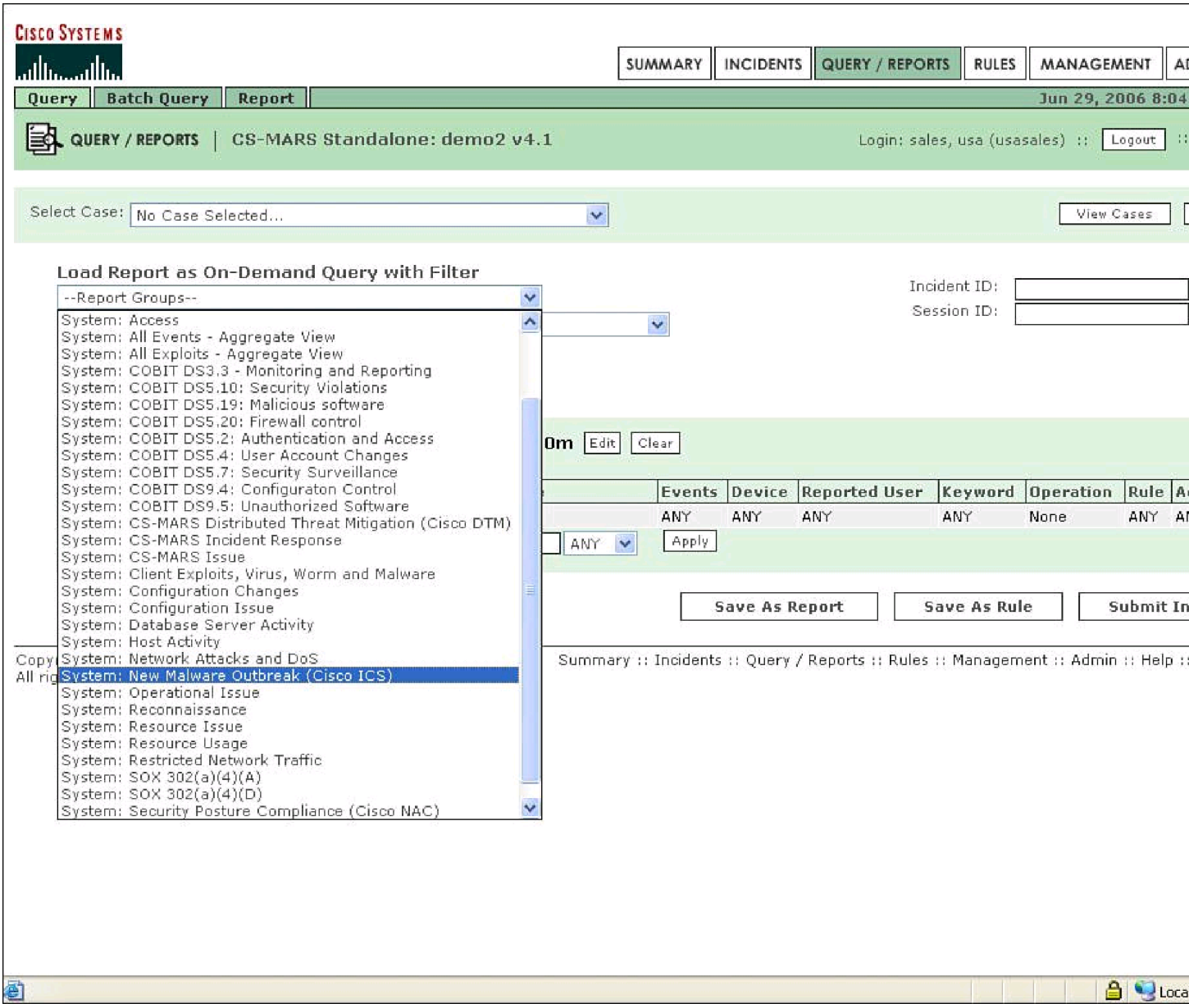
Push

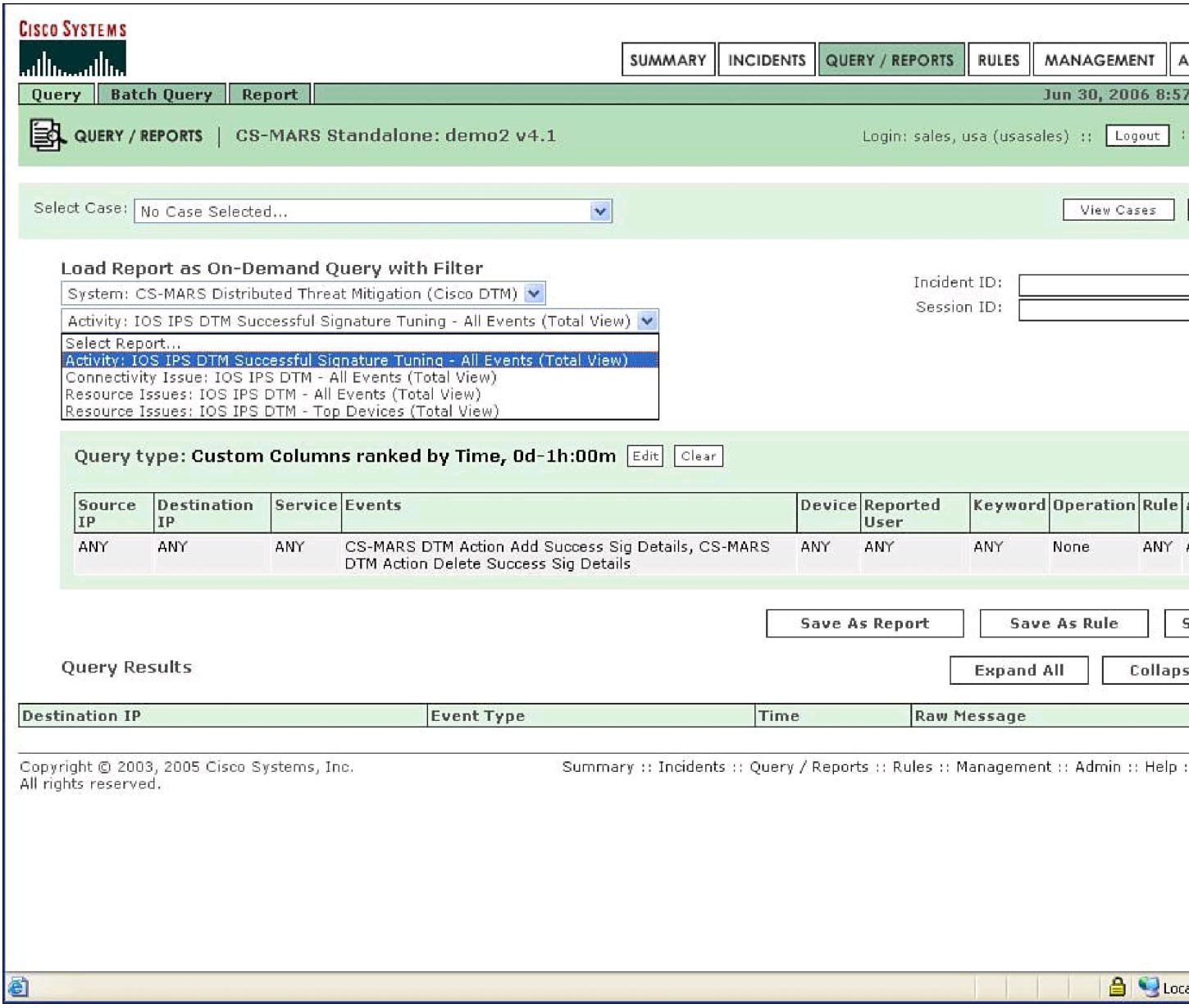
Attack Diagram

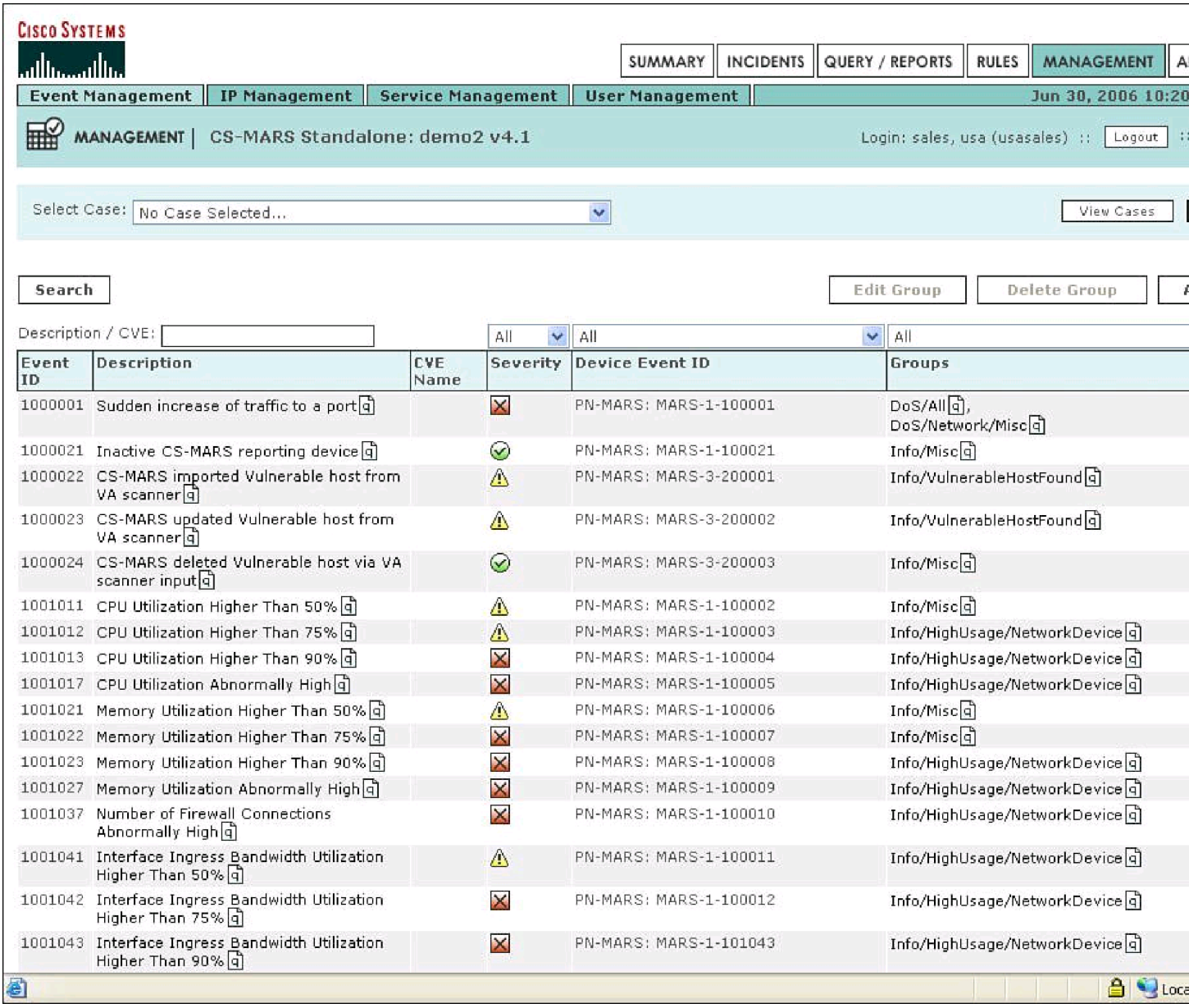


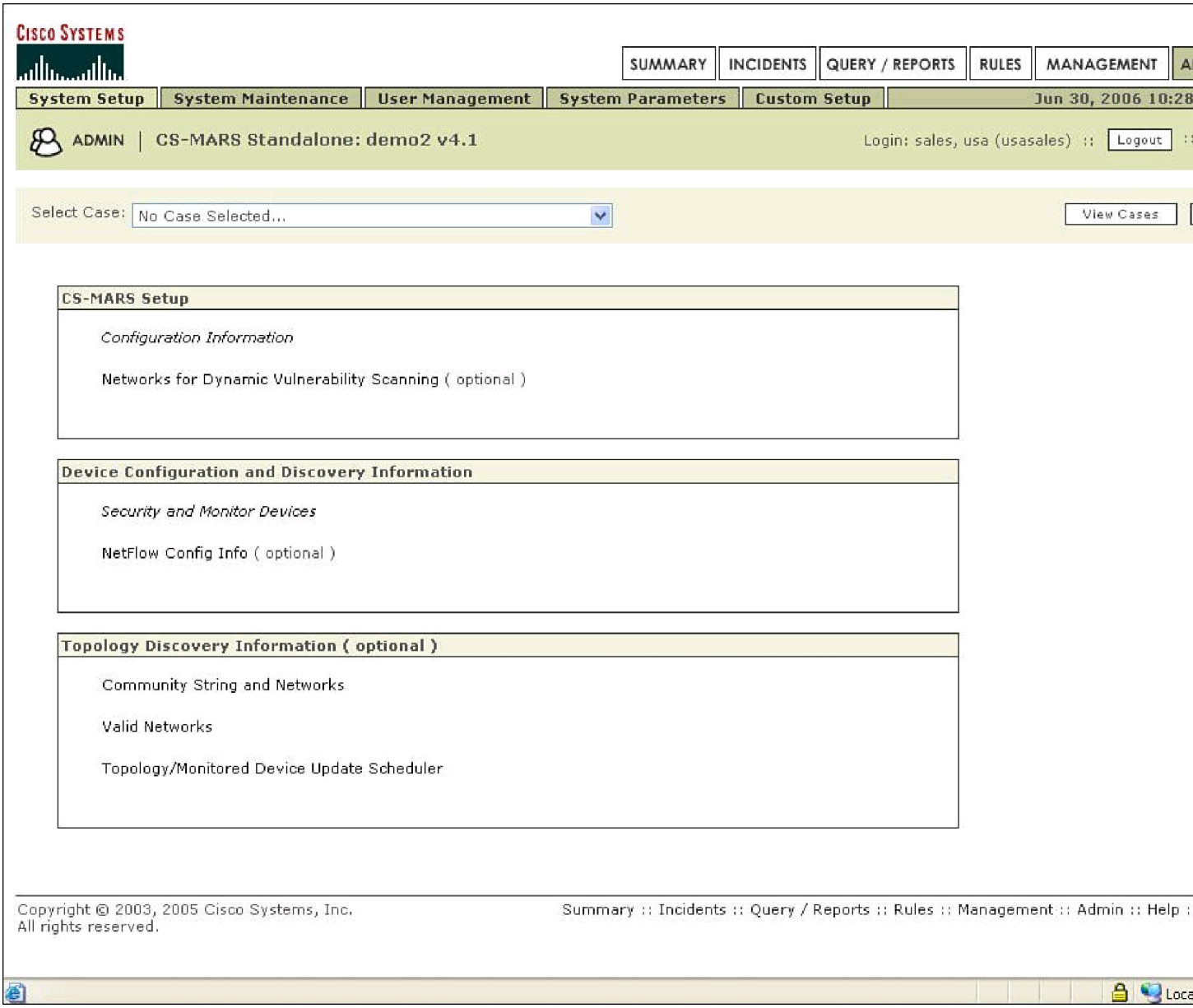


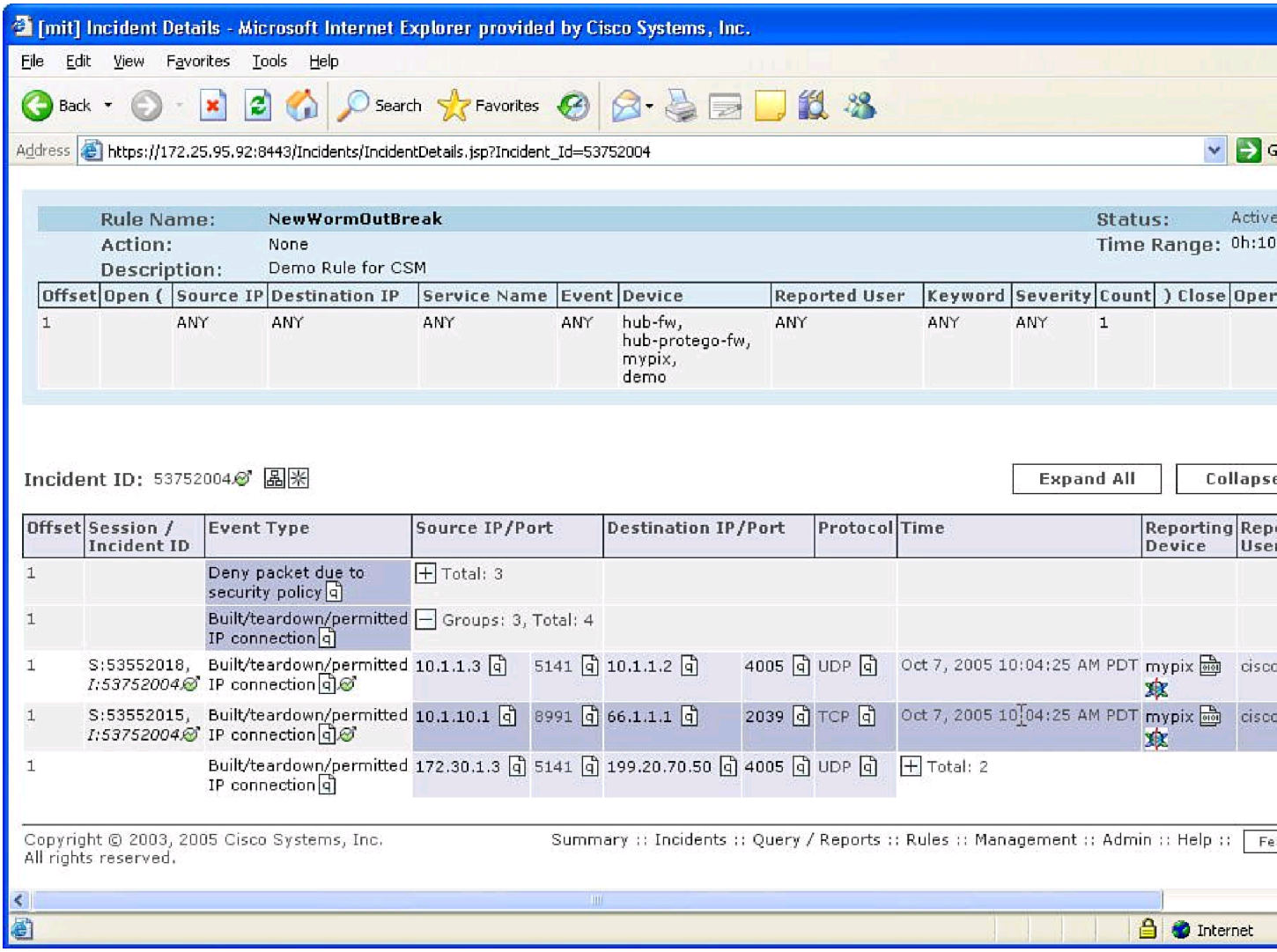
Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keywo
1	(	ANY	SAME, $TARGET01, ANY	ANY	Penetrate/Backdoor/Rootkit/Connect, Penetrate/Backdoor/Trojan/Connect, Penetrate/Backdoor/Trojan/SYN, Penetrate/Backdoor/CommandShell, Penetrate/Backdoor/RemoteControlApp/Connect	ANY	None	ANY
2		SAME, $TARGET01, ANY	ANY	ANY	Penetrate/Backdoor/RemoteControlApp/Response, Penetrate/Backdoor/Trojan/Response, Penetrate/Backdoor/Trojan/SYN-ACK	ANY	None	ANY
3	((	SAME, $TARGET01, ANY	DISTINCT, ANY	SAME_ANY_DEST_PORT	AttacksProtected, FirewallPolicyViolation/ACL, FirewallPolicyViolation/NAT	ANY	None	ANY
4		SAME, $TARGET01, ANY	ANY	ANY	DoS/Network/TCP, DoS/Network/UDP, DoS/Network/ICMP, DoS/Network/Misc, DoS/Distributed, Probe/HostInfo/All, Propagate/CopyFiles, Propagate/Worm, Penetrate/Backdoor/CovertChannel	ANY	None	ANY
5		ANY	SAME, $TARGET01, ANY	ANY	Persist/All, Penetrate/Backdoor/CovertChannel	ANY	None	ANY

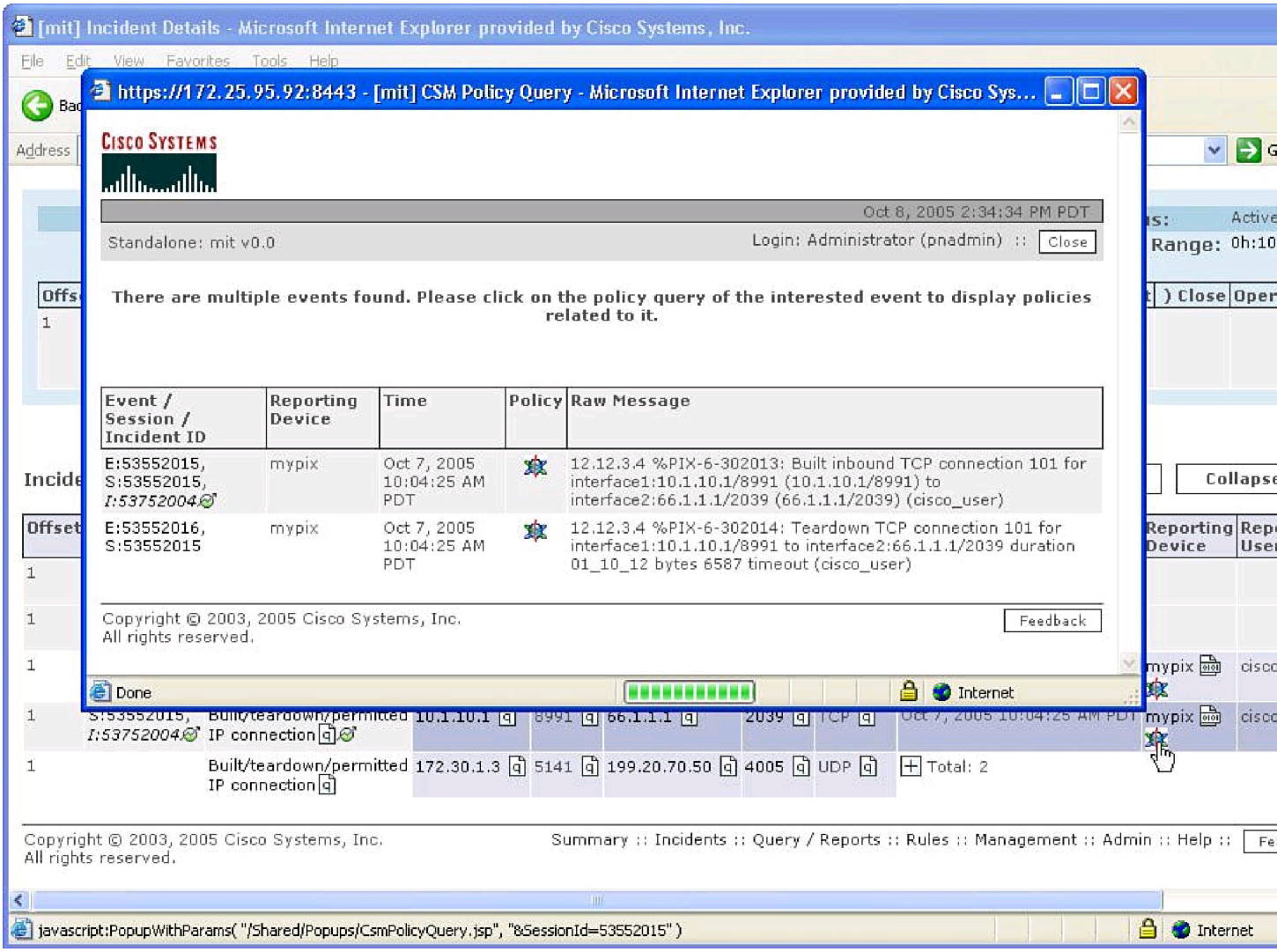

Cisco Systems
SUMMARY
INCIDENTS
QUERY / REPORTS
RULES
MANAGEMENT
Query
Batch Query
Report
Jun 29, 2006 8:04
QUERY / REPORTS | CS-MARS Standalone: demo2 v4.1
Login: sales, usa (usasales) :: Logout
Select Case: No Case Selected...
View Cases
Load Report as On-Demand Query with Filter
--Report Groups--
System: Access
System: All Events - Aggregate View
System: All Exploits - Aggregate View
System: COBIT DS3.3 - Monitoring and Reporting
System: COBIT DS5.10: Security Violations
System: COBIT DS5.19: Malicious software
System: COBIT DS5.20: Firewall control
System: COBIT DS5.2: Authentication and Access
System: COBIT DS5.4: User Account Changes
System: COBIT DS5.7: Security Surveillance
System: COBIT DS9.4: Configuraton Control
System: COBIT DS9.5: Unauthorized Software
System: CS-MARS Distributed Threat Mitigation (Cisco DTM)
System: CS-MARS Incident Response
System: CS-MARS Issue
System: Client Exploits, Virus, Worm and Malware
System: Configuration Changes
System: Configuration Issue
System: Database Server Activity
System: Host Activity
System: Network Attacks and DoS
System: New Malware Outbreak (Cisco ICS)
System: Operational Issue
System: Reconnaissance
System: Resource Issue
System: Resource Usage
System: Restricted Network Traffic
System: SOX 302(a)(4)(A)
System: SOX 302(a)(4)(D)
System: Security Posture Compliance (Cisco NAC)
Incident ID:
Session ID:
0m
Edit
Clear
Events
Device
Reported User
Keyword
Operation
Rule
ANY
ANY
ANY
ANY
None
ANY
ANY
Apply
Save As Report
Save As Rule
Submit In
Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help ::

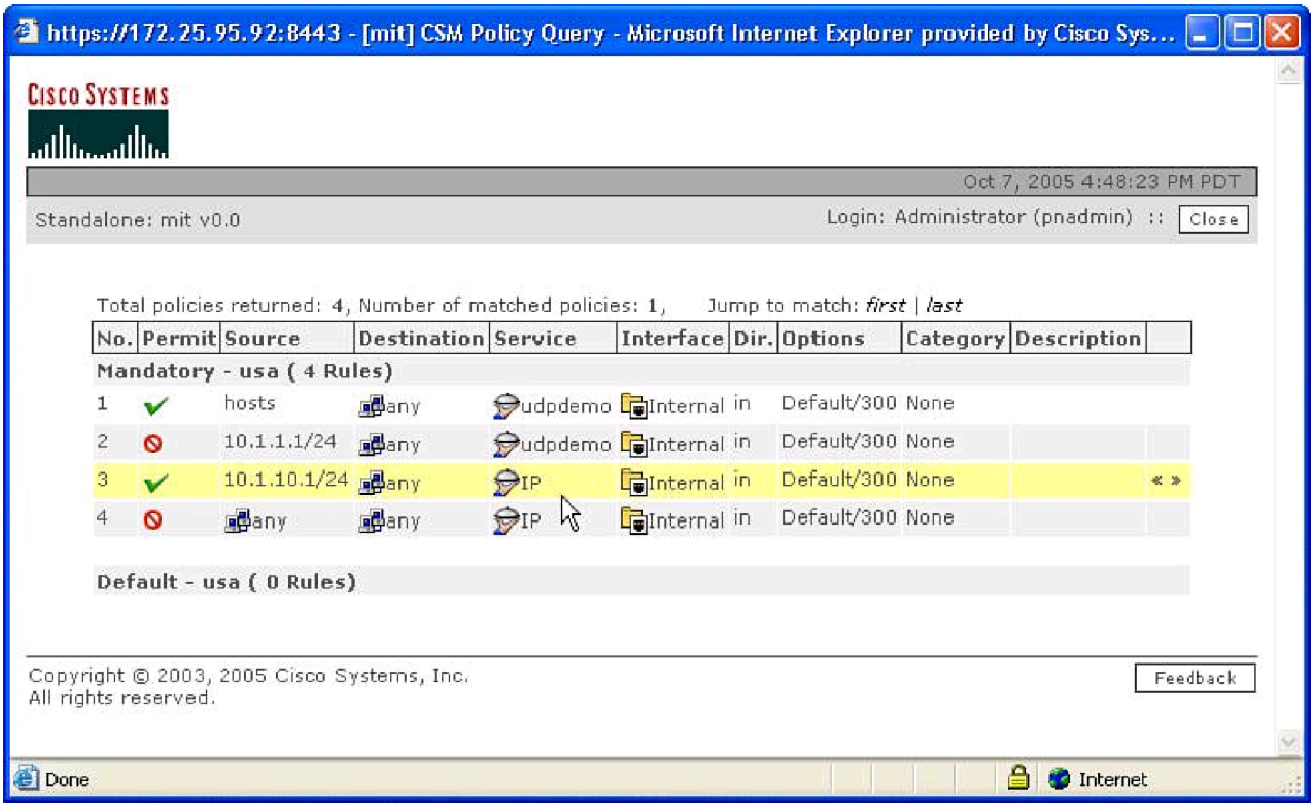

Cisco Systems
SUMMARY
INCIDENTS
QUERY / REPORTS
RULES
MANAGEMENT
Query
Batch Query
Report
Jun 30, 2006 8:57
QUERY / REPORTS | CS-MARS Standalone: demo2 v4.1
Login: sales, usa (usasales) :: Logout
Select Case: No Case Selected...
View Cases
Load Report as On-Demand Query with Filter
System: CS-MARS Distributed Threat Mitigation (Cisco DTM)
Activity: IOS IPS DTM Successful Signature Tuning - All Events (Total View)
Select Report...
Activity: IOS IPS DTM Successful Signature Tuning - All Events (Total View)
Connectivity Issue: IOS IPS DTM - All Events (Total View)
Resource Issues: IOS IPS DTM - All Events (Total View)
Resource Issues: IOS IPS DTM - Top Devices (Total View)
Incident ID:
Session ID:
Query type: Custom Columns ranked by Time, 0d-1h:00m
Edit
Clear
Source IP
Destination IP
Service
Events
Device
Reported User
Keyword
Operation
Rule
ANY
ANY
ANY
CS-MARS DTM Action Add Success Sig Details, CS-MARS DTM Action Delete Success Sig Details
ANY
ANY
ANY
None
ANY
Save As Report
Save As Rule
Query Results
Expand All
Destination IP
Event Type
Time
Raw Message
Copyright © 2003, 2005 Cisco Systems, Inc.
All rights reserved.
Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help


Cisco Systems
SUMMARY
INCIDENTS
QUERY / REPORTS
RULES
MANAGEMENT
Event Management
IP Management
Service Management
User Management
Jun 30, 2006 10:20
MANAGEMENT | CS-MARS Standalone: demo2 v4.1
Login: sales, usa (usasales) :: Logout
Select Case: No Case Selected...
View Cases
Search
Edit Group
Delete Group
Description / CVE:
All
All
All
Event ID
Description
CVE Name
Severity
Device Event ID
Groups
1000001 Sudden increase of traffic to a port PN-MARS: MARS-1-100001 DoS/All, DoS/Network/Misc
1000021 Inactive CS-MARS reporting device PN-MARS: MARS-1-100021 Info/Misc
1000022 CS-MARS imported Vulnerable host from VA scanner PN-MARS: MARS-3-200001 Info/VulnerableHostFound
1000023 CS-MARS updated Vulnerable host from VA scanner PN-MARS: MARS-3-200002 Info/VulnerableHostFound
1000024 CS-MARS deleted Vulnerable host via VA scanner input PN-MARS: MARS-3-200003 Info/Misc
1001011 CPU Utilization Higher Than 50% PN-MARS: MARS-1-100002 Info/Misc
1001012 CPU Utilization Higher Than 75% PN-MARS: MARS-1-100003 Info/HighUsage/NetworkDevice
1001013 CPU Utilization Higher Than 90% PN-MARS: MARS-1-100004 Info/HighUsage/NetworkDevice
1001017 CPU Utilization Abnormally High PN-MARS: MARS-1-100005 Info/HighUsage/NetworkDevice
1001021 Memory Utilization Higher Than 50% PN-MARS: MARS-1-100006 Info/Misc
1001022 Memory Utilization Higher Than 75% PN-MARS: MARS-1-100007 Info/Misc
1001023 Memory Utilization Higher Than 90% PN-MARS: MARS-1-100008 Info/HighUsage/NetworkDevice
1001027 Memory Utilization Abnormally High PN-MARS: MARS-1-100009 Info/HighUsage/NetworkDevice
1001037 Number of Firewall Connections Abnormally High PN-MARS: MARS-1-100010 Info/HighUsage/NetworkDevice
1001041 Interface Ingress Bandwidth Utilization Higher Than 50% PN-MARS: MARS-1-100011 Info/HighUsage/NetworkDevice
1001042 Interface Ingress Bandwidth Utilization Higher Than 75% PN-MARS: MARS-1-100012 Info/HighUsage/NetworkDevice
1001043 Interface Ingress Bandwidth Utilization Higher Than 90% PN-MARS: MARS-1-101043 Info/HighUsage/NetworkDevice


CISCO SYSTEMS
SUMMARY
INCIDENTS
QUERY / REPORTS
RULES
MANAGEMENT
System Setup
System Maintenance
User Management
System Parameters
Custom Setup
Jun 30, 2006 10:28
ADMIN | CS-MARS Standalone: demo2 v4.1
Login: sales, usa (usasales) :: Logout
Select Case: No Case Selected...
View Cases
CS-MARS Setup
Configuration Information
Networks for Dynamic Vulnerability Scanning (optional)
Device Configuration and Discovery Information
Security and Monitor Devices
NetFlow Config Info (optional)
Topology Discovery Information (optional)
Community String and Networks
Valid Networks
Topology/Monitored Device Update Scheduler
Copyright © 2003, 2005 Cisco Systems, Inc.
All rights reserved.
Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help


[mit] Incident Details - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites
Address https://172.25.95.92:8443/Incidents/IncidentDetails.jsp?Incident_Id=53752004
Rule Name: NewWormOutBreak
Status: Active
Action: None
Time Range: 0h:10
Description: Demo Rule for CSM
Offset | Open (| Source IP | Destination IP | Service Name | Event | Device | Reported User | Keyword | Severity | Count |) Close | Oper
1 | | ANY | ANY | ANY | ANY | hub-fw, hub-protego-fw, mypix, demo | ANY | ANY | ANY | 1 | |
Incident ID: 53752004
Expand All
Collapse
Offset | Session / Incident ID | Event Type | Source IP/Port | | Destination IP/Port | | Protocol | Time | Reporting Device | Rep User
1 | | Deny packet due to security policy | Total: 3 | | | | | | | |
1 | | Built/teardown/permitted IP connection | Groups: 3, Total: 4 | | | | | | | |
1 | S:53552018, I:53752004 | Built/teardown/permitted IP connection | 10.1.1.3 | 5141 | 10.1.1.2 | 4005 | UDP | Oct 7, 2005 10:04:25 AM PDT | mypix | cisco
1 | S:53552015, I:53752004 | Built/teardown/permitted IP connection | 10.1.10.1 | 8991 | 66.1.1.1 | 2039 | TCP | Oct 7, 2005 10:04:25 AM PDT | mypix | cisco
1 | | Built/teardown/permitted IP connection | 172.30.1.3 | 5141 | 199.20.70.50 | 4005 | UDP | Total: 2 | | |
Copyright © 2003, 2005 Cisco Systems, Inc.
All rights reserved.
Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help ::
Internet


[mit] Incident Details - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
https://172.25.95.92:8443 - [mit] CSM Policy Query - Microsoft Internet Explorer provided by Cisco Sys...
Cisco Systems
Oct 8, 2005 2:34:34 PM PDT
Standalone: mit v0.0
Login: Administrator (pnadmin) :: Close
There are multiple events found. Please click on the policy query of the interested event to display policies related to it.
Event / Session / Incident ID
Reporting Device
Time
Policy
Raw Message
E:53552015, S:53552015, I:53752004
mypix
Oct 7, 2005 10:04:25 AM PDT
12.12.3.4 %PIX-6-302013: Built inbound TCP connection 101 for interface1:10.1.10.1/8991 (10.1.10.1/8991) to interface2:66.1.1.1/2039 (66.1.1.1/2039) (cisco_user)
E:53552016, S:53552015
mypix
Oct 7, 2005 10:04:25 AM PDT
12.12.3.4 %PIX-6-302014: Teardown TCP connection 101 for interface1:10.1.10.1/8991 to interface2:66.1.1.1/2039 duration 01_10_12 bytes 6587 timeout (cisco_user)
Copyright © 2003, 2005 Cisco Systems, Inc.
All rights reserved.
Feedback
Done
Internet
Collapse
Offset
Reporting Device
Built/teardown/permitted IP connection
10.1.10.1
8991
66.1.1.1
2039
TCP
Oct 7, 2005 10:04:25 AM PDT
mypix
Built/teardown/permitted IP connection
172.30.1.3
5141
199.20.70.50
4005
UDP
Total: 2
Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help ::
javascript:PopupWithParams("/Shared/Popups/CsmPolicyQuery.jsp", "&SessionId=53552015")
Internet


https://172.25.95.92:8443 - [mit] CSM Policy Query - Microsoft Internet Explorer provided by Cisco Sys...
Cisco Systems
Oct 7, 2005 4:48:23 PM PDT
Standalone: mit v0.0
Login: Administrator (pnadmin) :: Close
Total policies returned: 4, Number of matched policies: 1, Jump to match: first | last
No. Permit Source Destination Service Interface Dir. Options Category Description
Mandatory - usa (4 Rules)
1 hosts any udpdemo Internal in Default/300 None
2 10.1.1.1/24 any udpdemo Internal in Default/300 None
3 10.1.10.1/24 any IP Internal in Default/300 None
4 any any IP Internal in Default/300 None
Default - usa (0 Rules)
Copyright © 2003, 2005 Cisco Systems, Inc.
All rights reserved.
Feedback
Done
Internet