DefensePro
Version 8.x

Training Lab Manual
Configure Out of State Protection

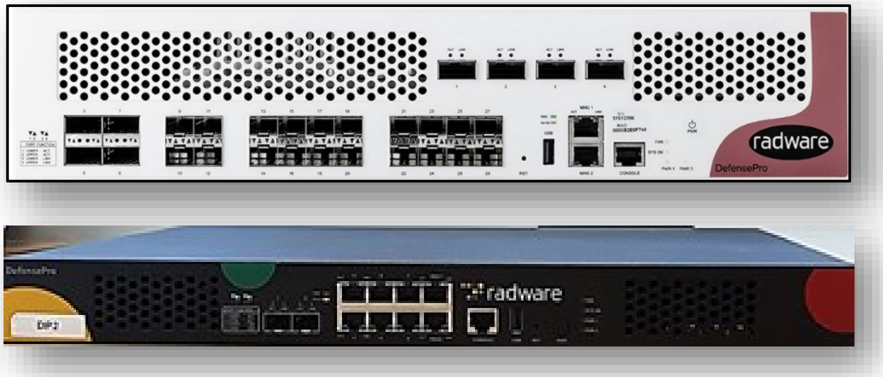


Table of Contents

Contents

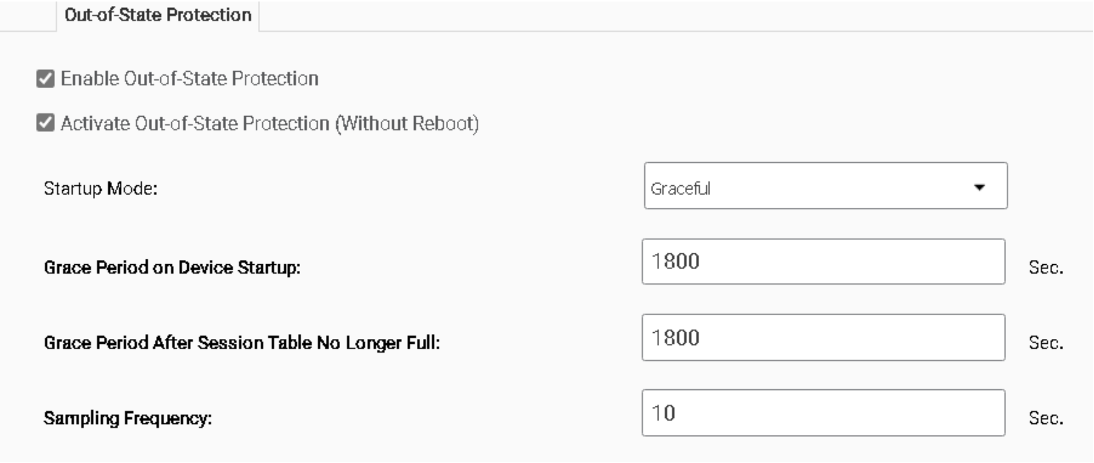
OVERVIEW 3
SETUP OUT OF STATE PROTECTION 3
CONFIGURE OUT OF STATE PROTECTION 3
TEST THE CONFIGURATION 4

Overview

An Out of State attack is a network level denial of service attack where first packet isn't SYN. Due to the way TCP protocol works the Behavioral DoS mechanism isn't suitable for defense againgst ACK and PSH-ACK floods. In such cases Out of Stat protection is an opton.

Setup Out of State Protection

1. Select the **Configuration** perspective.
2. In **Setup** section, select **Security Settings** and then **Out-of-State Protection**.
3. By default this feature is enabled.
4. You can configure:
    a. Startup mode
       Set this one to **On** in the lab.
        i. **On** — Start Out-of-State Protection action immediately after startup (with no time to learn traffic and sessions). Sessions that started before startup get dropped. Only new, valid sessions are allowed.
        ii. **Off** — Do not start Out-of-State Protection after startup or reboot.
        iii. **Graceful** — After startup, start learning sessions (and updating the Session table) for the time specified by the Startup Timer parameter. Then, begin Out-of-State Protection actions.
    b. Grace Period on Device Startup (default 1800)
    c. Grace Period After Session Table No Longer full (default 1800)
    d. Sampling Frequency (default 10)



Out-of-State Protection

☑ Enable Out-of-State Protection

☑ Activate Out-of-State Protection (Without Reboot)

Startup Mode: Graceful

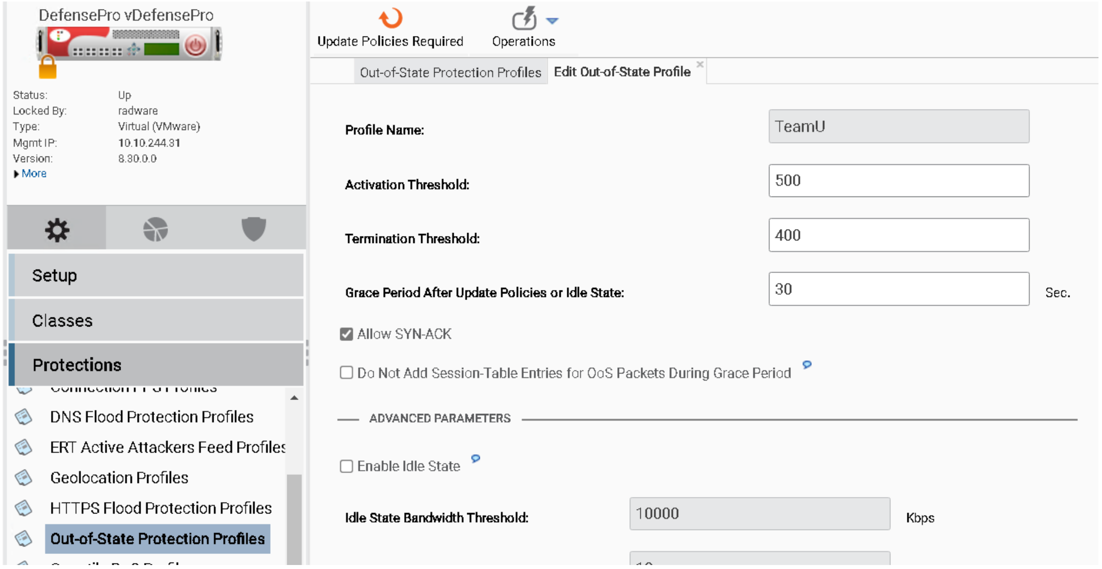
Grace Period on Device Startup: 1800 Sec.

Grace Period After Session Table No Longer Full: 1800 Sec.

Sampling Frequency: 10 Sec.

Configure Out of State Protection

1. Select the **Configuration → Protections → Out-of-State Protection Profiles**
2. Click **+** to **Out-of-State Profile**.
3. In **Add New Out-of-State Profile** tab type the **Profile Name**: ***TeamXX*** (where XX are your initials)
4. Leave rest of the parameters default.


DefensePro vDefensePro
Update Policies Required
Operations
Out-of-State Protection Profiles
Edit Out-of-State Profile
Setup
Classes
Protections
DNS Flood Protection Profiles
ERT Active Attackers Feed Profiles
Geolocation Profiles
HTTPS Flood Protection Profiles
Out-of-State Protection Profiles

Status: Up
Locked By: radware
Type: Virtual (VMware)
Mgmt IP: 10.10.244.31
Version: 8.30.0.0
More

Profile Name: TeamU
Activation Threshold: 500
Termination Threshold: 400
Grace Period After Update Policies or Idle State: 30 Sec.
☑ Allow SYN-ACK
□ Do Not Add Session-Table Entries for OoS Packets During Grace Period

ADVANCED PARAMETERS

□ Enable Idle State
Idle State Bandwidth Threshold: 10000 Kbps

5. Click **Submit** button to add protection to profile.
6. Go to **Configuration → Protections → Protection Policies**.
7. Edit your protection policy in **Profiles** tab select your newly created profile as your **Out-of-State Profile**.
8. Click **Submit**.
9. Click **Update Policies Required** button.

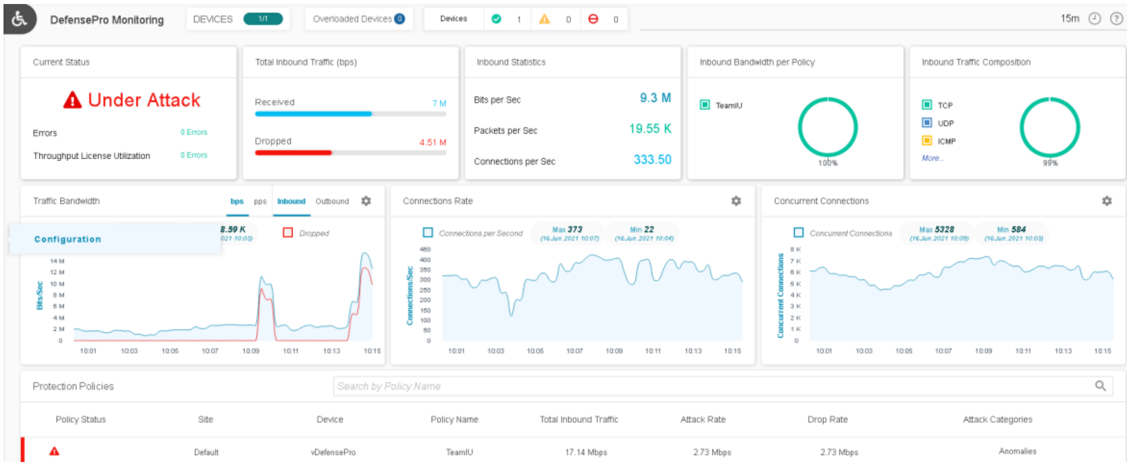
Test the Configuration

Use hping3 to send Out-of-State Attack

1. In the shell prompt type: **hping3 -p 80 -A --rand-source --flood 27.1.31.100**

   Soon after the attack is initiated from the Attack-PC, you see traps in the CLI/Syslog.

2. Use Vision to View Out-of-State Attack. Select the **Analytics AMS → DefensePro Monitoring** perspective.


DefensePro Monitoring | DEVICES 1/1 | Overloaded Devices 0 | Devices ✓ 1 ⚠ 0 ⊖ 0 | 15m

Current Status: ⚠ Under Attack
Errors 0 Errors
Throughput License Utilization 0 Errors

Total Inbound Traffic (bps)
Received 7 M
Dropped 4.51 M

Inbound Statistics
Bits per Sec 9.3 M
Packets per Sec 19.55 K
Connections per Sec 333.50

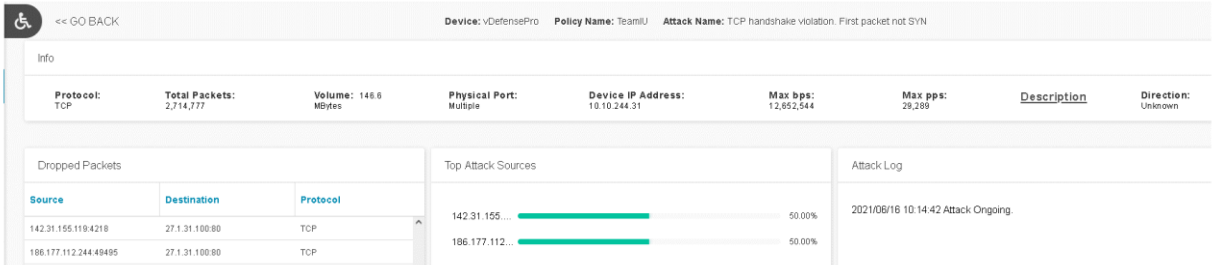
Inbound Bandwidth per Policy: 🟩 TeamIU 100%

Inbound Traffic Composition: 🟩 TCP 🟦 UDP 🟨 ICMP More... 99%

Protection Policies — Search by Policy Name

Policy Status	Site	Device	Policy Name	Total Inbound Traffic	Attack Rate	Drop Rate	Attack Categories
⚠	Default	vDefensePro	TeamIU	17.14 Mbps	2.73 Mbps	2.73 Mbps	Anomalies

3. View your policy under **Protection Policies**, select **Anomalies** in the **Protection** section**,** select the ongoing Out-of-State attack to open Attack Details.


<< GO BACK — **Device:** vDefensePro **Policy Name:** TeamIU **Attack Name:** TCP handshake violation. First packet not SYN

Info

Protocol: TCP
Total Packets: 2,714,777
Volume: 146.6 MBytes
Physical Port: Multiple
Device IP Address: 10.10.244.31
Max bps: 12,652,544
Max pps: 29,289
Description
Direction: Unknown

Dropped Packets

Source	Destination	Protocol
142.31.155.119:4218	27.1.31.100:80	TCP
186.177.112.244:49495	27.1.31.100:80	TCP

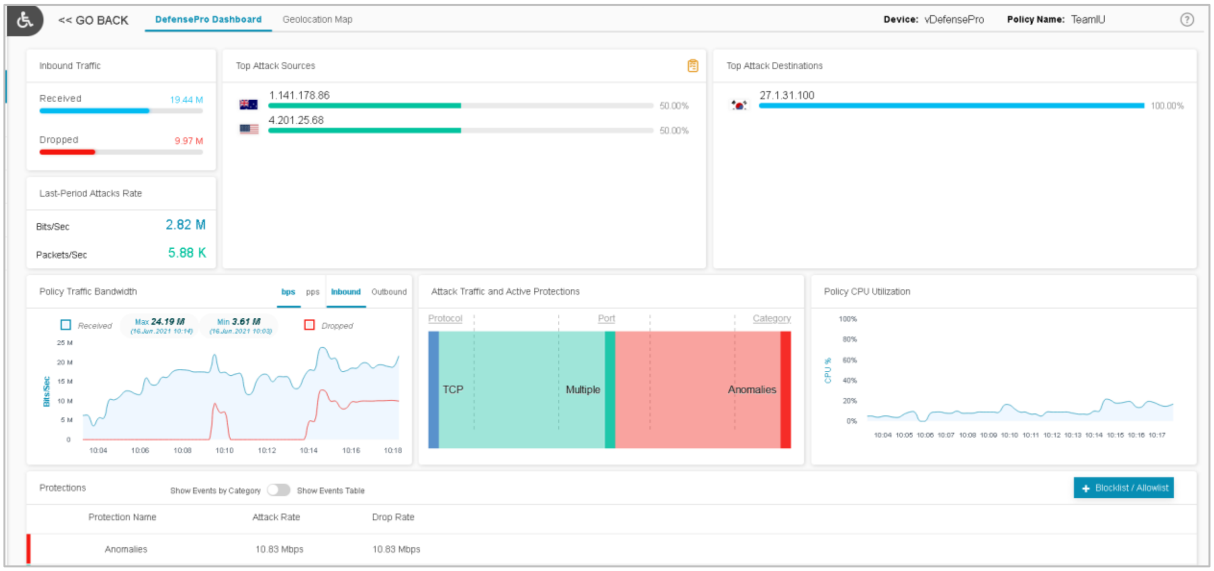
Top Attack Sources

142.31.155....	50.00%
186.177.112...	50.00%

Attack Log

2021/06/16 10:14:42 Attack Ongoing.

4. The graph display in **DefensePro Dashboard**. As you can see the Out-of-State is listed as **Anomalies**, **TCP handshake violation. First packet not SYN**.


<< GO BACK | DefensePro Dashboard | Geolocation Map — **Device:** vDefensePro **Policy Name:** TeamIU

Inbound Traffic
Received 19.44 M
Dropped 9.97 M

Last-Period Attacks Rate
Bits/Sec 2.82 M
Packets/Sec 5.88 K

Top Attack Sources

1.141.178.86	50.00%
4.201.25.68	50.00%

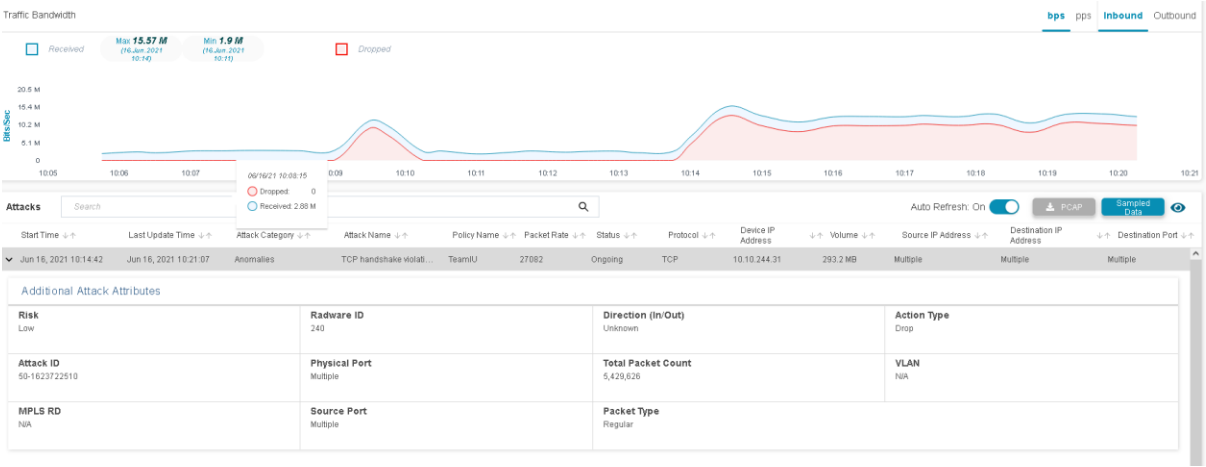
Top Attack Destinations

27.1.31.100	100.00%

Protections — Show Events by Category ○ Show Events Table — + Blocklist / Allowlist

Protection Name	Attack Rate	Drop Rate
Anomalies	10.83 Mbps	10.83 Mbps

5. You can view on the **Analytics AMS → DefensePro Attacks** select the ongoing Out-of-State attack to see details.



Start Time	Last Update Time	Attack Category	Attack Name	Policy Name	Packet Rate	Status	Protocol	Device IP Address	Volume	Source IP Address	Destination IP Address	Destination Port
Jun 16, 2021 10:14:42	Jun 16, 2021 10:21:07	Anomalies	TCP handshake violati...	TeamIU	27082	Ongoing	TCP	10.10.244.31	293.2 MB	Multiple	Multiple	Multiple

Additional Attack Attributes

Risk Low	**Radware ID** 240	**Direction (In/Out)** Unknown	**Action Type** Drop
Attack ID 50-1623722510	**Physical Port** Multiple	**Total Packet Count** 5,429,626	**VLAN** N/A
MPLS RD N/A	**Source Port** Multiple	**Packet Type** Regular	

6. At Attacker shell **stop** the attack. (CTRL-C).
7. Try a PSH-ACK flood: hping3 -p 80 -PA --rand-source --flood 27.1.31.100
8. Repeat the views above to examine the attack.
9. **Export** and save configuration file as **dp8-OOSLab-config.txt**.

For questions, contact training@Radware.com