radware

Alteon
34.x

Alteon Level 1 Lab Manual SSL Services

Table of Contents

Objectives

After viewing the “SSL Services” training module and completing this lab, you should be able to:

- Enable and configure SSL services on Alteon.
- Create Certificate and SSL policy.

Overview

In this lab, we enable SSL -- Alteon’s services for acceleration and offloading capabilities.
Secure Sockets Layer (SSL) is a security layer that can be added to various communication protocols.
SSL performs encryption, decryption, and verification of transmissions between clients and servers.

SSL relieves the back-end servers of tasks, thus enabling the servers to maximize their performance and efficiency, resulting in faster server response times and increased server capacity to handle more concurrent users.

Lab Preparations: Restore SLB

Before you begin this lab:
a. You should have successfully completed SLB configuration.
b. Access Alteon management port and login.
Import SLB configuration or make sure it is already the Alteon configuration.
c. Verify your SLB configuration works properly before continuing.

Lab Activities

Here is a summary of what you will be doing in lab:

1. SSL Acceleration
   - Enable SSL globally
   - Create a certificate
   - Define SSL Policy
   - Associate to virtual service
2. Validate your configuration

SSL Acceleration

IMPORTANT: Enable SSL globally to begin this lab.
Radware lab uses Alteon version 34.x and SSL is already enabled by default.

a) **Configuration → Application Delivery → SSL**
b) Check “**Enable SSL**”

IMPORTANT: For these labs we use HA setup. All certificates need present on both Alteon. Therefore, we enable certificate synchronization. If not already configured, do the steps below.

a) **Configuration → Network → High Availability → Configuration Sync → Modules to Sync**
b) Check “**Certificates**”
c) **Certificate Passphrase** use **“Radware2”** and confirm by a same value.
d) **Apply** and **Sync** configuration to Alteon-B
e) Verify configuration of Alteon-B, is a same sync configuration there? No, it isn’t since the secret can’t configured by sync. Therefore, redo this change again on device B.

Step 1: Certificate Management

Continue configuration on device A. Generate a self-signed server certificate for a service (key will be added).

Self signed Server Certificate	
Certificate ID	Team1
Certificate Name	MyTeam1Cert
Certificate Common Name	www.radware.lab
Any other values	Use default settings or as desired

Verify that self-signed certificate, certificate signing request and key are added.

a) **Configuration → Application Delivery → SSL → Certificate Repository**
b) Click + [add to certificate repository]
   - Certificate ID: Team1
   - Common Name: www.radware.lab
   - Description: MyTeam1Cert
c) Click Submit
d) Select Team1 Server Certificate
e) Click Generate

NOTE: You might need to click refresh (Alteon GUI top right next to the alert bell) to see the certificate status change to “Generated”.

Step 2: SSL Policy Definition

Define SSL Policy which will govern SSL behavior.

SSL Policy	
SSL policy ID	MyPolicy
SSL policy Name	EasySSLPolicy
cipher	main

Remember to enable the policy.

GUI:

a) **Configuration → Application Delivery → SSL → SSL Policy**
b) Click + [add SSL policy]
   - Check Enable SSL Policy
   - Policy ID: MyPolicy
   - Description: EasySSLPolicy
   - Cipher Suite: Main
c) Submit
d) Apply

Step 3: Virtual Service Association

Associate to virtual service.

a. Associate HTTPS service (defined).
b. Bind Certificate to service
c. Bind SSL Policy to service
d. Add PIP (proxy IP) 10.200.1.15 on service 443 https.

Remember to apply configuration changes

GUI:

a) **Configuration → Application Delivery → Virtual Services**
b) Double-click on virtual service Virt1 to edit
c) Virtual Service tab:
    a. Click + to add service
    b. Add HTTPS virtual service
        i. Application: HTTPS
        ii. Service Port: 443
        iii. Group ID: Group1
        iv. Properties tab:
            1. Real server Port: 80
            2. Delayed Binding: Force Proxy
        v. SSL tab:
            1. Server Certificate Type: Certificate
            2. Server Certificate: Team1
            3. SSL Policy: MyPolicy
        vi. Proxy IP tab:
            1. Client NAT Mode: Address/Subnet
            2. Client NAT IPv4 Address: 10.200.1.15
            3. Mask: 255.255.255.255
d) Apply
e) Save
f) Sync

Validate your Configuration

1. Check SLB configuration.

CLI:

```
/c/slb/cur
```

2. Verify configuration by generating test-traffic to your servers.

a. Connect to your server(s) from your RDP PC by browsing to https://www.radware.lab/
b. View statistics on your virtual server connection -- then clear statistics.

CLI:

```
/stat/slb/clear
/stat/slb/virt Virt1 443
```

GUI:

Monitoring → Overview → Service Status View

GUI Cyber Controller:

Analytics ADC → Applications

*Be sure to select Virt1:443 app from the applications list.

3. Export configuration.

Name exported file: SSL_Services.

For questions, contact training@Radware.com