SSL Insight and Load Balancing for Thunder ADC
Table of Contents

1 Overview ........................................................................................................................................................................... 3
2 Deployment Prerequisites ...................................................................................................................................................... 3
3 Architecture Overview .......................................................................................................................................................... 3
   3.1 SSL Insight with an Inline Security Deployment .................................................................................................. 4
   3.2 Firewall Load Balancing .............................................................................................................................................. 5
4 Configuration Overview ........................................................................................................................................................ 6
   4.1 CA Certificate ............................................................................................................................................................... 6
   4.2 Thunder ADC Appliance Configuration Overview .................................................................................................... 7
      4.2.1 L2/L3 and High Availability ................................................................................................................................ 7
      4.2.2 Firewall Load Balancing Configuration Overview ................................................................................................ 7
      4.2.3 SSL Insight Configuration Overview .................................................................................................................... 8
   4.3 Security Device Configuration Overview ..................................................................................................................... 9
5 Configuration Steps for Thunder ADC Appliance .............................................................................................................. 9
   5.1 L2/L3 and High Availability on the Thunder ADC Appliances ..................................................................................... 9
   5.2 FWLB Configuration on the Thunder ADC Appliances ............................................................................................ 18
      5.2.1 Internal Thunder ADC Appliance ...................................................................................................................... 18
      5.2.2 External Thunder ADC Appliance .................................................................................................................... 24
   5.3 SSL Insight Configuration on the Thunder ADC Appliances ...................................................................................... 25
      5.3.1 Internal Thunder ADC Appliance ...................................................................................................................... 25
      5.3.2 External Thunder ADC Appliance .................................................................................................................... 31
6 Configuration Steps for Security Device ............................................................................................................................ 33
7 Summary ............................................................................................................................................................................... 33

Appendix A. Complete Configuration File for the Thunder ADC Appliance ........................................................................... 34
Appendix B. Detailed Walkthrough of SSL Insight Packet Flow ........................................................................................... 39
Appendix C. SSL Insight Certificate Installation Guide ....................................................................................................... 40
   Generating a CA Certificate .............................................................................................................................................. 40
   Exporting a Certificate from Thunder ADC .................................................................................................................. 40
   Installing a Certificate in Microsoft Windows 7 for Internet Explorer ......................................................................... 41
   Installing Certificate in Google Chrome ......................................................................................................................... 47
   Installing a Certificate in Mozilla Firefox ...................................................................................................................... 50
About A10 Networks .................................................................................................................................................................. 52

Disclaimer

This document does not create any express or implied warranty about A10 Networks or about its products or services, including but not limited to fitness for a particular use and noninfringement. A10 Networks has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks assumes no responsibility for its use. All information is provided “as is.” The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact A10 Networks for current information regarding its products or services. A10 Networks’ products and services are subject to A10 Networks’ standard terms and conditions.
1 Overview
A wide range of security devices require visibility into network traffic—including encrypted traffic—to discover attacks, intrusions, and data exfiltration. Growing SSL bandwidth, coupled with increasing SSL key lengths and more computationally complex SSL ciphers, make it difficult for even the most powerful inline security devices to decrypt SSL traffic. On top of today’s SSL performance challenges, many types of security devices are deployed non-inline to monitor network traffic. Often, these devices cannot decrypt outbound SSL traffic.

To eliminate the SSL blind spot in corporate defenses, A10 Networks® has introduced SSL Insight™, a feature included in the A10 Thunder® Application Delivery Controller (ADC) product line. A10 Networks SSL Insight decrypts SSL traffic and enables third party security products to inspect the unencrypted traffic.

When configured for SSL Insight, the Thunder ADC intercepts SSL traffic, decrypts it and forwards it to a security device such as a firewall, an Intrusion Prevention System (IPS) or an advanced threat prevention platform. Thunder ADC can also mirror the unencrypted traffic to non-inline security devices such as analytics or forensics products. A second Thunder ADC appliance then takes this traffic and encrypts it again, and sends it to the remote destination.

Using A10’s Application Delivery Partitions (ADPs), SSL Insight can be configured with a single Thunder ADC appliance for encryption, decryption, and load balancing.

2 Deployment Prerequisites
The requirements for SSL Insight deployment are:

- One or more Thunder ADC appliance(s) with A10 Networks Advance Core Operating System (ACOS®) version 2.7.0 or later.
- A third-party security device such as a firewall, security analytics or forensics appliance or threat prevention platform.

Note: The CLI commands and GUI screenshots presented in this guide are based on ACOS version 2.7.2.

3 Architecture Overview
This section illustrates a joint solution of A10 Networks Thunder ADCs and a third party security device for SSL Insight. The SSL Insight services are provided by the Thunder ADC appliances while the traffic inspection and monitoring services are provided by the third party security devices. This deployment also utilizes firewall load balancing (FWLB) and VRRP-A features, which makes the SSL Insight solution highly available and efficient.

Notes:

- VRRP-A is a Thunder ADC high availability protocol optimized for Server Load Balancing (SLB), and differs significantly from the industry-standard implementation of Virtual Router Redundancy Protocol (VRRP). For purposes of operational familiarity, VRRP-A borrows concepts from VRRP, but is not VRRP. VRRP-A will not inter-operate with VRRP.
- The security devices in this deployment guide are set up in Layer 2 (L2) mode.
### 3.1 SSL Insight with an Inline Security Deployment

The objective of the SSL Insight feature is to transparently intercept SSL traffic, decrypt it and send it through the security device(s) in clear text. After the security device has inspected the intercepted traffic, it is re-encapsulated in SSL and sent to the destination. A ladder-diagram is provided in Appendix B to show this process in more detail.

There are three distinct stages for traffic in such a solution, depicted in Figure 2:

1. From client to the internal Thunder ADC appliance, where traffic is encrypted.
2. From the internal Thunder ADC appliance to the external Thunder ADC appliance, through the security device. Traffic is in clear text in this segment.
3. Traffic from the external Thunder ADC appliance to the remote server, where traffic is encrypted again.

**Note:** Please refer to the ACOS Application Delivery & Server Load Balancing Guide for additional details on the SSL Insight feature.
3.2 Firewall Load Balancing

The firewall load balancing (FWLB) feature allows load sharing between multiple security devices. The typical deployment is in a sandwich style design where the Thunder ADC appliance load balances the external and internal zones of the security devices. The number of security devices in the solution can be extended as required. The A10 firewall load balancing solution can work with HTTP, HTTPS, Generic TCP, Generic UDP, DNS, SIP and FTP.

This design can scale up to fifteen separate firewall load balancing paths.
4 Configuration Overview

The configuration for the SSL Insight solution can be divided into the following portions:

1. Layer 2/3 (L2/L3) and High Availability on the Thunder ADC appliance
2. SSL Insight configuration on the Thunder ADC appliance
3. FWLB configuration on the Thunder ADC appliance
4. Configuration on the third-party security device

4.1 CA Certificate

A prerequisite for configuring the SSL Insight feature is a CA certificate with a known private key, such as a self-signed CA certificate generated on the A10 Thunder appliance or on a Linux system.

The following CLI command generates and initializes a self-signed CA certificate on the Thunder ADC appliance.

```
slb ssl-create certificate <certificate name>
```

The following two commands generate and initialize a CA Certificate on a Linux system with an OpenSSL package installed.

```
openssl genrsa -out <name>.key
openssl req -new -x509 -days 3650 -key <name>.key -out <name>.crt
```
Once generated, the certificate can be imported onto the Thunder ADC appliances in the internal zone using SFTP or SCP.

```
import ssl-cert <certificate name> scp://[user@]host/<source file>
```

This CA certificate must also be pushed to all client machines on the internal network. If the CA certificate is not pushed, the internal hosts will get an SSL “untrusted root” error whenever they try to connect to a site with SSL enabled. This can be done manually (Appendix C), or using an automated service such as Microsoft Group Policy Manager. Automated login scripts can achieve the same result for organizations that use Linux or UNIX clients.


### 4.2 Thunder ADC Appliance Configuration Overview

The following sections provide more information about the Thunder ADC configuration items listed above.

#### 4.2.1 L2/L3 and High Availability

The solution has a pair of Thunder ADC appliances in the external zone of the security devices and another pair in the internal zone of the security devices. Each pair is running VRRP-A to provide redundancy.

A key requirement of this solution is to have each security device in a separate VLAN. The topology shown in Figure 1 has a Red VLAN and a Green VLAN. There is one security device in the Red VLAN and one in the Green VLAN. Each security device is tied to one VRRP-A instance on the external appliance pair, and one VRRP-A instance on the internal appliance pair. The VRIDs must be unique on either side of the security device to avoid MAC address conflicts.

Each VRRP-A instance is attached to a single VLAN and tracks the member interface and the upstream interface that connects to the gateway. This ensures that a failover occurs under any of the following circumstances:

- An interface goes down
- A cable is disconnected
- The entire device goes down

#### 4.2.2 Firewall Load Balancing Configuration Overview

Firewall load balancing configuration is required in order to ensure that all traffic is load balanced across all available security devices. The FWLB configuration is slightly different on the external Thunder ADC appliance pair compared to the internal Thunder ADC appliance pair. Additionally, the configuration is identical on both devices in the same high availability pair, except for the VRRP-A priority. This guide discusses the configuration of only one external Thunder ADC appliance and one internal Thunder ADC appliance.

**Load Balancing Configuration on Internal Thunder ADC Appliance**

- All TCP and UDP traffic is intercepted.
  - Access Control List (ACL) is created to define traffic of interest.
  - Wildcard VIP is defined, and uses this ACL.
  - TCP port 0, UDP port 0 and “others” port 0 are defined under the wildcard VIP.
- The remote VRRP-A address of each VLAN is added as an SLB server. Each security device path is associated with a single VLAN and thus traffic from the internal Thunder ADC potentially will traverse each security device.
  - The command `slb server` is used to define security device paths.
- Once traffic is intercepted, it is routed to one of the security devices based on the configured algorithm (in this case, round-robin). Destination-NAT is disabled for this traffic.
  - The command `no-dest-nat` helps achieve this.
Load Balancing Configuration on External Thunder ADC Appliance

Another wildcard VIP is configured on the external Thunder ADC pair. This wildcard VIP intercepts all incoming traffic from the security devices, and sends it to the default router. However, while doing so, the Thunder ADC appliance also creates internal sessions. The MAC address of the security device from which the traffic was received is also stored in this session. This step is to ensure that the return traffic belonging to this session will be sent through the same security device from which it was received.

- All TCP, UDP and IP traffic is intercepted.
  - ACL is created to define traffic of interest.
  - Wildcard VIP is defined with this ACL.
  - TCP port 0, UDP port 0 and "others" port 0 are defined on the wildcard VIP.
- Next-hop gateway (default router) is defined and added to a service group.
  - The command `slb server` is used to define the default router IP address.
- The source MAC address of the incoming traffic is preserved so that the response traffic can be sent through the same security device path.
  - The command `use-rcv-hop-for-resp` is used for this.
- Destination-NAT is disabled for this traffic.
  - The command `no-dest-nat` helps achieve this.

4.2.3 SSL Insight Configuration Overview

The SSL Insight configuration has many similarities to the FWLB configuration. The primary difference is that client-SSL and server-SSL templates are required on the internal and the external Thunder ADC appliances respectively. Additionally, only SSL traffic is intercepted.

Just like FWLB, the SSL Insight configuration is slightly different on the external Thunder ADC appliances compared to the internal Thunder ADC appliances. Also, the configuration is identical on both devices in the same high availability pair, except for the VRRP-A priority. This guide discusses the configuration of only one external Thunder ADC appliance and one internal Thunder ADC appliance.

**Note:** SSL Insight can decrypt HTTPS traffic only. In ACOS 4.0.1, SSL Insight will also support SMTPS and XMPP traffic.

SSL Insight Configuration on Internal Thunder ADC Appliance

SSL Insight configuration on the internal Thunder ADC appliance has the following key elements:

- SSL traffic entering on port 443 is intercepted.
  - Port 443 is defined under a wildcard VIP to achieve this.
- The SSL server certificate is captured during the SSL handshake; all X.509 DN attributes are duplicated, except for the issuer and base64 encoded public key.
  - Client-SSL template is used for this. The Client-SSL template includes the required command `forward-proxy-enabled`, along with the local CA certificate (from 4.1) and its private key which is used for signing dynamically forged certificates.
- The remote VRRP-A address of each VLAN is added as an SLB server. Each security device path is associated with a single VLAN and thus traffic from the internal Thunder ADC potentially will traverse each security device. Port 8080 is defined for each security device path.
  - The command `slb server` defines a security device path and port number 8080 is added.
- Along with the protocol (HTTPS to HTTP), the destination port also gets changed from 443 to 8080.
  - Service group is defined with port 8080 and bound to the virtual port.
- However, the destination IP (i.e. Internet Server IP) remains unchanged.
  - The command `no-dest-nat port-translation` achieves this.
- The incoming SSL traffic is intercepted and decrypted, and is then forwarded in clear text over HTTP on port 8080 through the security device.
SSL Insight Configuration on External Thunder ADC Appliance

SSL Insight configuration on the external Thunder ADC appliance is simpler than on the internal Thunder ADC appliance; it has the following characteristics:

- Clear-Text HTTP traffic entering on port 8080 is intercepted.
  - Port 8080 is defined under a wildcard VIP to achieve this.
- The next-hop gateway (default router) is defined as an SLB server.
  - The command `slb server` defines the default router IP address and port number 443 is added.
- Along with the protocol (HTTP to HTTPS), the destination port also gets changed from 8080 to 443.
- Service group is defined with port 443 and bound to the virtual port.
  - However, the destination IP (i.e. Internet Server IP) remains unchanged.
  - The command `no-dest-nat port-translation` achieves this.
- The source MAC of the incoming traffic is preserved so that the response traffic can be sent through the same security device path.
  - The command `use-rcv-hop-for-resp` is used for this.
- Incoming HTTP traffic is converted into SSL traffic and sent out on port 443.
  - A server-SSL template is defined and applied to the virtual port. The template includes the command `forward-proxy-enable`. Optionally, a root CA certificate store file also may be applied to the server-SSL template.

4.3 Security Device Configuration Overview

The security devices must be configured according to the recommend best practices of the security vendor. The key requirements for an SSL Insight and load balancing deployment are:

- ARP packets should be allowed for VRRP-A packets on both internal and external Thunder ADC appliances.
- Health-check packets should be allowed from internal Thunder ADC appliances to the VRRP-A addresses on the external Thunder ADC appliances, since the security devices are configured as SLB servers.

5 Configuration Steps for Thunder ADC Appliance

This section provides detailed steps for configuring the Thunder ADC appliances for SSL Insight. In order to avoid redundancy, most of the CLI commands and GUI screenshots will focus on the primary, internal Thunder ADC, unless explicitly specified. Complete configuration from both internal and external Thunder ADC pairs is given in Appendix A.

5.1 L2/L3 and High Availability on the Thunder ADC Appliances

The steps in this section configure the following L2/L3 parameters:

- VLANs and their router interfaces.
- Virtual Ethernet (VE) interfaces, which are IP addresses assigned to VLAN router interfaces.
- VRRP-A for high availability.
The goal is to achieve the following IP addressing scheme on all four Thunder ADC appliances as shown in Figure 1:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>VE IP Address</th>
<th>Interface</th>
<th>VRID</th>
<th>VRID IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inside Primary ADC</td>
<td>10</td>
<td>10.10.1.2 /24</td>
<td>eth1</td>
<td>default</td>
</tr>
<tr>
<td></td>
<td>15</td>
<td>10.15.1.2 /24</td>
<td>eth5</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>10.16.1.2 /24</td>
<td>eth6</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>99</td>
<td>10.99.1.1 /24</td>
<td>eth18</td>
<td>n/a</td>
</tr>
<tr>
<td>Inside Secondary ADC</td>
<td>10</td>
<td>10.10.1.3 /24</td>
<td>eth1</td>
<td>default</td>
</tr>
<tr>
<td></td>
<td>15</td>
<td>10.15.1.3 /24</td>
<td>eth5</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>10.16.1.3 /24</td>
<td>eth6</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>99</td>
<td>10.99.1.2 /24</td>
<td>eth18</td>
<td>n/a</td>
</tr>
<tr>
<td>Outside Primary ADC</td>
<td>20</td>
<td>20.1.1.2 /24</td>
<td>eth1</td>
<td>default</td>
</tr>
<tr>
<td></td>
<td>15</td>
<td>20.1.1.12 /24</td>
<td>eth5</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>20.1.1.12 /24</td>
<td>eth6</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>199</td>
<td>20.1.1.12 /24</td>
<td>eth18</td>
<td>n/a</td>
</tr>
<tr>
<td>Outside Secondary ADC</td>
<td>20</td>
<td>20.1.1.3 /24</td>
<td>eth1</td>
<td>default</td>
</tr>
<tr>
<td></td>
<td>15</td>
<td>20.1.1.13 /24</td>
<td>eth5</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>20.1.1.13 /24</td>
<td>eth6</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>199</td>
<td>20.1.1.13 /24</td>
<td>eth18</td>
<td>n/a</td>
</tr>
</tbody>
</table>

Configure the VLANs and add Ethernet and Router Interfaces

Configure the following VLAN parameters as shown in Figure 1:

- VLAN-10: This is the uplink to the internal network. Add `router-interface ve 10` along with the Ethernet interface.
- VLAN-15: This is the path to the external Thunder ADC appliances through security device-1. Add `router-interface ve 15` along with the Ethernet interface.
- VLAN-16: This is the path to the external Thunder ADC appliances through security device-2. Add `router-interface ve 16` along with the Ethernet interface.
- VLAN-99: This is the VLAN for VRRP-A sync messages. Add `router-interface ve 99` along with the Ethernet interface.

Using the CLI:

```
ACOS (config) #vlan 10
ACOS (config-vlan:10) #untagged ethernet 1
ACOS (config-vlan:10) #router-interface ve 10
ACOS (config-vlan:10) #exit
ACOS (config) #vlan 15
ACOS (config-vlan:15) #untagged ethernet 5
ACOS (config-vlan:15) #router-interface ve 15
ACOS (config-vlan:15) #exit
ACOS (config) #vlan 16
ACOS (config-vlan:16) #untagged ethernet 6
ACOS (config-vlan:16) #router-interface ve 16
ACOS (config-vlan:16) #exit
ACOS (config) #vlan 99
ACOS (config-vlan:99) #untagged ethernet 18
ACOS (config-vlan:99) #router-interface ve 99
ACOS (config-vlan:99) #exit
ACOS (config) #
```
Using the GUI:

1. Navigate to **Config Mode > Network > VLAN > VLAN**.
2. Click **Add**.
3. Enter the **VLAN ID**, select the interfaces, and enter the VE ID (same as the VLAN number).
4. Click **OK**.
5. Repeat for each VLAN.

![Figure 4. VLAN configuration](image)

The VLAN configuration should look similar to the following after all four VLANs have been added.

![Figure 5. VLAN settings](image)
Configure IP Addresses on the VLAN Router Interfaces

Make sure to enable the promiscuous VIP option under ve10, in order to subject inbound traffic to Wildcard VIP (more to be discussed later).

**Using the CLI:**

ACOS (config) #interface ve 10
ACOS (config-if:ve10) #ip address 10.10.1.2 /24
ACOS (config-if:ve10) #ip allow-promiscuous-vip
ACOS (config-if:ve10) #exit
ACOS (config) #interface ve 15
ACOS (config-if:ve15) #ip address 10.15.1.2 /24
ACOS (config-if:ve15) #exit
ACOS (config) #interface ve 16
ACOS (config-if:ve16) #ip address 10.16.1.2 /24
ACOS (config-if:ve16) #exit
ACOS (config) #interface ve 99
ACOS (config-if:ve99) #ip address 10.99.1.1 /24
ACOS (config-if:ve99) #exit

**Using the GUI:**

1. Navigate to **Config Mode > Interface > Virtual**. The interfaces configured above should be visible.
2. Click on “ve-10” and configure the IPv4 address.
3. Click on **VIP** to display the configuration options.
4. Select **Allow Promiscuous VIP**.
5. Click **OK** when done.
6. Repeat for each VE.

*Figure 6. Virtual Ethernet (VE) interface configuration*
Configure VRRP-A on the Internal Thunder ADC Appliances

1. Set unique VRRP-A device IDs on both Thunder ADC appliances.
2. Configure the same set ID on both Thunder ADC appliances.
3. Configure VRIDs and assign floating IPs.
   
   In this step, the following VRIDs are configured:
   - VRID-Default: This VRID will be used for the enterprise switch, floating IP 10.10.1.1.
   - VRID-15: This VRID will be used for VLAN-15, floating IP 10.15.1.1.
   - VRID-16: This VRID will be used for VLAN-16, floating IP 10.16.1.1.
4. Configure and enable a VRRP-A interface.
5. Repeat the steps above on the external Thunder ADC appliance pair.

*Note*: The VRIDs must be unique on the internal and external Thunder ADC appliances.

**Using the CLI:**

ACOS(config)#vrrp-a device-id 1
ACOS(config)#vrrp-a set-id 1
ACOS(config)#vrrp-a vrid default
ACOS(config-vrid-default)#floating-ip 10.10.1.1
ACOS(config-vrid-default)#priority 200
ACOS(config-vrid-default)#tracking-options
ACOS(config-vrid-tracking)#interface ethernet 1 priority-cost 60
ACOS(config-vrid-tracking)#interface ethernet 5 priority-cost 60
ACOS(config-vrid-tracking)#interface ethernet 6 priority-cost 60
ACOS(config-vrid-tracking)#exit
ACOS(config-vrid-default)#vrrp-a vrid 5
ACOS(config-vrid)#floating-ip 10.15.1.1
ACOS(config-vrid)#priority 200
ACOS(config-vrid)#tracking-options
ACOS(config-vrid-tracking)#interface ethernet 1 priority-cost 60
ACOS(config-vrid-tracking)#interface ethernet 5 priority-cost 60
ACOS(config-vrid-tracking)#interface ethernet 6 priority-cost 60
ACOS(config-vrid-tracking)#exit
ACOS(config-vrid)#vrrp-a vrid 6
ACOS(config-vrid)#floating-ip 10.16.1.1
ACOS(config-vrid)#priority 200
ACOS(config-vrid)#tracking-options
ACOS(config-vrid-tracking)#interface ethernet 1 priority-cost 60
ACOS(config-vrid-tracking)#interface ethernet 5 priority-cost 60
ACOS(config-vrid-tracking)#interface ethernet 6 priority-cost 60
ACOS(config-vrid-tracking)#exit
ACOS(config-vrid)#exit
ACOS(config)#vrrp-a interface ethernet 18 vlan 99
ACOS(config)#vrrp-a enable

Repeat on the external Thunder ADC appliance pair. Make sure to use unique IP addresses.
Using the GUI:

1. Navigate to **Config Mode > System > VRRP-A > Setting > VRRP-A Global**.
2. Select the **Device ID**. Each device in the VRRP-A set must have a unique VRRP-A device ID.
3. In the **Set ID** field, enter ‘1’.
4. Click on **VRID** to display the options.
   a. Select ‘default’ from the **VRID** drop-down list.
   b. Enter priority ‘200’.
   c. Click **Add**.

![Figure 7. VRRP-A global configuration](image-url)
5. Repeat for VRIDs 5 and 6.
6. Click **Float IP Address** to display floating IP address options.
   a. Select “default” from the VRID drop-down list.
   b. Add IPv4 address 10.10.1.1.
   c. Click **Add**.
   d. Repeat for VRIDs 5 and 6.
7. Click **VRRP-A Tracking** to display VRRP-A tracking options.
   a. Under **Interface**: Select “5” from the **VRID** drop-down list.
   b. Select “Ethernet1” from the **Interface** drop-down list.
   c. Enter “60” under Priority Cost.
   d. Click **Add**.
   e. Repeat for Interfaces Ethernet5 and Ethernet6.
   f. Repeat for VRIDs “default” and “6”.
   a. Click on Ethernet 18.
   b. Configure VLAN 99.
   c. Enable all options: Status, VRRP-A Status, and Heartbeat.
   d. Click OK.
9. Repeat the steps above on the external Thunder ADC appliance pair. Make sure to use unique IP addresses.


### 5.2 FWLB Configuration on the Thunder ADC Appliances

The following commands will configure firewall load balancing configuration on the Thunder ADC appliances.

#### 5.2.1 Internal Thunder ADC Appliance

The steps in this section configure load balancing parameters on the internal Thunder ADC appliance.

**Configure Servers for VLAN-15 and VLAN-16**

These steps configure an `slb server` with TCP port 0 and UDP port 0, and with the VRRP-A address of the first VLAN. Then a second server is configured, with the VRRP-A address of the second VLAN.

**Using the CLI:**

```
ACOS (config)#slb server SecurityDevice1_Path 10.15.1.11
ACOS (config-real server)#port 0 tcp
ACOS (config-real server-node port)#no health-check
ACOS (config-real server)#port 0 udp
ACOS (config-real server-node port)#no health-check
ACOS (config-real server-node port)#exit
ACOS (config)#exit
ACOS (config)#slb server SecurityDevice2_Path 10.16.1.11
ACOS (config-real server)#port 0 tcp
ACOS (config-real server-node port)#no health-check
ACOS (config-real server)#port 0 udp
ACOS (config-real server-node port)#no health-check
ACOS (config-real server-node port)#exit
```
Using the GUI:

1. Navigate to Config Mode > SLB > Service > Server.
2. Click Add.
3. Enter the following settings:
   a. Name: "SecurityDevice1_Path"
   b. IP Address: 10.15.1.11
4. Enter Port parameters:
   a. Port: “0”
   b. Protocol: "TCP"
   d. Click Add.
   e. Repeat for UDP port 0.
5. Click OK.

![Server configuration (internal)](image-url)
6. Repeat for the second VLAN, using a unique IP address.

Configure a Service Group

These steps add the SLB servers to SLB service groups.

**Using the CLI:**

```
ACOS (config) # slb service-group LB_Paths_TCP tcp
ACOS (config-slb svc group) # member SecurityDevice1_Path:0
ACOS (config-slb svc group) # member SecurityDevice2_Path:0
ACOS (config-slb svc group) # exit
ACOS (config) # slb service-group LB_Paths_UDP udp
ACOS (config-slb svc group) # member SecurityDevice1_Path:0
ACOS (config-slb svc group) # member SecurityDevice2_Path:0
ACOS (config-slb svc group) # exit
```
Using the GUI:
1. Navigate to Config Mode > SLB > Service > Service Group.
2. Click Add.
3. Enter the following parameters:
   a. Name: “LB_Paths_TCP”
   b. Type: “TCP”
4. Click on Server.
6. Select the Port, “0”.
7. Click Add.
8. Repeat for UDP port 0.
10. Click OK.

Figure 15. Service group configuration (internal)
Configure the ACL

These steps configure an extended ACL to intercept incoming traffic on VLAN-10. This ACL will be used as part of the wildcard VIP configuration, below.

**Using the CLI:**

```
ACOS (config) #access-list 100 permit ip any any vlan 10
```

**Using the GUI:**

1. Navigate to **Config Mode > Security > Network > ACL > Extended**.
2. Click **Add**.
3. Enter or select the following settings:
   a. **ID**: "100"
   b. **Action**: "Permit"
   c. **Protocol**: "IP"
   d. **Source Address**: "Any"
   e. **Destination Address**: "Any"
   f. **VLAN ID**: "10"
4. Click **OK**.

![Figure 16. Servers (internal)](image-url)
Add UDP port 0, TCP port 0 and Others Port 0 to a Wildcard VIP

These commands add the service groups to TCP, UDP and “others” wildcard VIP ports. The `no-dest-nat` command is used to preserve the destination IP address load-balanced traffic. The “others” wildcard port can take an already defined TCP service group or UDP service group. In this example, the UDP service group is used.

```
ACOS (config)#slb virtual-server Outbound_Wildcard_VIP 0.0.0.0 acl 100
ACOS (config-slb vserver)#port 0 tcp
ACOS (config-slb vserver-vport)#service-group LB_Paths_TCP
ACOS (config-slb vserver-vport)#no-dest-nat
ACOS (config-slb vserver)#exit
ACOS (config-slb vserver)#port 0 udp
ACOS (config-slb vserver-vport)#service-group LB_Paths_UDP
ACOS (config-slb vserver-vport)#no-dest-nat
ACOS (config-slb vserver)#port 0 others
ACOS (config-slb vserver-vport)#service-group LB_Paths_UDP
ACOS (config-slb vserver-vport)#no-dest-nat
ACOS (config-slb vserver)#exit
ACOS (config-slb vserver)#exit
```

**Using the GUI:**

1. Navigate to Config Mode > Service > SLB > Virtual Server.
2. Click Add.
3. Enter or select the following settings:
   a. **Name:** “Outbound_Wildcard_VIP”
   b. **Wildcard:** Select the checkbox.
   c. **Access List:** “100”
4. Click Add in the Port section.
5. Enter or select the following settings:
   a. Type: "TCP"
   b. Port: "0"
   c. Service Group: "LB_Paths_TCP"
   d. Direct Server Return: Select Enabled.

6. Click OK to exit the Virtual Server Port configuration page.
7. Click OK to exit the Virtual Server configuration page.

---

5.2.2 External Thunder ADC Appliance

The steps in this section configure FWLB parameters on the external Thunder ADC appliance.

**Note:** For brevity, only the CLI commands are shown in this section.

**Add TCP Port 0 and UDP Port 0 to the Gateway Path**

ACOS (config)#slb server Default_Gateway 20.1.1.10
ACOS (config-real server)#port 0 tcp
ACOS (config-real server-node port)#no health-check
ACOS (config-real server-node port)#exit
ACOS (config-real server)#port 0 udp
ACOS (config-real server-node port)#no health-check
ACOS (config-real server-node port)#exit
ACOS (config-real server)#exit
Add the TCP and UDP Gateway Path to Service Groups

ACOS(config)#slb service-group DG_TCP tcp
ACOS(config-slb svc group)#member Default_Gateway:0
ACOS(config-slb svc group)#exit
ACOS(config)#slb service-group DG_UDP udp
ACOS(config-slb svc group)#member Default_Gateway:0
ACOS(config-slb svc group)#exit

Configure an ACL to Intercept Incoming Traffic on VLAN-15 and VLAN-16 for a Wildcard VIP

These steps configure an extended ACL to intercept traffic on VLAN-15 and VLAN-16. This ACL will be used as part of the wildcard VIP configuration, below.

Using the CLI:

ACOS(config)#access-list 101 permit ip any any vlan 15
ACOS(config)#access-list 101 permit ip any any vlan 16

Add UDP port 0, TCP port 0 and Others Port 0 to a Wildcard VIP

These commands add the service groups to TCP, UDP and 'others' wildcard VIP ports. The no-dest-nat command is used to preserve the destination IP address load-balanced traffic. The command use-rcv-hop-for-resp is used so that response traffic goes back through the same path through which the request traffic arrives.

ACOS(config)#slb virtual-server Inside_To_Outside 0.0.0.0 acl 101
ACOS(config-slb vserver)#port 0 tcp
ACOS(config-slb vserver-vport)#service-group DG_TCP
ACOS(config-slb vserver-vport)#use-rcv-hop-for-resp
ACOS(config-slb vserver-vport)#no-dest-nat
ACOS(config-slb vserver-vport)#exit
ACOS(config-slb vserver-vport)#port 0 udp
ACOS(config-slb vserver-vport)#service-group DG_UDP
ACOS(config-slb vserver-vport)#use-rcv-hop-for-resp
ACOS(config-slb vserver-vport)#no-dest-nat
ACOS(config-slb vserver-vport)#exit
ACOS(config-slb vserver-vport)#port 0 others
ACOS(config-slb vserver-vport)#service-group DG_UDP
ACOS(config-slb vserver-vport)#use-rcv-hop-for-resp
ACOS(config-slb vserver-vport)#no-dest-nat
ACOS(config-slb vserver-vport)#exit
ACOS(config-slb vserver)#exit

5.3 SSL Insight Configuration on the Thunder ADC Appliances

SSL Insight configuration is very similar to FWLB configuration, with the following difference: The internal Thunder ADC will intercept traffic on TCP port 443, decrypt it, and send it in clear text over TCP port 8080 to the security devices. Consequently, the external Thunder ADC will intercept clear text traffic arriving on TCP port 8080 and encrypt it back before sending it to the remote hosts.

The same ACL wildcard VIPs used for FWLB can be used for SSL Intercept.

5.3.1 Internal Thunder ADC Appliance

Use the following steps to configure SSL Insight parameters in the internal Thunder ADC appliance.

Configure Servers for VLAN-15 and VLAN-16

These steps configure TCP port 8080, under the SLB servers configured in FWLB configuration.
Using the CLI:
ACOS (config) #slb server SecurityDevice1_Path 10.15.1.11
ACOS (config-real server) #port 8080 tcp
ACOS (config-real server-node port) #no health-check
ACOS (config-real server-node port) #exit
ACOS (config-real server) #exit
ACOS (config) #slb server SecurityDevice2_Path 10.16.1.11
ACOS (config-real server) #port 8080 tcp
ACOS (config-real server-node port) #no health-check
ACOS (config-real server-node port) #exit

Using the GUI:
1. Navigate to Config Mode > SLB > Service > Server.
2. Select slb server "SecurityDevice1_Path" and click Edit.
3. Enter Port parameters:
   a. Port: "8080"
   b. Protocol: "TCP"
   d. Click Add.
4. Click OK.
5. Repeat for the slb server "SecurityDevice2_Path" as well.

![Figure 19. Server port configuration (internal)](image)

Configure a Service Group
These steps add the servers to a service group.

Using the CLI:
ACOS (config) #slb service-group SSLi tcp
ACOS (config-slb svc group) #member SecurityDevice1_Path:8080
ACOS (config-slb svc group) #member SecurityDevice2_Path:8080
ACOS (config-slb svc group) #exit
Using the GUI:
1. Navigate to Config Mode > SLB > Service > Service Group.
2. Click Add.
3. Enter the following parameters:
   a. Name: “SSLi”
   b. Type: “TCP”
4. Click on Server.
6. Select the Port, “8080”.
7. Click Add.
9. Click OK.

![Figure 20. Service group configuration (internal)]
Configure the Client-SSL Template

These steps configure the client-SSL template. The command `forward-proxy-enable` essentially enables SSL Insight on the client-ssl template. The `forward-proxy` is an A10 specific term and is different than the traditional explicit-proxy function.

**Note:** These steps assume that the CA certificate and the private key has been uploaded to the Thunder ADC appliance. For instructions on uploading CA certificates and keys, please refer to the ACOS Application Delivery and Server Load Balancing Guide

**Using the CLI:**

```
ACOS (config)#slb template client-ssl SSLInsight_ClientSide
ACOS (config-client ssl)#forward-proxy-ca-cert SSLi-CA
ACOS (config-client ssl)#forward-proxy-ca-key SSLi-CA
ACOS (config-client ssl)#forward-proxy-enable
ACOS (config-client ssl)#exit
```

**Using the GUI:**

1. Navigate to **Config Mode > SLB > Template > SSL > Client SSL**.
2. Click **Add**.
3. Enter a **Name**, “SSLInsight_ClientSide”.
4. Select **Enabled** next to **SSL Forward Proxy**.
5. Select the CA certificate from the **CA Certificate** drop-down list.
6. Select the private key from the **CA Private Key** drop-down list.
7. Click **OK**.
Configure the Wildcard VIP

These steps will use the same wildcard VIP from FWLB configuration add virtual port 443 for SSL Insight configuration. The no-dest-nat port-translation command is used to convert incoming 443 traffic to port 8080, while preserving the destination IP address.

**Using the CLI:**
```
ACOS(config) #slb virtual-server Outbound_Wildcard_VIP 0.0.0.0 acl 100
ACOS(config-slb vserver)#port 443 https
ACOS(config-slb vserver-vport)#service-group SSLi
ACOS(config-slb vserver-vport)#template client-ssl SSLInsight_ClientSide
ACOS(config-slb vserver-vport)#no-dest-nat port-translation
ACOS(config-slb vserver-vport)#exit
ACOS(config-slb vserver)#exit
```

**Using the GUI:**
1. Navigate to Config Mode > SLB > Service > Virtual Server.
2. Select the “Outbound_Wildcard_VIP” and click **Edit**.
3. Click **Add** in the **Port** section.

4. Enter or select the following settings:
   a. **Type:** "HTTPS"
   b. **Port:** "443"
   c. **Service Group:** "SSLi"
   d. **Direct Server Return:** Select Enabled, and select the **Port Translation** checkbox.
   e. **Client-SSL Template:** "SSLInsight_ClientSide"

5. Click **OK** to exit the Virtual Server Port configuration page.

6. Click **OK** to exit the Virtual Server configuration page.

![Figure 23. Virtual server port configuration (internal)]
5.3.2 External Thunder ADC Appliance

Use the following steps to configure SSL Insight parameters in the external Thunder ADC appliance.

*Note: For brevity, only the CLI commands are shown in this section.*

Add TCP Port 443 to the FWLB Gateway Path

These steps add TCP port 443 for HTTPS traffic under the default gateway path in FWLB configuration.

*Using the CLI:*

ACOS (config) #slb server Default_Gateway 20.1.1.10
ACOS (config-real server) #port 443 tcp
ACOS (config-real server-node port) #no health-check
ACOS (config-real server-node port) #exit
ACOS (config-real server) #exit

Add the Server Port Configuration to a Service Group

These steps add the server port to a service group.

*Using the CLI:*

ACOS (config) #slb service-group DG_SSL tcp
ACOS (config-slb svc group) #member Default_Gateway:443
ACOS (config-slb svc group) #exit

Configure the Server-SSL Template

These steps configure the server-SSL template.

*Using the CLI:*

ACOS (config) #slb template server-ssl SSLInsight_ServerSide
ACOS (config-server ssl) #forward-proxy-enable
ACOS (config-server ssl) #exit

*Using the GUI:*

1. Navigate to *Config Mode > SLB > Template > SSL > Server SSL.*
2. Click *Add.*
3. Enter a *Name,* “SSLInsight_ServerSide”.
4. Select *Enabled next to SSL Forward Proxy.*
5. Leave other fields blank.
6. Click *OK.*
Figure 24. Server-SSL configuration (external)

Configure the Wildcard VIP

These steps will use the same wildcard VIP from FWLB configuration add virtual port 8080 for SSL Insight configuration. The `no-dest-nat port-translation` command is used to convert incoming TCP port 8080 traffic to HTTPS port 443, while preserving the destination IP address. The command `use-rcv-hop-for-resp` is used so that response traffic goes back through the same path through which the request traffic arrives.

**Using the CLI:**

```
ACOS(config)#slb virtual-server Inside_To_Outside 0.0.0.0 acl 101
ACOS(config-slb vserver)#port 8080 http
ACOS(config-slb vserver)#service-group DG_SSL
ACOS(config-slb vserver-vport)#template server-ssl SSLInsight_ServerSide
ACOS(config-slb vserver-vport)#no-dest-nat port-translation
ACOS(config-slb vserver-vport)#use-rcv-hop-for-resp
ACOS(config-slb vserver-vport)#exit
ACOS(config-slb vserver)#exit
```
6 Configuration Steps for Security Device
For this deployment guide, the security devices need to be configured in Layer-2, transparent mode. Refer to the configuration steps from the security device documentation.

7 Summary
The sections above show how to deploy the Thunder ADC device with a third party security device for SSL Insight. SSL Insight, included as a standard feature of Thunder ADC, offers organizations a powerful load-balancing, high availability and SSL decryption solution. Using SSL Insight, organizations can:

• Analyze all network data, including encrypted data, for complete threat protection
• Deploy best-of-breed content inspection solutions to fend off cyber attacks
• Maximize the performance, availability and scalability of corporate networks by leveraging A10’s 64-bit ACOS platform, Flexible Traffic Acceleration (FTA) technology and specialized security processors

For more information about Thunder ADC products:
• http://www.a10networks.com/resources/solutionsheets.php
• http://www.a10networks.com/resources/casestudies.php
## Appendix A. Complete Configuration File for the Thunder ADC Appliance

<table>
<thead>
<tr>
<th>Internal Primary Unit Configuration</th>
<th>Internal Standby Unit Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrrp-a device-id 1</td>
<td>vrrp-a device-id 2</td>
</tr>
<tr>
<td>vrrp-a set-id 1</td>
<td>vrrp-a set-id 1</td>
</tr>
<tr>
<td>hostname ACOS</td>
<td>hostname ACOS</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td>vlan 10</td>
<td>vlan 10</td>
</tr>
<tr>
<td>untagged ethernet 1</td>
<td>untagged ethernet 1</td>
</tr>
<tr>
<td>router-interface ve 10</td>
<td>router-interface ve 10</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td>vlan 15</td>
<td>vlan 15</td>
</tr>
<tr>
<td>untagged ethernet 5</td>
<td>untagged ethernet 5</td>
</tr>
<tr>
<td>router-interface ve 15</td>
<td>router-interface ve 15</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td>vlan 16</td>
<td>vlan 16</td>
</tr>
<tr>
<td>untagged ethernet 6</td>
<td>untagged ethernet 6</td>
</tr>
<tr>
<td>router-interface ve 16</td>
<td>router-interface ve 16</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td>vlan 99</td>
<td>vlan 99</td>
</tr>
<tr>
<td>tagged ethernet 18</td>
<td>tagged ethernet 18</td>
</tr>
<tr>
<td>router-interface ve 99</td>
<td>router-interface ve 99</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td>access-list 100 permit ip any any</td>
<td>access-list 100 permit ip any any</td>
</tr>
<tr>
<td>vlan 10</td>
<td>vlan 10</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td>interface ve 10</td>
<td>interface ve 10</td>
</tr>
<tr>
<td>ip address 10.10.1.2 255.255.255.0</td>
<td>ip address 10.10.1.3 255.255.255.0</td>
</tr>
<tr>
<td>ip allow-promiscuous-vip</td>
<td>ip allow-promiscuous-vip</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td>interface ve 15</td>
<td>interface ve 15</td>
</tr>
<tr>
<td>ip address 10.15.1.2 255.255.255.0</td>
<td>ip address 10.15.1.3 255.255.255.0</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td>interface ve 16</td>
<td>interface ve 16</td>
</tr>
<tr>
<td>ip address 10.16.1.2 255.255.255.0</td>
<td>ip address 10.16.1.3 255.255.255.0</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td>interface ve 99</td>
<td>interface ve 99</td>
</tr>
<tr>
<td>ip address 10.99.1.1 255.255.255.0</td>
<td>ip address 10.99.1.2 255.255.255.0</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td>VRRP-A enable</td>
<td>VRRP-A enable</td>
</tr>
<tr>
<td>vrrp-a vrid default</td>
<td>vrrp-a vrid default</td>
</tr>
<tr>
<td>floating-ip 10.10.1.1</td>
<td>floating-ip 10.10.1.1</td>
</tr>
<tr>
<td>priority 200</td>
<td>priority 180</td>
</tr>
<tr>
<td>tracking-options</td>
<td>tracking-options</td>
</tr>
<tr>
<td>interface ethernet 1 priority-cost 60</td>
<td>interface ethernet 1 priority-cost 60</td>
</tr>
<tr>
<td>interface ethernet 5 priority-cost 60</td>
<td>interface ethernet 5 priority-cost 60</td>
</tr>
<tr>
<td>interface ethernet 6 priority-cost 60</td>
<td>interface ethernet 6 priority-cost 60</td>
</tr>
</tbody>
</table>
## Appendix B. Detailed Walkthrough of SSL Insight Packet Flow

<table>
<thead>
<tr>
<th>Internal Primary Unit Configuration</th>
<th>Internal Standby Unit Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>vrrp-a vrid 5</td>
<td>vrrp-a vrid 5</td>
</tr>
<tr>
<td>floating-ip 10.15.1.1</td>
<td>floating-ip 10.16.1.1</td>
</tr>
<tr>
<td>priority 200</td>
<td>priority 180</td>
</tr>
<tr>
<td>tracking-options</td>
<td>tracking-options</td>
</tr>
<tr>
<td>interface ethernet 1 priority-</td>
<td>interface ethernet 1 priority-</td>
</tr>
<tr>
<td>cost 60</td>
<td>cost 60</td>
</tr>
<tr>
<td>interface ethernet 5 priority-</td>
<td>interface ethernet 5 priority-</td>
</tr>
<tr>
<td>cost 60</td>
<td>cost 60</td>
</tr>
<tr>
<td>interface ethernet 6 priority-</td>
<td>interface ethernet 6 priority-</td>
</tr>
<tr>
<td>cost 60</td>
<td>cost 60</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>vrrp-a vrid 6</td>
<td>vrrp-a vrid 6</td>
</tr>
<tr>
<td>floating-ip 10.16.1.1</td>
<td>floating-ip 10.16.1.1</td>
</tr>
<tr>
<td>priority 200</td>
<td>priority 180</td>
</tr>
<tr>
<td>tracking-options</td>
<td>tracking-options</td>
</tr>
<tr>
<td>interface ethernet 1 priority-</td>
<td>interface ethernet 1 priority-</td>
</tr>
<tr>
<td>cost 60</td>
<td>cost 60</td>
</tr>
<tr>
<td>interface ethernet 5 priority-</td>
<td>interface ethernet 5 priority-</td>
</tr>
<tr>
<td>cost 60</td>
<td>cost 60</td>
</tr>
<tr>
<td>interface ethernet 6 priority-</td>
<td>interface ethernet 6 priority-</td>
</tr>
<tr>
<td>cost 60</td>
<td>cost 60</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>VRRP-A interface ethernet 18 vlan 99</td>
<td>VRRP-A interface ethernet 18 vlan 99</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>slb server SecurityDevice1_Path 10.15.1.11</td>
<td>slb server SecurityDevice1_Path 10.15.1.11</td>
</tr>
<tr>
<td>port 0 tcp</td>
<td>port 0 tcp</td>
</tr>
<tr>
<td>no health-check</td>
<td>no health-check</td>
</tr>
<tr>
<td>port 0 udp</td>
<td>port 0 udp</td>
</tr>
<tr>
<td>no health-check</td>
<td>no health-check</td>
</tr>
<tr>
<td>port 8080 tcp</td>
<td>port 8080 tcp</td>
</tr>
<tr>
<td>no health-check</td>
<td>no health-check</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>slb server SecurityDevice2_Path 10.16.1.11</td>
<td>slb server SecurityDevice2_Path 10.16.1.11</td>
</tr>
<tr>
<td>port 0 tcp</td>
<td>port 0 tcp</td>
</tr>
<tr>
<td>no health-check</td>
<td>no health-check</td>
</tr>
<tr>
<td>port 0 udp</td>
<td>port 0 udp</td>
</tr>
<tr>
<td>no health-check</td>
<td>no health-check</td>
</tr>
<tr>
<td>port 8080 tcp</td>
<td>port 8080 tcp</td>
</tr>
<tr>
<td>no health-check</td>
<td>no health-check</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>slb service-group LB_Paths_UDP udp</td>
<td>slb service-group LB_Paths_UDP udp</td>
</tr>
<tr>
<td>member SecurityDevice1_Path:0</td>
<td>member SecurityDevice1_Path:0</td>
</tr>
<tr>
<td>member SecurityDevice2_Path:0</td>
<td>member SecurityDevice1_Path:0</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>slb service-group LB_Paths_TCP tcp</td>
<td>slb service-group LB_Paths_TCP tcp</td>
</tr>
<tr>
<td>member SecurityDevice1_Path:0</td>
<td>member SecurityDevice1_Path:0</td>
</tr>
<tr>
<td>member SecurityDevice2_Path:0</td>
<td>member SecurityDevice2_Path:0</td>
</tr>
</tbody>
</table>
### Internal Primary Unit Configuration

```conf
! slb service-group SSLi tcp
    member SecurityDevice1_Path:8080
    member SecurityDevice2_Path:8080
! slb template client-ssl SSLInsight_ClientSide
    forward-proxy-enable
    forward-proxy-ca-cert SSLi-CA
    forward-proxy-ca-key SSLi-CA
!
slb virtual-server Outbound_Wildcard_VIP 0.0.0.0 acl 100
  port 0  tcp
    service-group LB_Paths_TCP
    no-dest-nat
  port 0  udp
    service-group LB_Paths_UDP
    no-dest-nat
  port 0  others
    service-group LB_Paths_UDP
    no-dest-nat
  port 443  https
    service-group SSLi
    template client-ssl SSLInsight_ClientSide
    no-dest-nat port-translation
!
end
```

### Internal Standby Unit Configuration

```conf
! slb service-group SSLi tcp
    member SecurityDevice1_Path:8080
    member SecurityDevice2_Path:8080
! slb template client-ssl SSLInsight_ClientSide
    forward-proxy-enable
    forward-proxy-ca-cert SSLi-CA
    forward-proxy-ca-key SSLi-CA
!
slb virtual-server Outbound_Wildcard_VIP 0.0.0.0 acl 100
  port 0  tcp
    service-group LB_Paths_TCP
    no-dest-nat
  port 0  udp
    service-group LB_Paths_UDP
    no-dest-nat
  port 0  others
    service-group LB_Paths_UDP
    no-dest-nat
  port 443  https
    service-group SSLi
    template client-ssl SSLInsight_ClientSide
    no-dest-nat port-translation
!
end
```

### External Primary Unit Configuration

```conf
vrrp-a set-id 2
hostname ACOS
!
vlan 20
  untagged ethernet 1
  router-interface ve 20
!
vlan 15
  untagged ethernet 5
  router-interface ve 15
!
vlan 16
  untagged ethernet 6
  router-interface ve 16
!
vlan 99
  tagged ethernet 18
  router-interface ve 99
```

### External Standby Unit Configuration

```conf
vrrp-a set-id 2
hostname ACOS
!
vlan 20
  untagged ethernet 1
  router-interface ve 20
!
vlan 15
  untagged ethernet 5
  router-interface ve 15
!
vlan 16
  untagged ethernet 6
  router-interface ve 16
!
vlan 99
  tagged ethernet 18
  router-interface ve 99
```
<table>
<thead>
<tr>
<th>External Primary Unit Configuration</th>
<th>External Standby Unit Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>! access-list 101 permit ip any any</td>
<td>! access-list 101 permit ip any any</td>
</tr>
<tr>
<td>vlan 15 access-list 101 permit ip any any vlan 16</td>
<td>vlan 15 access-list 101 permit ip any any vlan 16</td>
</tr>
<tr>
<td>interface ve 20 ip address 20.1.1.2 255.255.255.0</td>
<td>interface ve 20 ip address 20.1.1.3 255.255.255.0</td>
</tr>
<tr>
<td>interface ve 15 ip address 10.15.1.12 255.255.255.0 ip allow-promiscuous-vip</td>
<td>interface ve 15 ip address 10.15.1.13 255.255.255.0 ip allow-promiscuous-vip</td>
</tr>
<tr>
<td>interface ve 16 ip address 10.16.1.12 255.255.255.0 ip allow-promiscuous-vip</td>
<td>interface ve 16 ip address 10.16.1.13 255.255.255.0 ip allow-promiscuous-vip</td>
</tr>
<tr>
<td>interface ve 199 ip address 10.199.1.1 255.255.255.0</td>
<td>interface ve 199 ip address 10.199.1.2 255.255.255.0</td>
</tr>
<tr>
<td>VRRP-A enable vrrp-a vrid default floating-ip 20.1.1.1 priority 200 tracking-options interface ethernet 1 priority-cost 60 interface ethernet 5 priority-cost 60 interface ethernet 6 priority-cost 60</td>
<td>VRRP-A enable vrrp-a vrid default floating-ip 20.1.1.1 priority 180 tracking-options interface ethernet 1 priority-cost 60 interface ethernet 5 priority-cost 60 interface ethernet 6 priority-cost 60</td>
</tr>
<tr>
<td>vrrp-a vrid 15 floating-ip 10.15.1.11 priority 200 tracking-options interface ethernet 1 priority-cost 60 interface ethernet 5 priority-cost 60 interface ethernet 6 priority-cost 60</td>
<td>vrrp-a vrid 15 floating-ip 10.15.1.11 priority 180 tracking-options interface ethernet 1 priority-cost 60 interface ethernet 5 priority-cost 60 interface ethernet 6 priority-cost 60</td>
</tr>
<tr>
<td>vrrp-a vrid 16 floating-ip 10.16.1.11 priority 200 tracking-options interface ethernet 1 priority-cost 60 interface ethernet 5 priority-cost 60 interface ethernet 6 priority-cost 60</td>
<td>vrrp-a vrid 16 floating-ip 10.16.1.11 priority 180 tracking-options interface ethernet 1 priority-cost 60 interface ethernet 5 priority-cost 60 interface ethernet 6 priority-cost 60</td>
</tr>
</tbody>
</table>
### External Primary unit Configuration

```text
! VRRP-A interface ethernet 18 vlan 99
! slb template server-ssl SSLInsight_ServerSide
    forward-proxy-enable
! slb server Default_Gateway 20.1.1.10
    port 0 tcp
    no health-check
    port 0 udp
    no health-check
    port 443 tcp
    no health-check
! slb service-group DG_TCP tcp
    member Default_Gateway:0
! slb service-group DG_UDP udp
    member Default_Gateway:0
! slb service-group DG_SSL tcp
    member Default_Gateway:443
! slb virtual-server Inside_To_Outside 0.0.0.0 acl 101
    port 0 tcp
    service-group DG_TCP
    use-rcv-hop-for-resp
    no-dest-nat
    port 0 udp
    service-group DG_UDP
    use-rcv-hop-for-resp
    no-dest-nat
    port 0 others
    service-group DG_UDP
    use-rcv-hop-for-resp
    no-dest-nat
    port 8080 http
    service-group DG_SSL
    use-rcv-hop-for-resp
    template server-ssl SSLInsight_ServerSide
    no-dest-nat port-translation
! end
```

### External Standby unit Configuration

```text
! VRRP-A interface ethernet 18 vlan 99
! slb template server-ssl SSLInsight_ServerSide
    forward-proxy-enable
! slb server Default_Gateway 20.1.1.10
    port 0 tcp
    no health-check
    port 0 udp
    no health-check
    port 443 tcp
    no health-check
! slb service-group DG_TCP tcp
    member Default_Gateway:0
! slb service-group DG_UDP udp
    member Default_Gateway:0
! slb service-group DG_SSL tcp
    member Default_Gateway:443
! slb virtual-server Inside_To_Outside 0.0.0.0 acl 101
    port 0 tcp
    service-group DG_TCP
    use-rcv-hop-for-resp
    no-dest-nat
    port 0 udp
    service-group DG_UDP
    use-rcv-hop-for-resp
    no-dest-nat
    port 0 others
    service-group DG_UDP
    use-rcv-hop-for-resp
    no-dest-nat
    port 8080 http
    service-group DG_SSL
    use-rcv-hop-for-resp
    template server-ssl SSLInsight_ServerSide
    no-dest-nat port-translation
! end
```
Appendix B. Detailed Walkthrough of SSL Insight Packet Flow

1. If the certificate exists in cache, send it to client and move to (2). Otherwise, establish SSL connection with the remote server.

2. Extract header information from server certificate. Change the Issuer and the Public Key as defined in Client-SSL-Template. Re-sign the new certificate using the CA-Certificate as specified in Client-SSL-Template. Send the reconstructed Server-Hello to client.

3. Data encrypted and sent in cleat-text through the security device.

4. New SSL session initiated with remote server. Data encrypted and sent to remote server.

5. Response is decrypted and sent through the security device.

6. Response is encrypted again and sent to the client.
Appendix C. SSL Insight Certificate Installation Guide

A prerequisite for configuring Thunder ADC’s SSL Insight feature is generating a CA certificate with a known private key. This CA certificate must then be installed to all client machines on the internal network. If the CA certificate is not installed, internal users will see an SSL “untrusted root” error whenever they try to connect to an SSL-enabled website.

This guide includes the following contents:

- Generating a CA Certificate
- Exporting a Certificate from Thunder ADC
- Installing a Certificate in Microsoft Windows 7 for Microsoft Internet Explorer
- Installing a Certificate in Google Chrome
- Installing a Certificate in Mozilla Firefox

Generating a CA Certificate

The SSLI insight feature relies on an SSL certificate and key pair to encrypt traffic between clients and the Thunder ADC appliance. A self-signed certificate can be generated by the Thunder ADC appliance or can be created by a Linux system with OpenSSL installed. Alternatively, from the Thunder ADC appliance, an ADC administrator can request and install a CA-signed certificate. For instructions on requesting a CA-signed certificate, please see the “Application Delivery and Server Load Balancing Guide.”

To generate a self-signed certificate from Thunder ADC in ACOS version 2.7.2:

1. Select Config Mode > SLB > Service > SSL Management.
2. On the menu bar, select Certificate.
3. Click Add.
4. Enter the name for certificate.
5. In the Issuer drop-down list, select Self.
6. Enter the rest of the certificate information in the remaining fields of the Certificate section.

Note: If you need to create a wildcard certificate, use an asterisk as the first part of the common name.

7. From the Key drop-down list, select the length in bits for the key.
8. Click OK. The ACOS device generates the self-signed certificate and a key. The new certificate and key appear in the certificate list. The certificate is ready to be used in client-SSL and server-SSL templates.

Instead of creating a self-signed certificate within Thunder ADC, administrators can generate a certificate from a Linux server. The following two commands generate and initialize a CA Certificate on a Linux system with an OpenSSL package installed. Once generated, the certificate can be imported onto the Thunder ADC device using FTP or SCP.

```bash
openssl genrsa -out ca.key
openssl req -new -x509 -days 3650 -key ca.key -out ca.crt
```

The root certificate must be imported onto the client machines. This can be done manually or using an automated service such as Microsoft Group Policy Manager.


Exporting a Certificate from Thunder ADC

To export a self-signed certificate from Thunder ADC from the Thunder ADC GUI in ACOS 2.7.2:

1. Select Config Mode > SLB > Service > SSL Management.
2. On the menu bar, select Certificate.
3. To export a certificate:
a. Select the Certificate checkbox.
b. Click Export.

*Note: If the browser security settings normally block downloads, you may need to override the settings. For example, in Internet Explorer, hold the Ctrl key while clicking Export.*

4. Click Save.
5. Navigate to the save location.
6. Click Save again.
7. To export a key:
a. Select the SSL key.
b. Click Export.
c. Click Save. Navigate to the save location.
d. Click Save again.

See the "Application Delivery and Server Load Balancing Guide" for more information and for instructions for the command line interface (CLI).

**Installing a Certificate in Microsoft Windows 7 for Internet Explorer**

To import an untrusted or self-signed CA certificate into your Windows 7 computer, you must be logged on as an administrator, and the untrusted or self-signed CA certificate should have been imported onto your computer already.

1. Open Certificate Manager by clicking the Start button, typing certmgr.msc into the search box, and then pressing Enter. If you're prompted for an administrator password or confirmation, type the password or provide confirmation.
2. In Certificate Manager, select the folder that you want to import the certificate into. In this exercise, we have selected the folder: Trusted Root Certification Authorities > Certificates.

3. Click the Action menu, point to All Tasks, and then click Import.
4. In Certificate Import Wizard, click Next to proceed to the File Import page.

5. Select Browse to locate the certificate file that is to be imported.

Note: the Open dialog box only displays X.509 certificates by default. If you want to import another type of certificate, select the certificate type you want to import in the Open dialog box and click Open.
6. Click the **Next** button.

7. Click the **Next** button.
8. Confirm your selections and click Finish.

9. In the Security Warning popup, select Yes, since you made an informed decision to import this certificate.
10. If the import is successful, you will see a dialog box with the message “The import was successful.”

11. You can see the newly installed CA certificate under the specified folder.
Installing Certificate in Google Chrome

1. To install the CA certificate on Google Chrome, open the Chrome browser.
2. Click the "Customize and Control Google Chrome" option located on the right hand corner of the browser window.
3. Navigate to the HTTPS/SSL section of Chrome Settings and click the Manage certificates button.
4. In the certificate folder on the Trusted Root Certification Authorities tab, click the Import button and a Certificate Import Wizard will appear.

5. In the Certificate Import Wizard, click the Next button.
6. Click the **Next** button to browse to the location of the CA certificate.

7. Once the correct certificate has been located, click **Next** to install the certificate in the “Trusted Root Certificate Authorities” certificate store. Click **Next** and **Finish** and then click **OK**.
Installing a Certificate in Mozilla Firefox

Mozilla Firefox utilizes a certificate store and all root CA certificates are stored within the certificate store. In order for SSL Insight to perform properly, each client must download and install the SSL root certificate. Otherwise, Firefox will generate an error message warning clients about SSL error connection attempts.

1. To install a SSL root certificate in Firefox, launch the Firefox browser and open the Options window.
2. From the Options window, select the Advanced settings option and then click the Certificate tab. From the Certificates window, click the View Certificates button. Mozilla will display the Certificate Manager dialog.

3. Click the Import button.

4. Navigate to where the certificate is located and click Open. A Downloading Certificate window will be displayed.

5. Select the Trust this CA to identify websites checkbox and click OK. Now, the certificate should be imported and the client machine can access HTTPS applications without receiving an error message.
About A10 Networks

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: www.a10networks.com