DEPLOYMENT GUIDE

A10 SSL INSIGHT AND FIREWALL LOAD BALANCING FOR PALO ALTO NETWORKS FIREWALLS

OVERVIEW

With the growth in encrypted traffic, increasing SSL key lengths and more computationally complex SSL ciphers, it is increasingly difficult for inline security devices to decrypt SSL traffic. Even if the SSL decryption is enabled on the inline security devices, the overall performance is degraded significantly. A10 Networks® SSL Insight® technology using A10 Thunder SSLi® or A10 Networks Thunder® Convergent Firewall (CFW) products provides high-performance SSL decryption, helps eliminate the SSL blind spot in corporate defenses and enables security devices to inspect encrypted traffic such as HTTPS, not just clear text data in HTTP traffic.

This guide provides step-by-step instructions for the deployment of an A10 Networks SSL Insight configuration with Firewall Load Balancing (FWLB) for Palo Alto Networks firewalls. It is based on a use case with a Layer 3 deployment of two pairs of A10 Thunder SSLi devices along with a pair of Palo Alto Networks firewalls in Layer 2 mode. One (inside) Thunder SSLi appliance decrypts the traffic and sends it to an inline, Layer 2 Palo Alto firewall, which inspects the traffic. It then sends the inspected traffic to the second (outside) Thunder SSLi appliance, which re-encrypts the traffic and sends it out to the remote destination.

TABLE OF CONTENTS

TABLE OF CONTENTS

DEPLOYMENT PREREQUISITES

To deploy the SSL Insight solution with Palo Alto Networks firewalls, the following are required:

- A10 Networks Advanced Core Operating System (ACOS®) 4.1.0 or higher (supported with hardware-based Thunder SSLi or Thunder CFW appliances)
- A10 URL Classification Service (optional)
- CA Certificate for SSLi and certificate chain (required)
- Palo Alto Networks firewall appliance running code version 7.0.5h2 or higher (preferably 7.1.3)

SSL INSIGHT TECHNOLOGY

A10 Networks SSL Insight is the technology which enables users to transparently intercept SSL traffic, decrypt it and send it through a firewall or other security devices. After the firewall has inspected the clear-text traffic, it is re-encrypted and sent to the destination. SSL Insight can be deployed using either a single Thunder SSLi appliance (using partitions) or two Thunder SSLi appliances. One of the two appliances (or partition) decrypts SSL traffic and the second appliance (or partition) re-encrypts traffic. The appliance/partition that decrypts outbound SSL traffic is referred to as “SSLi Inside.” The appliance/partition that encrypts outbound SSL traffic is referred to as “SSLi Outside.”

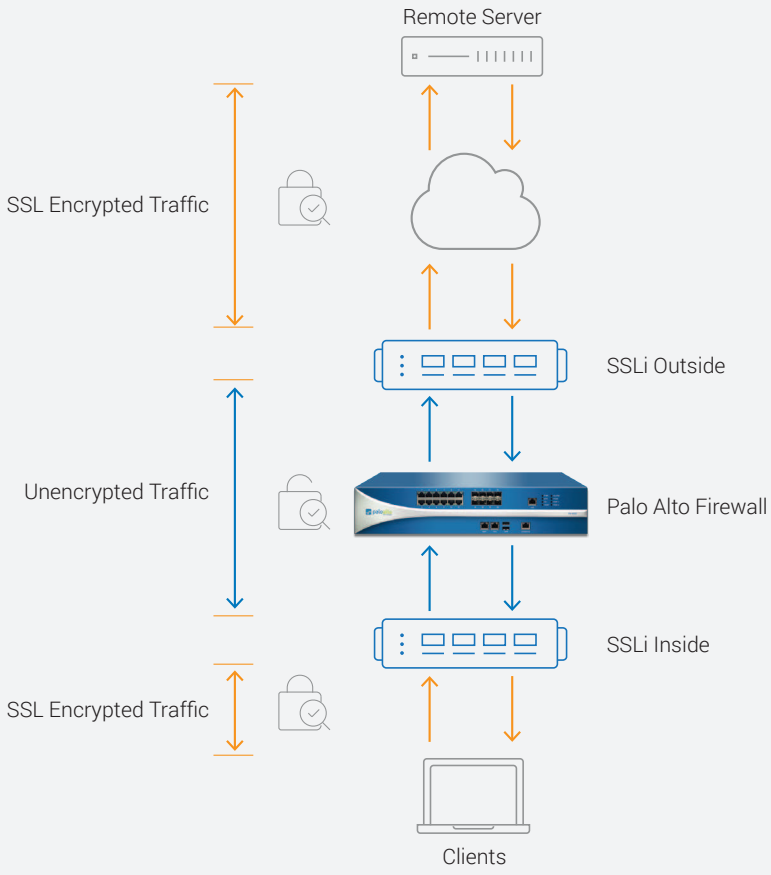


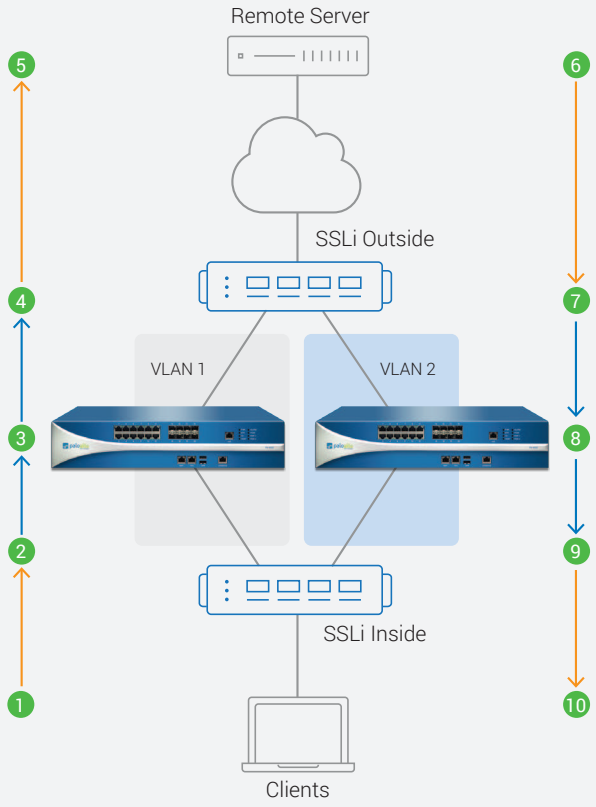
Figure 1: SSL Insight technology overview

There are three distinct states for traffic in this deployment scenario, depicted in Figure 1:

1. From client to SSLi Inside, where traffic is decrypted
2. From SSLi Inside to SSLi Outside, through the Palo Alto Networks firewall, where traffic is in clear text
3. Traffic from SSLi Outside to the remote server, where traffic is encrypted again

FIREWALL LOAD BALANCING (FWLB)

The FWLB feature allows load sharing between multiple firewalls. In a typical deployment, there is a Thunder SSLi sandwich with two or more firewalls in the middle. The Thunder SSLi appliances load balance between the two firewalls, using the round robin algorithm by default. The number of firewalls in the solution can be extended as required. The A10 FWLB solution can work with HTTP, HTTPS, generic TCP, generic UDP, DNS, SIP and FTP. This design can scale up to sixteen separate firewall load-balancing paths. Figure 2 shows how SSL Insight with FWLB works:



1. SSL/TLS encrypted traffic (such as HTTPS) originates from an internal client.
2. Traffic is intercepted and decrypted by SSLi Inside and the traffic, in clear text, is load balanced to one of the Palo Alto Networks firewalls.
3. The Palo Alto Networks firewall inspects the data in clear text and forwards it to the next hop.
4. SSLi Outside intercepts and encrypts the traffic. At this point:
   a. An encrypted session is created with the destination server.
   b. A source Media Access Control (MAC) address of the traffic is stored for this session entry.
   c. Outbound traffic is forwarded to the default gateway.

Figure 2: SSL Insight with Firewall Load Balancing (FWLB)

5. The destination server receives the encrypted request.
6. The destination server sends back the encrypted response.
7. SSLi Outside decrypts the response and forwards the traffic to clients, in clear text, through the Palo Alto Networks firewall. At this point:
   a. The traffic is matched to the session entry.
   b. The source MAC address is retrieved from the entry and used as the destination MAC in L2 header.
   c. Traffic is sent back via the Palo Alto Networks firewall that had inspected the original traffic before.
8. The Palo Alto Networks firewall inspects the response contents in clear text and forwards it to SSLi Inside.
9. SSLi Inside receives the clear-text traffic from the Palo Alto Networks firewall, encrypts it and sends it to the client.
10. The client receives the encrypted response.

***NOTE**: Firewall Load Balancing can scale up to 16 firewall paths within a Thunder SSLi "sandwich."*

DEPLOYMENT ARCHITECTURE OVERVIEW

This section illustrates the joint solution of A10 Networks Thunder SSLi appliances and Palo Alto Networks PA series firewalls providing SSL Insight technology and FWLB capabilities. This solution has high availability (HA) using A10's proprietary VRRP-A for failover on the Thunder SSLi devices, and on multiple redundant paths for the Palo Alto PA series firewalls.

In this deployment guide, two Palo Alto Networks PA series firewall appliances are placed between a set of four Thunder SSLi devices with a pair on either side, as shown in Figure 3. SSL Insight technology and FWLB functionalities are provided by the Thunder SSLi appliances, while the traffic inspection services are provided by the Palo Alto PA series firewalls.

NOTES:

- *The internal firewalls (in between the Thunder SSLi "sandwich") are set up in Layer 2 (L2) mode. The solution can work with firewalls in vWire mode as well; a sample of this design is included in Appendix B. Keep in mind that the number of ports required on the Thunder SSLi appliances increase significantly while the firewall is in a vWire mode.*
- *VRRP-A is an A10 Networks proprietary HA protocol optimized for the A10 Thunder series devices, 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 interoperate with VRRP.*
- *SSL Insight technology is supported on Thunder SSLi or A10 Networks vThunder® line of virtual appliances with the presence of hardware-based SSL cards. SSL Insight technology is also supported on vThunder CFW virtual appliances with software-based SSL.*

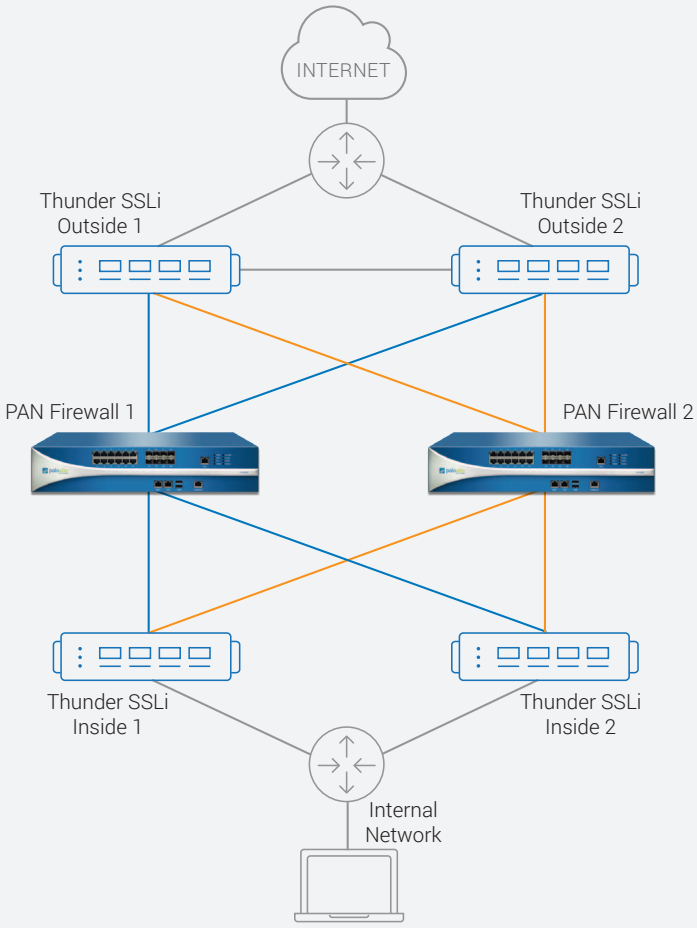


Figure 3: Deployment architecture overview

ACCESS CREDENTIALS

This section lists default access credentials for the Thunder SSLi appliances and the Palo Alto Networks PA series firewall appliances.

A10 NETWORKS THUNDER SSLI ACCESS DEFAULTS

- Default username: "admin"
- Default password: "a10"
- Default management IP address of the device: "172.31.31.31"

PALO ALTO NETWORKS PA SERIES FIREWALL ACCESS DEFAULTS

- Default username: "admin"
- Default password: "admin"
- Default management IP address of the device: "192.168.1.1"

Both the Thunder SSLi and PA series appliances support a Graphical User Interface (GUI) and Command Line Interface (CLI).

- To access the CLI for both Thunder SSLi and PA series appliances, you will need to use an SSH client such as putty.exe.
- To access the GUI for both Thunder SSLi and PA series appliances, you will need to use a web browser such as Google Chrome or Mozilla Firefox, using HTTPS.

***NOTE**: All HTTP requests will automatically be translated to HTTPS when the GUI is accessed.*

THUNDER SSLI CONFIGURATION

This section details the configuration of the Thunder SSLi appliances used in this deployment. First step is to configure high availability, using VRRP-A on each of the devices. The next step is to configure SSL Insight technology settings on Thunder SSLi Inside and Thunder SSLi Outside. All of the configurations will be applied using both the CLI and the GUI. A complete running configuration can be found in Appendix A.

HIGH AVAILABILITY CONFIGURATION

The first step in the configuration of Thunder SSLi devices is to configure the HA settings using VRRP-A. Once HA is configured and both the pairs of SSLi Inside and Outside devices are synced up, we can move on to configuring SSL Insight.

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

- VLANs and their router interfaces
- Virtual Ethernet (VE) interfaces, which are used to assign IP addresses to VLAN router interfaces
- VRRP-A for high availability

CONFIGURE THE VLANS AND ADD ETHERNET AND ROUTER INTERFACES

Configure the following VLAN parameters for both the Thunder SSLi Inside and Outside devices:

- **VLAN-100**: This links the client side on the inside, and the server side to the outside network. Add router-interface ve 100 along with the Ethernet interface.
- **VLAN-10**: This is the path to the Thunder SSLi Outside device through **Firewall 1**. Add router-interface ve 10 along with the Ethernet interface.
- **VLAN-20**: This is the path to the Thunder SSLi Outside device through **Firewall 2**. Add router-interface ve 20 along with the Ethernet interface.
- **VLAN-30**: This is the VLAN for VRRP-A sync messages. Add router-interface ve 30 along with the Ethernet interface.

***NOTE**: This configuration is identical on all four Thunder SSLi devices. Repeat this step on each Thunder SSLi appliance.*

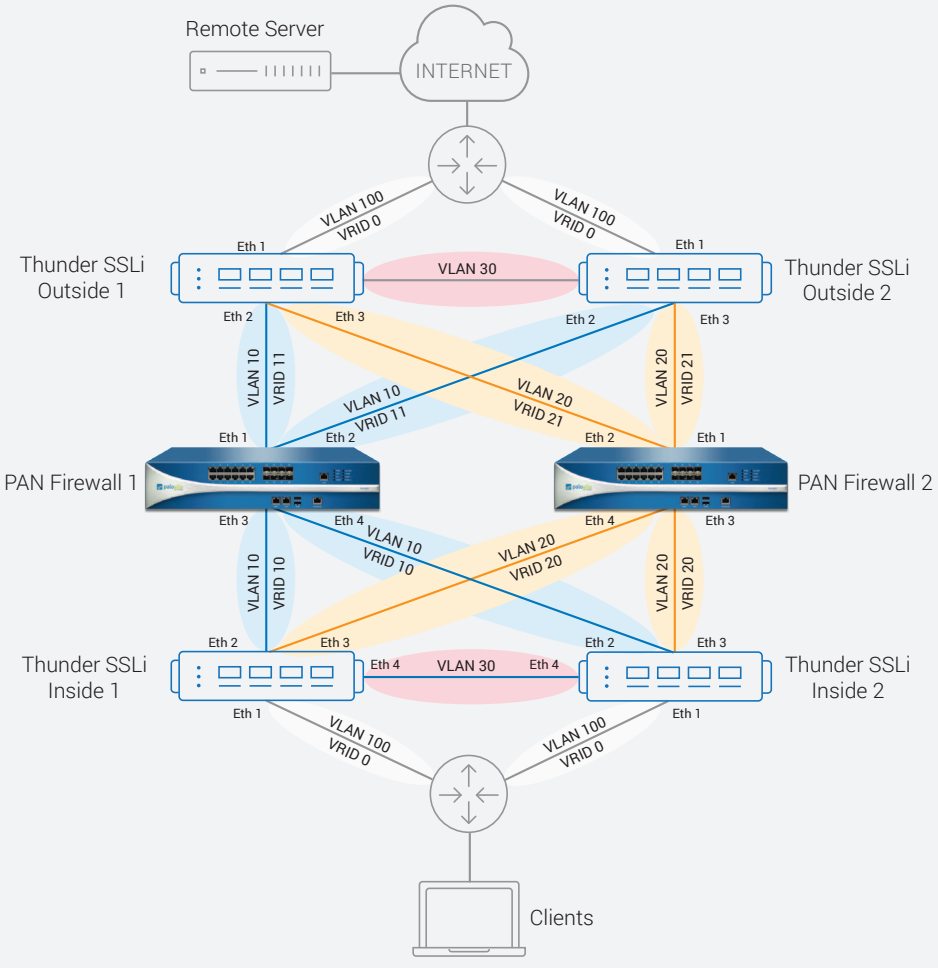


Figure 4: Network topology with Layer 2 information

Using the CLI

```
vlan 100
  untagged ethernet 1
  router-interface ve 100
!
vlan 10
  untagged ethernet 2
  router-interface ve 10
!
vlan 20
  untagged ethernet 3
  router-interface ve 20
!
vlan 30
  untagged ethernet 4
  router-interface ve 30
```

Using the GUI

Navigate to **Network > VLAN**

- Click CREATE.
- Enter the VLAN ID, select the CREATE VIRTUAL INTERFACE option, and select the interface in the UNTAGGED section.
- Click CREATE VLAN.
- Repeat for each VLAN.

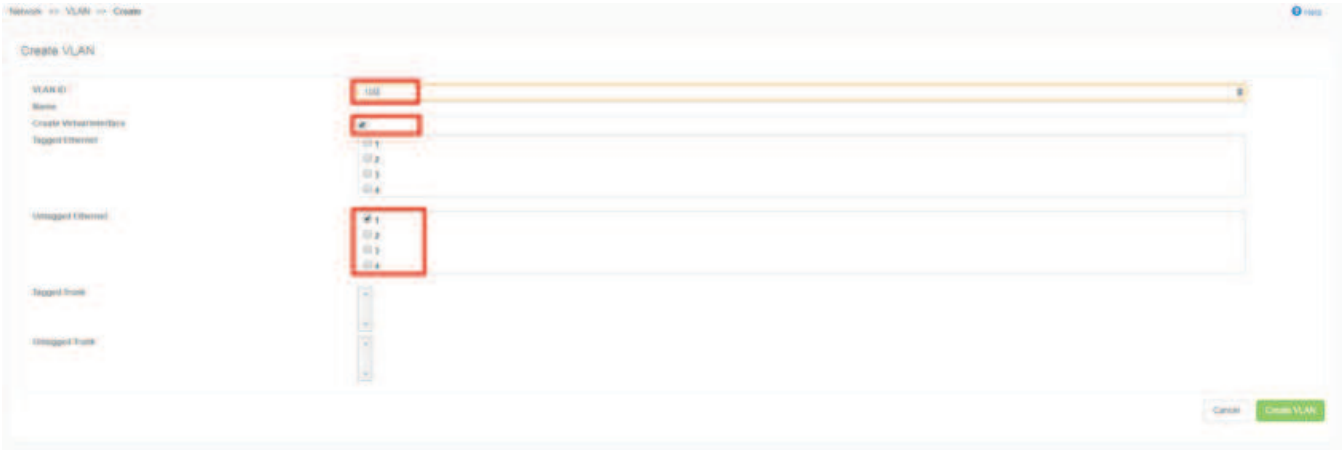


Figure 5: VLAN configuration

Once all of the VLANs have been added, the list should look like this:

Figure 6: List of configured VLANs

CONFIGURE IP ADDRESSES ON THE VLAN ROUTER INTERFACES

Figure 7 shows the Layer 3 information of this deployment (IP addresses and subnets).

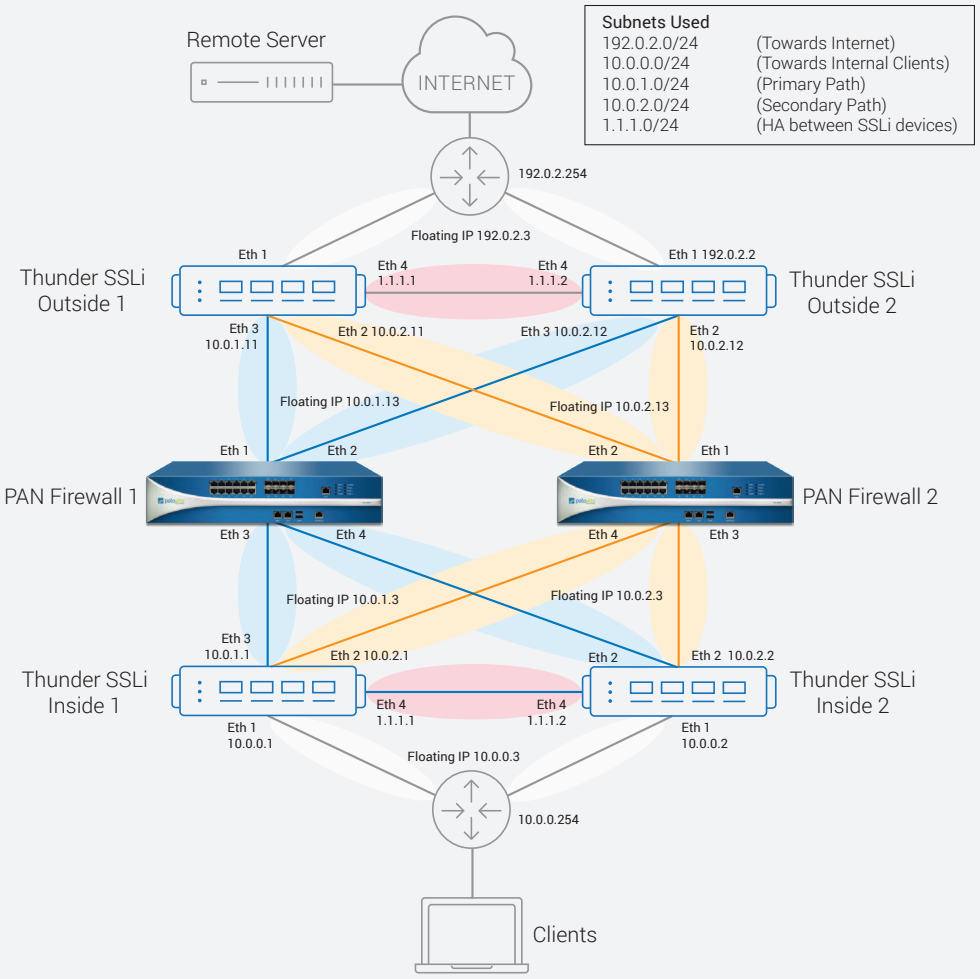


Figure 7: Network topology with Layer 3 information

Initiate Virtual Ethernet interfaces (ve) on the **Thunder SSLi Inside** devices and assign IP addresses to them. Following is the VE interface configuration for Thunder SSLi Inside 1 device. Repeat this step on the Thunder SSLi Inside 2 by referring to Figure 7 for appropriate IP addresses.

Using the CLI

```
interface ve 100
  name INSIDE
  ip address 10.0.0.1 255.255.255.0
  ip allow-promiscuous-vip
!
interface ve 10
  name PATH1
  ip address 10.0.1.1 255.255.255.0
!
interface ve 20
```

```
  name PATH2
  ip address 10.0.2.1 255.255.255.0
!
interface ve 30
  name SYNC-PATH
  ip address 1.1.1.1 255.255.255.0
```

***NOTE**: The **ip allow-promiscuous-vip** command is required for any configuration that uses a wildcard virtual IP (VIP) 0.0.0.0. This command enables client traffic received on this interface and addressed to any destination IP to be processed by the wildcard VIP.*

For the **Thunder SSLi Outside** devices, the configuration will be as follows:

***NOTE**: Following shows the configuration for Thunder SSLi Outside 1. Repeat it on the Thunder SSLi Outside 2 with appropriate IP addresses.*

Using the CLI

```
interface ve 100
  name OUTSIDE
  ip address 192.0.2.1 255.255.255.0
!
interface ve 10
  name PATH1
    ip address 10.0.1.11 255.255.255.0
  ip allow-promiscuous-vip
!
interface ve 20
  name PATH2
  ip address 10.0.2.11 255.255.255.0
  ip allow-promiscuous-vip
!
interface ve 30
  name SYNC-PATH
  ip address 1.1.1.1 255.255.255.0
```

***NOTE**: The ip allow-promiscuous-vip command is required for any configuration that uses a wildcard virtual IP (VIP) 0.0.0.0. This command enables client traffic received on this interface and addressed to any destination IP to be processed by the wildcard VIP.*

Using the GUI

This section describes general GUI configuration steps for a VE interface. Repeat the steps for each VE interface on all Thunder SSLi devices. For IP address information, refer to Figure 7.

Navigate to Network > Interfaces > Virtual Ethernets

- Click EDIT for Virtual Ethernet interface 10.
- Select ACTION as ENABLE from the drop-down menu.
- Open the **IP** menu.
- Enter the IP ADDRESS, enter the NETMASK and click ADD.
- Select the ALLOW PROMISCUOUS VIP option.
- Click UPDATE.
- Repeat for each Virtual Ethernet interface.

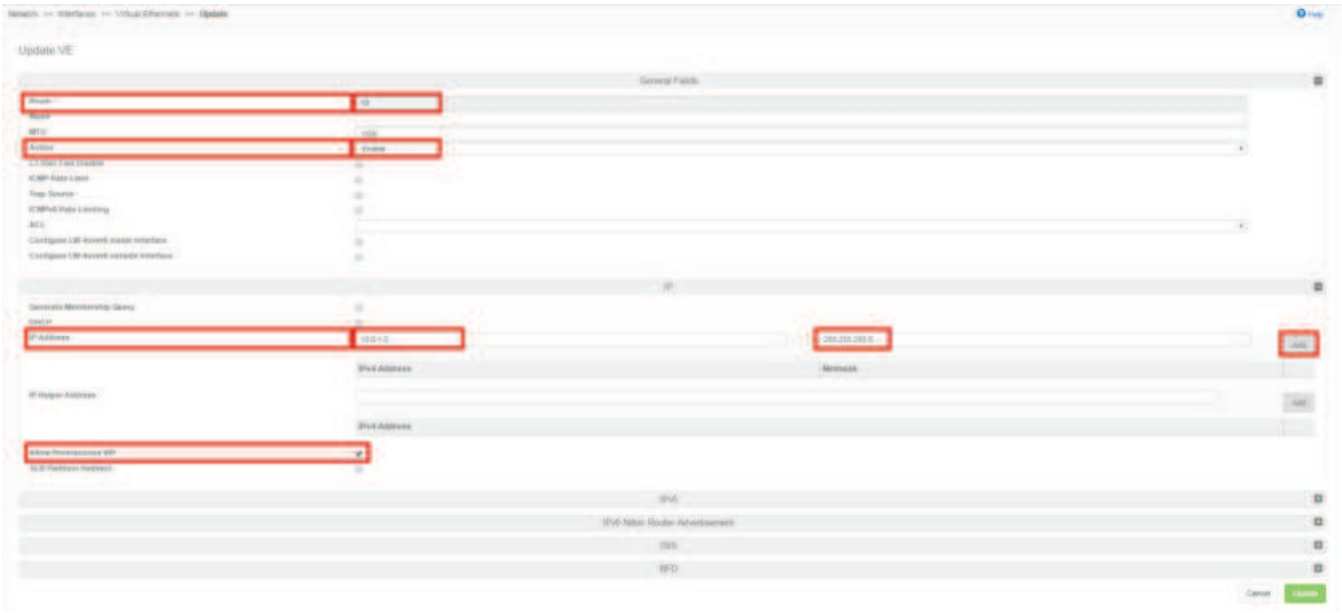


Figure 8: Virtual Ethernet (VE) interface configuration

CONFIGURE VRRP-A ON THUNDER SSLI INSIDE 1 AND 2, AND OUTSIDE 1 AND 2

Here are the steps to configure VRRP-A on the **Thunder SSLi Inside** appliances:

1. Set unique VRRP-A **device IDs** on both Inside SSLi devices, i.e., **Thunder SSLi Inside 1 and 2**.
2. Configure the same **set ID** on both Thunder SSLi Inside devices.
3. Each set should have two devices as follows:

SET ID	*DEVICE ID*			
	SSLI INSIDE 1	*SSLI INSIDE 2*	*SSLI OUTSIDE 1*	*SSLI OUTSIDE 2*
1	1	2	-	-
2	-	-	1	2

Table 1: VRRP-A set and device IDs for Thunder SSLi Inside and Outside

***NOTE**: Set IDs must be unique within the scope of the device, while device IDs must be unique within the scope of a set.*

4. Configure Virtual Router Identification (VRIDs) and assign floating IPs.
   The next step is to configure the following VRIDs on the Thunder SSLi **Inside 1 and 2** devices:

VLAN	*VRID*	*FLOATING IP*	*PRIORITY (INSIDE 1)*	*PRIORITY (INSIDE 2)*
100	0	10.0.0.3	200	180
10	10	10.0.1.3	200	180
20	20	10.0.2.3	200	180

Table 2: VLAN, VRID and floating IPs for Thunder SSLi Inside devices

- **VRID-0**: This VRID will be used for the enterprise switch, floating IP 10.0.0.3
- **VRID-10**: This VRID will be used for **VLAN-10**, floating IP 10.0.1.3
- **VRID-20**: This VRID will be used for **VLAN-20**, floating IP 10.0.2.3

And the following on the Thunder SSLi **Outside** device:

VLAN	*VRID*	*FLOATING IP*	*PRIORITY (OUTSIDE 1)*	*PRIORITY (OUTSIDE 2)*
100	0	192.0.2.3	200	180
10	11	10.0.1.13	200	180
20	21	10.0.2.13	200	180

Table 3: VLAN, VRID and floating IPs for Thunder SSLi Outside devices

- **VRID-0**: This VRID will be used for the gateway router, floating IP 192.0.2.3
- **VRID-11**: This VRID will be used for **VLAN-10**, floating IP 10.0.1.13
- **VRID-21**: This VRID will be used for **VLAN-20**, floating IP 10.0.2.13

5. Configure and enable a VRRP-A interface between the two devices for the exchange of sync messages.

***NOTE**: The VRIDs must be unique on all Thunder SSLi Inside and Outside devices.*

Here is the sample CLI configuration of VRRP-A for **Thunder SSLi Inside 1**.

***NOTE**: The basic configuration will remain as follows, with changes made only to the ID values and IP addresses. Relevant values and IP addresses from Tables 1-3 can be used to configure Thunder SSLi Inside 2, Outside 1 and Outside 2 devices.*

Using the CLI

```
vrrp-a common
  device-id 1
  set-id 1
  enable
```

***NOTE**: The vrrp-a common command allows access to global VRRP-A settings.*

```
vrrp-a vrid 0
  floating-ip 10.0.0.3
  blade-parameters
    priority 200
!
vrrp-a vrid 10
  floating-ip 10.0.1.3
  blade-parameters
    priority 200
!
vrrp-a vrid 20
  floating-ip 10.0.2.3
  blade-parameters
    priority 200
```

***NOTE**: VRRP-A priorities on the secondary/backup devices, i.e., Thunder SSLi Inside 2 and Outside 2, should be set to less than the value on the primary devices, i.e., Thunder SSLi Inside 1 and Outside 1. An example of priorities is 200 on the primary devices and 180 on the secondary devices.*

***NOTE**: As a recommended practice, VRRP-A **tracking options** should be enabled for each VRID for their corresponding interfaces or VLANS. Tracking options enable the tracking of an interface or VLAN, resulting in a faster failover. The VRRP-A tracking options can be enabled at the **blade parameters** configuration level.*

Once all VRIDs have been configured, enter the command below to enable VRRP-A synchronization for Interface Ethernet 4 over VLAN 30. This command makes sure that the active and passive Thunder SSLi devices can send synchronization messages (heartbeats) to each other to maintain their respective statuses.

```
vrrp-a interface ethernet 4
  vlan 30
```

Using the GUI

Navigate to System > VRRP-A > Global

- Select VRRP-A ENABLE as ENABLE.
- Enter the DEVICE ID.
- Enter the SET ID.
- Click OK.

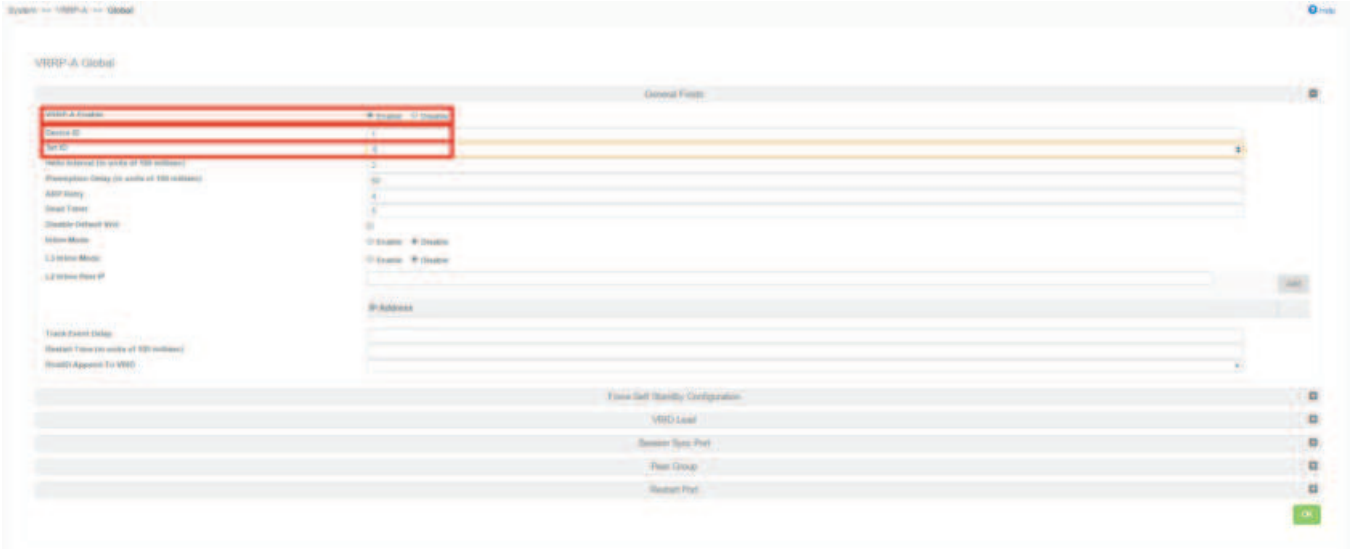


Figure 9: VRRP-A global configuration

Switch to Global VRID configuration by navigating to System > VRRP-A > VRID

- Click CREATE.
- Enter VRID.
- Select PREEMPT MODE as ENABLE.
- For VRID FLOATING IP, select IPv4 from the drop-down menu and enter the IP address.
- Open the BLADE PARAMETERS menu and enter PRIORITY.
- Click CREATE.
- Repeat for each VRID.

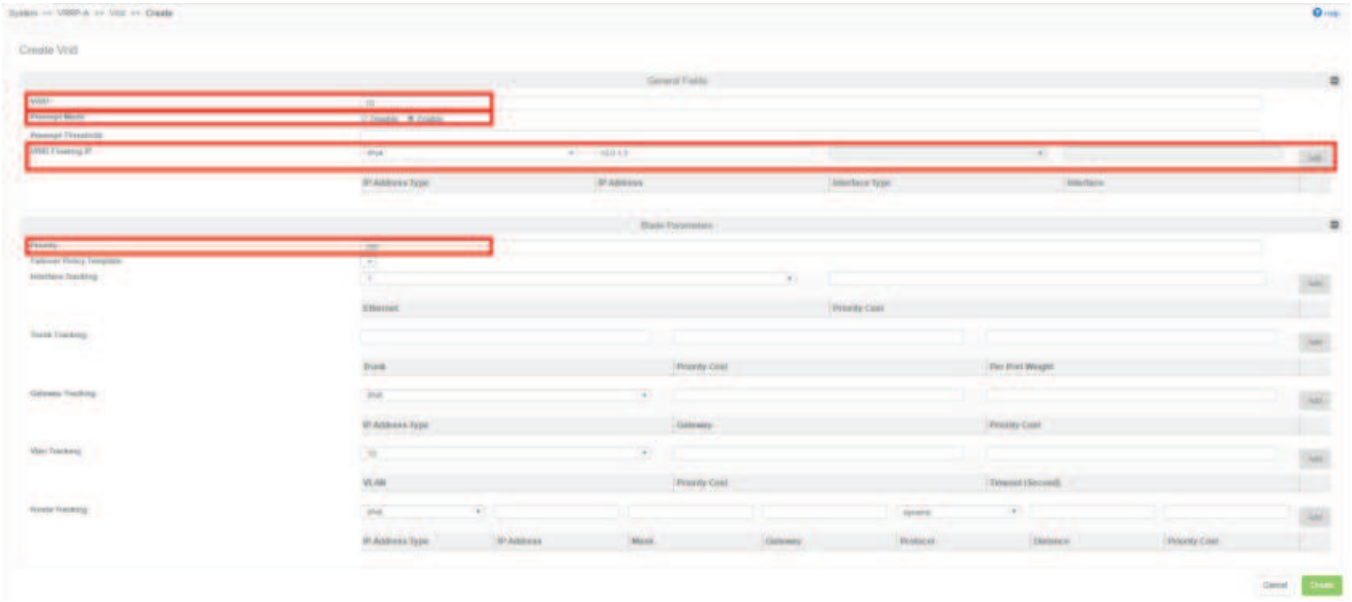


Figure 10: VRRP-A VRID configuration

Navigate to System > VRRP-A > Ethernet

- Click EDIT for Interface Ethernet 4. This will be our synchronization interface between active and passive devices.
- Once opened, click ENABLE for VRRP-A STATUS.
- For HEARTBEAT, click ENABLE.
- Enter VLAN as 30.
- Click UPDATE VRRP-A INTERFACE.

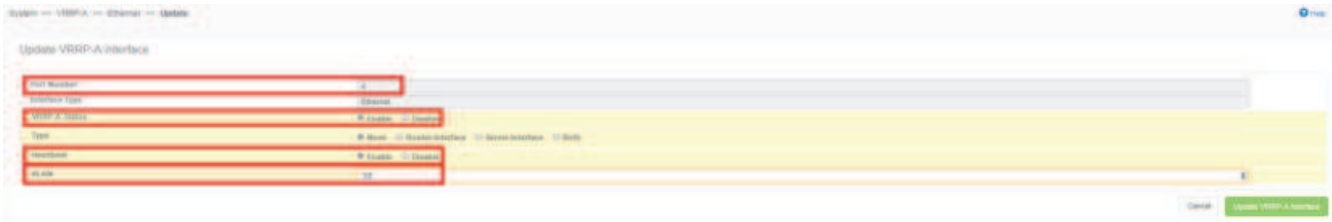


Figure 11: VRRP-A interface configuration

SSL INSIGHT TECHNOLOGY CONFIGURATION

Once the Thunder SSLi devices have been configured for high availability using VRRP-A, the next step is to configure SSLi for all devices. This phase of the configuration is divided into two parts. In the first part, the Thunder SSLi Inside devices will be configured, while in the second part, the Thunder SSLi Outside devices will be configured.

THUNDER SSLI INSIDE CONFIGURATION

The following steps are used to configure SSL Insight technology on the Thunder SSLi Inside devices. We will configure one device here. The configuration can be copied onto the second Thunder SSLi Inside device as it is configured exactly the same way as the first one.

CONFIGURE SERVERS FOR VLAN 10 AND VLAN 20

These steps configure a server load balancing server with the VRRP-A address of the first VLAN (floating IP for VRID 10). Then a second server is configured with the VRRP-A address of the second VLAN (floating IP for VRID 20).

Wildcard ports, e.g., port 0 tcp and port 0 udp, are configured under each server to ensure that both TCP and UDP traffic types are handled. Port 8080 tcp is used for decrypted traffic once port translation takes place and HTTPS traffic is converted to HTTP.

Using the CLI

```
slb server PATH1 10.0.1.13
  user-tag Security
  port 0 tcp
    health-check-disable
  port 0 udp
    health-check-disable
  port 8080 tcp
    health-check-disable
!
slb server PATH2 10.0.2.13
  user-tag Security
  port 0 tcp
    health-check-disable
  port 0 udp
    health-check-disable
  port 8080 tcp
    health-check-disable
```

***NOTE**: Health checks for all ports under the server must be disabled using the **health-check-disable** command.*

***NOTE**: The command **user-tag Security** is required for visibility of Thunder SSLi related objects inside ACOS and helps the GUI differentiate between A10 Networks Thunder ADC line of Application Delivery Controllers and Thunder SSLi related objects.*

Using the GUI

Navigate to Security > SSLi > Servers

- Click CREATE.
- Enter the NAME of the server as PATH1.
- Enter the IP ADDRESS and the NETMASK for the server.
- Select the DISABLE HEALTH-CHECK option.
- Click ADD PORT.
- Enter the PORT as 8080.

- Select the PROTOCOL as TCP from the drop-down menu.
- Select HEALTH CHECK as DISABLE.
- Click UPDATE.
- Repeat the steps for Port 0 TCP and Port 0 UDP ports for the same server.
- Repeat all of these steps for each server.

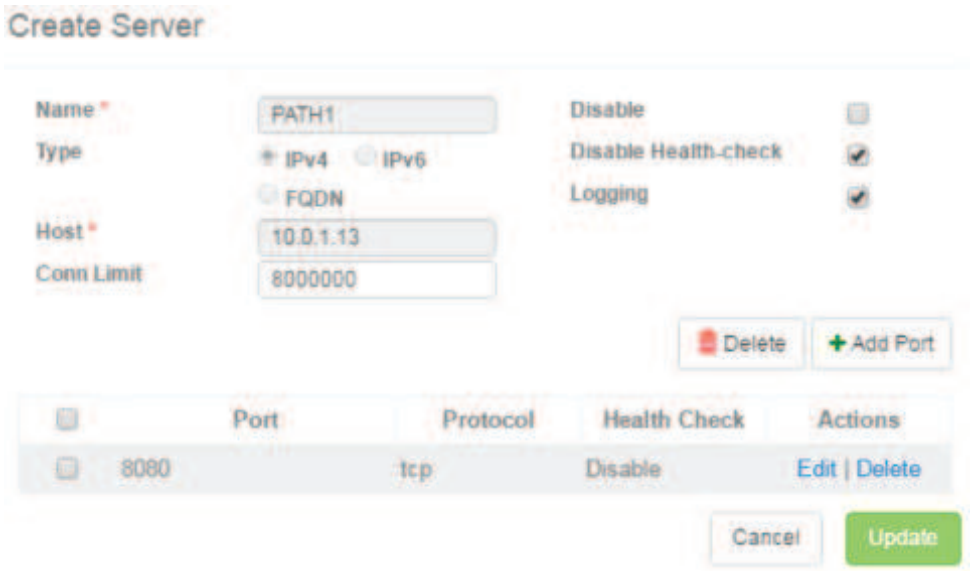


Figure 12: Server configuration

CONFIGURE SERVICE GROUP

These steps add the servers to service groups. In essence, this is where the Firewall Load Balancing (FWLB) happens. When you add multiple servers within a service group, the Thunder SSLi device uses the round robin algorithm by default to load balance between all of the servers being added.

Using the CLI

```
slb service-group SSLi_INSIDE_TCP tcp
  user-tag Security
  member PATH1 0
  member PATH2 0
slb service-group SSLi_INSIDE_UDP udp
  user-tag Security
  member PATH1 0
  member PATH2 0
slb service-group SSLi_INSIDE_FP tcp
  user-tag Security
  member PATH1 8080
  member PATH2 8080
```

***NOTE**: The load-balancing algorithm can be modified by using the command **method** at the service group configuration level.*

Using the GUI

Navigate to Security > SSLi > Service Groups

- Click CREATE.
- Enter the NAME of the service group as SSLi_INSIDE_TCP.
- Select the PROTOCOL as TCP.
- Select the ALGORITHM as ROUND ROBIN.
- Click ADD MEMBER.
- Select the STATUS as ENABLE.
- At the **NAME** option, select the existing server.
- Enter PORT as 8080.
- Click CREATE.
- Repeat all of these steps for each service group.

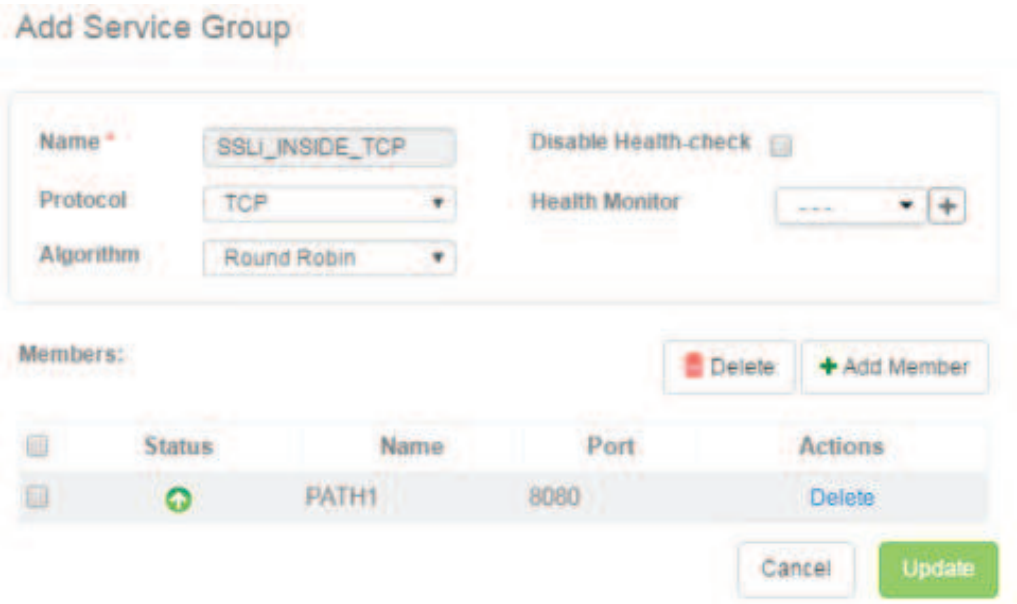


Figure 13: Service group configuration

CONFIGURE THE ACCESS CONTROL LIST

These steps configure an extended access control list (ACL) to filter incoming traffic on **VLAN-100** for interception. The ACL is configured and then bound to the wildcard VIP to define traffic of interest.

Using the CLI

```
access-list 100 permit ip any any vlan 100
```

Using the GUI

Navigate to **Security > Access List > Extended**

- Click CREATE.
- Enter the ID of the ACL as 100 (can be a value between 100 and 199).

- Select the ACTION as PERMIT.
- Select the PROTOCOL as IP.
- Select SOURCE ADDRESS and ANY.
- Select DESTINATION ADDRESS and ANY.
- Enter the VLAN as 100.
- Click CREATE.

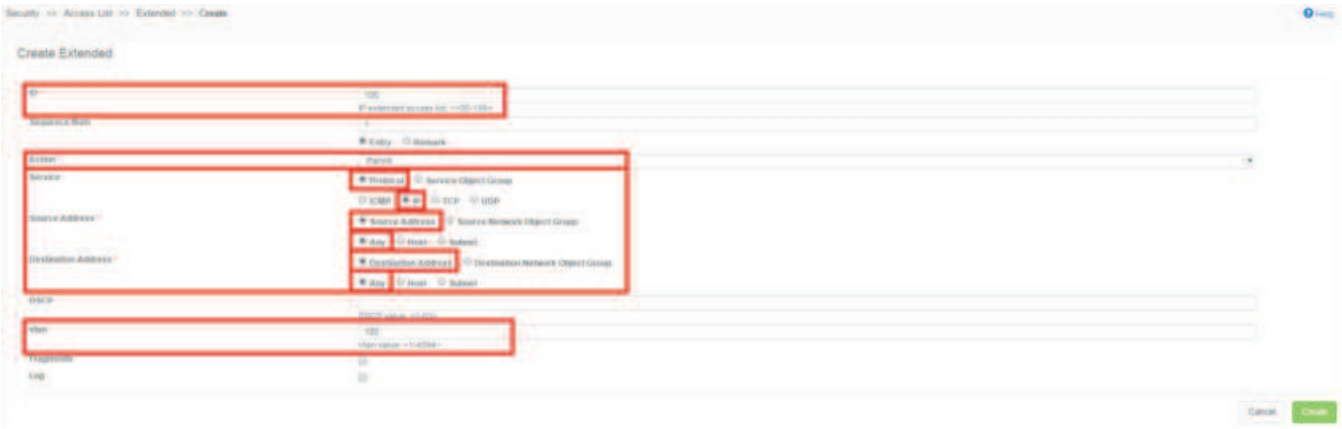


Figure 14: ACL configuration

***NOTE**: For recommended best practices related to ACLs, refer to Appendix F.*

CONFIGURE THE CLIENT SSL TEMPLATE

The following steps configure the Client SSL template, which defines the SSL decryption parameters. Bypass configuration options are also configured here, if required.

Using the CLI

```
slb template client-ssl SSLInsight_Client_Side
  user-tag Security
  template cipher cl_cipher_template
  chain-cert SSLiChain
  forward-proxy-ca-cert SSLiCA
  forward-proxy-ca-key SSLiCA
  forward-proxy-enable
```

***NOTE**: The forward-proxy-ca-cert SSLiCA and forward-proxy-ca-key SSLiCA commands are used to add the Thunder SSLi CA certificate and key already installed on the device. The command chain-cert SSLiChain can be used if an intermediate CA certificate chain exists. For more details on how to create or import certificates on the Thunder SSLi device, refer to SSL Insight Certification Installation Guide.*

The command **slb template cipher cl_cipher_template** is used to bind a cipher template to the **client-ssl template**. This cipher template is created to specify the SSL/TLS cipher suites used for the Thunder SSLi device during SSL handshakes. Here is a sample cipher template configuration:

```
slb template cipher cl_cipher_template
  user-tag Security
  SSL3_RSA_DES_192_CBC3_SHA
```

```
TLS1_RSA_AES_128_SHA
TLS1_RSA_AES_256_SHA
TLS1_ECDHE_ECDSA_AES_128_GCM_SHA256
TLS1_ECDHE_ECDSA_AES_128_SHA
TLS1_ECDHE_ECDSA_AES_128_SHA256
TLS1_ECDHE_ECDSA_AES_256_SHA
TLS1_ECDHE_RSA_AES_128_GCM_SHA256
TLS1_ECDHE_RSA_AES_128_SHA
TLS1_ECDHE_RSA_AES_128_SHA256
TLS1_ECDHE_RSA_AES_256_SHA
```

***NOTE**: A10 recommends including the same cipher suites in the list on both Inside and Outside Thunder SSLi devices. Ciphers can also be added individually inside the Client or Server SSL template rather than through the cipher template.*

***NOTE**: If you do not specify any cipher template under the Client SSL template, the default is assumed; all ciphers available on the Thunder SSLi appliance are presented during SSL handshakes.*

Using the GUI

Navigate to Security > SSLi > Templates

- Click CREATE and select Client SSL.
- Enter the NAME of the Client SSL template.
- Select the FWD PROXY ENABLE option.
- Import CA CERT and KEY using the IMPORT button.
- In the CIPHERS section, click on the + button and add a new cipher template named cl_cipher_template.
- Add all the ciphers you wish to be in the cipher suite.
- Click OK.

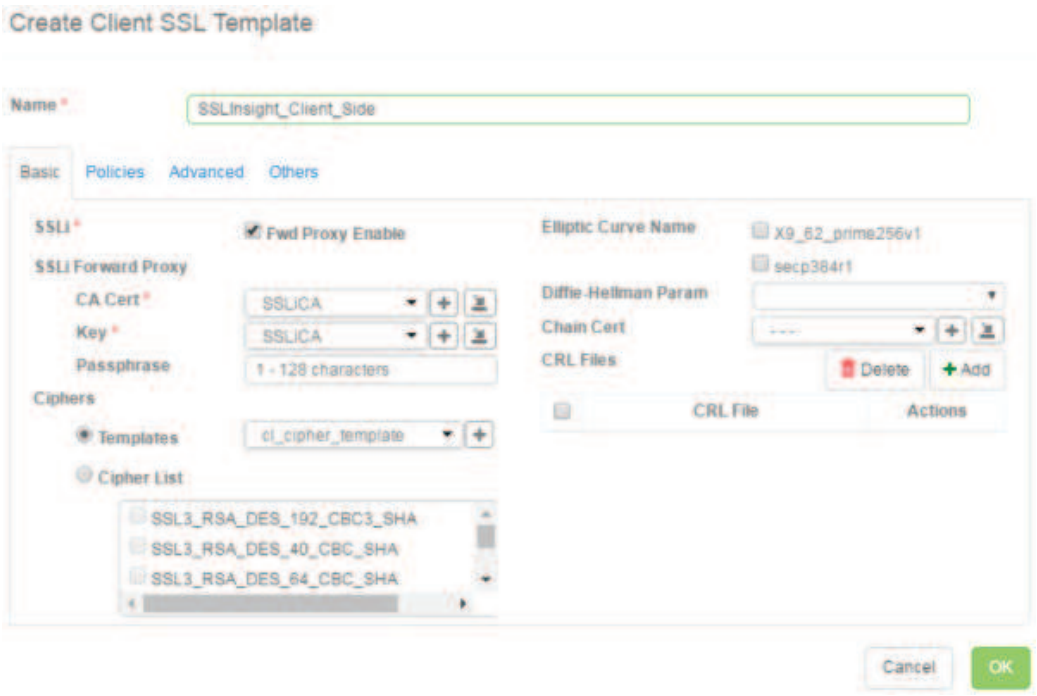


Figure 15: Client SSL template configuration

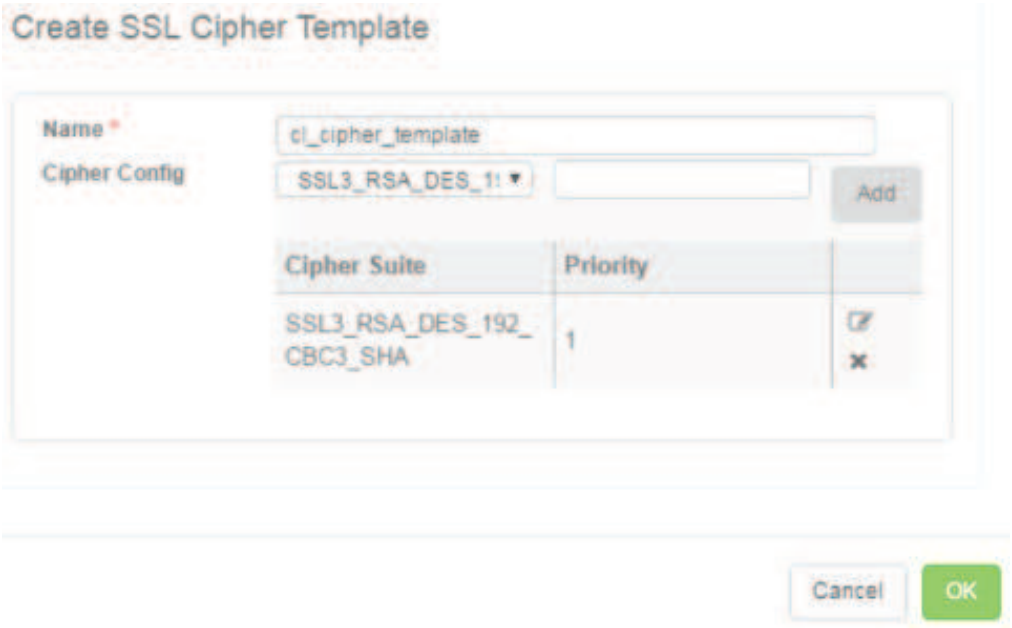


Figure 16: Cipher template configuration

CONFIGURE A WILDCARD VIP

The following steps configure the wildcard VIP for the Thunder SSLi Inside device. The Client SSL template, along with the service groups, will be configured under the wildcard "SSLi_INSIDE."

Using the CLI

```
slb virtual-server SSLi_INSIDE 0.0.0.0 acl 100
  user-tag Security
  port 0 tcp
    service-group SSLi_INSIDE_TCP
    no-dest-nat
  port 0 udp
    service-group SSLi_INSIDE_UDP
    no-dest-nat
  port 0 others
    service-group SSLi_INSIDE_UDP
    no-dest-nat
  port 443 https
    service-group SSLi_INSIDE_FP
    template client-ssl SSLInsight_Client_Side
    no-dest-nat port-translation
```

***NOTE**: The command **no-dest-nat port-translation** is used to ensure that destination Network Address Translation (NAT) is not used. The port translation part of the command enables Thunder SSLi devices to translate the destination port from 443 to 8080.*

***NOTE**: For recommended best practices, refer to Appendix F.*

Using the GUI

Navigate to **Security > SSLi > Services**

- Click **CREATE**.
- Select the **TYPE** as **INSIDE (DECRYPT)**.
- Enter the **NAME** as **SSLi_INSIDE**.

At this point, the GUI has auto-generated an ACL, service groups, servers and a Client SSL Template.

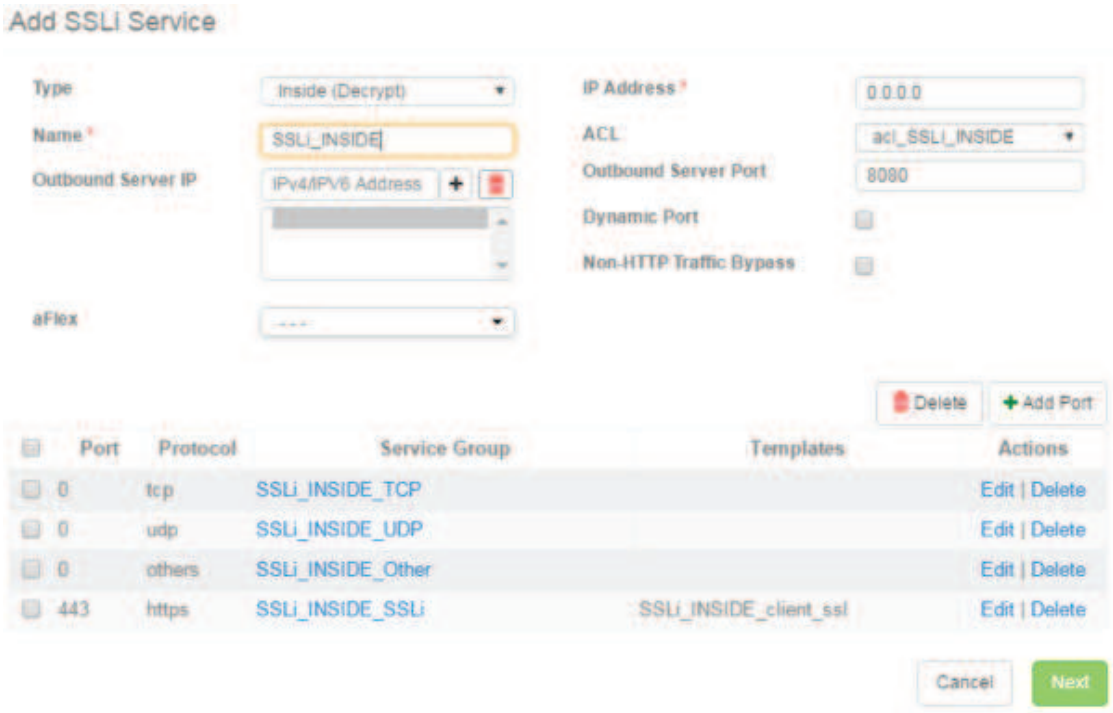


Figure 17: Thunder SSLi Inside wildcard VIP configuration (auto-generated)

Since we have created everything ourselves, according to the deployment requirements, delete the auto-generated configurations and replace them by adding the previously configured ACL, service groups, servers inside the service groups, and the Client SSL Template. This can be done using the following steps:

- Select ACL as 100 from the drop-down list.
- Add service groups (configured earlier).
- Add Client SSL template SSLInsight_Client_Side to the service group SSLi_INSIDE_FP.
- Click NEXT.
- Click OTHERS.
- Click DONE.

***NOTE**: The Client SSL Template can also be created at this stage as well. Once the VIP is configured and the **NEXT** button is clicked, the Client SSL Template creation options as well as optional Bypass Configurations are presented.*

Your final Wildcard VIP configuration should look like this:

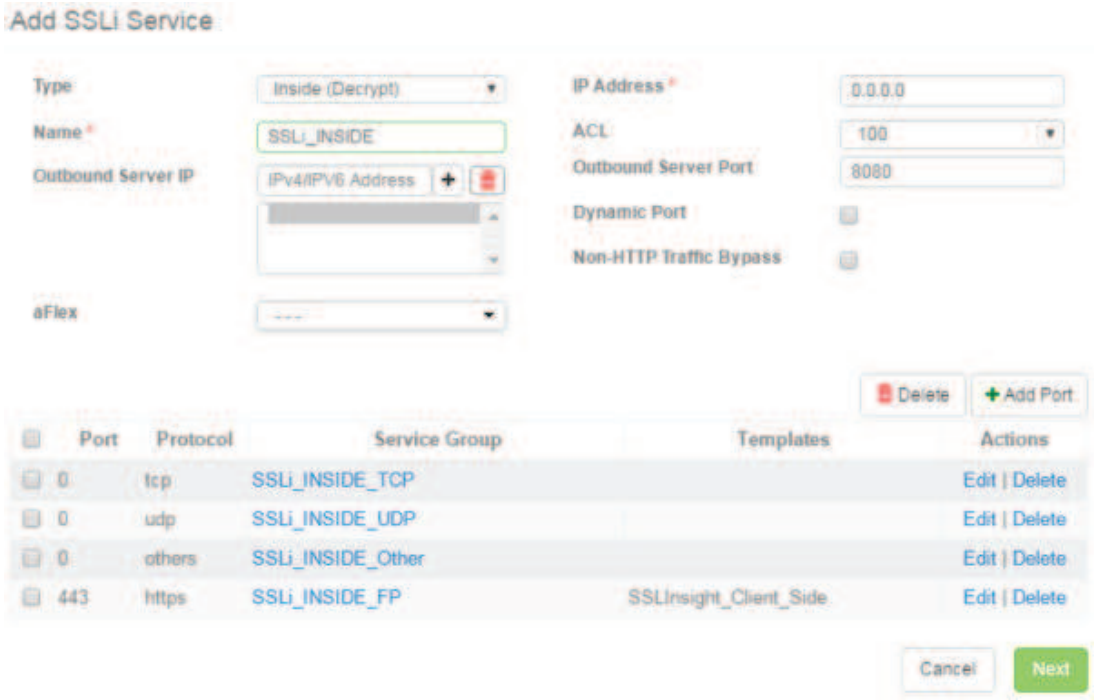


Figure 18: Thunder SSLi Inside wildcard VIP configuration (after editing)

THUNDER SSLI OUTSIDE CONFIGURATION

The following steps are used to configure SSL Insight technology on the Thunder SSLi Outside devices. We will configure one device here. The configuration can be copied onto the second Outside device, as it is configured exactly the same way as the first one.

CONFIGURE SERVER FOR DEFAULT GATEWAY

These steps configure a server load balancing server with the IP address of the default router, i.e., 192.0.2.254. This server will be used to forward traffic to the gateway router, through which traffic will reach the Internet. Wildcard ports, e.g., port 0 tcp and port 0 udp, are configured under each server to ensure that both TCP and UDP traffic types are handled. Port 443 tcp is used for encrypted traffic once port translation takes place and the incoming HTTP traffic is converted to HTTPS.

Using the CLI

```
slb server GATEWAY 192.0.2.254
  user-tag Security
  port 0 tcp
    health-check-disable
  port 0 udp
    health-check-disable
  port 443 tcp
    health-check-disable
```

***NOTE**: Health checks for all ports under the server must be disabled using the **health-check-disable** command.*

Using the GUI

Servers on Thunder SSLi Inside and SSLi Outside devices are configured the same way. Refer to the Thunder SSLi Inside Server Configuration section for details.

CONFIGURE SERVICE GROUP

These steps add the gateway server to service groups.

Using the CLI

```
slb service-group SSLi_OUTSIDE_TCP tcp
  user-tag Security
  member GATEWAY 0
slb service-group SSLi_OUTSIDE_UDP udp
  user-tag Security
  member GATEWAY 0
slb service-group SSLi_OUTSIDE_FP tcp
  user-tag Security
  member GATEWAY 443
```

Using the GUI

Service groups on Thunder SSLi Inside and SSLi Outside are configured the same way. Refer to the Thunder SSLi Inside Service Group Configuration section for details.

CONFIGURE THE ACCESS CONTROL LIST

These steps configure an extended ACL to intercept incoming traffic on **VLAN-10** and **VLAN-20**. The ACL is configured and then bound to the wildcard VIP to define traffic of interest.

Using the CLI

```
access-list 100 permit ip any any vlan 10
access-list 100 permit ip any any vlan 20
```

Using the GUI

ACLs on Thunder SSLi Inside and SSLi Outside are configured the same way. Refer to the Thunder SSLi Inside Access List Configuration section for details.

***NOTE**: For recommended best practices related to ACLs, refer to Appendix F.*

CONFIGURE THE SERVER SSL TEMPLATE

The following steps configure the Server SSL template. This template is used to re-encrypt the traffic, previously decrypted by the Thunder SSLi Inside device.

Using the CLI

```
slb template server-ssl SSLInsight_Server_Side
  user-tag Security
  forward-proxy-enable
  template cipher sr_cipher_template
```

The Server SSLi template, along with the service groups, will be configured under the virtual server with the wildcard vip 0.0.0.0.

The command **slb template cipher sr_cipher_template** is used to bind a cipher template to the **server-ssl template**. This cipher template is added on the Outside device, and it is used to specify the cipher suite the Thunder SSLi will present during SSL handshakes with the remote servers. The cipher template is created manually in the configuration mode:

```
slb template cipher sr_cipher_template
  user-tag Security
  SSL3_RSA_DES_192_CBC3_SHA
  TLS1_RSA_AES_128_SHA
  TLS1_RSA_AES_256_SHA
  TLS1_ECDHE_ECDSA_AES_128_GCM_SHA256
  TLS1_ECDHE_ECDSA_AES_128_SHA
  TLS1_ECDHE_ECDSA_AES_128_SHA256
  TLS1_ECDHE_ECDSA_AES_256_SHA
  TLS1_ECDHE_RSA_AES_128_GCM_SHA256
  TLS1_ECDHE_RSA_AES_128_SHA
  TLS1_ECDHE_RSA_AES_128_SHA256
  TLS1_ECDHE_RSA_AES_256_SHA
```

***NOTE**: A10 recommends including the same cipher suites in the list on both Inside and Outside Thunder SSLi devices. Ciphers can also be added individually inside the Client or Server SSL template rather than through the cipher template.*

***NOTE**: If you do not specify any cipher template under the client-ssl template, the default is assumed, i.e., all ciphers available on the Thunder SSLi appliance are presented during SSL handshakes.*

Using the GUI

Navigate to Security > SSLi > Templates

- Click CREATE and select Server SSL.
- Enter the NAME of the Server SSL template.
- Select the FWD PROXY ENABLE option.
- In the CIPHERS section, click on the + button and add a new cipher template named sr_cipher_template.
- Add all ciphers you want to be in the cipher suite.
- Click OK.

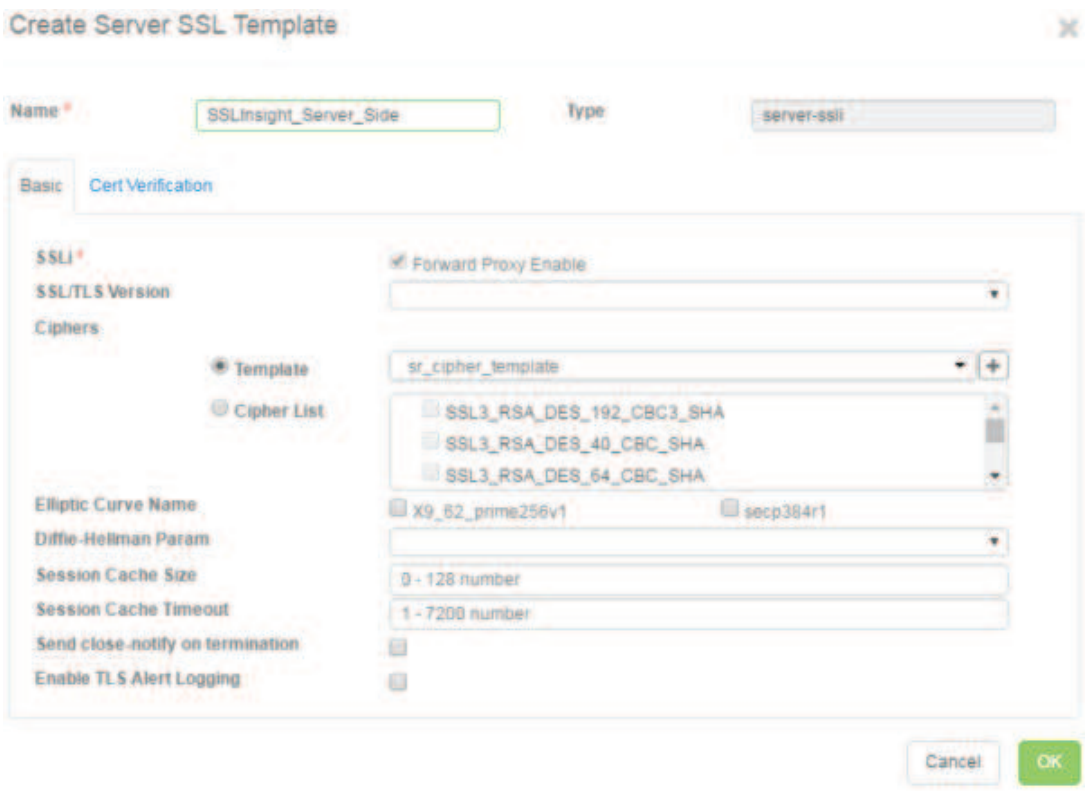


Figure 19: Server SSL template configuration

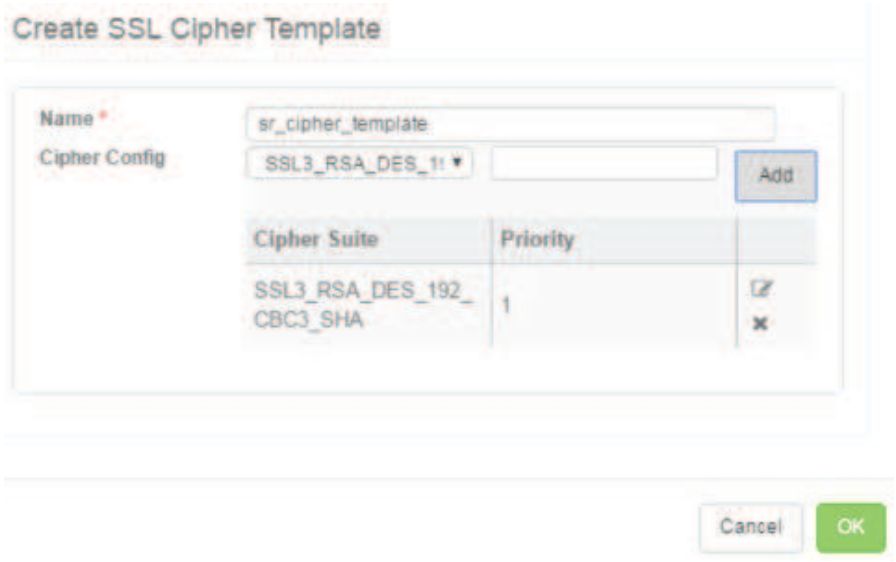


Figure 20: Cipher template configuration

CONFIGURE A WILDCARD VIP

The following steps configure the wildcard VIP for the Thunder SSLi Outside device. The server-ssl template, along with the service groups, will be configured under the wildcard VIP "SSLi_OUTSIDE".

Using the CLI

```
slb virtual-server SSLi_OUTSIDE 0.0.0.0 acl 100
  user-tag Security
  port 0 tcp
    service-group SSLi_OUTSIDE_TCP
    use-rcv-hop-for-resp
    no-dest-nat
  port 0 udp
    service-group SSLi_OUTSIDE_UDP
    use-rcv-hop-for-resp
    no-dest-nat
  port 0 others
    service-group SSLi_OUTSIDE_UDP
    use-rcv-hop-for-resp
    no-dest-nat
  port 8080 http
    service-group SSLi_OUTSIDE_FP
    template server-ssl SSLInsight_Server_Side
    use-rcv-hop-for-resp
    no-dest-nat port-translation
```

***NOTE**: The command use-rcv-hop-for-resp is used to ensure that the returning traffic is forwarded to the same security device that was traversed when going from Inside to Outside.*

***NOTE**: The command no-dest-nat port-translation is used to ensure that destination NAT is not used. The port translation part of the command enables Thunder SSLi to translate the destination port from 8080 to 443.*

***NOTE**: For recommended best practices, refer to Appendix F.*

Using the GUI

Navigate to Security > SSLi > Services

- Click CREATE.
- Select the TYPE as OUTSIDE (RE-ENCRYPT).
- Enter the NAME as SSLi_OUTSIDE.

At this point, the GUI has auto-generated an ACL, service groups, servers and a Server SSL template.

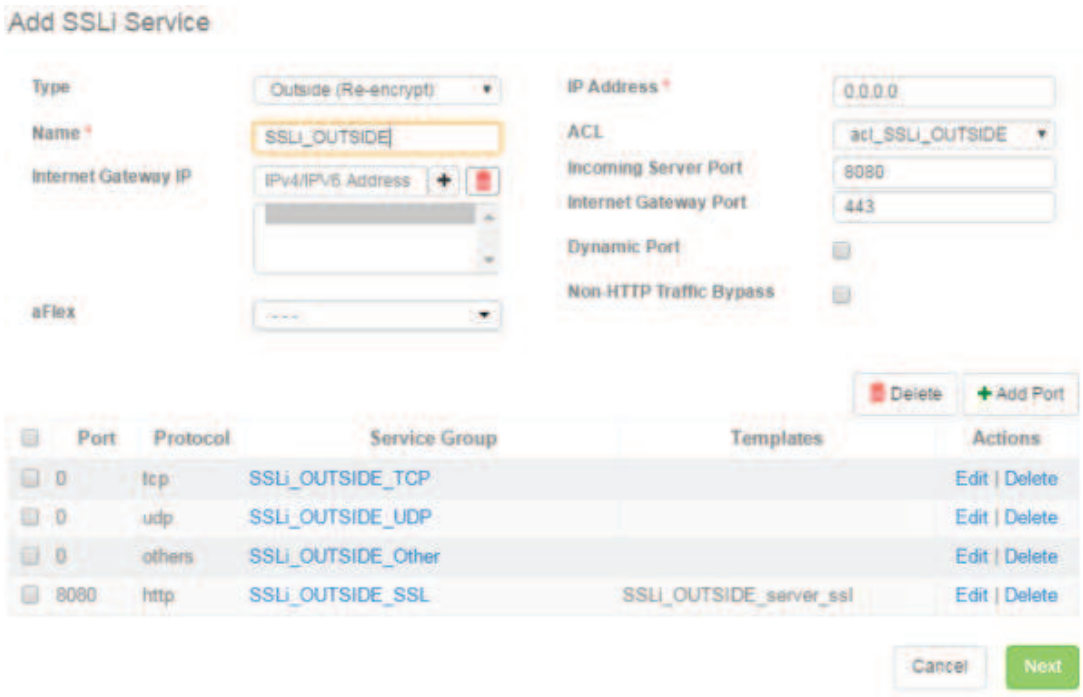


Figure 21: Thunder SSLi Outside wildcard VIP configuration (auto-generated)

Since we have created everything ourselves according to the deployment requirements, delete the auto-generated configurations and replace them by adding the previously configured ACL, service groups, servers inside the service groups, and the Client SSL template. This can be done using the following steps:

- Select ACL as 100 from the drop-down list.
- Add service groups (configured earlier).
- Add Client SSL template SSLInsight_Server_Side to the service group SSLi_OUTSIDE_FP.
- Click NEXT.
- Click OTHERS.
- Click DONE.

***NOTE**: The Server SSL template can be created at this stage as well. Once the VIP is configured and the NEXT button is clicked, the Server SSL template creation options are presented.*

Your final Wildcard VIP configuration should look like this:

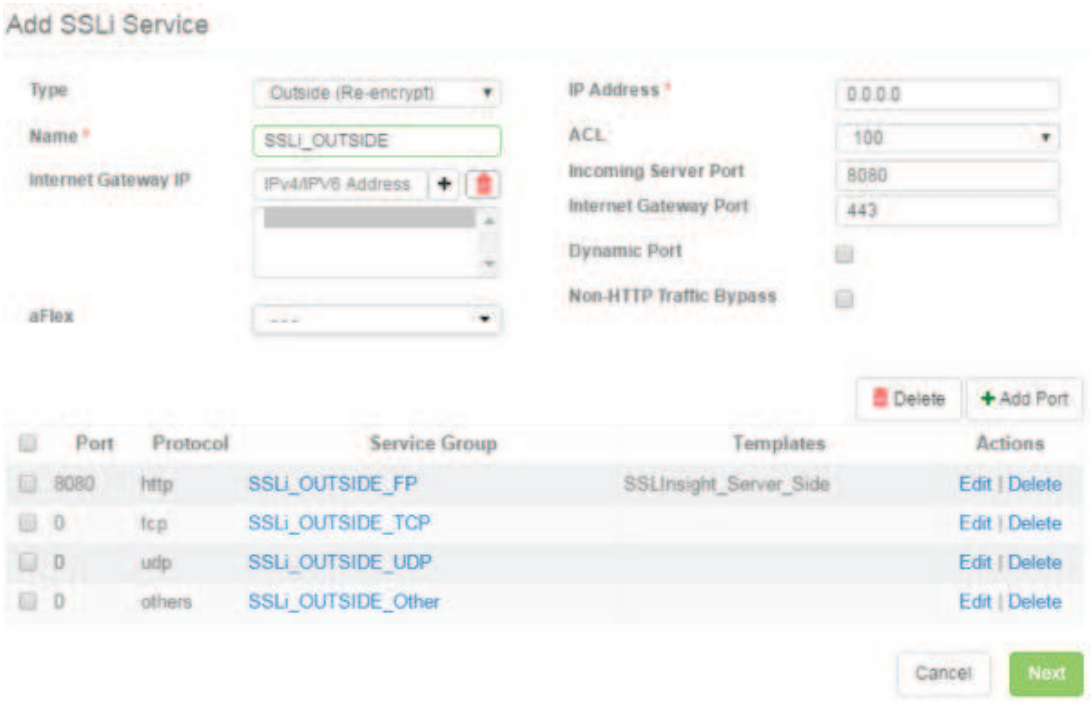


Figure 22: SSLi Outside wildcard VIP configuration (after editing)

PALO ALTO NETWORKS FIREWALL

This section provides basic configuration steps for setting up the Palo Alto Networks (PAN) PA firewalls for A10 Thunder SSL Insight. No special configuration is required on the PAN firewalls for integration with the Thunder SSLi devices.

ZONE CONFIGURATION

For traffic to flow properly and as a general rule, the firewalls are configured with two zones; trusted and untrusted. Zones are named to show flow from the inside, i.e., trusted zone of the network towards the outside, which is the untrusted zone. The terminology simplifies the configuration of L2 mode deployment of the PANs as well as helping in the configuration of some basic policies.

For vWire and L2 mode deployments of PAN firewalls, zoning helps in the flow of traffic from the inside device to the outside device.

On the PAN firewalls, navigate to **Network > Zone** and create both the zones as follows:

NAME	*LOCATION*	*TYPE*
Trusted	vsys1	Layer 2
Untrusted	vsys1	Layer 2

Table 4: Palo Alto Networks firewalls zoning

Logically, the trusted zone is the network segment on the “inside” while the untrusted zone is the network segment on the “outside” of the PAN firewall.

VLAN INTERFACE CONFIGURATION

In a Layer 2 PAN deployment, switching is done based on VLANs. Interfaces are added to the VLANs and then based on policies.

Navigate to Network > VLAN.

- Click ADD.
- Enter NAME as vlan 10.
- Select VLAN INTERFACE as vlan.
- In the INTERFACES section, click ADD and select the interfaces you wish to add to the VLAN.
- Click OK.

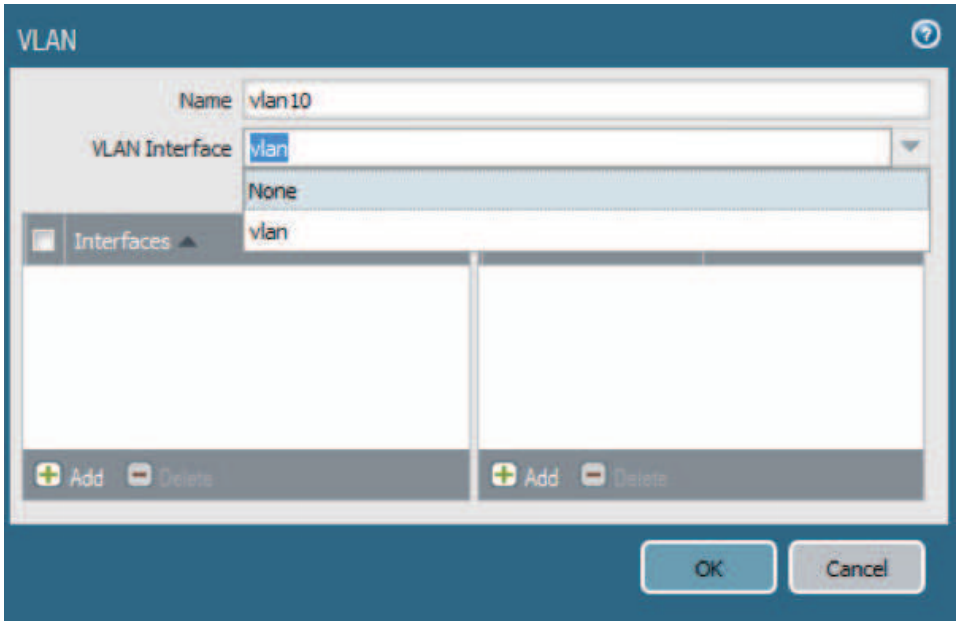


Figure 23: VLAN interface configuration

Interfaces can also be added to a VLAN as follows:

Navigate to Network > Ethernet.

- Click on ETHERNET1/1.
- Select INTERFACE TYPE as LAYER2.
- In the CONFIG tab, select NEW VLAN from the VLAN drop-down menu.
- Click ADD.
- Enter NAME as vlan 10.
- Select VLAN INTERFACE as vlan.
- In the INTERFACES section, click ADD and select the interfaces you wish to add to the VLAN.
- Click OK.
- Add other interfaces to the VLAN.

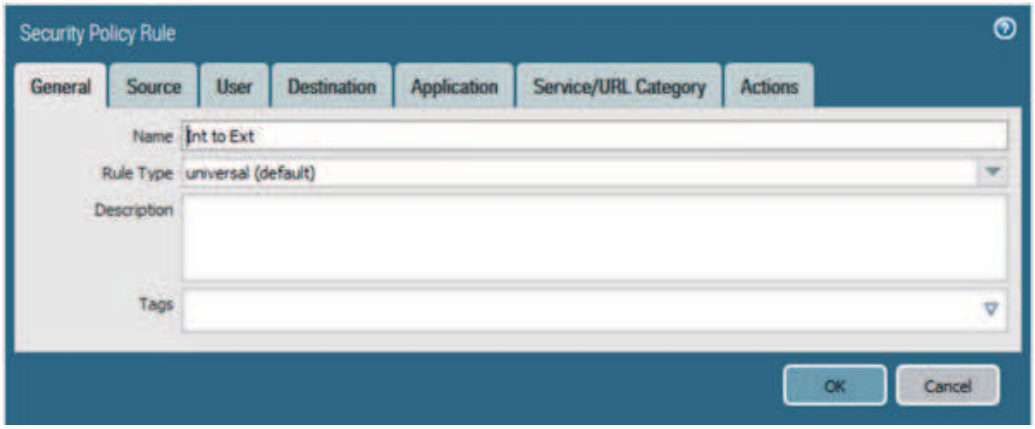


Figure 24: Adding a new VLAN to interface

POLICY CONFIGURATION

This section shows the configuration of security policies on the PAN firewall. A set of two policies will be needed to specify the behavior of the PAN firewall for outbound and inbound traffic. Every network will have its own policy so the default configuration within the PAN firewall will be used as a reference configuration.

For the Outbound traffic, navigate to the Security Policies section and click ADD.

- For the SECURITY POLICY RULE, in the GENERAL tab, enter NAME as Int to Ext.
- Select RULE TYPE as UNIVERSAL (DEFAULT).
- In the SOURCE tab, select TRUST as your source zone.
- In the DESTINATION tab, select UNTRUST as your destination zone.
- In the ACTIONS tab, select ACTION as ALLOW.
- Everything else should be left as DEFAULT.
- Click OK.

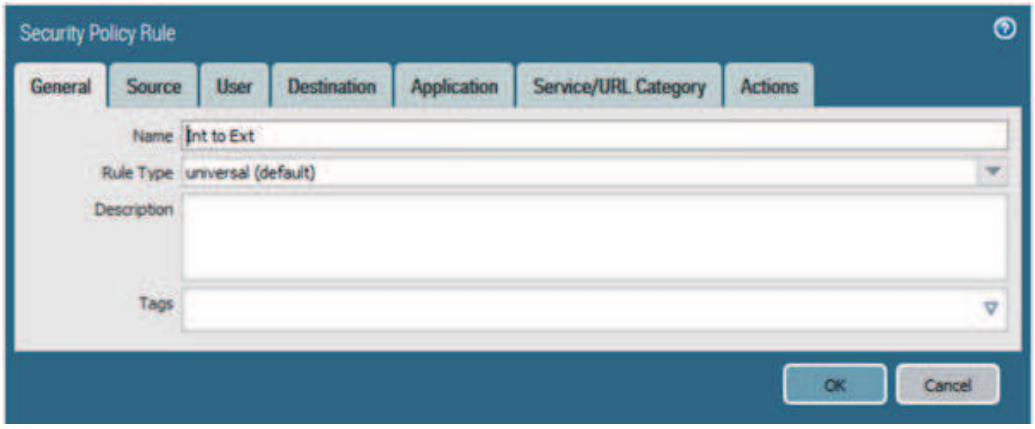


Figure 25: Security Policy Rule configuration – General

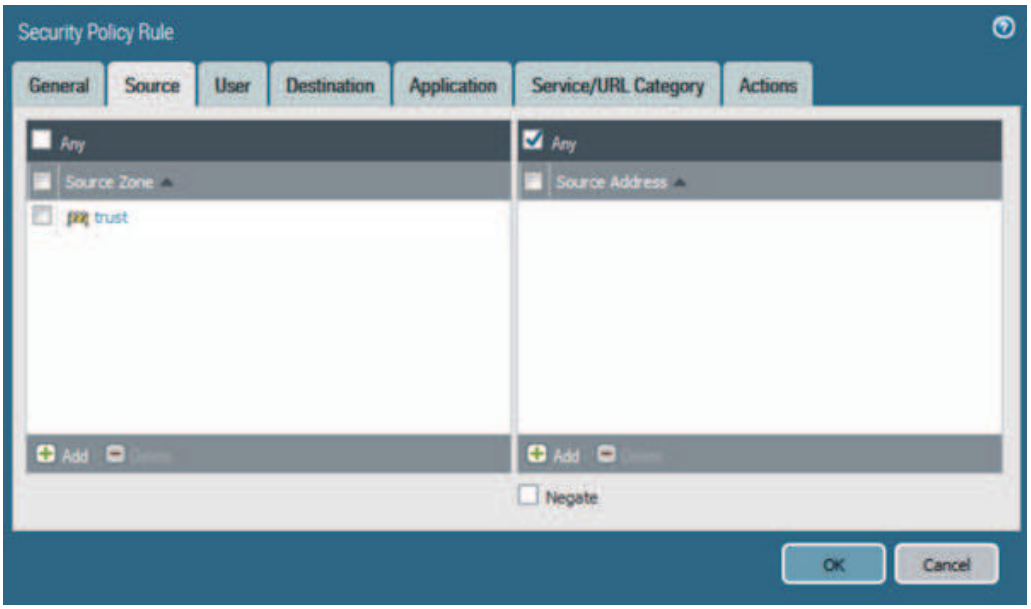


Figure 26: Security Policy Rule configuration – Source

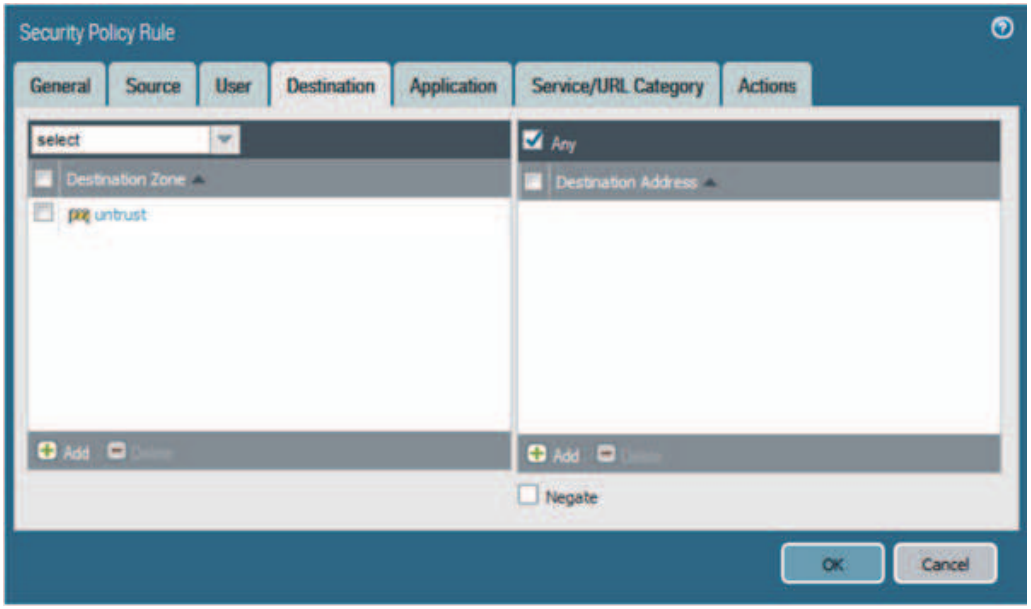


Figure 27: Security Policy Rule configuration – Destination

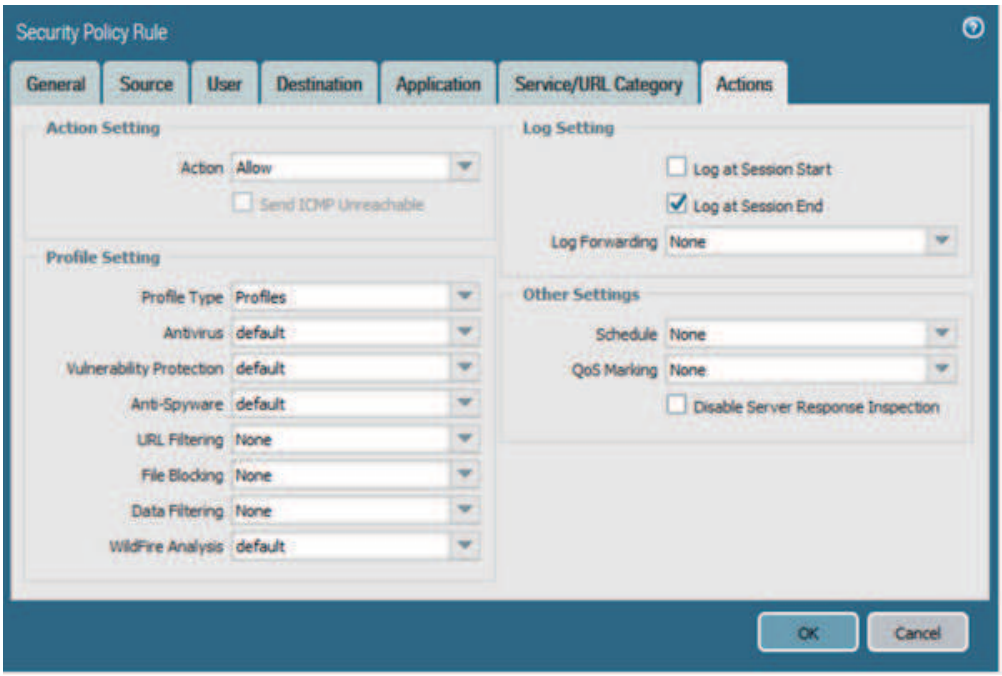


Figure 28: Security Policy Rule configuration – Actions

For **inbound traffic**, repeat all steps but switch **SOURCE** and **DESTINATION**. The final summary should look like this:

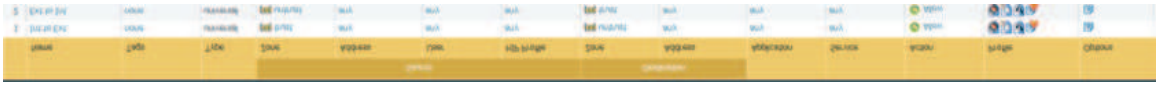


Figure 29: Security Policy Rule configuration – Summary

SUMMARY

The growth in encrypted traffic, coupled with increasing SSL key lengths and more computationally complex SSL ciphers, makes it difficult for inline security devices to decrypt SSL traffic. A wide range of security devices, including Palo Alto Networks PA firewall appliances, require visibility into encrypted traffic to discover attacks, intrusions and malware. This guide lays out the steps required to configure A10 Thunder SSL Insight with Palo Alto Networks PA firewalls. Once you have completed the steps described in this guide, you will be ready to use your new deployment to decrypt SSL traffic.

SSL Insight technology, included as a standard feature of A10 Thunder SSLi or A10 Thunder CFW, offers organizations a powerful solution for load balancing, high availability and SSL inspection. Using SSLi, organizations can:

- Analyze all network data, including encrypted data, eliminating blind spots in their threat protection solution
- Detect encrypted malware, insider abuse and attacks transported over SSL/TLS
- Deploy best-of-breed content inspection solutions to fend off cyber attacks
- Maximize the performance, availability and scalability of the security infrastructure by offloading SSL decryption and re-encryption tasks to SSLi, while leveraging A10's 64-bit ACOS platform, Flexible Traffic Acceleration (FTA) technology and specialized security processors.

For more information about Thunder SSLi products, please visit:

https://www.a10networks.com/products/ssl-insight-securing-encrypted-traffic

https://www.a10networks.com/resources/solution-briefs

https://www.a10networks.com/resources/case-studies

APPENDIX A – COMPLETE CONFIGURATION FILES FOR PRIMARY THUNDER SSLI INSIDE AND OUTSIDE DEVICES

Thunder SSLi Inside 1

```
vrrp-a common
  device-id 1
  set-id 1
  enable
!
access-list 100 permit ip any any vlan 100
!
vlan 100
  untagged ethernet 1
  router-interface ve 100
!
vlan 10
  untagged ethernet 2
  router-interface ve 10
!
vlan 20
  untagged ethernet 3
  router-interface ve 20
!
vlan 30
  untagged ethernet 4
  router-interface ve 30
!
interface ve 100
  name INSIDE
  ip address 10.0.0.1 255.255.255.0
  ip allow-promiscuous-vip
!
interface ve 10
  name PATH1
  ip address 10.0.1.1 255.255.255.0
  ip allow-promiscuous-vip
!
interface ve 20
  name PATH2
  ip address 10.0.2.1 255.255.255.0
  ip allow-promiscuous-vip
!
interface ve 30
  name SYNC-PATH
  ip address 1.1.1.1 255.255.255.0
!
```

Thunder SSLi Outside 1

```
vrrp-a common
  device-id 1
  set-id 2
  enable
!
access-list 100 permit ip any any vlan 10
!
access-list 100 permit ip any any vlan 20
!
vlan 100
  untagged ethernet 1
  router-interface ve 100
!
vlan 10
  untagged ethernet 2
  router-interface ve 10
!
vlan 20
  untagged ethernet 3
  router-interface ve 20
!
vlan 30
  untagged ethernet 4
  router-interface ve 30
!
interface ve 100
  name OUTSIDE
  ip address 192.0.2.1 255.255.255.0
  ip allow-promiscuous-vip
!
interface ve 10
  name PATH1
    ip address 10.0.1.11 255.255.255.0
  ip allow-promiscuous-vip
!
interface ve 20
  name PATH2
 ip address 10.0.2.11 255.255.255.0
  ip allow-promiscuous-vip
!
interface ve 30
  name SYNC-PATH
```

```
!
vrrp-a interface ethernet 4
  vlan 30
!
ip route 0.0.0.0 /0 10.0.1.13
!
vrrp-a vrid 0
vrrp-a vrid 0
  floating-ip 10.0.0.3
  blade-parameters
    priority 200
!
vrrp-a vrid 10
  floating-ip 10.0.1.3
  blade-parameters
    priority 200
!
vrrp-a vrid 20
  floating-ip 10.0.2.3
  blade-parameters
    priority 200
!
slb server PATH1 10.0.1.13
  user-tag Security
  port 0 tcp
    health-check-disable
  port 0 udp
    health-check-disable
  port 8080 tcp
    health-check-disable
!
slb server PATH2 10.0.2.13
  user-tag Security
  port 0 tcp
    health-check-disable
  port 0 udp
    health-check-disable
port 8080 tcp
    health-check-disable
!
slb service-group SSLi_INSIDE_TCP tcp
  user-tag Security
  member PATH1 0
  member PATH2 0
slb service-group SSLi_INSIDE_UDP udp
  user-tag Security
  ip address 1.1.1.1 255.255.255.0
!
!
vrrp-a interface ethernet 4
  vlan 30
!
ip route 0.0.0.0 /0 192.0.2.254
!
vrrp-a vrid 0
  floating-ip 192.0.2.3
  blade-parameters
    priority 200
!
vrrp-a vrid 11
  floating-ip 10.0.1.13
  blade-parameters
    priority 200
!
vrrp-a vrid 21
  floating-ip 10.0.2.13
  blade-parameters
    priority 200
!
slb server GATEWAY 192.0.2.254
  user-tag Security
  port 0 tcp
    health-check-disable
  port 0 udp
    health-check-disable
  port 443 tcp
    health-check-disable
!
slb service-group SSLi_OUTSIDE_TCP tcp
  user-tag Security
  member GATEWAY 0
slb service-group SSLi_OUTSIDE_UDP udp
user-tag Security
  member GATEWAY 0
slb service-group SSLi_OUTSIDE_FP tcp
  user-tag Security
  member GATEWAY 443
!
slb template server-ssl SSLInsight_Server_
Side
  user-tag Security
  forward-proxy-enable
```

```
  member PATH1 0
  member PATH2 0
slb service-group SSLi_INSIDE_FP tcp
  user-tag Security
  member PATH1 8080
  member PATH2 8080
!
slb template client-ssl SSLInsight_Client_
Side
  user-tag Security
  template cipher cl_cipher_template
chain-cert SSLiChain
  forward-proxy-ca-cert SSLiCA
  forward-proxy-ca-key SSLiCA
 forward-proxy-enable
!
slb virtual-server SSLi_INSIDE 0.0.0.0 acl
100
  user-tag Security
  port 0 tcp
    service-group SSLi_INSIDE_TCP
    no-dest-nat
  port 0 udp
    service-group SSLi_INSIDE_UDP
    no-dest-nat
  port 0 others
    service-group SSLi_INSIDE_UDP
    no-dest-nat
  port 443 https
    service-group SSLi_INSIDE_FP
    template client-ssl SSLInsight_Client_
Side
    no-dest-nat port-translation
!
end
```

```
  template cipher sr_cipher_template
!
slb virtual-server SSLi_OUTSIDE 0.0.0.0 acl
100
  user-tag Security
  port 0 tcp
service-group SSLi_OUTSIDE_TCP
    use-rcv-hop-for-resp
    no-dest-nat
  port 0 udp
    service-group SSLi_OUTSIDE_UDP
    use-rcv-hop-for-resp
    no-dest-nat
  port 0 others
service-group SSLi_OUTSIDE_UDP
    use-rcv-hop-for-resp
    no-dest-nat
  port 8080  http
    service-group SSLi_OUTSIDE_FP
    template server-ssl SSLInsight_Server_
Side
    use-rcv-hop-for-resp
    no-dest-nat port-translation
!
end
```

APPENDIX B – ALTERNATE DESIGN FOR PAN FIREWALLS IN VWIRE MODE

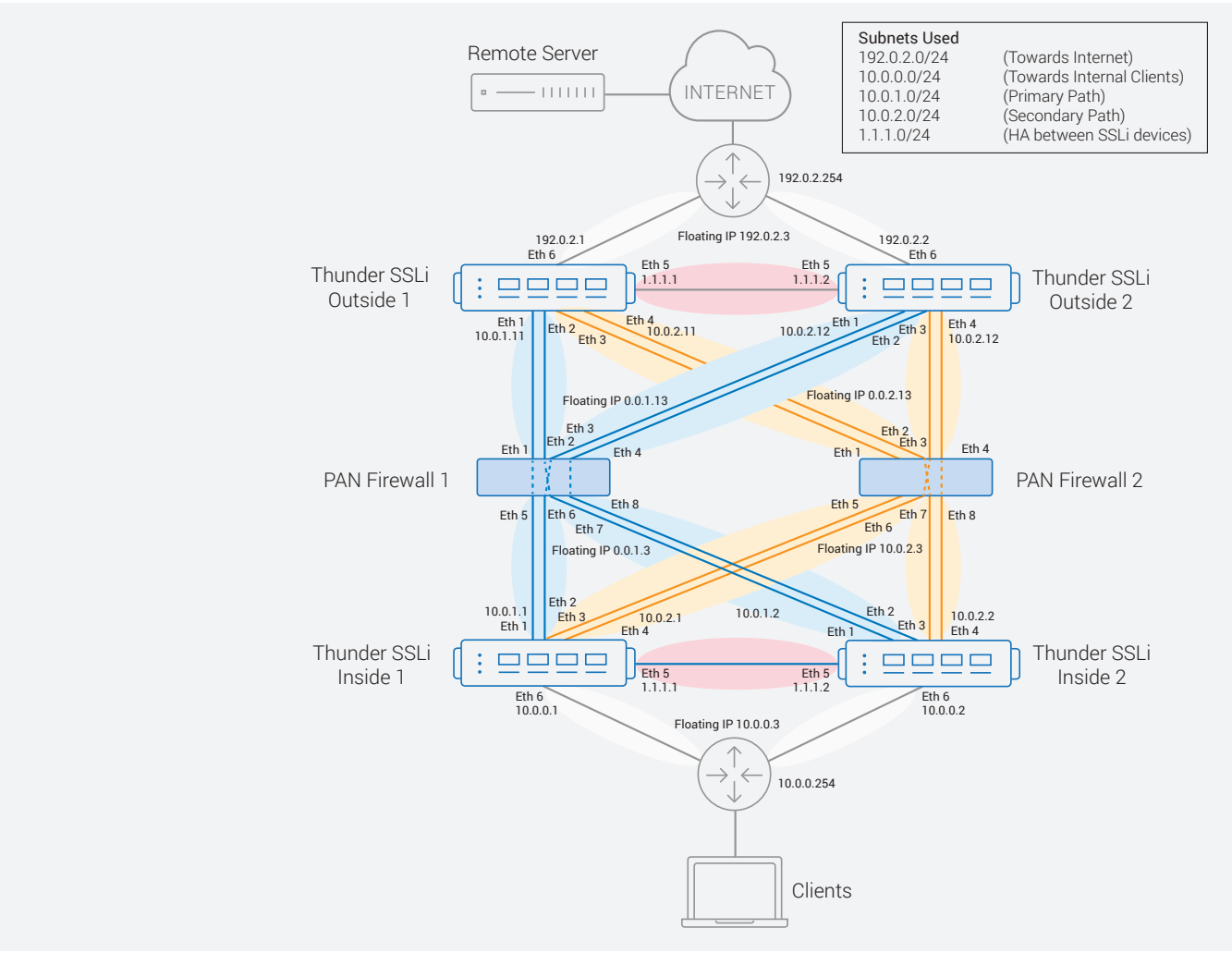


Figure 30: A10 Thunder SSL Insight with PA Networks firewalls in vWire mode

***NOTE**: Configuration changes for vWire mode deployment will primarily be made to the PAN firewalls. The only major change in the Thunder SSLi devices' configurations would be the addition of two more interfaces, i.e., one per existing links going to each PAN firewall. The rest of the configuration will stay the same.*

APPENDIX C – DETAILED WALKTHROUGH OF THUNDER SSLI PACKET FLOW

When traversing through the Thunder SSL Insight network, traffic is subjected to the following steps:

1. If the certificate already exists in cache, send it to the client and move to step 2. Otherwise, establish an SSL connection with the remote server and get the server certificate.
2. Extract header information from the server certificate. Change the issuer and the public key as it exists in the Client SSL Template. Re-assign the new certificate using the CA-Certificate as it exists in the Client SSL Template. Send the reconstructed Server-Hello to client.
3. At his point, the data is decrypted and sent in clear text through the firewall.
4. A new SSL session is initiated with the remote server; data is encrypted and sent to remote server.
5. Response is decrypted and sent through the firewall.
6. Response is encrypted again and sent to the client.

The following figure details the packet flow and communication messages through a Thunder SSL Insight network, as discussed above:

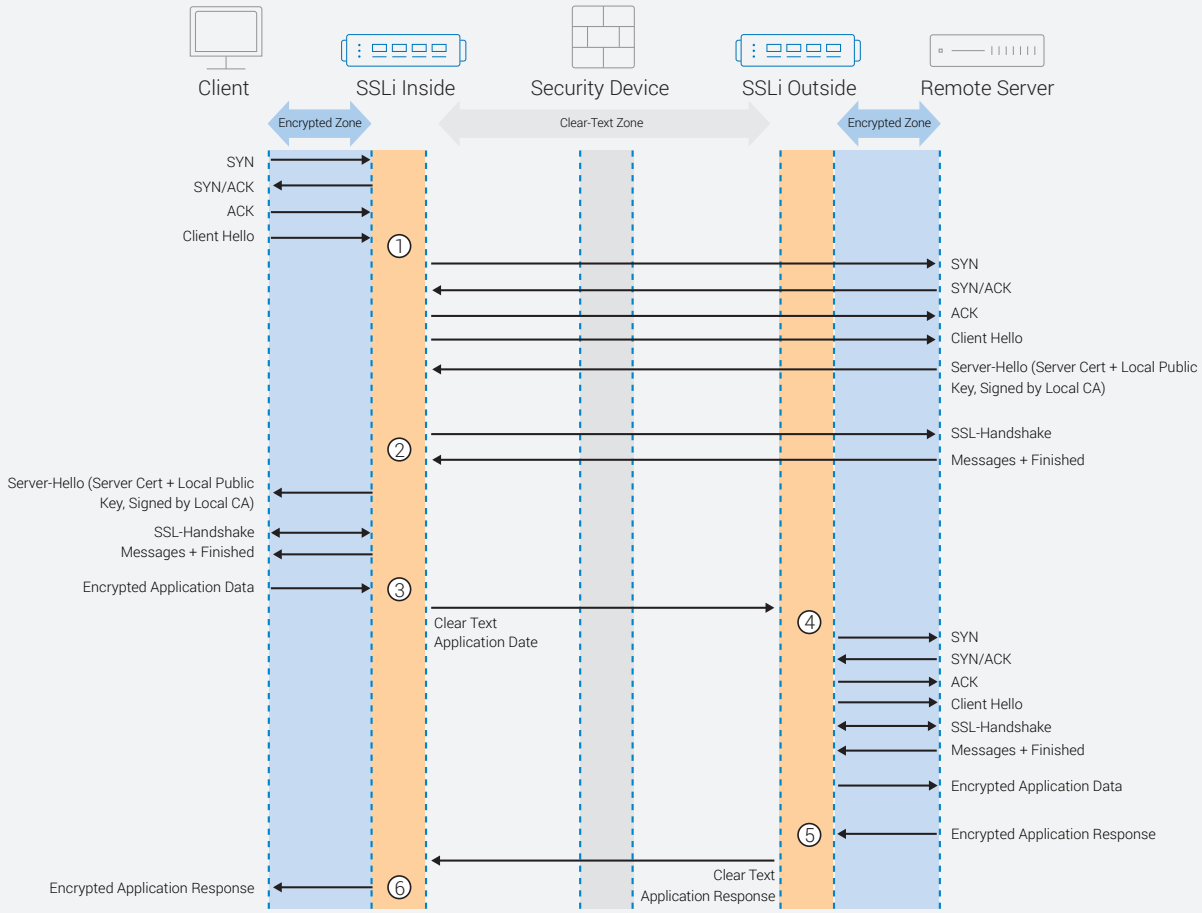


Figure 31: Detailed walkthrough of Thunder SSL Insight packet flow

APPENDIX D – DESIGN AND CONFIGURATION FOR ADDING A DMZ

A DMZ can be added to the main design. The basic concepts are the same except that new wildcard VIPs are configured on the Inside and Outside Thunder SSLi devices. These new wildcard VIPs will intercept incoming traffic from the external network and send it either to the DMZ or to the internal network.

In general, the configuration on the DMZ Thunder SSLi devices will be similar to what was configured on the Thunder SSLi Outside devices. In essence, there will be one wildcard VIP listening for traffic entering from the firewalls on both VLANs with the required command **use-rcv-hop-for-resp**. Optionally, additional wildcard VIPs can be configured to intercept traffic moving from the DMZ to either the external or internal networks.

Attention should be paid to the ACL definitions, as traffic now must be classified based on the destination. In particular, the ACL on the Inside Thunder SSLi device is modified and SSLi chooses the appropriate next-hop address.

Firewall policies should be updated in accordance with enterprise security policies.

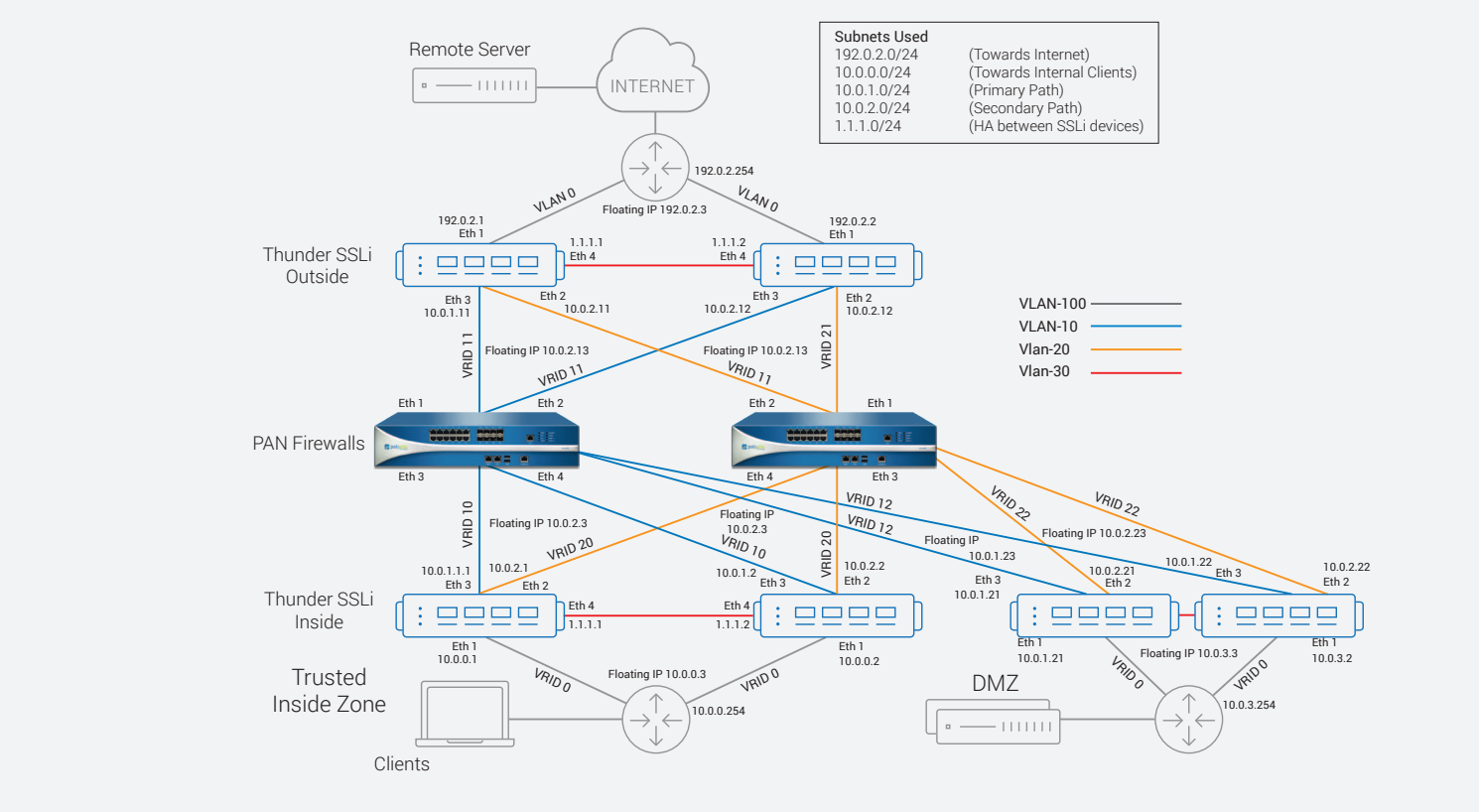


Figure 32: A10 Thunder SSL Insight and PAN firewalls with a DMZ

The following shows a sample configuration of the Primary Inside, Outside and DMZ devices

COMPLETE CONFIGURATION FILES FOR PRIMARY THUNDER SSLI INSIDE, OUTSIDE AND DMZ DEVICES

Thunder SSLi Inside 1

```
!
vrrp-a common
  device-id 1
  set-id 1
  enable
!
vlan 100
  untagged ethernet 1
  router-interface ve 100
!
vlan 10
  untagged ethernet 2
  router-interface ve 10
!
vlan 20
  untagged ethernet 3
  router-interface ve 20
!
vlan 30
  untagged ethernet 4
  router-interface ve 30
!
access-list 100 deny ip any 10.0.3.0 0.0.0.255
vlan 100
access-list 100 permit ip any any vlan 100
access-list 105 permit ip any 10.0.3.0
0.0.0.255 vlan 100
access-list 106 permit ip any any vlan 10
access-list 106 permit ip any any vlan 20
!
!
!
interface ve 100
  name INSIDE
  ip address 10.0.0.1 255.255.255.0
  ip allow-promiscuous-vip
!
interface ve 10
  name PATH1
  ip address 10.0.1.1 255.255.255.0
  ip allow-promiscuous-vip
!
```

Thunder SSLi Outside 1

```
!
vrrp-a common
  device-id 1
  set-id 2
  enable
!
vlan 100
  untagged ethernet 1
  router-interface ve 100
!
vlan 10
  untagged ethernet 2
  router-interface ve 10
!
vlan 20
  untagged ethernet 3
  router-interface ve 20
!
vlan 30
  untagged ethernet 4
  router-interface ve 30
!
access-list 100 deny ip any 10.0.1.0 /24
access-list 100 deny ip any 10.0.2.0 /24
access-list 100 permit ip any any vlan 10
access-list 100 permit ip any any vlan 20
access-list 105 permit ip any 10.0.3.0
0.0.0.255 vlan 100
access-list 106 deny ip any 10.0.3.0 0.0.0.255
vlan 100
access-list 106 permit ip any any vlan 100
!
interface ve 100
  name OUTSIDE
  ip address 192.0.2.1 255.255.255.0
  ip allow-promiscuous-vip
!
interface ve 10
  name PATH1
    ip address 10.0.1.11 255.255.255.0
  ip allow-promiscuous-vip
!
```

```
interface ve 20
  name PATH2
  ip address 10.0.2.1 255.255.255.0
  ip allow-promiscuous-vip
!
interface ve 30
  name SYNC-PATH
  ip address 1.1.1.1 255.255.255.0
!
ip route 192.0.2.0 /24 10.0.1.13
ip route 10.0.3.0 /24 10.0.1.23
!
!
vrrp-a interface ethernet 4
  vlan 30
!
vrrp-a vrid 0
  floating-ip 10.0.0.3
  blade-parameters
    priority 200
!
vrrp-a vrid 10
  floating-ip 10.0.1.3
  blade-parameters
    priority 200
!
vrrp-a vrid 20
  floating-ip 10.0.2.3
  blade-parameters
    priority 200
!
!
slb server PATH1 10.0.1.13
  port 0 tcp
    health-check-disable
  port 0 udp
   health-check-disable
  port 8080 tcp
    health-check-disable
!
slb server PATH2 10.0.2.13
  port 0 tcp
    health-check-disable
  port 0 udp
    health-check-disable
  port 8080 tcp
    health-check-disable
!
```

```
interface ve 20
  name PATH2
  ip address 10.0.2.11 255.255.255.0
  ip allow-promiscuous-vip
!
interface ve 30
  name SYNC-PATH
  ip address 1.1.1.1 255.255.255.0
!
ip route 10.0.0.0 /24 10.0.1.3
ip route 10.0.3.0 /16 10.0.1.23
!
!
vrrp-a interface ethernet 4
  vlan 30
!
vrrp-a vrid 0
  floating-ip 192.0.2.3
  blade-parameters
    priority 200
!
vrrp-a vrid 11
  floating-ip 10.0.1.13
  blade-parameters
    priority 200
!
vrrp-a vrid 21
  floating-ip 10.0.2.13
  blade-parameters
    priority 200
!
slb template server-ssl SSLInsight_Server_Side
  forward-proxy-enable
  template cipher sr_cipher_template
!!
slb server GATEWAY 192.0.2.254
  port 0 tcp
    health-check-disable
  port 0 udp
    health-check-disable
  port 443 tcp
    health-check-disable
!
slb server PATH1_ToInside 10.0.1.3
  port 0 tcp
    health-check-disable
  port 0 udp
    health-check-disable
```

```
slb server PATH1_ToDMZ 10.0.1.23
  port 0 tcp
    health-check-disable
  port 0 udp
    health-check-disable
  port 8080 tcp
    health-check-disable
!
slb server PATH2_ToDMZ 10.0.2.23
  port 0 tcp
    health-check-disable
  port 0 udp
    health-check-disable
  port 8080 tcp
    health-check-disable
!
slb server Inside_GW 10.0.0.254
  port 0 tcp
    health-check-disable
  port 0 udp
    health-check-disable
  port 8080 tcp
    health-check-disable
!
slb service-group SSLi_INSIDE_UDP udp
  member PATH1 0
  member PATH2 0
!
slb service-group SSLi_INSIDE_TCP tcp
 member PATH1 0
  member PATH2 0
!
slb service-group SSLi_INSIDE_FP tcp
  member PATH1 8080
  member PATH2 8080
!
slb service-group SSLi_INSIDE_UDP_ToDMZ udp
 member PATH1_ToDMZ 0
 member PATH2_ToDMZ 0
!
slb service-group SSLi_INSIDE_TCP_ToDMZ tcp
 member PATH1_ToDMZ 0
 member PATH2_ToDMZ 0
!
slb service-group Inside_GW_UDP udp
 member Inside_GW 0
!
slb service-group Inside_GW_TCP tcp
!
slb server PATH2_ToInside 10.0.2.3
  port 0 tcp
    health-check-disable
  port 0 udp
    health-check-disable
!
slb server PATH1_ToDMZ 10.0.1.23
  port 0 tcp
    health-check-disable
  port 0 udp
    health-check-disable
!
slb server PATH2_ToDMZ 10.0.2.23
  port 0 tcp
    health-check-disable
  port 0 udp
    health-check-disable
!
slb service-group SSLi_OUTSIDE_TCP tcp
  member GATEWAY 0
!
slb service-group SSLi_OUTSIDE_UDP udp
  member GATEWAY 0
!
slb service-group SSLi_OUTSIDE_FP tcp
  member GATEWAY 443
!
slb service-group SSLi_OUTSIDE_ToINSIDE_UDP
udp
 member PATH1_ToInside 0
 member PATH2_ToInside 0
!
slb service-group SSLi_OUTSIDE_ToINSIDE_TCP
tcp
 member PATH1_ToInside 0
 member PATH2_ToInside 0
!
slb service-group SSLi_OUTSIDE_UDP_ToDMZ udp
 member PATH1_ToDMZ 0
 member PATH2_ToDMZ 0
!
slb service-group SSLi_OUTSIDE_TCP_ToDMZ tcp
 member PATH1_ToDMZ 0
 member PATH2_ToDMZ 0
!
!
slb virtual-server SSLi_EGRESS 0.0.0.0 acl 100
  port 0 tcp
```

```
 member Inside_GW 0
!
!
slb template client-ssl SSLInsight_Client_Side
  template cipher cl_cipher_template
  chain-cert SSLiChain
  forward-proxy-ca-cert SSLiCA
  forward-proxy-ca-key SSLiCA
  forward-proxy-enable
!
!
slb virtual-server SSLi_INGRESS 0.0.0.0 acl
100
  port 0 tcp
    name Inside1_in_to_out
    service-group SSLi_INSIDE_TCP
    no-dest-nat
  port 0 udp
    name Inside1_in_to_out_UDP
    service-group SSLi_INSIDE_UDP
   no-dest-nat
  port 0 others
    name Inside1_in_to_out_others
    service-group SSLi_INSIDE_UDP
    no-dest-nat
  port 443 https
    name Inside1_in_to_out_443
    service-group SSLi_INSIDE_FP
    template client-ssl SSLInsight_Client_Side
    no-dest-nat port-translation
!
slb virtual-server SSLi_ToDMZ 0.0.0.0 acl 105
  port 0 tcp
    name Inside1_in_to_DMZ_TCP
    service-group SSLi_INSIDE_TCP_ToDMZ
    no-dest-nat
  port 0 udp
    name Inside1_in_to_DMZ_UDP
    service-group SSLi_INSIDE_UDP_ToDMZ
    no-dest-nat
  port 0 others
    name Inside1_in_to_DMZ_UDP
    service-group SSLi_INSIDE_UDP_ToDMZ
    no-dest-nat
!
slb virtual-server SSLi_ToDMZ 0.0.0.0 acl 105
  port 0 tcp
    name Inside1_in_to_DMZ_TCP
    service-group SSLi_INSIDE_TCP_ToDMZ
    service-group SSLi_OUTSIDE_TCP
    use-rcv-hop-for-resp
   no-dest-nat
  port 0 udp
   service-group SSLi_OUTSIDE_UDP
   use-rcv-hop-for-resp
   no-dest-nat
  port 8080  http
    service-group SSLi_OUTSIDE_FP
    template server-ssl SSLInsight_Server_Side
    use-rcv-hop-for-resp
    no-dest-nat port-translation
!
slb virtual-server SSLi_ToDMZ 0.0.0.0 acl 105
  port 0 tcp
    name Outside1_in_to_DMZ_TCP
    service-group SSLi_OUTSIDE_TCP_ToDMZ
   no-dest-nat
  port 0 udp
    name Outside1_in_to_DMZ_UDP
    service-group SSLi_OUTSIDE_UDP_ToDMZ
    no-dest-nat
  port 0 others
    name Outside1_in_to_DMZ_UDP
    service-group SSLi_OUTSIDE_UDP_ToDMZ
    no-dest-nat
!
slb virtual-server SSLi_ToInsideGW 0.0.0.0 acl
106
  port 0 tcp
    name Outside_out_to_in_TCP
    service-group SSLi_OUTSIDE_ToINSIDE_TCP
    use-rcv-hop-for-resp
    no-dest-nat
 port 0 udp
    name Outside_out_to_in_UDP
    service-group SSLi_OUTSIDE_ToINSIDE_UDP
    use-rcv-hop-for-resp
    no-dest-nat
!
end
```

```
    no-dest-nat
  port 0 udp
    name Inside1_in_to_DMZ_UDP
    service-group SSLi_INSIDE_UDP_ToDMZ
    no-dest-nat
  port 0 others
    name Inside1_in_to_DMZ_UDP
    service-group SSLi_INSIDE_UDP_ToDMZ
    no-dest-nat
!
slb virtual-server SSLi_ToInsideGW 0.0.0.0 acl
106
  port 0 tcp
    name Inside_out_to_in_TCP
    service-group Inside_GW_TCP
    use-rcv-hop-for-resp
    no-dest-nat
 port 0 udp
    name Inside_out_to_in_UDP
    service-group Inside_GW_UDP
    use-rcv-hop-for-resp
    no-dest-nat
!
end
```

Thunder SSLi DMZ 1

```
!
vrrp-a common
  device-id 1
  set-id 3
  enable
!
vlan 100
  untagged ethernet 1
  router-interface ve 100
!
vlan 10
  untagged ethernet 2
  router-interface ve 10
!
vlan 20
  untagged ethernet 3
  router-interface ve 20
!
vlan 30
  untagged ethernet 4
  router-interface ve 30
!
access-list 100 deny ip any 10..0.1.0 /24
access-list 100 deny ip any 10.0.2.0 /24
access-list 100 permit ip any any vlan 10
access-list 100 permit ip any any vlan 20
access-list 105 permit ip any 10.0.3.0
0.0.0.255 vlan 100
access-list 106 deny ip any 10.0.3.0 0.0.0.255
vlan 100
access-list 106 permit ip any any vlan 100
!
!
interface ve 10
ip address 10.1.240.22 255.255.255.0
ip allow-promiscuous-vip
!
interface ve 20
ip address 10.1.250.22 255.255.255.0
ip allow-promiscuous-vip
!
interface ve 100
ip address 15.1.250.2 255.255.255.0
ip allow-promiscuous-vip
```

```
!
interface ve 30
ip address 99.1.1.1 255.255.255.0
!
ip route 20.1.1.0 /24 10.1.240.11
ip route 10.1.1.0 /24 10.1.240.1
!
!
vrrp-a interface ethernet 4
  vlan 30
!
vrrp-a vrid 0
  floating-ip 10.0.3.3
  blade-parameters
    priority 200
!
vrrp-a vrid 12
  floating-ip 10.0.1.23
  blade-parameters
    priority 200
!
vrrp-a vrid 22
  floating-ip 10.0.2.23
  blade-parameters
    priority 200
!
!
slb server DMZ-GW 10.0.3.254
  port 0 tcp
    health-check-disable
  port 0 udp
    health-check-disable
!
slb server PATH1_ToInside 10.0.1.3
  port 0 tcp
    health-check-disable
  port 0 udp
    health-check-disable
!
slb server PATH2_ToInside 10.0.2.3
  port 0 tcp
    health-check-disable
  port 0 udp
    health-check-disable
!
slb server PATH1_ToOutside 10.0.1.13
  port 0 tcp
    health-check-disable
  port 0 udp
    health-check-disable
!
slb server PATH2_ToOutside 10.0.2.13
  port 0 tcp
    health-check-disable
  port 0 udp
    health-check-disable
!
slb service-group SSLi_DMZ_TCP tcp
 member DMZ-GW 0
!
slb service-group SSLi_DMZ_UDP udp
 member DMZ-GW 0
!
slb service-group SSLi_ToINSIDE_UDP udp
  member PATH1_ToInside 0
  member PATH2_ToInside 0
!
slb service-group SSLi_ToINSIDE_TCP tcp
  member PATH1_ToInside 0
  member PATH2_ToInside 0
!
slb service-group SSLi_ToOUTSIDE_UDP udp
  member PATH1_ToOutside 0
  member PATH2_ToOutside 0
!
slb service-group SSLi_ToOUTSIDE_TCP tcp
  member PATH1_ToOutside 0
  member PATH2_ToOutside 0
!
!
slb virtual-server SSLi_ToDMZ 0.0.0.0 acl 100
  port 0 tcp
    name DMZ_TCP
    service-group SSLi_DMZ_TCP
    use-rcv-hop-for-resp
    no-dest-nat
  port 0 udp
    name DMZ_UDP
    service-group SSLi_DMZ_UDP
    use-rcv-hop-for-resp
    no-dest-nat
!
slb virtual-server SSLi_ToInside 0.0.0.0 acl
105
  port 0 tcp
    name Outside_out_to_in_TCP
    service-group SSLi_ToOUTSIDE_TCP
```

```
    use-rcv-hop-for-resp
    no-dest-nat
 port 0 udp
    name Outside_out_to_in_UDP
    service-group SSLi_ToOUTSIDE_UDP
    use-rcv-hop-for-resp
    no-dest-nat
!
slb virtual-server SSLi_ToOutside 0.0.0.0 acl
106
  port 0 tcp
    name Outside_out_to_in_TCP
    service-group SSLi_ToINSIDE_TCP
    use-rcv-hop-for-resp
    no-dest-nat
 port 0 udp
    name Outside_out_to_in_UDP
    service-group SSLi_ToINSIDE_UDP
    use-rcv-hop-for-resp
    no-dest-nat
!
end
```

APPENDIX E – A10 URL CLASSIFICATION SERVICE

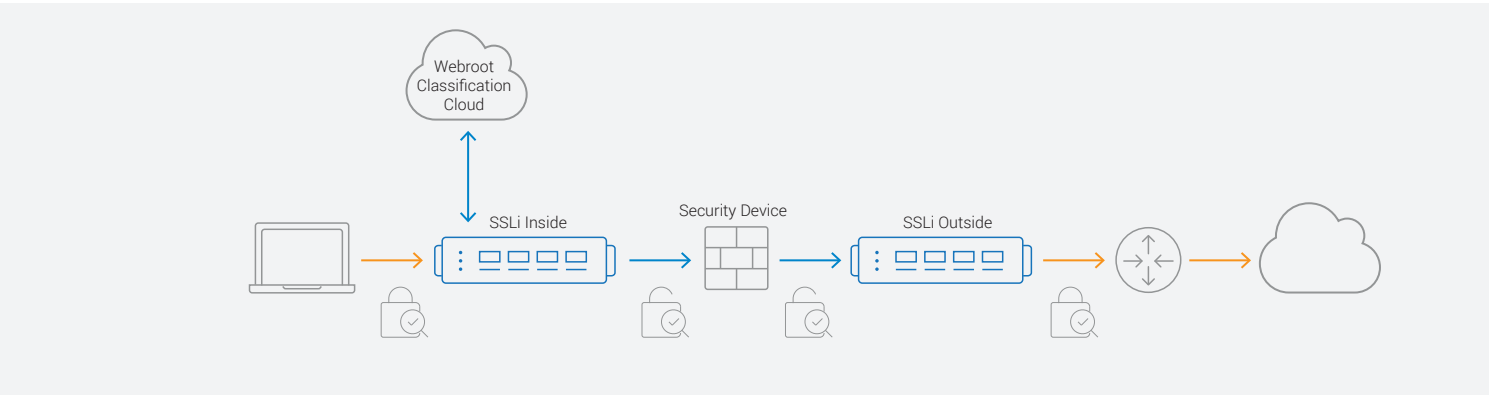


Figure 33: A10 Networks and Webroot architecture

SSL Insight technology includes an optional, paid subscription service called A10 URL Classification Service. This service allows customers to granularly control which types of SSL traffic to decrypt and which types to forward without inspection. Thunder SSLi/ Thunder CFW customers can analyze and secure SSL traffic while bypassing communications to sensitive sites such as banking, healthcare and other applications.

When a client browser sends a request to a URL, the Thunder SSLi device checks the category of the URL.

- If the category of the URL is allowed by the configuration, the Thunder SSLi Inside device leaves the data encrypted and sends it to the Thunder SSLi Outside device, which sends the encrypted data to the server.
- If the category of the URL is not allowed by the configuration, the Thunder SSLi Inside device decrypts the traffic and sends it to the traffic inspection device.

INSTALLATION REQUIREMENTS

- Must have an A10 URL Classification subscription with each Thunder SSLi device license (contact your Regional Sales Director for pricing).
- Inside partition of the Thunder SSLi device must have access to the Internet for database server access in the cloud.
- DNS configuration is required.

To install the URL classification feature, you must have a URL Classification Service token license sent from the A10 Global License Manager (GLM). Once received, initiate the following command within the CLI:

import web-category-license “license token name”

Once the license has been imported, initiate a web-category enable command. This feature enables the Thunder SSLi device to communicate with the web category database server and download the URL classification database. When the download is complete and if the import is successfully initiated, there will be a “Done” confirmation from the CLI; otherwise, an error message will appear.

```
import web-category-license license use-mgmt-port
scp://example@10.100.2.20/home/jsmith/webroot_license.json
```

Done (This brief message confirms successful import of the license.)

If a failure occurs, ACOS will display an error message similar to the following:

```
import web-category-license license use-mgmt-port

scp://example@10.100.2.20/home/jsmith/webroot_license.json
```

Communication with license server failed (This message indicates failed import.)

***NOTE**: The URL classification database will download from the data interface by default. There is an option to configure from the management interface but it is not recommended.*

To enable the A10 URL Classification feature, you must have the “forward-proxy-bypass web-category” configuration within the Client SSL template.

Here is a sample configuration:

```
slb template client-ssl SSLInsight_Client_Side
   forward-proxy-enable
   forward-proxy-bypass web-category financial-services
   forward-proxy-bypass web-category business-and-economy
   forward-proxy-bypass web-category health-and-medicine
```

APPENDIX F – A10 RECOMMENDED BEST PRACTICES

When SSL Insight is deployed in a network, it will encounter traffic of different kinds, originated from different devices and applications, using different protocols. To cope with any hidden surprises and out-of-the-ordinary situations, A10 Networks recommends the use of some additional configurations for the Thunder SSLi products. Some of these configurations are listed below, separated into "SSLi Inside" and "SSLi Outside" sections for easy understanding and identification of where they should be applied.

SSLI INSIDE

On the Thunder SSLi Inside device, the following commands should be applied for the reasons stated below.

1. Object groups

Object groups simplify the management of access lists and IP addresses/domains that are included in the access lists. These should be used wherever necessary so that configurations can be streamlined. Object groups are created as follows:

```
object-group network SSLI_bypass
   description internal_client_bypass
   host 192.0.2.10
   host 192.0.2.18
```

Once created, this object group can be used in the configuration as follows:

```
access-list 100 deny ip object-group SSLI_bypass any vlan 100
access-list 100 permit ip host any any vlan 100
```

In this example, traffic from hosts with IP addresses 192.0.2.10 and 192.0.2.18 will bypass the decryption process and will be forwarded through to the default gateway.

2. HTTP template for bypassing non-HTTP traffic

By default, the ACOS device will drop non-HTTP requests that are sent to an HTTP/HTTPS port. This can include applications using proprietary video or voice applications over HTTP. To avoid dropping this traffic, A10 recommends the use of an HTTP template with the **non-http-bypass** command enabled, which will redirect non-HTTP traffic to a specific service group. This feature can be configured as follows:

```
slb template http non-http-bypass
   non-http-bypass service-group SSLi_INSIDE_FP
```

SSLi_INSIDE_FP is the service group used to forward traffic through the security device onto the SSLi Outside device, over a different TCP port. Once created, the template should be bound to the **virtual port 443 https** under the virtual server on the SSLi Inside device.

3. Handling traffic using the Google QUIC Protocol

Quick UDP Internet Connections (QUIC) is a proprietary secure protocol developed by Google Inc. It is extensively used by the Chrome web browser while accessing or using Google Apps. The protocol uses UDP port 443. Due to the proprietary nature of QUIC, Thunder SSLi cannot decrypt QUIC encrypted sessions. However, Chrome reverts to normal SSL encryption on TCP port 443, if QUIC fails to work, e.g., if QUIC is blocked by a firewall. Since Google Chrome is one of the most commonly used web browsers, A10 recommends a workaround configuration. An inbound access list should be configured to block UDP port 443, but permit everything else, so that Chrome is forced to revert to using TCP port 443. This access list should then be bound to the inbound interface on the SSLi Inside device.

```
access-list 110 deny udp any any eq 443
access-list 110 permit ip any any
interface ve 100
   name INSIDE
   enable
   access-list 110 in
   ip address 10.0.0.1 255.255.255.0
   ip allow-promiscuous-vip
```

All the inbound traffic on the interface ve 100 will now be matched against the access list 110.

SSLI OUTSIDE

On the Thunder SSLi Outside device, the following commands should be applied for the reasons stated below.

1. Object Groups

Object groups should be used in the same way as on the SSLi Inside device to simplify management of access lists.

2. HTTP template for bypassing non-HTTP traffic

An HTTP template should be configured for bypassing non-HTTP traffic in the same way as on the SSLi Inside device. The only difference would be the application of the HTTP template. On the SSLi Outside device, this template will be directing traffic to the service group responsible for forwarding the re-encrypted traffic to the gateway, i.e., **SSLi_OUTSIDE_FP**. The template is created as follows:

```
slb template http non-http-bypass
   non-http-bypass service-group SSLi_OUTSIDE_FP
```

Once created, the template should be bound to the **virtual port 8080 ttp** under the virtual server.

3. Template for ignoring maximum segment lifetime (MSL)

TCP sockets can sometimes be stuck in a time-wait state after session termination in the certificate fetching process. This can cause timeouts. To immediately reuse TCP sockets after session termination, without waiting for the MSL time to expire and to avoid timeouts, we need to add the following virtual port template to our configuration:

```
slb template virtual-port ignore-msl
   ignore-tcp-msl
```

Once created, this template should be bound to the wildcard **virtual port 0 tcp** under the virtual server.

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) provides Reliable Security Always™ through a range of high-performance solutions that enable intelligent automation with deep machine learning to ensure business critical applications are protected, reliable and always available. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.

For more information, visit: a10networks.com or tweet @a10Networks

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-DG-16120-EN-03 AUG 2018