

DEPLOYMENT GUIDE

SSL INSIGHT AND CISCO FIREPOWER DEPLOYMENT GUIDE



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. This guide provides step-by-step instructions for the deployment of A10 Networks® Thunder® SSL Insight® (SSLi®) with Cisco ASA with FirePOWER. The A10 SSL Insight technology helps eliminate SSL blind spots in corporate defenses and enables security devices to inspect encrypted traffic, not just cleartext. In this guide's use case, the decryption and inspection solution is based on a Layer 2 environment and can be deployed with a single Thunder SSLi device using Application Delivery Partitions (ADPs) to create multiple, logical Thunder SSLi instances.

TALK
WITH A10

.....
CONTACT US

a10networks.com/contact

TABLE OF CONTENTS

<i>OVERVIEW</i>	2
<i>SSL INSIGHT TECHNOLOGY</i>	5
<i>DEPLOYMENT REQUIREMENTS</i>	6
<i>DEPLOYMENT MODE</i>	6
<i>ACCESSING A10 THUNDER SSLI</i>	7
<i>THUNDER SSLI CONFIGURATION USING APPCENTRIC TEMPLATES</i>	8
<i>Wizard - Topology</i>	8
<i>Wizard - Decryption</i>	9
<i>Wizard - Re-Encryption</i>	10
<i>Wizard - Bypass Configuration</i>	11
<i>THUNDER SSLI CONFIGURATION USING THE CLI</i>	15
<i>Creating Partitions</i>	15
<i>Interface and VLAN Configuration</i>	15
<i>Configuring Servers, Service Groups, a Virtual Server and Client SSL Template on the Inside Thunder SSLi Instance</i>	17
<i>Configuring Servers, Service Groups, a Virtual Server and Client SSL Template on the Outside Thunder SSLi Instance</i>	20
<i>CISCO FIREPOWER CONFIGURATION</i>	22
<i>Accessing Cisco FirePOWER module</i>	22
<i>Adding a Device</i>	22
<i>Configuring Interfaces and Security Zones</i>	23
<i>Configuring the Access Control Policy</i>	23
<i>Configuring the Inspection Policy</i>	24
<i>Configuring the Network Analysis Policy</i>	25
<i>SUMMARY</i>	26
<i>APPENDIX A</i>	27
<i>A10 Shared Partition Configuration</i>	27
<i>A10 Inside Partition Configuration</i>	27
<i>A10 Outside Partition Configuration</i>	28
<i>APPENDIX B</i>	30
<i>SSL Insight Two-Device deployment</i>	30

TABLE OF CONTENTS

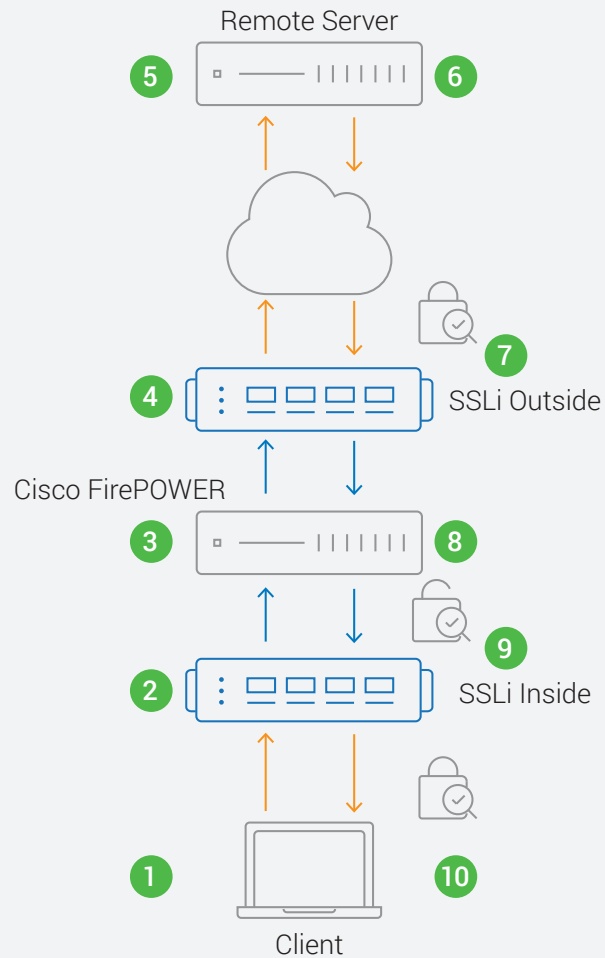
APPENDIX C	30
<i>Third-Party Web Proxy</i>	30
<i>Transparent Proxy Outside the SSLi Sandwich (Decrypt Zone)</i>	31
<i>Transparent Proxy Inside the SSLi Sandwich (Decrypt Zone)</i>	31
<i>Explicit Proxy Outside the SSLi Sandwich (Decrypt Zone)</i>	31
<i>Explicit Proxy Inside the SSLi Sandwich (Decrypt Zone)</i>	32
APPENDIX D	32
<i>A10 URL Classification Service</i>	32
<i>ABOUT A10 NETWORKS</i>	33

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.

SSL INSIGHT TECHNOLOGY

This guide describes the configuration of SSL Insight using a single Thunder SSLi device, with one partition decrypting SSL traffic and a second partition re-encrypting traffic. The partition that decrypts outbound SSL traffic is referred to as the “Inside Thunder SSLi Instance.” The partition that encrypts outbound SSL traffic is referred to as the “Outside Thunder SSLi Instance.” Here’s how SSL Insight works:



1. SSL/TLS-encrypted traffic (such as HTTPS) originates from an internal client.
2. Traffic is intercepted and decrypted by the Inside Thunder SSLi Instance and the cleartext content is forwarded to the Cisco FirePOWER device.
3. Cisco FirePOWER inspects the data in cleartext and forwards it to the gateway router.
4. The Outside Thunder SSLi Instance 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.
 - c. Outbound traffic is forwarded to the default gateway.
5. The destination server receives the encrypted request.
6. The destination server returns the encrypted response.

7. The Outside Thunder SSLi Instance decrypts the response and forwards the cleartext traffic to the Cisco FirePOWER. At this point:
 - a. The session is matched and the source MAC address is retrieved.
 - b. Traffic is returned via Cisco FirePOWER with the retrieved MAC address as destination MAC in L2 header.
8. The response traffic in cleartext is forwarded to the Cisco FirePOWER device for further inspection. If Thunder SSLi is load-balancing multiple FirePOWER devices, it will forward traffic to the same device that inspected the outbound request.
9. The Inside Thunder SSLi Instance receives the cleartext traffic from Cisco FirePOWER, encrypts it and returns it to the client.
10. The client receives the encrypted response.

DEPLOYMENT REQUIREMENTS

To deploy the SSL Insight solution with Cisco FirePOWER, the following are required:

- A10 Networks Advanced Core Operating System (ACOS®) 4.1.0 P4 or higher (supported with hardware-based Thunder SSLi devices)
- CA Certificate for SSLi and Certificate chain
- Cisco FirePOWER 4.5.1.1 or higher (supported with hardware-based Cisco FirePOWER devices)
- Cisco FirePOWER Sensor
- Cisco FirePOWER Defense Management Center

Note: This solution is deployed in Layer 2 mode.

DEPLOYMENT MODE

A10 recommends deploying the SSL Insight feature in a single-device topology. With ADPs, a single Thunder SSLi device may be partitioned with “Inside” and “Outside” partitions. The A10 Thunder SSLi device can support a minimum of 32 ADPs and a maximum of 1024 ADPs per device, depending on model.

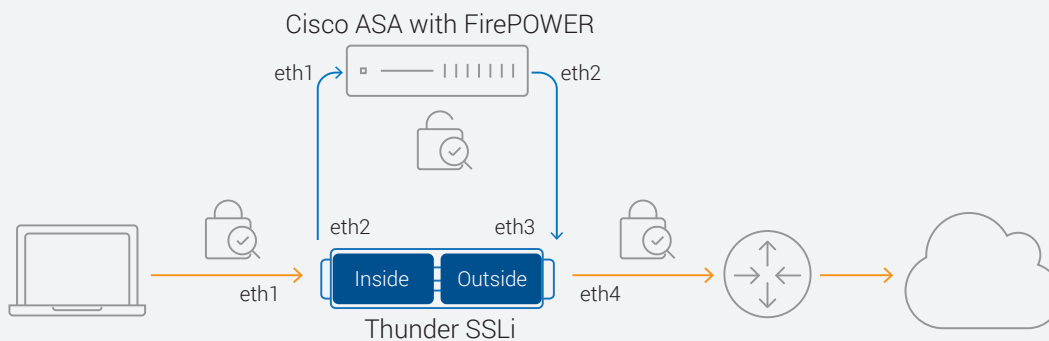


Figure 1: SSL Insight Single Device and Cisco ASA with FirePOWER deployment

For this deployment guide, the Thunder SSLi device is deployed in L2 (Bump in the Wire) mode. Interfaces on Thunder SSLi are connected as follows:

- A client Microsoft® Windows® machine is directly connected to the SSLi device via the interface Ethernet 1. Encrypted traffic from the client machine is received on this interface.
- Interface Ethernet 2 of the SSLi device is connected to the Ethernet 1 interface of the Cisco FirePOWER device. The client traffic, once decrypted, will be sent out to the Cisco FirePOWER via this interface in cleartext.
- Interface Ethernet 3 of the SSLi device is connected to the Ethernet 2 interface of the Cisco FirePOWER device. The cleartext traffic, at this point, will be inspected by Cisco FirePOWER and be received by the SSLi device via this interface.
- The fourth and final interface, Ethernet 4, is connected to the Gateway Router. Traffic will be re-encrypted and sent out via this interface as SSL traffic to the gateway.
- The Thunder SSLi interfaces, Ethernet 1 and 2, are part of the Inside partition while Ethernet 3 and 4 are part of the Outside partition.
- The Cisco FirePOWER interface Ethernet 1 is in the internal zone while the interface Ethernet 2 is in the external zone.

Deployment considerations:

- Appliance-based sensor deployment can support Layer 2 transparent mode only.
- Cisco FireSIGHT Management Center is required to manage the Cisco Sensors. Each Cisco FireSIGHT Management center can support up to 25 sensors.

This guide only provides a Cisco interface configuration as every packet inspection solution has different policies.

ACCESSING A10 THUNDER SSLI

Thunder SSLi can be accessed either from a Command Line Interface (CLI) or a Graphical User Interface (GUI):

- **CLI**

Text-based interface in which you type commands on a command line. You can access the CLI directly through the serial console or the network using either of the following protocols:

- a. Secure protocol – Secure Shell (SSH) version 2
- b. Unsecure protocol – Telnet (if enabled; not recommended)

- **AppCentric Templates (ACT)**

Web-based interface that provides you with access to template-based configurations of the Thunder SSLi device. You can access the GUI using the following protocol:

- c. Secure protocol – Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)

Note: HTTP requests are redirected to HTTPS by default on the Thunder SSLi device.

Default username: admin

Default password: a10

Default IP address of the device: 172.31.31.31

Note: Thunder SSLi can also be configured using the standard GUI that can be accessed by entering the management IP address in a Web browser's address bar (e.g., <https://172.31.31.31>) and using the default access credentials mentioned above.

Note: The AppCentric Templates can be accessed using the management IP address of the device followed by **/templates** (e.g., <https://172.31.31.31/templates>). Please note that without the **/templates** designation, the GUI will be accessed rather than the ACT.

Note: The first configuration to consider is to change the management IP address for CLI and ACT access. If you are using two separate devices to deploy SSL Insight, make sure that both systems are configured with a separate management IP address.

THUNDER SSLI CONFIGURATION USING APPCENTRIC TEMPLATES

This section is only valid for a single-device SSLi deployment; if you are deploying two devices – one to decrypt SSL traffic and a second to encrypt SSL traffic— you may skip this section and refer to Appendix B for details on the two-device deployment.

When deploying SSLi with a single device, please keep in mind the number of interfaces allocated within the platform. The number of interfaces available is limited; a single deployment with one security device will typically require four interfaces and every additional device will require a set of two interfaces each on Thunder SSLi (multiple security devices connected to a single Thunder SSLi device).

There are three main sections in the AppCentric Templates:

1. Wizard

The wizard provides users with a flow-based configuration of the SSLi device.

2. Dashboard

The dashboard gives users a view of different statistics related to the current state of the system, including CPU and memory usage, connection rate, traffic rate and device information, which includes information about the installed hardware.

3. Configuration

This section provides users with the current configuration of the device as well as access to some advanced options.

WIZARD - TOPOLOGY

Basic configuration of the SSLi device will be done in the **Wizard** section. The **Topology** is the first step in the configuration of an SSLi device using the AppCentric Templates. In this step, you will choose the network and deployment topology to use for SSL Insight solution based on the current deployment.

1. Navigate to **Wizard > Topology** and choose the topology you will be working with. In this example, **L2, Single Path topology** (default option) is selected. Click **NEXT**.

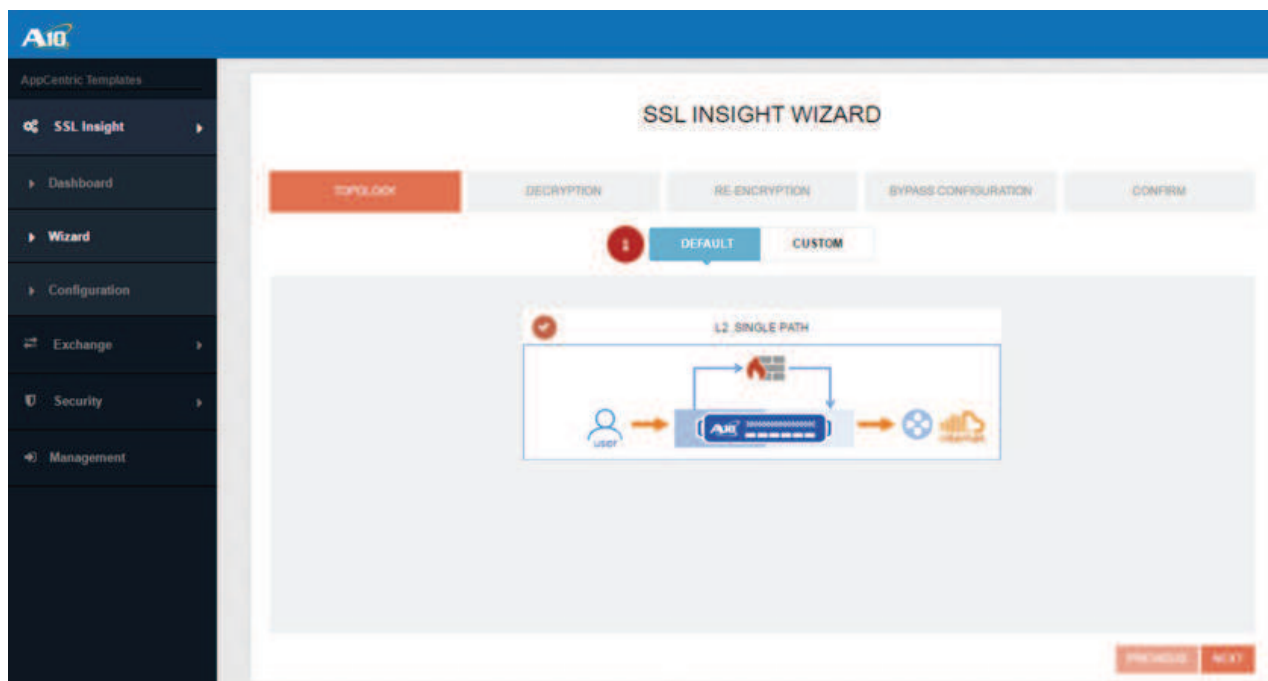


Figure 2: Wizard - Topology Configuration

Note: Thunder SSLi supports a number of different topologies. The topologies can be viewed and chosen from the Custom tab at the Topology choice step of the Wizard menu. For details on multi-device deployments, refer to Appendix B.

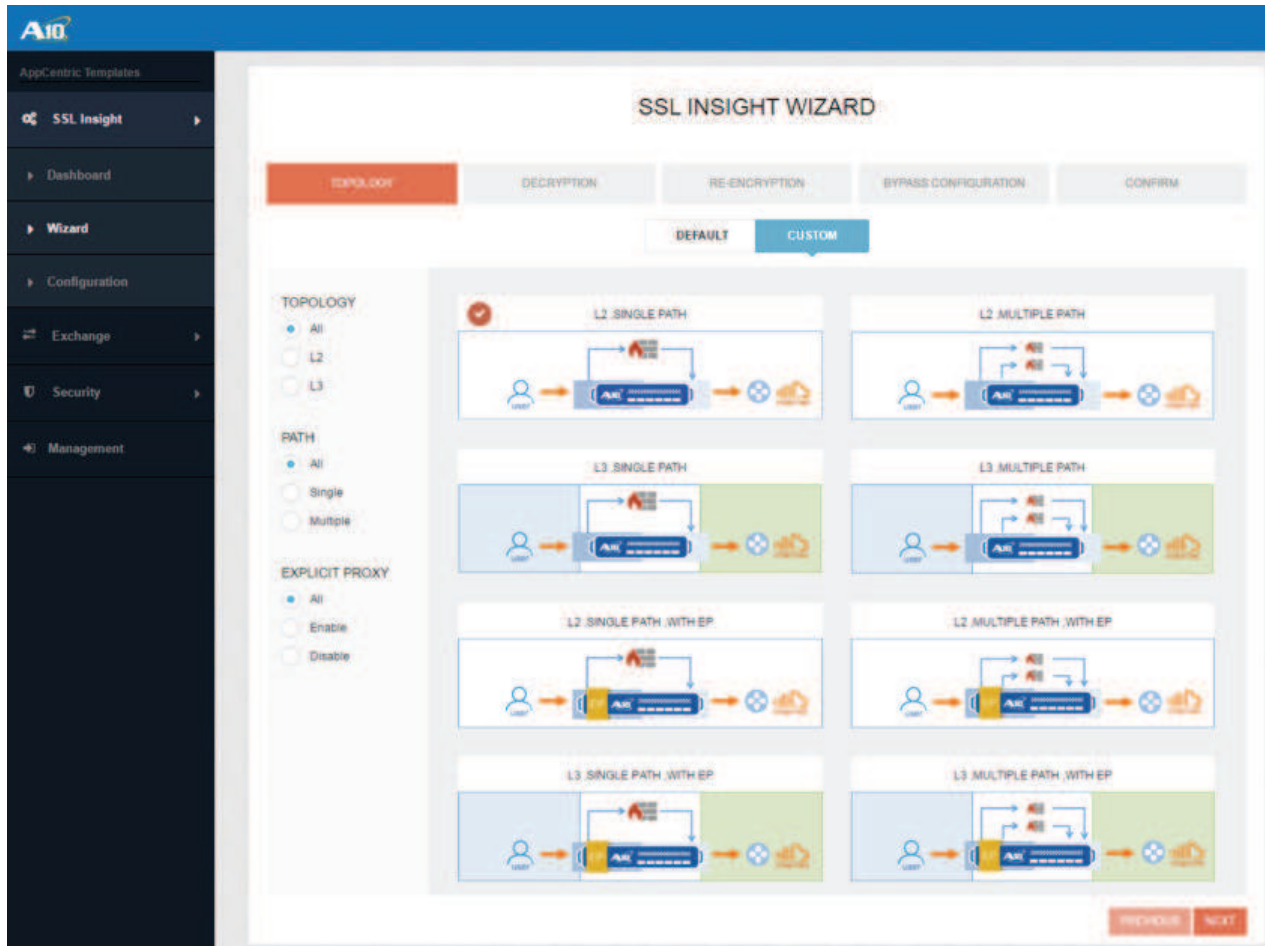


Figure 3: Selection of Custom Topology

WIZARD - DECRYPTION

The **Decryption** step deals with the SSLi Inside properties. In this step, we do the following:

2. Select an Ingress Interface (e.g., Ethernet 1). This is the interface that receives encrypted (SSL) traffic from the internal client.
3. Assign an IP address to the group of two interfaces in the SSLi Inside. (13.0.0.114 / 16)
4. Select **SSLi_Test** on SSL Certificate and Key. This is a self-signed SSL certificate and key for testing purposes.

SSL INSIGHT WIZARD

TOPOLOGY | **DECRYPTION** | RE-ENCRYPTION | BYPASS CONFIGURATION | CONFIRM

Ingress Interface All: ETHERNET 1 (2)

IP Address & Mask: 13.0.0.114 /16 (3)

SSL Certificate & Key: SSL_Test (4)

OutBound to Security Device: ETHERNET 2 (5)

DECRYPTION

USER → [AVG] → [Gateway Router] → [Internet]

L2_SINGLE PATH

PREVIOUS | NEXT

Figure 4: Wizard - Decryption

Note: If you already have a CA certificate (and key) prepared, you can import them on Thunder SSLi. Please see the detailed step here.


5. Select an interface on Outbound to Security Device, where the decrypted traffic is sent out toward the security device. In this example, Ethernet 2 is the outbound interface on the decryption side (SSLi Inside).

WIZARD - RE-ENCRYPTION

The re-encryption step deals with the SSLi Outside properties. In this step, we do the following:

6. Select an interface on Inbound from Security Device, where the inspected traffic is received from the security device. In this example, it's Ethernet 3.
7. Assign an IP address to the group of two interfaces in the SSLi Outside. In this example, 13.0.0.115 / 16.
8. Select an Egress Interface. This interface sends out the re-encrypted (SSL) traffic toward the Internet via the gateway router. In this example, Egress interface Ethernet 4.
9. Specify the IP address (e.g., 13.0.0.100) of the default gateway.

TOPOLOGY CONFIGURATION

TOPOLOGY	DECRYPTION	RE-ENCRYPTION	BYPASS CONFIGURATION	CONFIRM
Inbound from Security Device	ETHERNET 3	6	 <p>L2_SINGLE_PATH</p>	
IP Address & Mask	13.0.0.115 /16	7		
Egress Interface	ETHERNET 4	8		
Default Gateway	13.0.0.100	9		








PREVIOUS NEXT

Figure 5: Wizard - Re-Encryption

WIZARD - BYPASS CONFIGURATION

The Bypass Configuration is optional but important for SSL Insight. While you strengthen the security solution using SSL Insight, you need to make sure to protect – in other words not to decrypt/inspect – users' privacy information such as banking and healthcare data. Any traffic destined to the websites/IPs marked for the Bypass List will not be decrypted and inspected through SSL Insight.

TOPOLOGY CONFIGURATION

TOPOLOGY	DECRYPTION	RE-ENCRYPTION	BYPASS CONFIGURATION	CONFIRM
Bypass Category List	<input type="checkbox"/> 0 Categories Bypassed	 	 <p>L2_SINGLE_PATH</p>	
Bypass Domain List	<input type="checkbox"/> 0 Domains Bypassed	 		
Bypass IP List	<input type="checkbox"/> 0 IPs Bypassed	 		

PREVIOUS NEXT

Figure 6: Wizard - Bypass Configuration

The Bypass Configuration provides following three types of bypass list:

BYPASS CATEGORY LIST

The Bypass Category List is used to select website categories that you don't want to decrypt using SSL Insight. For example, if you select a category "financial-services," all websites under the category will be bypassed and will not be inspected through SSL Insight. By default, the "financial-services" and "health-and-medicine" options are selected. If required, the selected options can be removed from the right side-bar menu.

Note: This is subject to a URL Classification Service and the license key is required to activate the function.



Figure 7: Bypass Category List

BYPASS DOMAIN LIST

The Bypass Domain List is used to select certain words or phrases of website domains/URLs. If these words or phrases are contained in the URL, the traffic destined to the website/URL will be bypassed. For example, if a word "bank" is added to the Bypass Domain List, any traffic from websites containing "bank" in its URL, such as *bankofamerica.com* and *usbank.com*, will be bypassed and will not be inspected through SSL Insight. The **Add Default** button can be used to add a pre-defined list of 16 domains, commonly bypassed by users, to the list of bypassed domains. The list, once added, can be edited on the right side-bar menu.

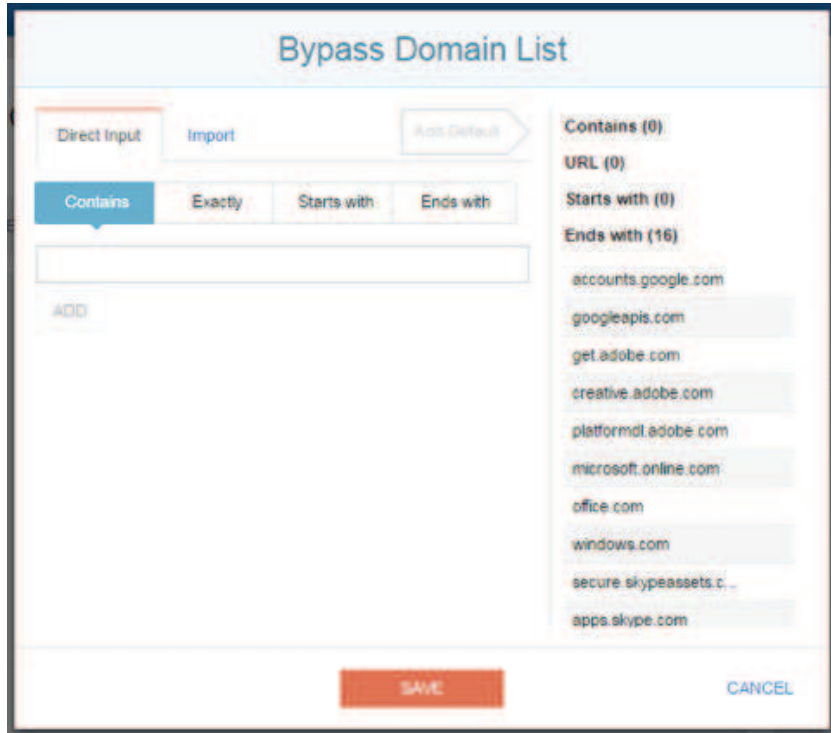


Figure 8: Bypass Domain List

BYPASS IP LIST

The Bypass IP List option is used to select source or destination IP addresses, based on which bypassing can occur. These IP addresses can either be specific host addresses or can be network addresses.

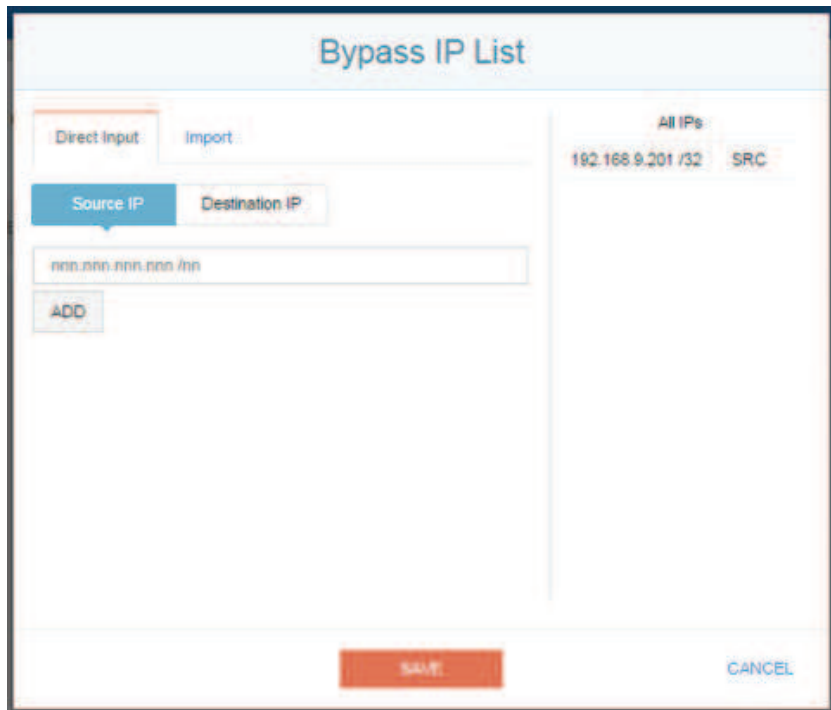


Figure 9: Bypass IP List

WIZARD - CONFIRM

10. On the Confirm tab, you can review a summary of the SSL Insight configuration properties executed so far. You can edit the configuration by clicking **PREVIOUS** or selecting the appropriate tab. If the configuration is confirmed and correct, click **FINISH** to finalize the SSL Insight topology configuration. This action opens a new window showing the actual CLI-based configuration.

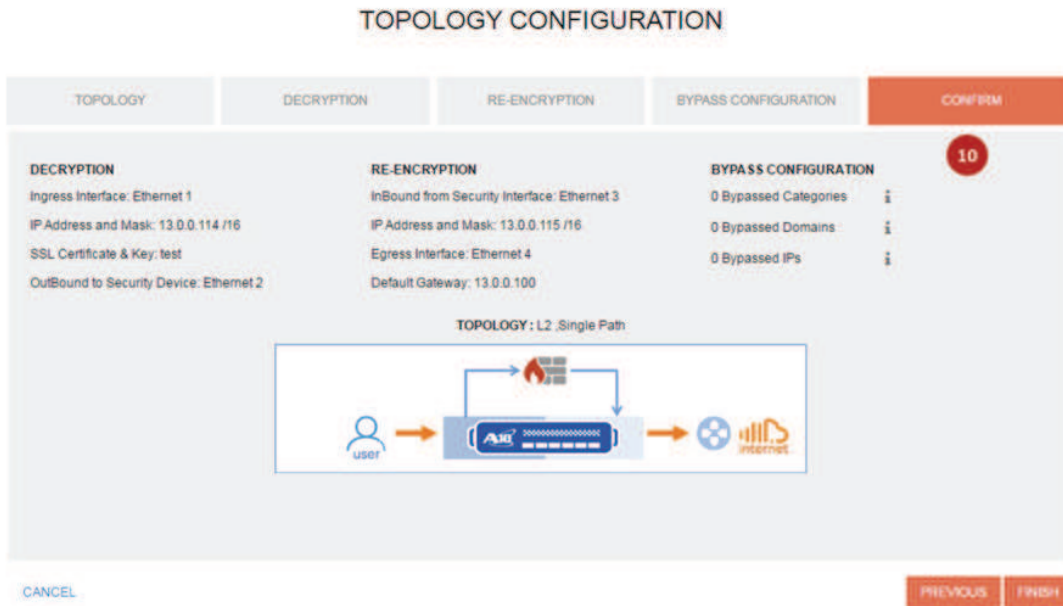


Figure 10: Wizard - Confirm

11. You can either click **APPLY** to activate the setting on the Thunder SSLi device, or you can click **COPY** to configure the SSLi setting manually through the CLI.



Figure 11: Wizard - Confirm

Once it's applied, you will be redirected to the SSL Configuration Template page where you can review the current configuration applied to the Thunder SSLi device.

Note: For details on URL Classification service licensing and functionality, as well as CLI configuration, refer to Appendix D.

THUNDER SSLI CONFIGURATION USING THE CLI

CREATING PARTITIONS

This section is only valid for a single-device SSLi deployment; if you are deploying two devices — one to decrypt SSL traffic and a second to encrypt SSL traffic — you may skip this section and refer to Appendix B for details on the two-device deployment. When using a single-device deployment, please keep in mind the number of interfaces allocated within the platform as its capacity is limited.

First step in the configuration of a Thunder SSLi device is to create partitions.

*Note: When configuring using the AppCentric Templates, the SSLi partitions will be given default names as **ssl_i_in** and **ssl_i_out**. For simplicity, we use the words *Inside* and *Outside* to refer to these partitions.*

Partitions are made using the CLI as follows:

```
partition Inside id 1
!
partition Outside id 2
```

To switch from one partition to another, the following commands can be used:

```
active-partition Inside
active-partition Outside
active-partition Shared
```

Once the active partition is changed, the prompt is changed and shown as follows:

Current active partition: Inside

```
SSLi [Inside] (config) #
```

Note: The prompt reverts to the original state when shared partition is active.

Once the SSL Insight partitions have been configured, the Thunder SSLi device should have at least three partitions: Shared, Inside and Outside.

*Note: Please make sure that you are on the correct partition when applying configurations. In addition, you will need to use the command **system ve-mac-scheme system-mac** to support MAC address duplication for a single-device solution.*

INTERFACE AND VLAN CONFIGURATION

Once the partitions are configured, select the interface required to deploy the SSL Insight solution. In this case, L2 mode is being used, hence untagged ports are required. In this deployment example, we will use 13.0.0.x / 16 network for internal addressing. For a simplified configuration, we recommend using the CLI to configure the ports.

Note: Ethernet numbers described below are used for reference purposes only.

INTERFACE ASSIGNMENTS

- Ethernet 1 interface connecting to the client networks (Ingress)
- Ethernet 2 interface connected to Cisco FirePOWER firewall (Outbound to Security Device)
- Ethernet 3 interface connected to Cisco FirePOWER firewall (Inbound from Security Device)
- Ethernet 4 interface connected to public network through gateway router (Egress)

Note: See Figure 1.

CONFIGURING INTERFACES AND VLAN ON THE INSIDE THUNDER SSLI INSTANCE

A VLAN will be configured on the Inside partition. In our example, it is VLAN 850. This VLAN will include the interfaces on the decryption side of SSLi (e.g., Ethernet 1 and 2).

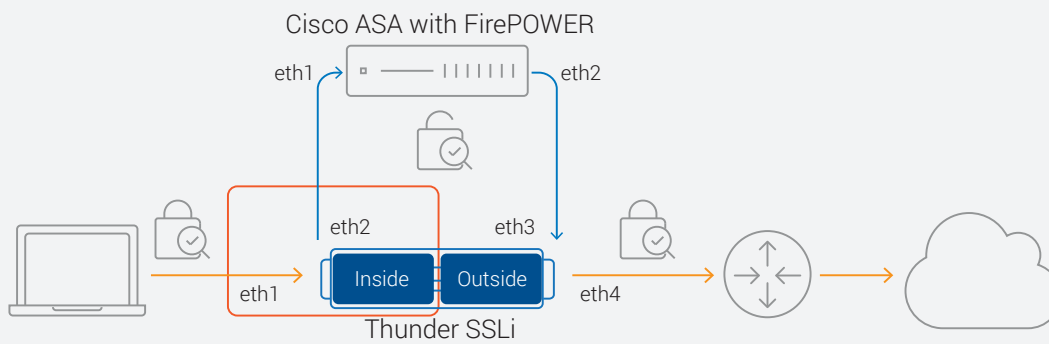


Figure 12: SSLi Inside Partition Configuration

```
vlan 850
  untagged ethernet 1 to 2
  router-interface ve 850
!
interface ethernet 1
  enable
!
interface ethernet 2
  enable
```

A virtual interface will also be created and will be assigned a single IP address. This virtual interface will group the two physical interfaces together under a single IP address. Even in L2 mode, an IP address will be required for addressability of the partitions.

```
interface ve 850
  ip address 13.0.0.114 255.255.0.0
  ip allow-promiscuous-vip
```

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 port to be load-balanced to any VIP address.

CONFIGURING INTERFACES AND VLAN ON THE OUTSIDE THUNDER SSLI INSTANCE

A VLAN will be configured on the Outside partition. In our example, it is VLAN 850. This VLAN will include the interfaces on the encryption side of SSLi (e.g., Ethernet 3 and 4.)

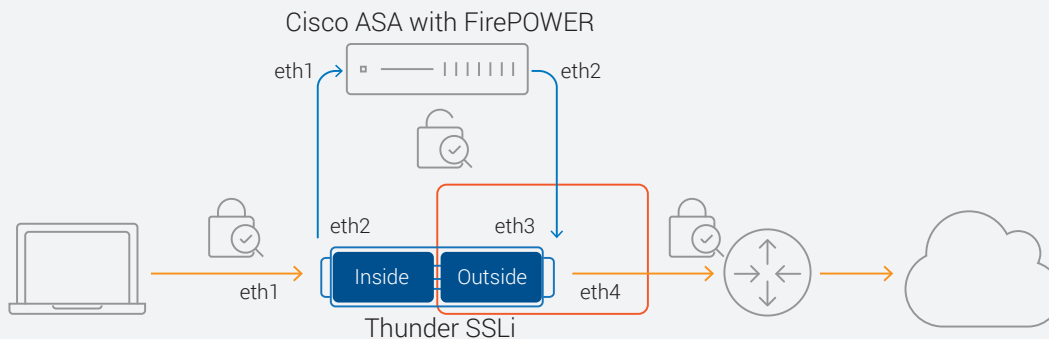


Figure 13: SSLi Outside Partition Configuration

```
vlan 860
  untagged ethernet 3
  untagged ethernet 4
  router-interface ve 860
!
interface ethernet 3
  enable
!
interface ethernet 4
  enable
```

A virtual interface will also be created and will be assigned a single IP address. This virtual interface will group the two physical interfaces together under a single IP address. Even in L2 mode, an IP address will be required for addressability of the partitions.

```
interface ve 860
  ip address 13.0.0.115 255.255.0.0
  ip allow-promiscuous-vip
```

Note: The `ip allow-promiscuous-vip` command is also required, for the same reason, on the Outside partition.

CONFIGURING SERVERS, SERVICE GROUPS, A VIRTUAL SERVER AND CLIENT SSL TEMPLATE ON THE INSIDE THUNDER SSLI INSTANCE

For SSLi to work, a number of servers require configuration. These servers will be included inside different service groups, which, in turn, will be included in the virtual server with the wildcard VIP 0.0.0.0.

On the Inside partition, one server will be configured and will have the IP address of the Outside partition. This will ensure that traffic is forwarded from the Inside partition to the Outside partition, being inspected by Cisco FirePOWER in transit. A total of three wildcard ports – port 0 tcp, port 0 udp and port 8443 tcp – will be configured under the server on the Inside partition, to ensure that both TCP and UDP traffic types are handled. Port 8443 tcp is used for decrypted traffic once port translation takes place and HTTPS traffic is converted to HTTP.

```

slb server fw1 13.0.0.115
  port 0 tcp
    health-check-disable
  port 0 udp
    health-check-disable
  port 8443 tcp
    health-check-disable

```

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

Note: 8443 is the default port number configured when using the AppCentric Templates. This can be changed in AppCentric Templates by navigating to **Configuration > Advanced > SSL Decrypted Port** option. Port number 8443 is used so that normal HTTP traffic (8080) can be differentiated from HTTPS traffic (443) that has been converted to HTTP.

Once the servers are configured, the three service groups will be configured as follows:

```

slb service-group SG_SSLLi_TCP tcp
  member fw1 0
!
slb service-group SG_SSLLi_UDP udp
  member fw1 0
!
slb service-group SG_SSLLi_Xlated tcp
  member fw1 8443

```

As with the servers, each service group is used to handle a separate type of traffic. Any TCP or UDP traffic that is intercepted must have an access control list (ACL) configured within the wildcard VIP to define traffic of interest. Once the ACL has been created with the correct IP address source and destination, the ACL can be applied within the VIP.

```

access-list 190 remark ssli_in
!
access-list 190 permit ip any any vln 850

```

After the service groups, the client SSL template will be configured. This template is used to decrypt 443 traffic to 8443 and apply any bypass configuration options, if needed. The configuration is as follows:

```

slb template client-ssl cl_ssl
  template cipher cl_cipher_template
  forward-proxy-ca-cert SSLiCA
  forward-proxy-ca-key SSLiCA
  forward-proxy-ocsp-disable
  forward-proxy-cert-expiry hours 1
  forward-proxy-enable
  forward-proxy-bypass web-category financial-services
  forward-proxy-bypass web-category health-and-medicine

```

In this example, “financial services” and “health and medicine” URLs will be bypassed. The client SSL template, along with the service groups, will be configured under the virtual server with the wildcard vip 0.0.0.0.

The **forward-proxy-ca-cert SSLiCA** and **forward-proxy-ca-key SSLiCA** commands are used to add the SSLi CA certificate and key already installed on the device. For more details on how to create or import certificates on the SSLi device, refer to SSL Insight Certification Management Guide.

The command template **ciper cl_cipher_template** is used to bind a cipher template to the **client-ssl** template. This cipher template is added on the Inside partition. It is used to specify the cipher suite the SSLi deployment will use. If AppCentric Templates are used, then this template is auto-generated. With CLI, the cipher template is created manually in the configuration mode:

```
slb template cipher cl_cipher_template
  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: The cipher suite used on the **client-ssl** template should match the one used on the **server-ssl** template.*

```
slb virtual-server SSLi_in_ingress 0.0.0.0 acl 190
  user-tag ssli_in
  port 0 udp
    service-group SG_SSLi_UDP
    no-dest-nat
  port 0 others
    service-group SG_SSLi_UDP
    no-dest-nat
  port 0 tcp
    service-group SG_SSLi_TCP
    no-dest-nat
  port 443 https
    service-group SG_SSLi_Xlated
    template client-ssl cl_ssl
    no-dest-nat port-translation
```

*Note: The command **no-dest-nat port-translation** is used to ensure destination NAT is not used. The port translation part of the command enables SSLi to translate the destination port from 443 to 8443.*

CONFIGURING SERVERS, SERVICE GROUPS, A VIRTUAL SERVER AND CLIENT SSL TEMPLATE ON THE OUTSIDE THUNDER SSLI INSTANCE

On the Outside partition, one server will be configured and will have the IP address of the gateway router. This will ensure that traffic is forwarded from the Outside partition toward the gateway router. A total of three wildcard ports – port 0 tcp, port 0 udp and port 443 tcp – will be configured under the server to ensure that both TCP and UDP traffic types are handled.

```
slb server GW 13.0.0.100
  user-tag ssl_i_out
  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.

Once the servers are configured, the three service groups will be configured:

```
slb service-group GW_SSL_443 tcp
  member GW 443
!
slb service-group GW_TCP_0 tcp
  member GW 0
!
slb service-group GW_UDP_0 udp
  member GW 0
```

As with the servers, each service group is used to handle a separate type of traffic.

Any TCP or UDP traffic that is intercepted must have an access control list (ACL) configured within the wildcard VIP to define traffic of interest. Once the ACL has been created with the correct IP address source and destination, the ACL can be applied within the VIP.

```
access-list 191 remark ssl_i_out
!
access-list 191 permit ip any any vln 860
```

After the service groups, the server SSL template will be configured. This template is used to encrypt traffic from 8443 back to 443. The configuration is as follows:

```
slb template server-ssl sr_ssl
  forward-proxy-enable
  template cipher sr_cipher_template
```

The server SSL 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 partition. It is used to specify the cipher suite the SSLi deployment will use. If AppCentric Templates are used, then this template is auto-generated. With CLI, the cipher template is created manually in the configuration mode:

```
slb template cipher sr_cipher_template
  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: The cipher suite used on the **client-ssl** template should match the one used on the **server-ssl** template.

```
slb virtual-server SSLi_out_ingress 0.0.0.0 acl 191
  user-tag ssli_out
  port 0 tcp
    service-group GW_TCP_0
    use-rcv-hop-for-resp
    no-dest-nat
  port 0 udp
    service-group GW_UDP_0
    use-rcv-hop-for-resp
    no-dest-nat
  port 0 others
    service-group GW_UDP_0
    use-rcv-hop-for-resp
    no-dest-nat
  port 8443 http
    service-group GW_SSL_443
    use-rcv-hop-for-resp
    template server-ssl sr_ssl
    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. The effects of this command can be seen when multiple security devices are used.

CISCO FIREPOWER CONFIGURATION

ACCESSING CISCO FIREPOWER MODULE

To access the Cisco FirePOWER module, use a Web browser and navigate to the management IP via HTTPS only.

Default access credentials:

Username: admin

Password: FirePOWER



Figure 14: FireSIGHT Login Portal

ADDING A DEVICE

To add a new Cisco Sensor to the ASA (e.g. FirePOWER), navigate to **Devices > Device Management** and click the **ADD** button in the top-right corner of the portal and select new device.

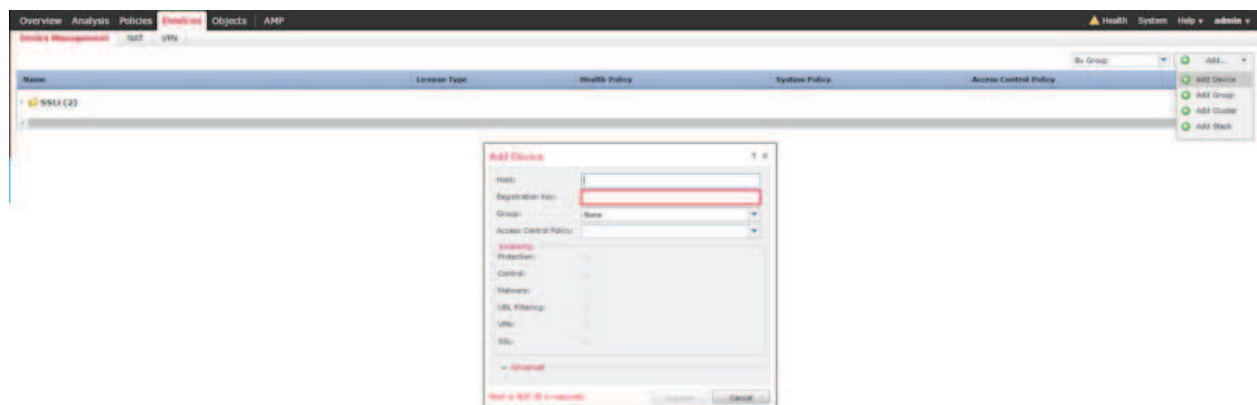


Figure 15: Adding a Device on the Cisco FirePOWER System Portal

In the Add Device section, enter the following:

Host: This is the IP address of the Cisco Sensor.

Registration Key: This is a unique identifier to register a device within FirePOWER.

Access Control Policy: This is a preconfigured access policy created within the Policy tab. Access policy configurations will vary as each company has different security policies. For this deployment, you will use the Default Access Control policy.

CONFIGURING INTERFACES AND SECURITY ZONES

Within FirePOWER, you will need two interfaces, configured in **Inline Mode**. The interfaces will be named Inside and Outside, connecting to the Inside and Outside SSLi partitions, respectively. With the interfaces, two security zones will also be created, namely Internal and External.

To configure and validate the interface settings, navigate to **Devices > Device Management**, select a Device from the list of devices, and click **INTERFACES**. Make sure that the interface is configured as **Default Inline Set**. This is the only supported interface configuration for Cisco FirePOWER.

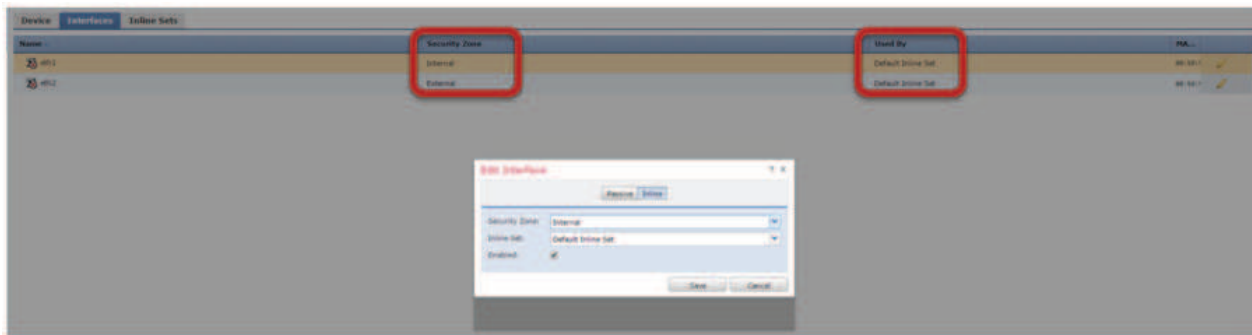


Figure 16: Device Interface Configuration

Once the interfaces are configured, they should be included in separate security zones (i.e., Inside and Outside). This can be done by navigating to **Devices > Device Management > Interfaces** and clicking on the Edit icon. In the pop-up window, open the drop-down menu for **Security Zone** and click **CREATE**. When the security zone is created, it can be selected for the interface using the drop down menu.

CONFIGURING THE ACCESS CONTROL POLICY

After configuring the security zones for the interfaces on the device, the next step is to modify the **Default Access Control** policy. For this deployment, the default options will remain as they are, but Port 8443 will have to be added to the list of destination ports allowed. To modify the **Default Access Control** policy, navigate to **Policies > Access Control > Default Access Control policy > Edit > Ports**. Enter the port number 8443 in the bottom-right text field and click **ADD**.

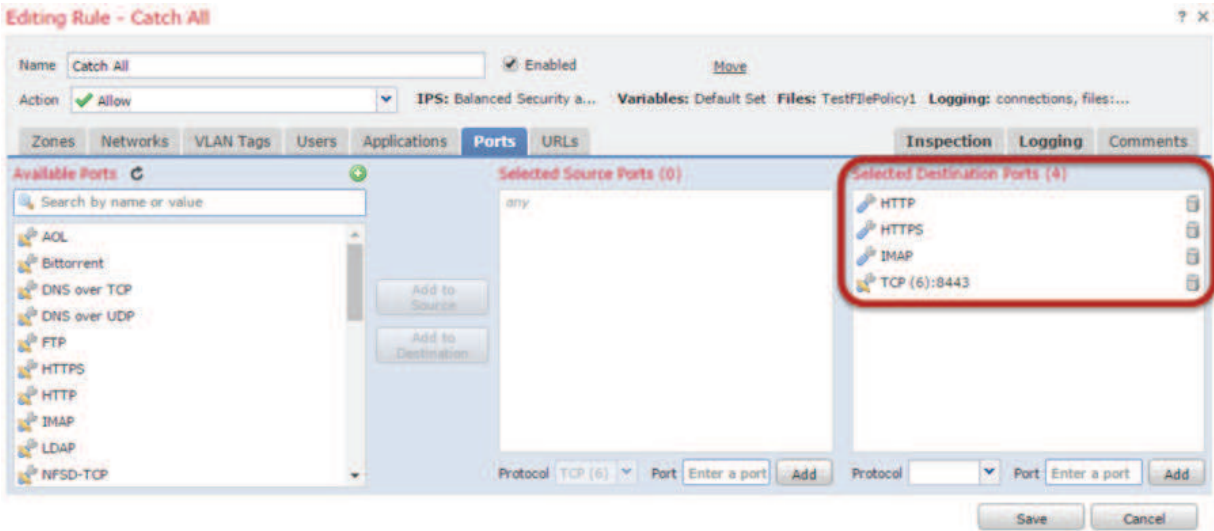


Figure 17: Access Control Policy Configuration

Note: If using the AppCentric Template default port 8443 as the destination for port translation in SSLi, then this step is mandatory. If the destination port was changed (in the Advance Configuration options) to a number that is already in the acceptable ports list on the FirePOWER module (e.g. 8080), then this step can be skipped.

CONFIGURING THE INSPECTION POLICY

The next step is to modify the **Inspection** policy for this deployment. Navigate to **Policies > Access Control > Default Access Control policy > Edit > Inspection > File Policy**. Create a new rule by clicking the **ADD FILE RULE** button in the upper-right corner. Here, select the option **Block Malware** from the drop-down menu and select the **Reset Connection** option. Leave the rest of the options unmodified.

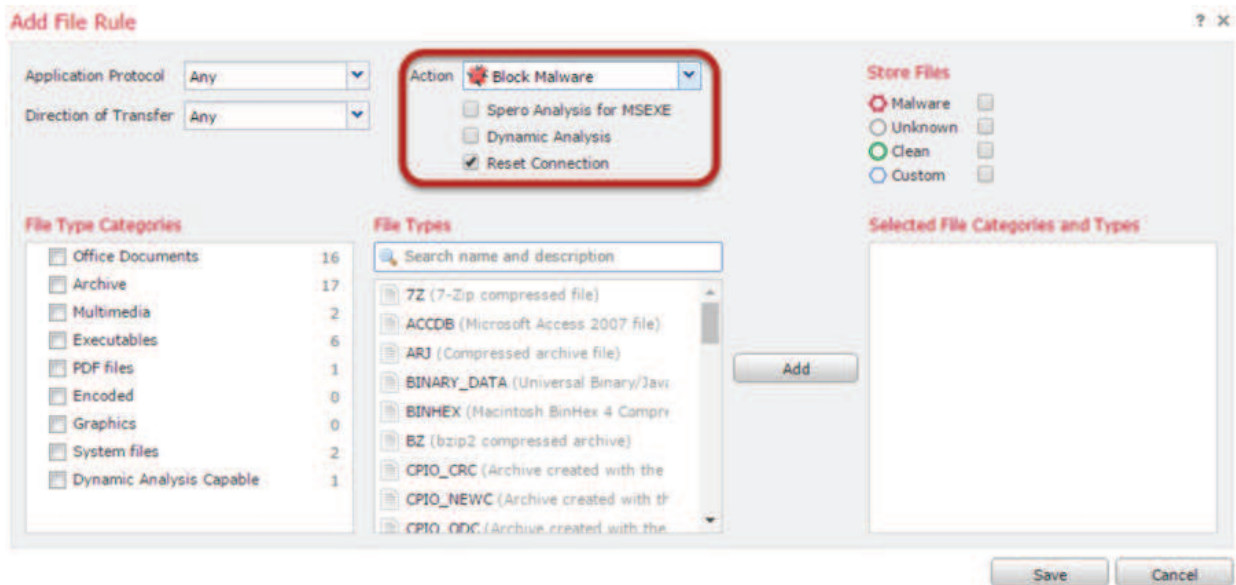


Figure 18: Inspection Policy Configuration

CONFIGURING THE NETWORK ANALYSIS POLICY

The last step in the Cisco FirePOWER device configuration is to add Port 8443 to the list of ports recognized as HTTP by the Network Analysis and Intrusion policy. Navigate to **Policies > Access Control > Default Access Control policy > Advanced > Network Analysis and Intrusion Policies > Network Analysis Policy List**. Here, create a custom policy (e.g., SSLi Policy) and navigate to the HTTP Configuration menu on the left side. Here, in the Ports section, add 8443 to the list of HTTP ports accepted by Cisco FirePOWER.

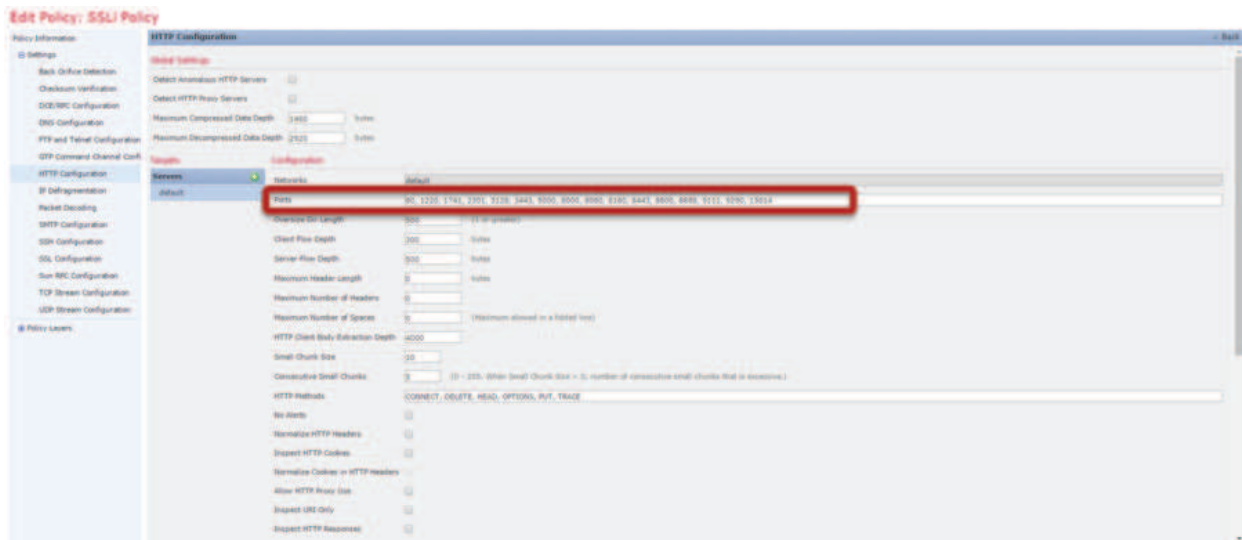


Figure 19: Network Analysis Policy Configuration

Note: This step can be skipped if a port number already accepted by Cisco FirePOWER is used in the SSLi configuration.

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 Cisco FirePOWER, require visibility into encrypted traffic to discover attacks, intrusions and malware.

This guide provided the detailed steps required to configure A10 Thunder SSLi with Cisco FirePOWER. Once completed, 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, offers organizations a powerful solution for load-balancing, high availability and SSL inspection. Using SSL Insight, organizations can:

- Analyze all network data, including encrypted data, eliminating blind spots in their threat protection solution
- Provide advanced SSL inspection features and SSL decryption for third-party security devices
- Detect encrypted malware, insider abuse and attacks transported over SSL/TLS
- Deploy best-of-breed content inspection solutions to defeat 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 SSLi products, please visit:

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

<https://www.a10networks.com/solution-briefs-handbooks>

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

APPENDIX A

The following sample configurations are based on a single-device configuration.

A10 SHARED PARTITION CONFIGURATION

```
system ve-mac-scheme system-mac
!
partition ssl_i_in id 1
!
partition ssl_i_out id 2
!
terminal idle-timeout 0
!
hostname SSLi
!
timezone America/Los_Angeles
!
interface management
  flow-control
  ip address 10.101.6.114 255.255.252.0
  ip default-gateway 10.101.4.1
!
interface ethernet 1
  name testsw-33.e10
  enable
!
interface ethernet 2
  name ASA.e1
!
interface ethernet 3
!
interface ethernet 4
!
interface ethernet 5
!
interface ethernet 6
!
interface ethernet 7
!
interface ethernet 8
!
interface ethernet 9
!
interface ethernet 10
!
```

```
web-category
  use-mgmt-port
  enable
!
logging syslog information
!
end
```

A10 INSIDE PARTITION CONFIGURATION

```
!multi-ctrl-cpu 2
active-partition ssl_i_in
!
!
access-list 190 remark ssl_i_in
!
access-list 190 permit ip any any vlan 850
!
vlan 850
  untagged ethernet 1 to 2
  router-interface ve 850
  name ssl_i_in_ingress_egress
  user-tag ssl_i_in_ingress_egress
!
interface ethernet 1
  name ssl_i_in_ingress
  enable
!
interface ethernet 2
  name ssl_i_in_egress
  enable
!
interface ve 850
  name ssl_i_in_ingress_egress
  ip address 13.0.0.114 255.255.0.0
  ip allow-promiscuous-vip
!
!
ip route 0.0.0.0 /0 13.0.0.115
!
slb template cipher cl_cipher_template
  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
user-tag ssl_i_in
!
slb server fw1 13.0.0.115
user-tag ssl_i_in
port 0 tcp
health-check-disable
user-tag ssl_i_in_1_tcp_port
port 0 udp
health-check-disable
user-tag ssl_i_in_1_udp_port
port 8443 tcp
health-check-disable
user-tag ssl_i_signaling
!
slb service-group SG_SSLLi_TCP tcp
user-tag ssl_i_in
member fw1 0
!
slb service-group SG_SSLLi_UDP udp
user-tag ssl_i_in
member fw1 0
!
slb service-group SG_SSLLi_Xlated tcp
user-tag ssl_i_in
member fw1 8443
!
slb template client-ssl cl_ssl
template cipher cl_cipher_template
forward-proxy-ca-cert SSLiCA
forward-proxy-ca-key SSLiCA
forward-proxy-ocsp-disable
forward-proxy-cert-expiry hours 1
forward-proxy-enable
forward-proxy-bypass web-category finan-
cial-services
forward-proxy-bypass web-category
health-and-medicine
user-tag ssl_i_in
!
slb virtual-server SSLi_in_ingress 0.0.0.0
acl 190
user-tag ssl_i_in

```

```

port 0 udp
service-group SG_SSLLi_UDP
no-dest-nat
port 0 others
service-group SG_SSLLi_UDP
no-dest-nat
port 0 tcp
service-group SG_SSLLi_TCP
no-dest-nat
port 443 https
service-group SG_SSLLi_Xlated
template client-ssl cl_ssl
no-dest-nat port-translation
!
end

```

A10 OUTSIDE PARTITION CONFIGURATION

```

!multi-ctrl-cpu 2
active-partition ssl_i_out
!
access-list 191 remark ssl_i_out
!
access-list 191 permit ip any any vlan 860
!
vlan 860
untagged ethernet 3
untagged ethernet 6
router-interface ve 860
name ssl_i_out_ingress_egress
user-tag ssl_i_out_ingress_egress
!
interface ethernet 3
name ssl_i_out_ingress
enable
!
interface ethernet 6
name ssl_i_out_egress
enable
!
interface ve 860
name ssl_i_out_ingress_egress
ip address 13.0.0.115 255.255.0.0
ip allow-promiscuous-vip
!
ip route 0.0.0.0 /0 13.0.0.100
!
slb template cipher sr_cipher_template

```

```

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
user-tag ssl_i_out
!
slb template server-ssl sr_ssl
  forward-proxy-enable
  template cipher sr_cipher_template
  user-tag ssl_i_out
!
slb server GW 13.0.0.100
  user-tag ssl_i_out
  port 0 tcp
    health-check-disable
    user-tag ssl_i_out_1_tcp_port
  port 0 udp
    health-check-disable
    user-tag ssl_i_out_1_udp_port
  port 443 tcp
    health-check-disable
!
slb service-group GW_SSL_443 tcp
  user-tag ssl_i_out
  member GW 443

```

```

!
slb service-group GW_TCP_0 tcp
  user-tag ssl_i_out
  member GW 0
!
slb service-group GW_UDP_0 udp
  user-tag ssl_i_out
  member GW 0
!
slb virtual-server SSL_i_out_ingress 0.0.0.0
acl 191
  user-tag ssl_i_out
  port 0 tcp
    service-group GW_TCP_0
    use-rcv-hop-for-resp
    no-dest-nat
  port 0 udp
    service-group GW_UDP_0
    use-rcv-hop-for-resp
    no-dest-nat
  port 0 others
    service-group GW_UDP_0
    use-rcv-hop-for-resp
    no-dest-nat
  port 8443 http
    service-group GW_SSL_443
    use-rcv-hop-for-resp
    template server-ssl sr_ssl
    no-dest-nat port-translation
end

```

APPENDIX B

SSL INSIGHT TWO-DEVICE DEPLOYMENT

In this deployment guide, the focus is on the SSL Insight single-device deployment where ADPs are used in place of separate devices for decryption and re-encryption. An **SSL Insight two-device deployment** consists of two Thunder SSLi devices.

The first device, **Thunder SSLi Inside**, is responsible for:

- Decrypting client traffic
- Forwarding decrypted client traffic to Cisco ASA device
- URL Classification service

The second device, **Thunder SSLi Outside**, is responsible for:

- Re-encrypting traffic that has been inspected by the Cisco ASA device
- Forwarding the re-encrypted traffic to the gateway route.

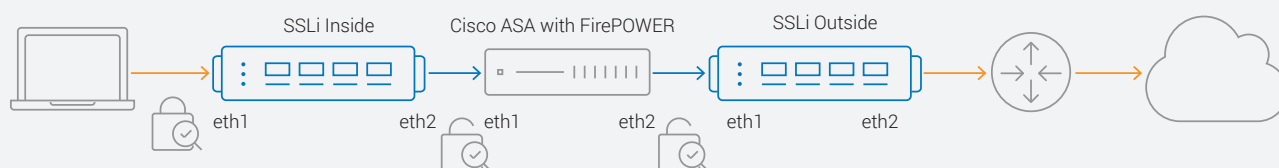


Figure 20: SSL Insight in a Two-Device Deployment

Note: The SSL Insight two-device deployment can only be configured using the CLI. AppCentric Templates do not support multiple device deployments.

APPENDIX C

THIRD-PARTY WEB PROXY

A10 Thunder SSLi delivers the flexibility to support third-party transparent and explicit proxy services. This feature is applicable when you have an existing Web proxy deployed, and when you want to deploy an SSL inspection solution while keeping the Web Proxy infrastructure intact.

The SSL Insight deployment modes and configuration will differ based on whether:

- The proxy being used is a Transparent Proxy or an Explicit Proxy
- Authentication is enabled or disabled

When authentication is enabled, an HTTP virtual port on the Thunder SSLi device intercepts the HTTP requests from the client, validates both the source and destination, and forwards only those requests that come from valid sources and destinations to permitted destinations.

Destinations are validated based on URL or hostname strings. For approved destinations, the DNS is used to obtain the IP addresses.

A10 Thunder SSLi may be deployed in three different topologies based on the type of third-party Web proxy being used and whether or not authentication services are required.

TRANSPARENT PROXY OUTSIDE THE SSLI SANDWICH (DECRYPT ZONE)

- No changes are required for such a deployment
- Special consideration is required when the proxy performs client authentication
- When authentication is required, then Explicit Proxy (EP) deployment is recommended. EP would be able to perform normal proxy functions without decrypting traffic (e.g., URL filtering based on user/group information)

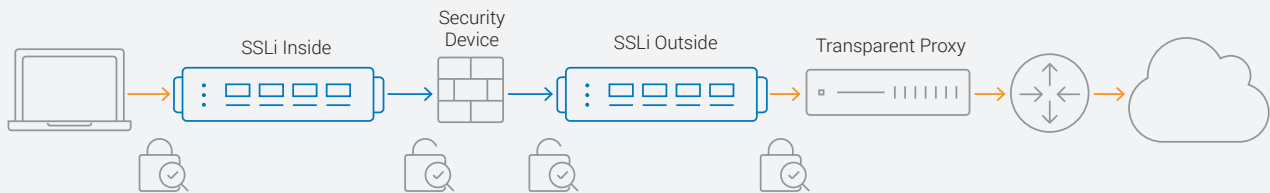


Figure 21: SSL Insight in a Two-Device Deployment with Transparent Proxy Outside Decrypt Zone

TRANSPARENT PROXY INSIDE THE SSLI SANDWICH (DECRYPT ZONE)

- No changes are required for such a deployment
- The Transparent Proxy may translate traffic to either Ports 80 or 8080. The SSLi Outside device needs to differentiate between cleartext traffic and traffic that was decrypted by SSLi Inside. The Inside device inserts a header in the traffic when decrypted. This enables the Outside to differentiate between different traffic types and helps in correctly re-encrypting the traffic.

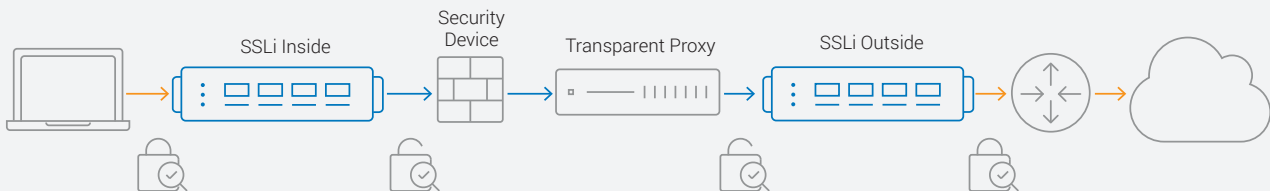


Figure 22: SSL Insight in a Two-Device Deployment with Transparent Proxy Inside Decrypt Zone

EXPLICIT PROXY OUTSIDE THE SSLI SANDWICH (DECRYPT ZONE)

- The Explicit Proxy will be placed after the re-encryption device (i.e., Thunder SSLi Outside) is outside the decryption zone
- In this deployment, the proxy can perform authentication services
- Proxy chaining is required on the SSLi Inside device. It is configured on the wildcard VIP of the device. Proxy chaining enables the Inside device to send a Connect message to the EP, enabling it to decrypt the encrypted traffic

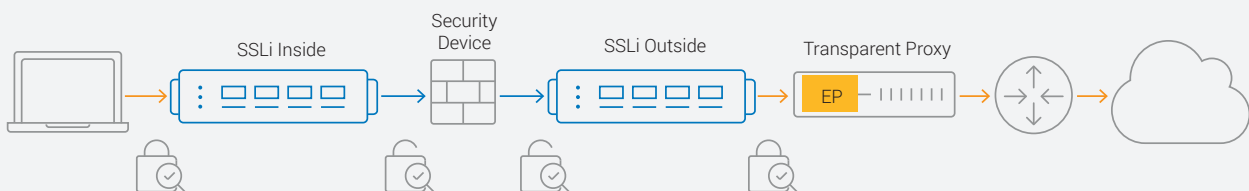


Figure 23: SSL Insight in a Two-Device Deployment with Explicit Proxy Outside Decrypt Zone

EXPLICIT PROXY INSIDE THE SSLI SANDWICH (DECRYPT ZONE)

- Such a deployment is not supported by Thunder SSLi
- As a workaround, the Explicit Proxy can be converted into a Transparent Proxy and placed inside the decrypt zone

APPENDIX D

A10 URL CLASSIFICATION SERVICE

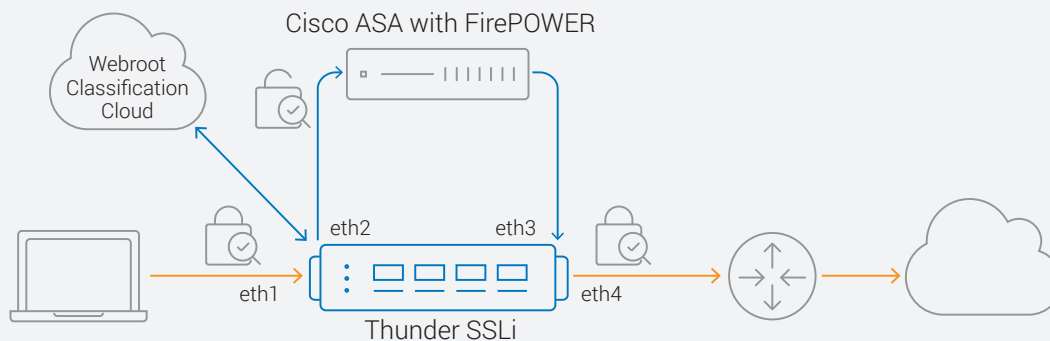


Figure 24: A10 and Webroot Architecture

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

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

- If the category of the URL is allowed by the configuration, the SSL Insight Inside partition leaves the data encrypted and sends it to the SSL Insight Outside partition, which sends the encrypted data to the server
- If the category of the URL is not allowed by the configuration, the SSL Insight Inside partition 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 licensing (contact your regional sales director for pricing)
- Inside partition of the Thunder SSLi 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 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 Webroot 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 Webroot URL classification feature, you must have the following configuration within the client SSL template.

Here is a sample configuration:

```
slb template client-ssl ssl-client-template
  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
```

Note: The fake-server and fake-sg are required as placeholders for action forward-to-internet.

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](https://twitter.com/a10Networks)

LEARN MORE

ABOUT A10 NETWORKS

[CONTACT US](#)

a10networks.com/contact

©2018 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Networks logo, ACOS, A10 Thunder, A10 Lightning, A10 Harmony and SSL Insight are trademarks or registered trademarks of A10 Networks, Inc. in the United States and other countries. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. For the full list of trademarks, visit: www.a10networks.com/a10-trademarks.

Part Number: A10-DG-16152-EN-06 MAY 2018