SSL Insight and Fidelis Network Deployment Guide

Table of Contents

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.

Overview

With the rise in encrypted traffic, the threat of hidden attacks has grown. Traditional security devices do not have the ability to decrypt traffic in order to inspect for these hidden threats. Some next-generation firewalls, Intrusion Prevention Systems (IPS) and anti-malware systems can decrypt SSL/TLS traffic, but due to increasing SSL key lengths and more computationally complex SSL ciphers, they experience dramatic performance degradation.

A10 Networks® SSL Insight® technology enables existing security solutions, deployed in a multitude of ways in the network, to inspect encrypted traffic. SSLi® decrypts enterprise traffic, forwards it in clear text to a preinstalled security solution within the network, and after inspection, re-encrypts the traffic to send it out to its destination.

This guide provides step-by-step instructions for the deployment of A10 Networks Thunder® SSLi® with Fidelis Network solutions. In this deployment, the SSL Insight technology enables Fidelis' next-generation IPS to inspect encrypted traffic and protect corporate networks from malicious activities.

SSL Insight Technology with Fidelis Network Solutions

A10 Networks enables organizations to analyze all data, including encrypted data, by intercepting SSL communications, decrypting and sending the traffic in clear text to third-party security devices such as firewalls, threat prevention platforms and forensic tools for inspection. The A10 Networks Thunder SSLi products feature SSL Insight technology, which eliminates the blind spot imposed by SSL encryption by offloading CPU-intensive SSL decryption and encryption functions from third-party security devices.

SSLi enables existing security solutions to inspect encrypted traffic. It decrypts enterprise traffic, forwards it in clear text to a pre-installed security solution within the network, and after inspection, re-encrypts the traffic to send it out to its destination.

The Fidelis Network solution stops modern threats and plays an important role in defending a network. It functions as a next-generation IPS, advanced malware protection system, data loss prevention (DLP) system and an advanced analytics engine. The Fidelis Network solution has multiple components that work in sync with each other. These include the Fidelis Direct sensors, which are used to sniff traffic from the network; a CommandPost that is used as a GUI as well as a controller; and a Collector, which collects raw metadata from the Direct sensor in real time and lets the CommandPost use the data to provide analytics and insights.

This guide describes the configuration of SSL Insight technology using a single Thunder SSLi device using Application Delivery Partitions (ADPs) to create multiple, logical Thunder SSLi instances. The partition that decrypts outbound SSL traffic is referred to as the **"Inside Thunder SSLi Instance**." The partition that re-encrypts outbound SSL traffic is referred to as the "**Outside Thunder SSLi Instance**." The Inside Thunder SSLi Instance decrypts SSL traffic and sends a copy to the Fidelis Direct sensor on a passive interface. The Outside Thunder SSLi Instance receives the traffic from the first partition in clear text and re-encrypts traffic.

Figure 1 shows how SSLi works with an out-of-band or passive Fidelis Direct deployment scenario, set up for this deployment guide.

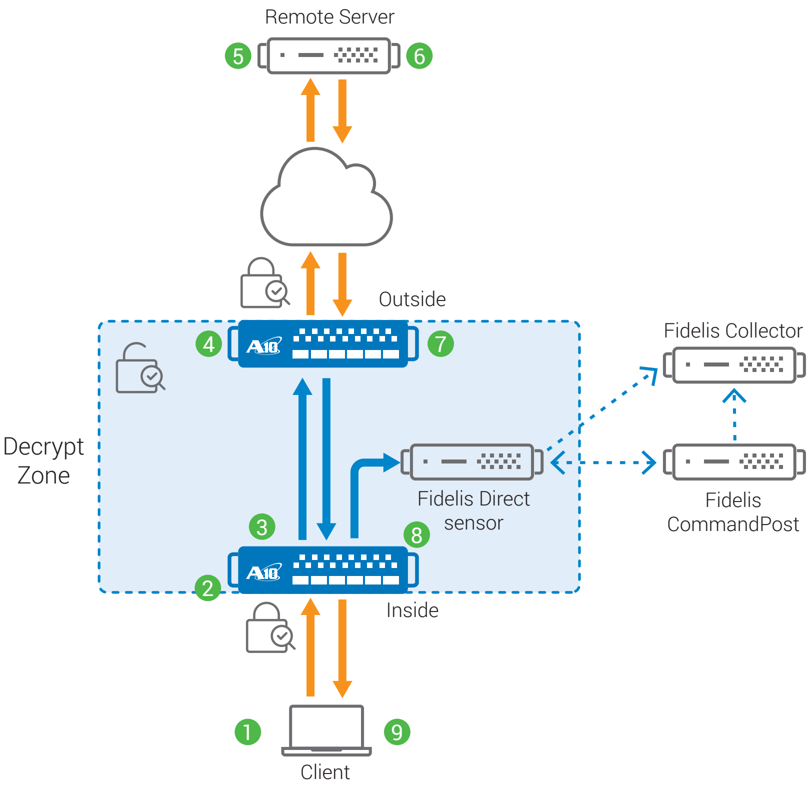


Figure 1: Traffic flow through an SSLi and Fidelis network deployment

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.
3. The clear-text content is forwarded to the Outside Thunder SSLi Instance on a back-to-back link and a copy is sent on the mirrored port to the Fidelis Direct sensor deployed out-of-band.
   a. Upon receiving the traffic, the Fidelis Direct sensor, based on the rules and policies installed, sniffs through the packets and figures out whether to issue an alert or not through the CommandPost. The data is also stored in the Collector in its raw form.
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 clear-text traffic to the Inside Thunder SSLi Instance. At this point:
   a. The session is matched and the source MAC address is retrieved. This is useful in case multiple inline devices are connected, so that traffic can be forwarded to the device that inspected it on the way out of the network.
   b. A copy of the traffic is sent out on the mirrored interface towards the Fidelis Direct sensor deployed out-of-band. The Fidelis Direct sensor inspects the traffic, issuing alerts whenever needed via the CommandPost. It also sends a copy of the raw traffic to the Collector.
8. The Inside Thunder SSLi Instance receives the clear-text traffic from the Outside Thunder SSLi Instance, encrypts it and returns it to the client.
9. The client receives the encrypted response.

Deployment Requirements

To deploy the Thunder SSLi solution with Fidelis, the following are required:

- A10 Networks Advanced Core Operating System (ACOS®) 4.1.0-P8 or higher (supported with hardware-based Thunder SSLi devices)
- CA certificate for SSLi and certificate chain[1]
- SSL Insight AppCentric Templates for configuration
- Fidelis Network 3.2.1 or above:
  - Fidelis Direct sensor – Passive deployment
  - Fidelis CommandPost – For management of the Direct sensor and Collector
  - Fidelis Collector – For metadata collection

Note*: This solution is deployed in Layer 2 mode.*

Deployment Mode

A10 recommends deploying the SSLi Insight technology 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.

The Fidelis Direct sensor will be deployed out-of-band, on a mirrored port off of the Thunder SSLi device. Direct sensors can also be deployed in-line but for this deployment, the focus is on passive deployment. Multiple Direct sensors can be deployed with a single CommandPost device for monitoring and controlling. A Fidelis Collector is also deployed and connected to each Direct sensor in the CommandPost. This device will collect raw traffic intercepted by the Direct sensor that can be seen and analyzed in the CommandPost GUI.

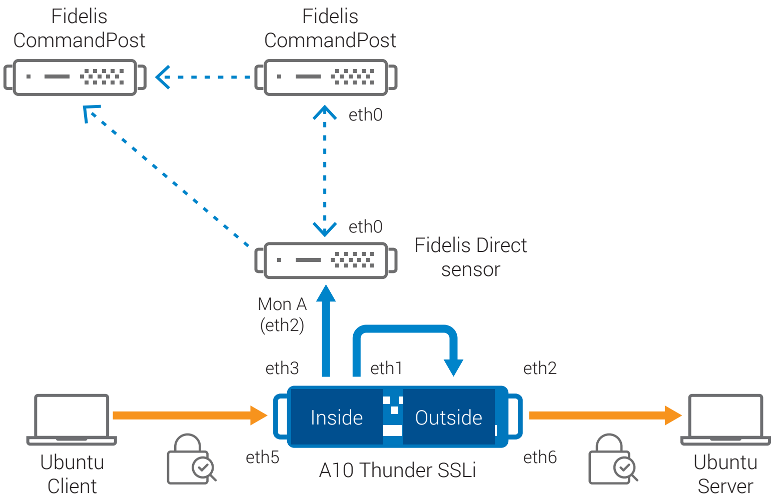


Figure 2: Thunder SSLi single device and Fidelis Direct sensor deployment

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 Ubuntu machine is directly connected to the Thunder SSLi device via the interface Ethernet 5. Encrypted traffic from the client machine is received on this interface.
- Ethernet 1 and Ethernet 2 interfaces of the Thunder SSLi device are connected back to back for traffic flow from Inside partition to Outside. Ethernet 3 is connected to Ethernet 2 of the Fidelis Direct

[1] For more detail on the CA Certificate for Thunder SSL Insight, refer to SSL Insight Certification Management Guide.

sensor. The client traffic, once decrypted, will be sent out from the Inside partition to the Outside partition and the traffic from Ethernet 1 of the Thunder SSLi device will be mirrored onto Ethernet 3, sending it in clear text to the Fidelis Direct sensor.

- Ethernet 6 is connected to the server. Traffic will be re-encrypted and sent out via this interface.
- The Thunder SSLi interfaces, Ethernet 1 and 5, are part of the Inside partition, while Ethernet 2 and 6 are part of the Outside partition.
- The Fidelis Direct sensor's interface Ethernet 2 is selected as MonitorA and is used to receive clear-text traffic from Thunder SSLi.
- The Fidelis Direct sensors, CommandPost and Collector, are connected via their respective Admin ports, i.e., Ethernet 0.

***Note**: This guide only provides a basic Fidelis Direct configuration based on default policies. Detailed packet inspection solutions may consist of different, custom policies.*

Accessing A10 Thunder SSLi

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

- CLI

  This is a 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 via SSHv2. The system default values are:

  Default username: admin

  Default password: a10

  Default IP address of the device: 172.31.31.31

- AppCentric Templates (ACT)

  This is the ACOS GUI extension that provides you with access to template-based configurations of the Thunder SSLi device. You can access ACT by navigating to System – Templates on the ACOS GUI over HTTPS.

***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 first configuration to consider is to change the management IP address for CLI and GUI 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 Thunder 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 Thunder 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 inline security device will typically require four interfaces. An out-of-band device will require an additional fifth interface. Every additional inline device will require a set of two interfaces each, while an out-of-band device will require one additional interface on Thunder SSLi (multiple security devices connected to a single Thunder SSLi device).

There are four main sections in the SSL Insight AppCentric Templates:

1. Wizard

   The wizard provides users with a flow-based initial configuration of the Thunder 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.

4. Troubleshooting

   This section provides users with the options to troubleshoot the functionality of Thunder SSLi.

Wizard – Topology

Basic configuration of the Thunder SSLi device will be done in the **Wizard** section. The **Topology** is the first step in the configuration of a Thunder SSLi device using the AppCentric Templates. In this step, you will choose the network and deployment topology to use for your 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.

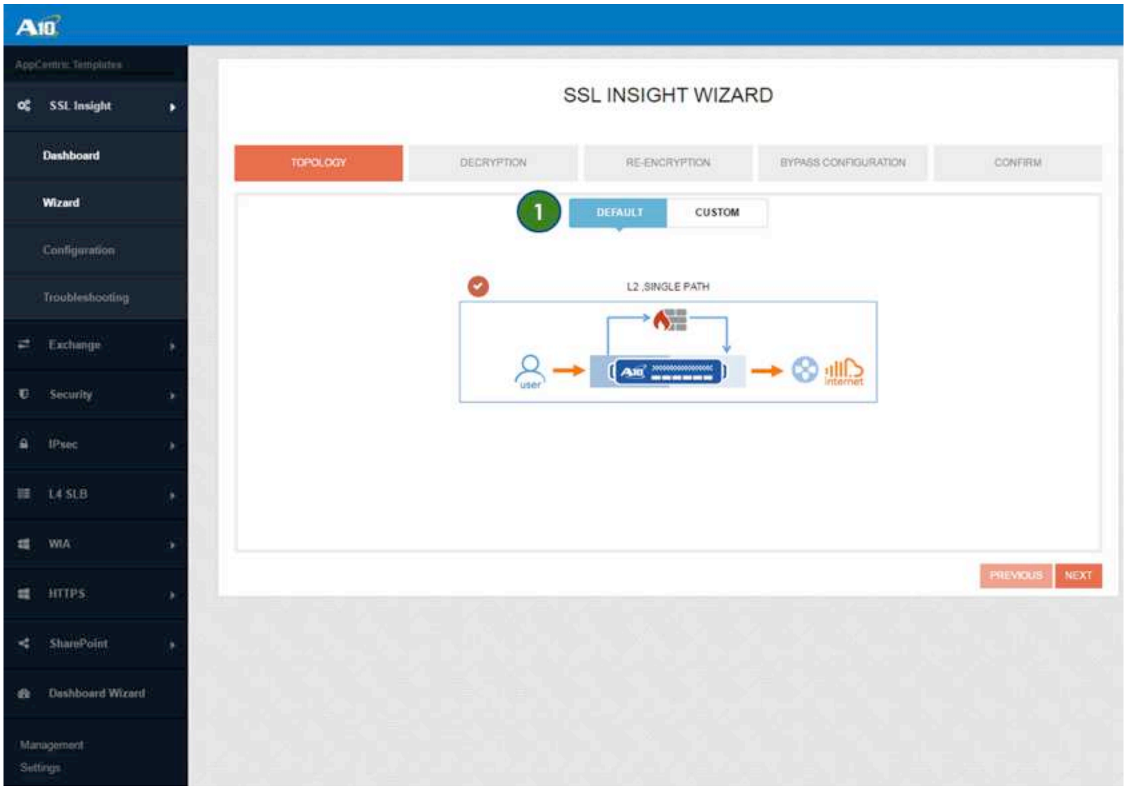


Figure 3: Wizard – Topology configuration

***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.*

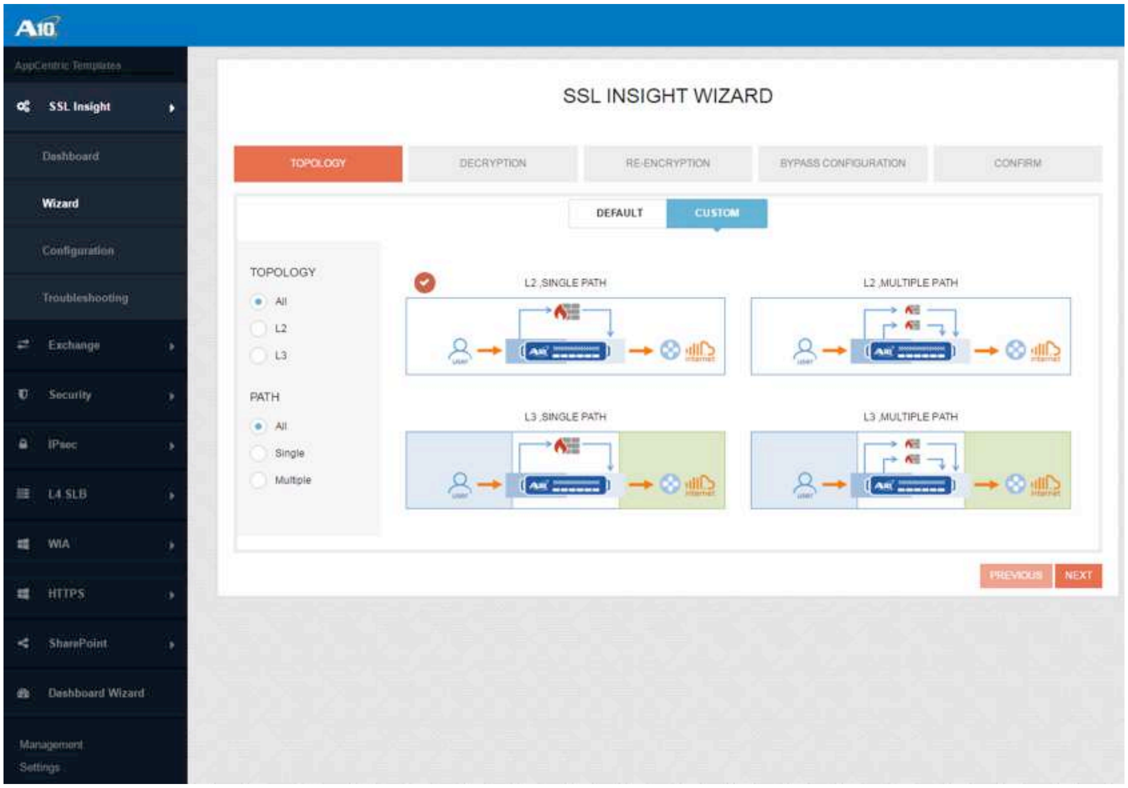
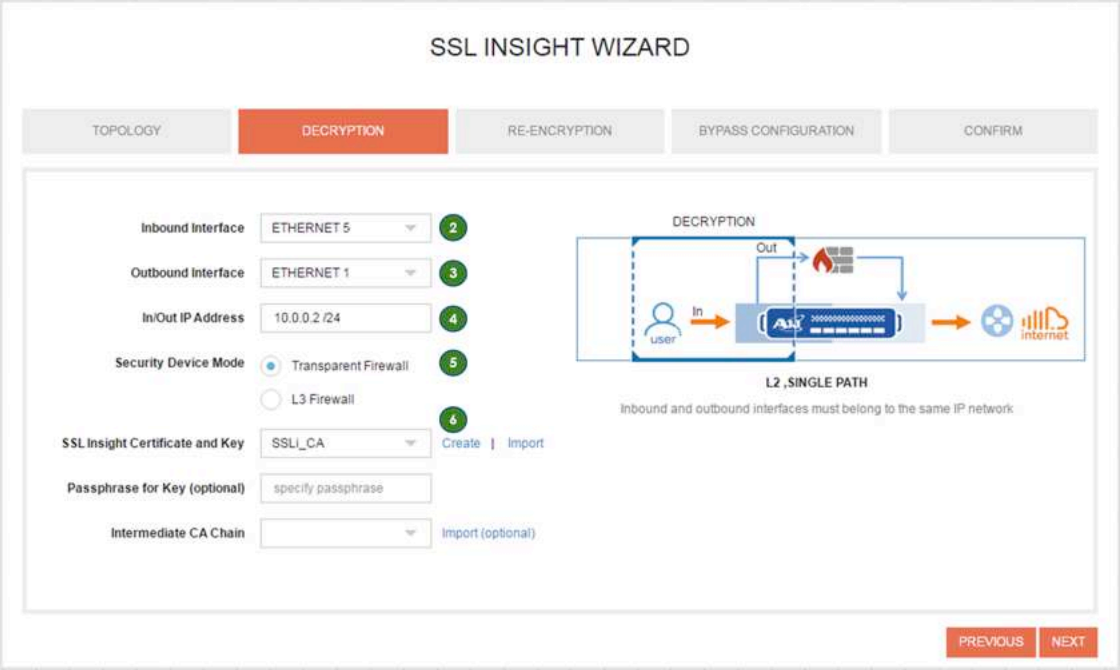


Figure 4: Selection of Custom Topology

Wizard – Decryption

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

2. Select the Inbound interface (e.g., Ethernet 5). This is the interface that receives encrypted (SSL) traffic from the internal client.
3. Select the Outbound interface (e.g., Ethernet 1). This is the interface that will send out decrypted traffic to SSLi Outside for re-encryption. Inline security devices can be inserted on this link for inline inspection.
4. Assign an IP address to the group of two interfaces in SSLi Inside (10.0.0.2 / 24).
5. Select the Security Device Mode. Since Fidelis Direct is deployed as a passive, transparent Bump in the Wire, we select the Transparent Firewall option.
6. Select **SSLi_CA** on SSL Certificate and Key. This is an SSL certificate and key signed by the Root CA certificate, provided for testing purposes. For this deployment, we do not have intermediate certificates; therefore, the Intermediate CA Chain option is left blank.



SSL INSIGHT WIZARD

Inbound Interface: ETHERNET 5 (2)

Outbound Interface: ETHERNET 1 (3)

In/Out IP Address: 10.0.0.2 /24 (4)

Security Device Mode (5): ● Transparent Firewall ○ L3 Firewall

SSL Insight Certificate and Key (6): SSLI_CA Create | Import

Passphrase for Key (optional): specify passphrase

Intermediate CA Chain: Import (optional)

Inbound and outbound interfaces must belong to the same IP network

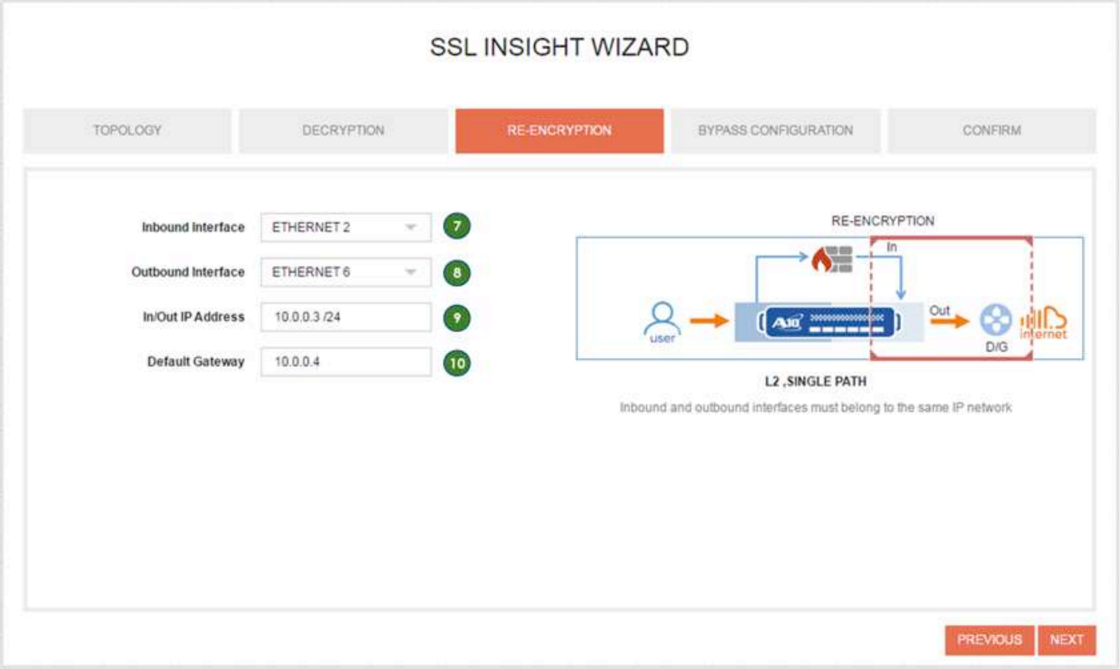
Figure 5: Wizard – Decryption

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

Wizard – Re-Encryption

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

7. Select the Inbound interface, where decrypted traffic from SSLi Inside will be received. In this example, it's Ethernet 2.
8. Assign an IP address to the group of two interfaces in the SSLi Outside (10.0.0.3 / 24).
9. Select the Outbound interface. This interface sends out the re-encrypted (SSL) traffic toward the Internet via the gateway router. In this example, we do not have a gateway router so Ethernet 6 is used to send the traffic directly to the server.
10. Specify the IP address (e.g., 10.0.0.4) of the default gateway. In this example, it is the IP address of the server machine.



SSL INSIGHT WIZARD

Inbound Interface: ETHERNET 2 (7)

Outbound Interface: ETHERNET 6 (8)

In/Out IP Address: 10.0.0.3 /24 (9)

Default Gateway: 10.0.0.4 (10)

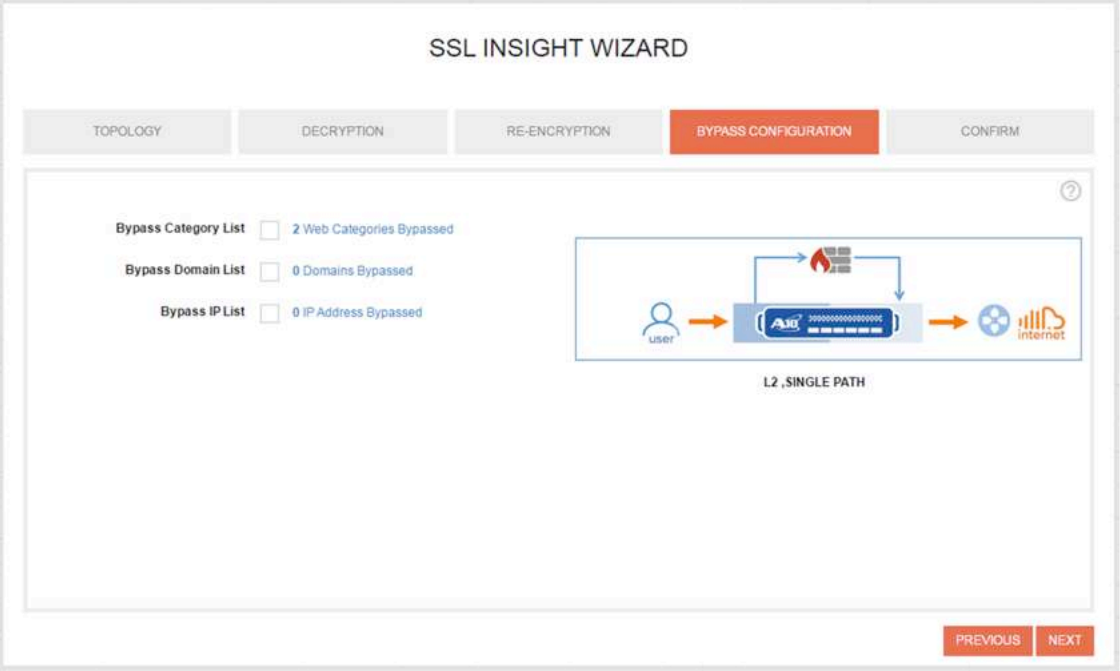
L2 ,SINGLE PATH

Inbound and outbound interfaces must belong to the same IP network

Figure 6: Wizard – Re-Encryption

Wizard – Bypass Configuration

The Bypass Configuration is optional but important for SSL Insight technology. While you strengthen the security solution using SSLi, 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 SSLi.



SSL INSIGHT WIZARD

Bypass Category List □ 2 Web Categories Bypassed

Bypass Domain List □ 0 Domains Bypassed

Bypass IP List □ 0 IP Address Bypassed

L2 ,SINGLE PATH

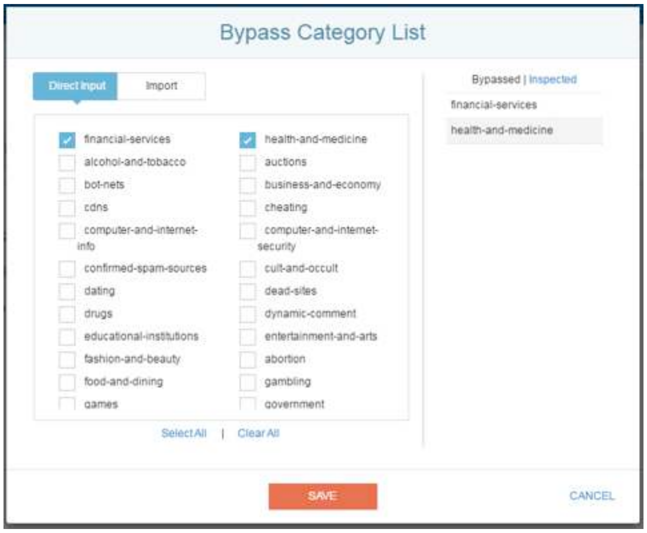
Figure 7: Wizard – Bypass Configuration

Bypass Configuration provides 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 SSLi. For example, if you select a category “financial-services,” all websites under the category will be bypassed and will not be inspected through SSLi. 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.*



Bypass Category List

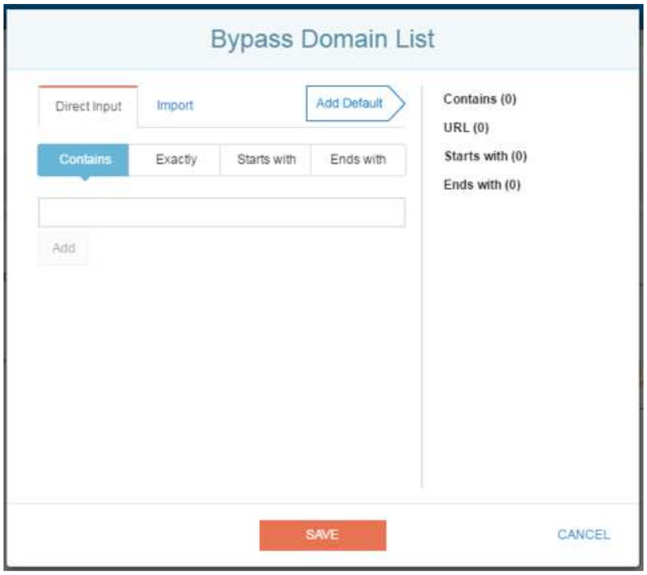
- ☑ financial-services
- ☐ alcohol-and-tobacco
- ☐ bot-nets
- ☐ cdns
- ☐ computer-and-internet-info
- ☐ confirmed-spam-sources
- ☐ dating
- ☐ drugs
- ☐ educational-institutions
- ☐ fashion-and-beauty
- ☐ food-and-dining
- ☐ games
- ☑ health-and-medicine
- ☐ auctions
- ☐ business-and-economy
- ☐ cheating
- ☐ computer-and-internet-security
- ☐ cult-and-occult
- ☐ dead-sites
- ☐ dynamic-comment
- ☐ entertainment-and-arts
- ☐ abortion
- ☐ gambling
- ☐ government

Bypassed:
financial-services
health-and-medicine

Figure 8: 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 SSLi. The **Add Default** button can be used to add a predefined 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.



Bypass Domain List

Contains (0)
URL (0)
Starts with (0)
Ends with (0)

Figure 9: Bypass Domain List

Bypass IP List

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

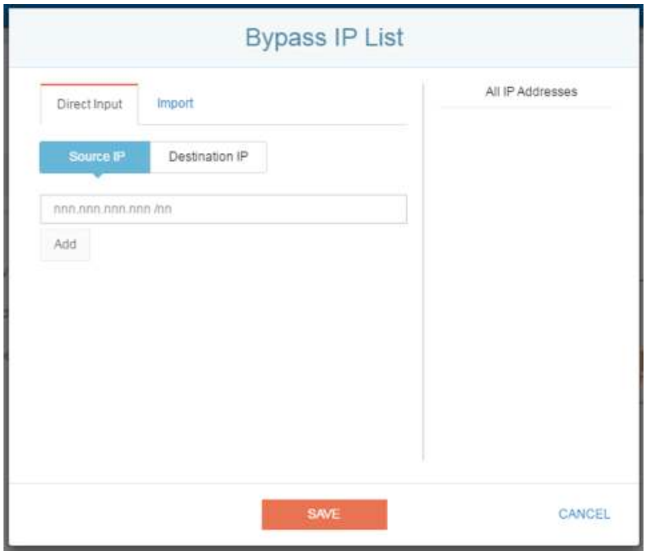
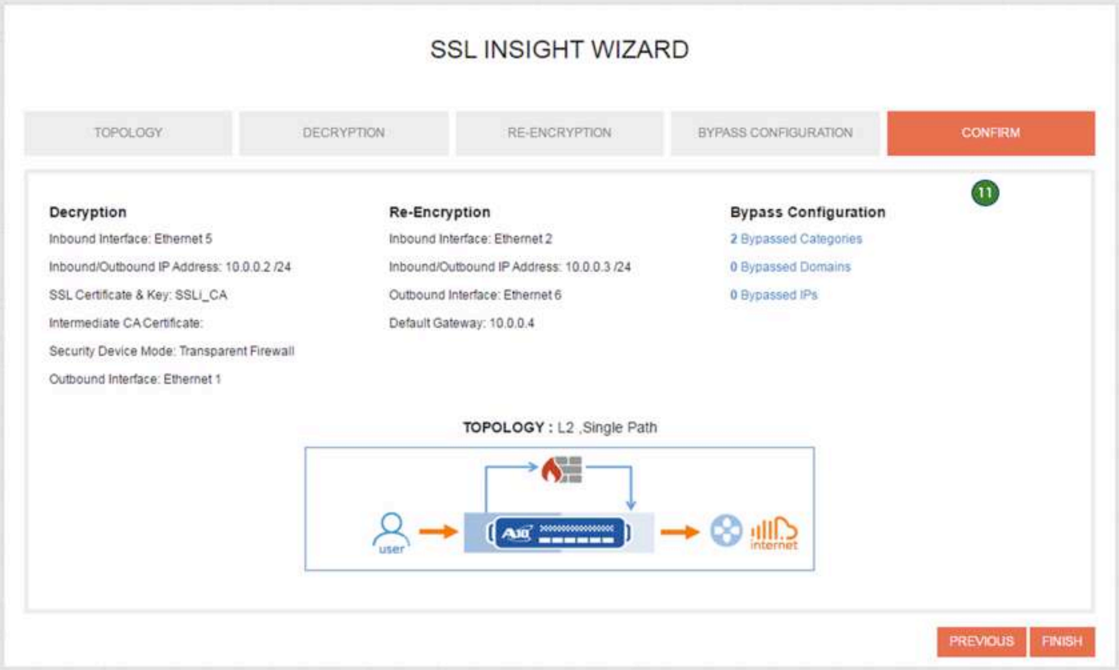


Figure 10: Bypass IP List

Wizard – Confirm

11. On the Confirm tab, you can review a summary of the SSLi 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 SSLi topology configuration. This action opens a new window showing the actual CLI-based configuration.



Decryption
Inbound Interface: Ethernet 5
Inbound/Outbound IP Address: 10.0.0.2 /24
SSL Certificate & Key: SSLi_CA
Intermediate CA Certificate:
Security Device Mode: Transparent Firewall
Outbound Interface: Ethernet 1

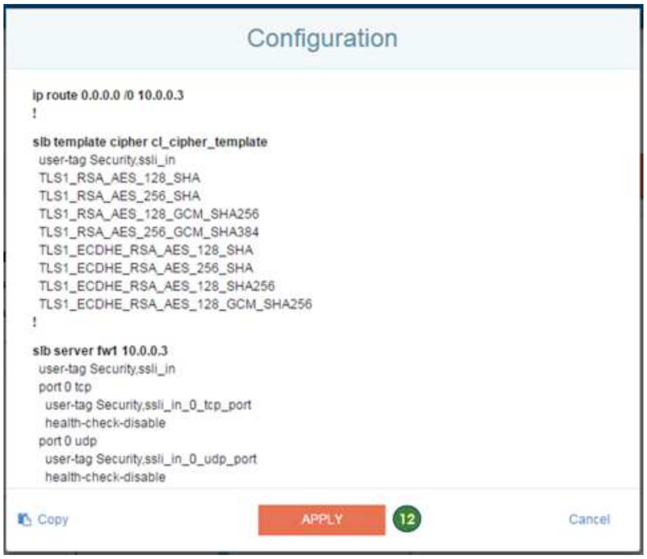
Re-Encryption
Inbound Interface: Ethernet 2
Inbound/Outbound IP Address: 10.0.0.3 /24
Outbound Interface: Ethernet 6
Default Gateway: 10.0.0.4

Bypass Configuration
2 Bypassed Categories
0 Bypassed Domains
0 Bypassed IPs

TOPOLOGY : L2 ,Single Path

Figure 11: Wizard – Confirm

12. 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.



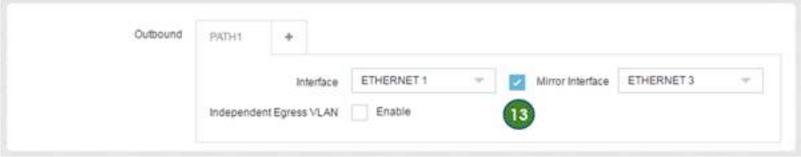
Configuration

```
ip route 0.0.0.0 /0 10.0.0.3
!
slb template cipher cl_cipher_template
 user-tag Security,ssli_in
 TLS1_RSA_AES_128_SHA
 TLS1_RSA_AES_256_SHA
 TLS1_RSA_AES_128_GCM_SHA256
 TLS1_RSA_AES_256_GCM_SHA384
 TLS1_ECDHE_RSA_AES_128_SHA
 TLS1_ECDHE_RSA_AES_256_SHA
 TLS1_ECDHE_RSA_AES_128_SHA256
 TLS1_ECDHE_RSA_AES_128_GCM_SHA256
!
slb server fw1 10.0.0.3
 user-tag Security,ssli_in
 port 0 tcp
  user-tag Security,ssli_in_0_tcp_port
  health-check-disable
 port 0 udp
  user-tag Security,ssli_in_0_udp_port
  health-check-disable
```

Figure 12: Wizard – Confirm

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

13. At this point, you can configure the mirrored port to send traffic out to the Fidelis Direct sensor. In the decryption section, go to the Outbound interface settings and select the check box for Mirror Interface next to Ethernet 1. Select Ethernet 3 as your mirrored interface. This configuration will ensure that decrypted traffic flowing both ways through Ethernet 1 is mirrored onto Ethernet 3, enabling Fidelis Direct to inspect the traffic in clear text.



Outbound: PATH1 +

Interface: ETHERNET 1 ☑ Mirror Interface: ETHERNET 3

Independent Egress VLAN: □ Enable

Figure 13: Configuration – Mirror Interface configuration

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

Fidelis Network Configuration

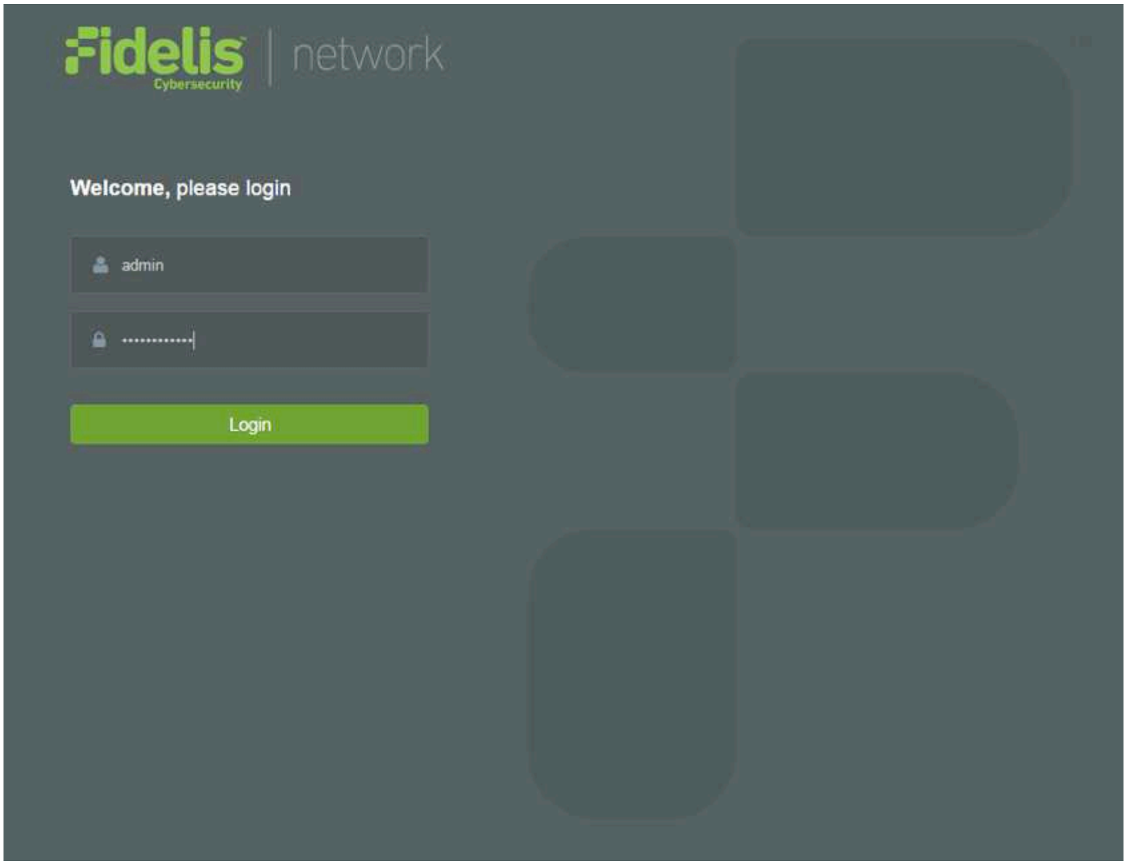
Accessing CommandPost GUI

To access the Fidelis CommandPost GUI, use a web browser and navigate to the management IP via HTTPS only.

Default access credentials are:

Username: admin

Password: system



Welcome, please login

admin

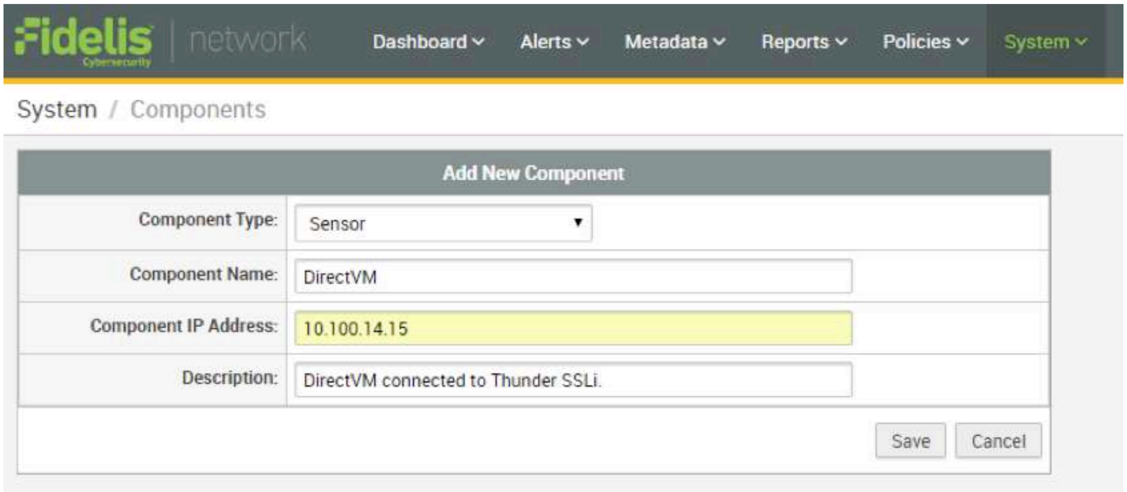
············

Figure 14: CommandPost login page

Note: *If the Fidelis devices are virtual machines being installed on a hypervisor, e.g., VMware ESXi, make sure the network adapters are of the E1000 kind and not the VMXNET3, as Fidelis does not support the latter.*

Connecting the Direct Sensor and Collector to CommandPost

To add a new Direct sensor to the CommandPost, navigate to System > Components > Add Component and enter the required information.



System / Components

Add New Component

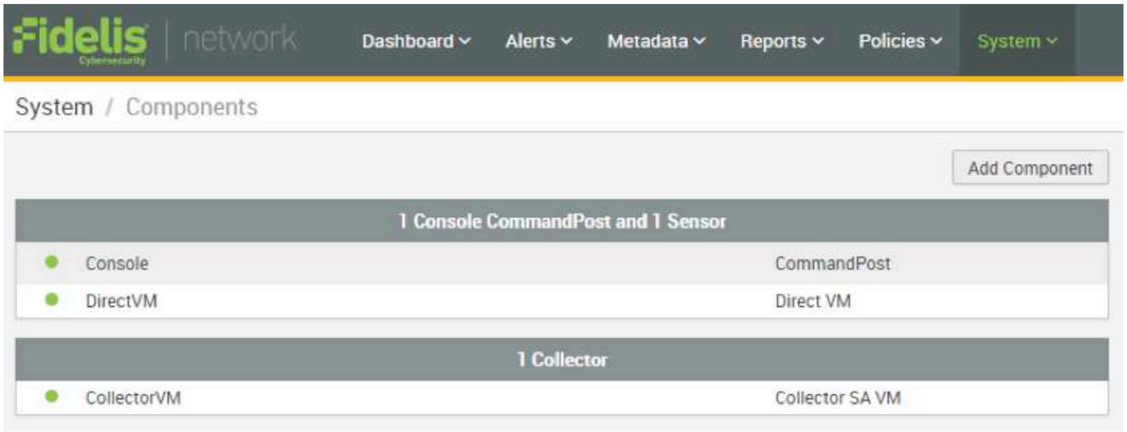
Component Type:	Sensor ▾
Component Name:	DirectVM
Component IP Address:	10.100.14.15
Description:	DirectVM connected to Thunder SSLi.

Figure 15: Adding a device on the CommandPost

After installation, the devices will be visible under the **System > Components** menu. At this point, register all components using the management IP address of each of the components. This ensures that the devices are connected to the CommandPost and relevant communications between all of the components are working.

Once the devices are installed and registered, their state is shown as follows:

- Green – Device installed and functioning properly.
- Red – Device is not functioning properly.
- Orange – System being updated. For example, the Direct sensor will be shown as orange when the policy database is being updated onto it.



System / Components

1 Console CommandPost and 1 Sensor		
●	Console	CommandPost
●	DirectVM	Direct VM

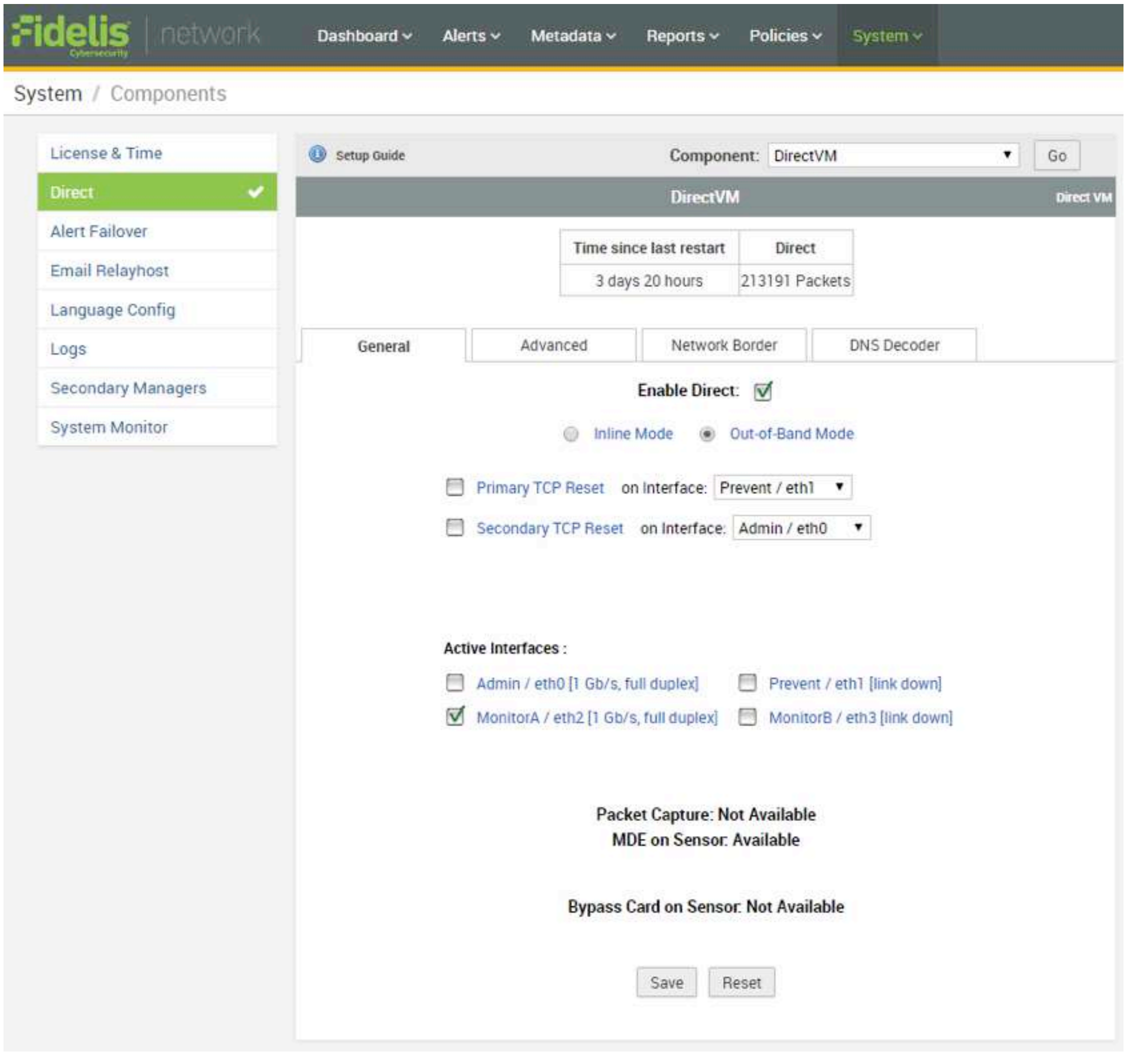
1 Collector		
●	CollectorVM	Collector SA VM

Figure 16: Components screen displaying all installed Fidelis components

Configuring the Direct Sensor

To configure the Direct sensor, navigate to **System > Components > Direct > Config.** Configure the following options:

1. Check the **Enable Direct** option to enable the device.
2. Select **Out-of-Band Mode** for passive deployment.
3. Select **Monitor A / eth2** as your Active interface. This ensures that the device can capture traffic coming in from Thunder SSLi.



Component: DirectVM

Time since last restart	Direct
3 days 20 hours	213191 Packets

Enable Direct: ☑

○ Inline Mode ● Out-of-Band Mode

□ Primary TCP Reset on Interface: Prevent / eth1

□ Secondary TCP Reset on Interface: Admin / eth0

Active Interfaces :

□ Admin / eth0 [1 Gb/s, full duplex] □ Prevent / eth1 [link down]

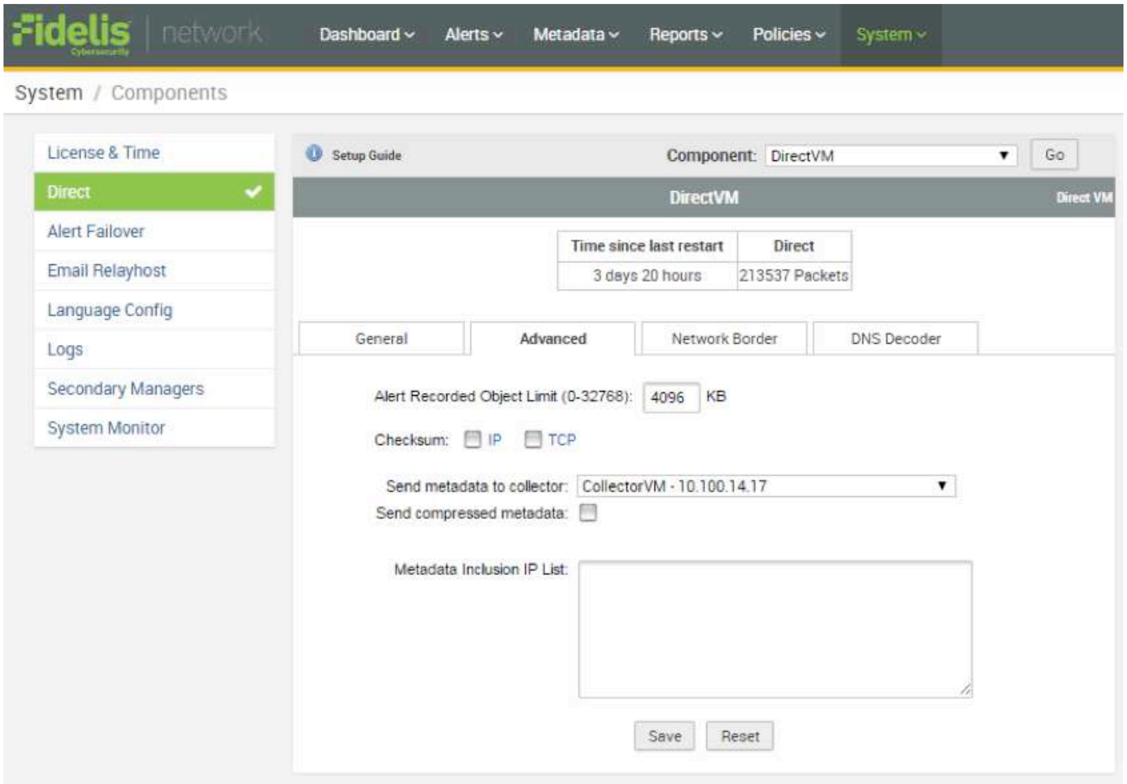
☑ MonitorA / eth2 [1 Gb/s, full duplex] □ MonitorB / eth3 [link down]

Packet Capture: Not Available
MDE on Sensor: Available

Bypass Card on Sensor: Not Available

Figure 17: Direct sensor interface configuration

Once the interfaces are configured, move to the **Advanced** settings tab. Here, the Direct sensor can be connected to the Fidelis Collector, to feed metadata, collected from the sensor, into the Collector.



Component: DirectVM

Time since last restart	Direct
3 days 20 hours	213537 Packets

Alert Recorded Object Limit (0-32768): 4096 KB

Checksum: □ IP □ TCP

Send metadata to collector: CollectorVM - 10.100.14.17

Send compressed metadata: □

Metadata Inclusion IP List:

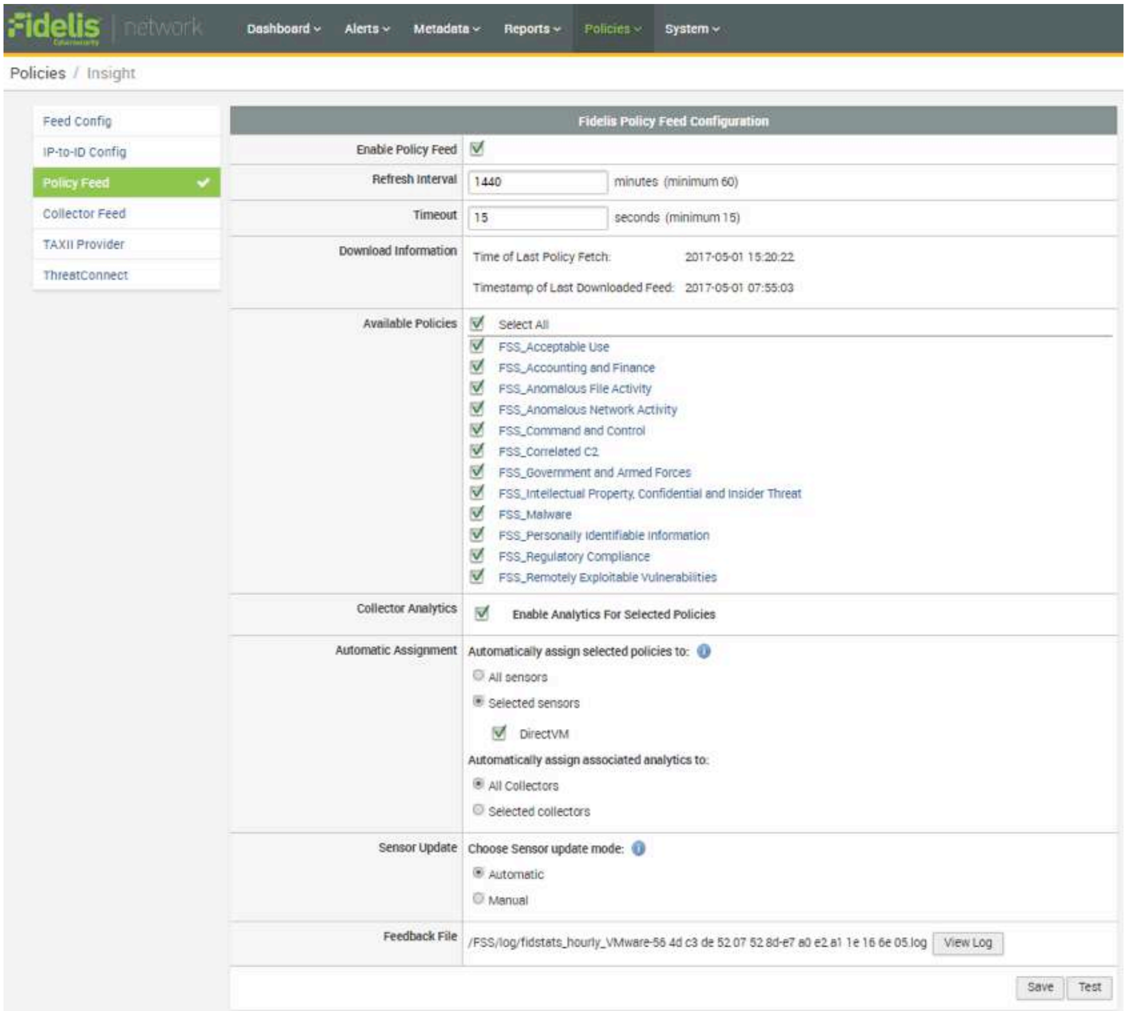
Figure 18: Connecting Fidelis Direct to the Collector

Configuring the Policies

Fidelis allows for users to generate detailed custom rules and policies. Policies can be created in the **Policies** section. Rules created in the **Rules** section can be assigned to the relevant policies. Once ready, these policies can be assigned to a sensor, i.e., Fidelis Direct through the **Assignments** section. Details about this can be found in the ***Fidelis Network Guide to Creating Policies***.

For this deployment, the default Rules and Policies are used for detection purposes. Navigate to **Policies > Insight > Policy Feed** and follow these steps:

1. Check the **Enable Policy Feed** option.
2. You can choose which policies to use in the **Available Policies** section. This list will be updated once the initial download is made from the Fidelis Cloud. Make sure you have Internet connectivity through your management network.
3. In the **Automatic Assignment** section, look for your sensor, i.e., the Direct sensor. You can either select a specific sensor or select **All sensors**.
4. Save the settings.



Fidelis Policy Feed Configuration

Enable Policy Feed ☑

Refresh Interval 1440 minutes (minimum 60)

Timeout 15 seconds (minimum 15)

Download Information
Time of Last Policy Fetch: 2017-05-01 15:20:22
Timestamp of Last Downloaded Feed: 2017-05-01 07:55:03

Available Policies
- ☑ Select All
- ☑ FSS_Acceptable Use
- ☑ FSS_Accounting and Finance
- ☑ FSS_Anomalous File Activity
- ☑ FSS_Anomalous Network Activity
- ☑ FSS_Command and Control
- ☑ FSS_Correlated C2
- ☑ FSS_Government and Armed Forces
- ☑ FSS_Intellectual Property, Confidential and Insider Threat
- ☑ FSS_Malware
- ☑ FSS_Personally Identifiable Information
- ☑ FSS_Regulatory Compliance
- ☑ FSS_Remotely Exploitable Vulnerabilities

Collector Analytics ☑ Enable Analytics For Selected Policies

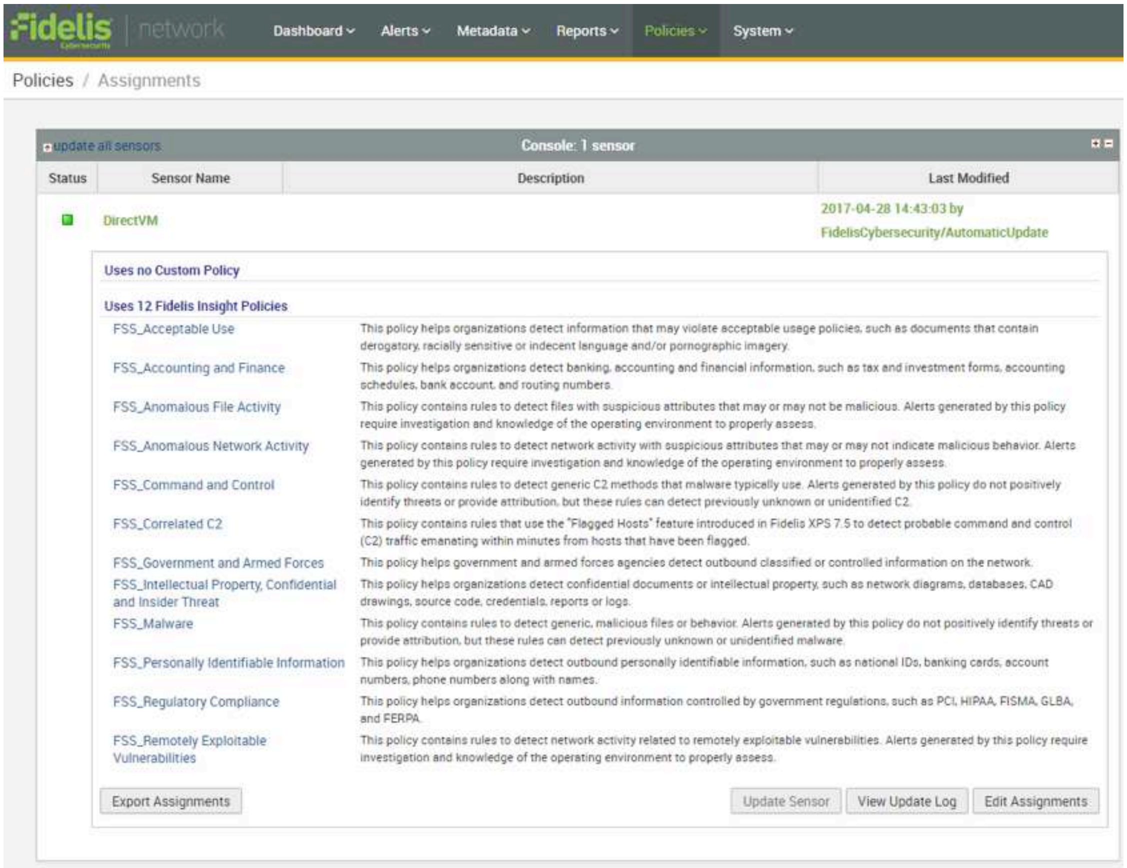
Automatic Assignment
Automatically assign selected policies to:
○ All sensors
● Selected sensors
☑ DirectVM
Automatically assign associated analytics to:
● All Collectors
○ Selected collectors

Sensor Update
Choose Sensor update mode:
● Automatic
○ Manual

Feedback File /FSS/log/fidstats_hourly_VMware-56 4d c3 de 52 07 52 8d-e7 a0 e2 a1 1e 16 6e 05.log

Figure 19: Enabling Policy Feed and downloading policies

Once the policies are downloaded, navigate to **Policies > Assignments** and select your sensor. Click the **Update Sensor** button to update the policies onto the Direct sensor. Once updated, the sensor should look as follows:



Status	Sensor Name	Description	Last Modified
🟩	DirectVM		2017-04-28 14:43:03 by FidelisCybersecurity/AutomaticUpdate

Uses no Custom Policy

Uses 12 Fidelis Insight Policies

FSS_Acceptable Use	This policy helps organizations detect information that may violate acceptable usage policies, such as documents that contain derogatory, racially sensitive or indecent language and/or pornographic imagery.
FSS_Accounting and Finance	This policy helps organizations detect banking, accounting and financial information, such as tax and investment forms, accounting schedules, bank account, and routing numbers.
FSS_Anomalous File Activity	This policy contains rules to detect files with suspicious attributes that may or may not be malicious. Alerts generated by this policy require investigation and knowledge of the operating environment to properly assess.
FSS_Anomalous Network Activity	This policy contains rules to detect network activity with suspicious attributes that may or may not indicate malicious behavior. Alerts generated by this policy require investigation and knowledge of the operating environment to properly assess.
FSS_Command and Control	This policy contains rules to detect generic C2 methods that malware typically use. Alerts generated by this policy do not positively identify threats or provide attribution, but these rules can detect previously unknown or unidentified C2.
FSS_Correlated C2	This policy contains rules that use the "Flagged Hosts" feature introduced in Fidelis XPS 7.5 to detect probable command and control (C2) traffic emanating within minutes from hosts that have been flagged.
FSS_Government and Armed Forces	This policy helps government and armed forces agencies detect outbound classified or controlled information on the network.
FSS_Intellectual Property, Confidential and Insider Threat	This policy helps organizations detect confidential documents or intellectual property, such as network diagrams, databases, CAD drawings, source code, credentials, reports or logs.
FSS_Malware	This policy contains rules to detect generic, malicious files or behavior. Alerts generated by this policy do not positively identify threats or provide attribution, but these rules can detect previously unknown or unidentified malware.
FSS_Personally Identifiable Information	This policy helps organizations detect outbound personally identifiable information, such as national IDs, banking cards, account numbers, phone numbers along with names.
FSS_Regulatory Compliance	This policy helps organizations detect outbound information controlled by government regulations, such as PCI, HIPAA, FISMA, GLBA, and FERPA.
FSS_Remotely Exploitable Vulnerabilities	This policy contains rules to detect network activity related to remotely exploitable vulnerabilities. Alerts generated by this policy require investigation and knowledge of the operating environment to properly assess.

Figure 20: Updating policies on the sensor

For details on other Fidelis configuration options, refer to ***Fidelis Network Enterprise Setup and Configuration Guide***.

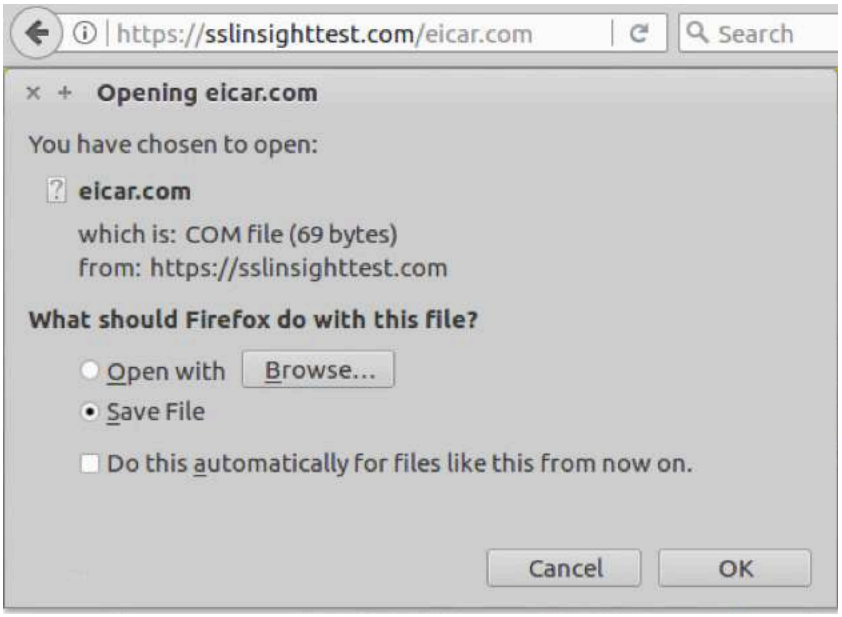
Verification

To verify that the Fidelis Network solution is working properly with Thunder SSLi and has gained visibility into encrypted traffic, you can conduct a simple test. Accessing a test malware file, e.g., eicar.com, hosted on the Ubuntu Server in this deployment, will help you ensure that encrypted threats can be seen by Fidelis with the introduction of the Thunder SSLi device. You can also use the test malware website www.wicar.org.

Note*: This setup is only going to detect the threat and issue an alert. It will not prevent an intrusion or infection by malware. For details on how to configure the Fidelis Direct sensor to prevent intrusions, refer to* ***Fidelis Network Enterprise Setup and Configuration Guide****.*

For this test case, open a web browser window on the client machine and access the malware file hosted on the server machine using HTTPS. We will access the file by accessing the URL https://sslinsighttest.com/eicar.com.

Since we are only detecting traffic and not preventing attacks in this use case, we will be able to download the file onto the client machine.



https://sslinsighttest.com/eicar.com

Search

Opening eicar.com

You have chosen to open:

eicar.com

which is: COM file (69 bytes)
from: https://sslinsighttest.com

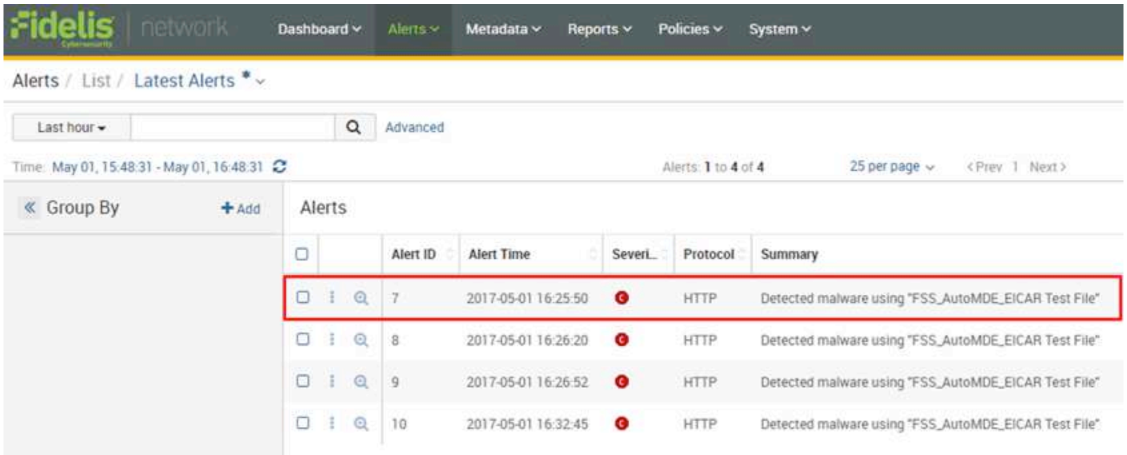
What should Firefox do with this file?

○ Open with Browse...
● Save File
□ Do this automatically for files like this from now on.

Cancel OK

Figure 21: Download allowed on the client machine

However, there will be an alert issued, which can be seen on the Fidelis CommandPost by navigating to **Alerts > List**. If no Thunder SSLi is present in the network to decrypt traffic for the Fidelis sensors, no alerts will be issued since the Fidelis sensors are blind to encrypted traffic.



Time: May 01, 15:48:31 - May 01, 16:48:31

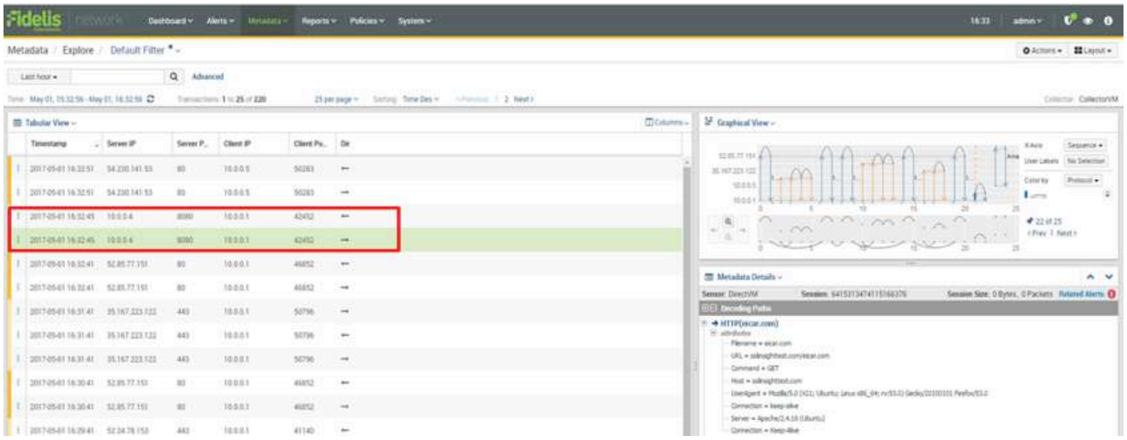
Alerts: 1 to 4 of 4 25 per page ‹Prev 1 Next›

Alerts

□		Alert ID	Alert Time	Severi...	Protocol	Summary
□		7	2017-05-01 16:25:50	●	HTTP	Detected malware using "FSS_AutoMDE_EICAR Test File"
□		8	2017-05-01 16:26:20	●	HTTP	Detected malware using "FSS_AutoMDE_EICAR Test File"
□		9	2017-05-01 16:26:52	●	HTTP	Detected malware using "FSS_AutoMDE_EICAR Test File"
□		10	2017-05-01 16:32:45	●	HTTP	Detected malware using "FSS_AutoMDE_EICAR Test File"

Figure 22: Alerts issued by Fidelis for multiple accesses to the eicar.com file from the client machine

To confirm that Fidelis is receiving traffic decrypted by Thunder SSLi, navigate to **Metadata > Explore**. Any traffic with the Server Port Number set to 8080 will be the traffic decrypted by Thunder SSLi. Normal HTTP traffic will have the Server Port Number 80.



Metadata / Explore / Default Filter *

Time: May 01, 15:32:56 - May 01, 16:32:56 Transactions: 1 to 25 of 220 25 per page Sorting: Time Des

Tabular View

Timestamp	Server IP	Server P...	Client IP	Client Po...	Dir
2017-05-01 16:32:51	54.230.141.53	80	10.0.0.5	50283	←
2017-05-01 16:32:51	54.230.141.53	80	10.0.0.5	50283	→
2017-05-01 16:32:45	10.0.0.4	8080	10.0.0.1	42452	←
2017-05-01 16:32:45	10.0.0.4	8080	10.0.0.1	42452	→
2017-05-01 16:32:41	52.85.77.151	80	10.0.0.1	46852	←
2017-05-01 16:32:41	52.85.77.151	80	10.0.0.1	46852	→
2017-05-01 16:31:41	35.167.223.122	443	10.0.0.1	50796	→
2017-05-01 16:31:41	35.167.223.122	443	10.0.0.1	50796	←
2017-05-01 16:31:41	35.167.223.122	443	10.0.0.1	50796	→
2017-05-01 16:30:41	52.85.77.151	80	10.0.0.1	46852	←
2017-05-01 16:30:41	52.85.77.151	80	10.0.0.1	46852	→
2017-05-01 16:29:41	52.24.78.153	443	10.0.0.1	41140	←

Metadata Details

Sensor: DirectVM Session: 6415313474115166376 Session Size: 0 Bytes, 0 Packets Related Alerts

Decoding Paths

```
HTTP(eicar.com)
  attributes
    Filename = eicar.com
    URL = sslinsighttest.com/eicar.com
    Command = GET
    Host = sslinsighttest.com
    UserAgent = Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:53.0) Gecko/20100101 Firefox/53.0
    Connection = keep-alive
    Server = Apache/2.4.18 (Ubuntu)
    Connection = Keep-Alive
```

Figure 23: Traffic decrypted by Thunder SSLi uses Port 8080

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 without compromising performance. A wide range of security devices, including Fidelis Network, require visibility into encrypted traffic to discover attacks, intrusions and malware.

This guide provides the detailed steps required to configure A10 Thunder SSL Insight with Fidelis Network's security devices. Once completed, you will be ready to use your new deployment to uncover threats hidden in SSL/TLS traffic.

A10 Thunder SSLi offers organizations a scalable and flexible solution for high-performance SSL inspection. Using Thunder SSLi, organizations can:

- Decrypt once and feed to multiple security devices
- Analyze all network data, including encrypted data, eliminating blind spots in their threat protection solution
- Control what to decrypt based on a policy which includes web category
- Provide advanced SSL inspection features such as URL filtering
- Deploy a comprehensive security solution that can 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 the 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/solutionsheets.php

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

Appendix A

The following sample configurations are based on a single-device configuration, generated by the AppCentric Templates.

A10 Shared Partition Configuration

```
system ve-mac-scheme system-mac
!
partition ssli_in id 1
!
partition ssli_out id 2
!
hostname SSLi
!
mirror-port 1 ethernet 3
!
interface management
  ip address 10.100.9.197 255.255.255.0
  ip default-gateway 10.100.9.1
!
interface ethernet 1
!
interface ethernet 2
!
interface ethernet 3
!
interface ethernet 4
!
interface ethernet 5
!
interface ethernet 6
!
interface ethernet 7
!
interface ethernet 8
!
interface ethernet 9
!
interface ethernet 10
!
interface ethernet 11
!
interface ethernet 12
!
interface ethernet 13
!
interface ethernet 14
!
interface ethernet 15
!
interface ethernet 16
!
interface ethernet 17
!
interface ethernet 18
```

```
!
!
end
```

A10 Inside Partition Configuration

```
active-partition ssli_in
!
!
access-list 190 remark ssli_in
!
access-list 190 permit ip any any vlan 850
!
vlan 850
  untagged ethernet 1
  untagged ethernet 5
  router-interface ve 850
  name ssli_in_ingress_egress
  user-tag Security,ssli_in_ingress_egress
!
interface ethernet 1
  name ssli_in_egress
  enable
  monitor both 1
  user-tag Security,ssli_in_egress
!
interface ethernet 3
  enable
!
interface ethernet 5
  name ssli_in_ingress
  enable
  user-tag Security,ssli_in_ingress
!
interface ve 850
  name ssli_in_ingress_egress
  user-tag Security,ssli_in_ingress_egress
  ip address 10.0.0.2 255.255.255.0
  ip allow-promiscuous-vip
!
!
ip route 0.0.0.0 /0 10.0.0.3
!
slb template cipher cl_cipher_template
  TLS1_RSA_AES_128_SHA
  TLS1_RSA_AES_256_SHA
  TLS1_RSA_AES_128_GCM_SHA256
  TLS1_RSA_AES_256_GCM_SHA384
  TLS1_ECDHE_RSA_AES_128_SHA
  TLS1_ECDHE_RSA_AES_256_SHA
  TLS1_ECDHE_RSA_AES_128_SHA256
  TLS1_ECDHE_RSA_AES_128_GCM_SHA256
  user-tag Security,ssli_in
!
slb server fw1 10.0.0.3
  user-tag Security,ssli_in
  port 0 tcp
    health-check-disable
    user-tag Security,ssli_in_0_tcp_port
  port 0 udp
    health-check-disable
    user-tag Security,ssli_in_0_udp_port
  port 8080 tcp
    health-check-disable
    user-tag Security,ssli_signaling
!
slb service-group SG_SSLi_TCP tcp
  user-tag Security,ssli_in
  member fw1 0
!
slb service-group SG_SSLi_UDP udp
  user-tag Security,ssli_in
  member fw1 0
!
slb service-group SG_SSLi_Xlated tcp
  user-tag Security,ssli_in
  member fw1 8080
!
slb template client-ssl cl_ssl
  template cipher cl_cipher_template
  forward-proxy-ca-cert SSLi_CA
  forward-proxy-ca-key SSLi_CA
  forward-proxy-ocsp-disable
  forward-proxy-crl-disable
  forward-proxy-cert-expiry hours 168
  forward-proxy-enable
  forward-proxy-failsafe-disable
  disable-sslv3
  user-tag Security,ssli_in
!
slb template http insertHeaders
  non-http-bypass service-group SG_SSLi_Xlated
  user-tag Security,ssli_in
!
slb virtual-server SSLi_in_ingress 0.0.0.0 acl 190
  user-tag Security,ssli_in
  port 0 tcp
    service-group SG_SSLi_TCP
    no-dest-nat
    user-tag Security,ssli_in_port_0tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
  port 0 udp
    service-group SG_SSLi_UDP
    no-dest-nat
    user-tag Security,ssli_in_port_0udp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
  port 0 others
    service-group SG_SSLi_UDP
    no-dest-nat
    user-tag Security,ssli_in_port_0others
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
  port 443 https
    service-group SG_SSLi_Xlated
    template http insertHeaders
    template client-ssl cl_ssl
    no-dest-nat port-translation
    user-tag Security,ssli_in_port_443https
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
!
end
```

A10 Outside Partition Configuration

```
active-partition ssli_out
!
!
access-list 191 remark ssli_out
!
access-list 191 permit ip any any vlan 860
!
vlan 860
  untagged ethernet 2
  untagged ethernet 6
  router-interface ve 860
  name ssli_out_ingress_egress
  user-tag Security,ssli_out_ingress_egress
!
interface ethernet 2
  name ssli_out_ingress
  enable
  user-tag Security,ssli_out_ingress
!
interface ethernet 6
  name ssli_out_egress
  enable
  user-tag Security,ssli_out_egress
!
interface ve 860
  name ssli_out_ingress_egress
  user-tag Security,ssli_out_ingress_egress
  ip address 10.0.0.3 255.255.255.0
  ip allow-promiscuous-vip
!
!
ip route 0.0.0.0 /0 10.0.0.4
!
slb template cipher sr_cipher_template
  TLS1_RSA_AES_128_SHA
  TLS1_RSA_AES_256_SHA
  TLS1_RSA_AES_128_GCM_SHA256
  TLS1_RSA_AES_256_GCM_SHA384
  TLS1_ECDHE_RSA_AES_128_SHA
  TLS1_ECDHE_RSA_AES_256_SHA
  TLS1_ECDHE_RSA_AES_128_SHA256
  TLS1_ECDHE_RSA_AES_128_GCM_SHA256
  user-tag Security,ssli_out
!
slb template server-ssl sr_ssl
  forward-proxy-enable
  template cipher sr_cipher_template
  user-tag Security,ssli_out
!
slb server GW 10.0.0.4
  user-tag Security,ssli_out
  port 0 tcp
    health-check-disable
    user-tag Security,ssli_out_0_tcp_port
  port 0 udp
    health-check-disable
    user-tag Security,ssli_out_0_udp_port
  port 443 tcp
    health-check-disable
!
slb service-group GW_SSL_443 tcp
  user-tag Security,ssli_out
  member GW 443
!
slb service-group GW_TCP_0 tcp
  user-tag Security,ssli_out
  member GW 0
!
slb service-group GW_UDP_0 udp
  user-tag Security,ssli_out
  member GW 0
!
slb template http removeHeaders
  non-http-bypass service-group GW_SSL_443
  user-tag Security,ssli_out
!
slb virtual-server SSLi_out_ingress 0.0.0.0 acl 191
  user-tag Security,ssli_out
  port 0 tcp
    service-group GW_TCP_0
    use-rcv-hop-for-resp
    no-dest-nat
    user-tag Security,ssli_out_port_0tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
  port 0 udp
    service-group GW_UDP_0
    use-rcv-hop-for-resp
    no-dest-nat
    user-tag Security,ssli_out_port_0udp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
  port 0 others
    service-group GW_UDP_0
    use-rcv-hop-for-resp
    no-dest-nat
    user-tag Security,ssli_out_port_0others
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
  port 443 tcp
    service-group GW_TCP_0
    use-rcv-hop-for-resp
    no-dest-nat
    user-tag Security,ssli_out_port_443tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
  port 8080 http
    service-group GW_SSL_443
    use-rcv-hop-for-resp
    template http removeHeaders
    template server-ssl sr_ssl
    no-dest-nat port-translation
    user-tag Security,ssli_out_port_8080http
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
!
end
```

Appendix B

SSL Insight Technology Two-Device Deployment

In this deployment guide, the focus is on the SSL Insight technology single-device deployment, where ADPs are used in place of separate devices for decryption and re-encryption. An **SSLi 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 a Fidelis Direct sensor
- URL Classification Service for URL filtering and bypassing

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

- Re-encrypting traffic that has been inspected by the Fidelis Direct sensor
- Forwarding the re-encrypted traffic to the gateway route

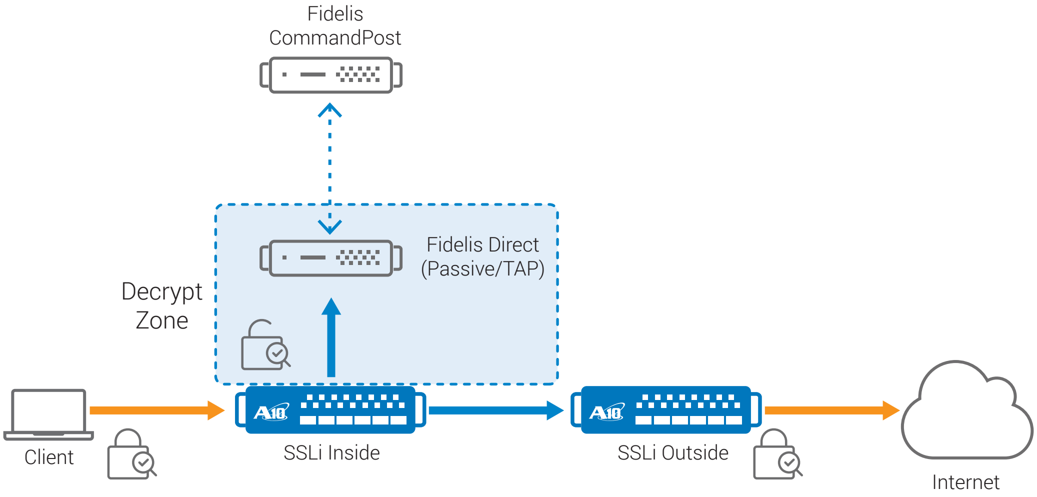


Figure 24: SSL Insight technology in a two-device deployment

***Note**: The SSLi two-device deployment can be configured using the CLI or GUI. 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 Thunder SSLi 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, as EP can perform normal proxy functions without decrypting traffic (e.g., URL filtering based on user/group information).

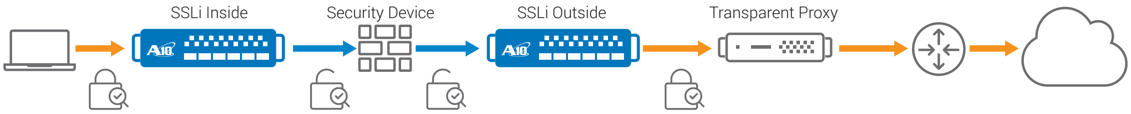


Figure 25: SSLi in a two-device deployment with Transparent Proxy Outside decrypt zone

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 clear-text traffic and traffic that was decrypted by SSLi Inside. The Inside device inserts a header in the traffic when decrypted. This enables the Outside device to differentiate between different traffic types and helps in correctly re-encrypting the traffic.

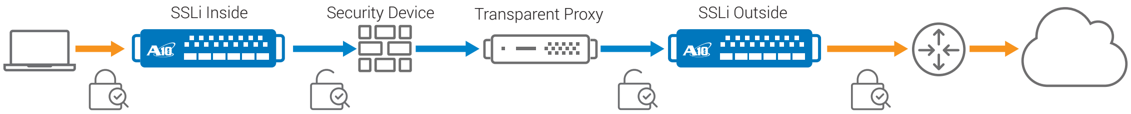


Figure 26: SSLi in a two-device deployment with Transparent Proxy Inside decrypt zone

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, and it is configured on the wildcard virtual IP (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.

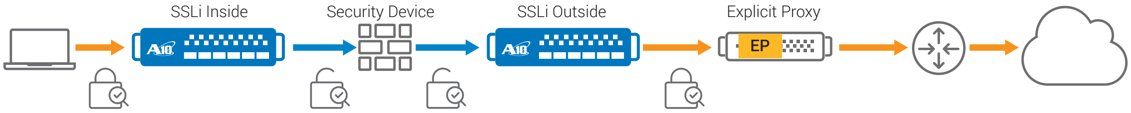


Figure 27: SSLi in a two-device deployment with Explicit Proxy Outside decrypt zone

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

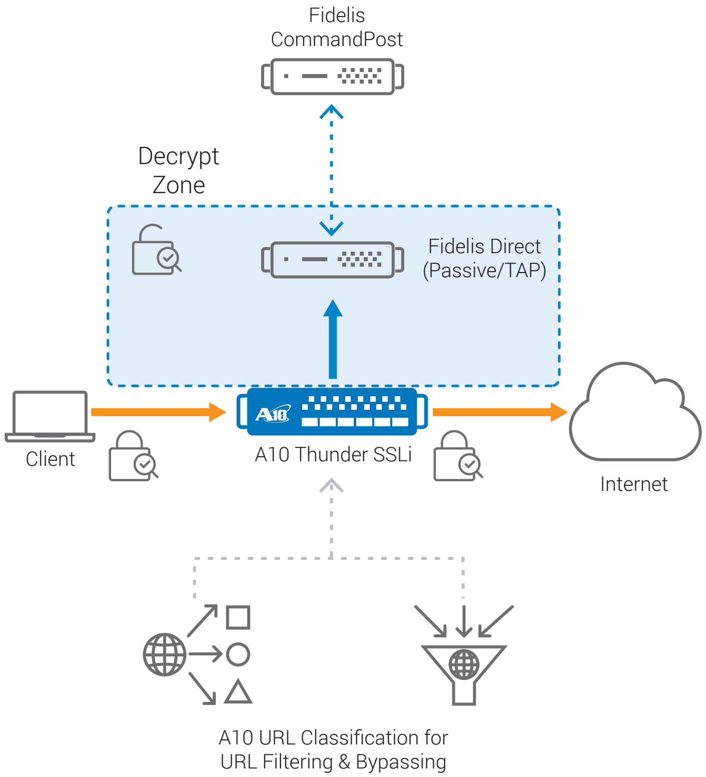


Figure 28: A10 URL Classification for URL filtering and bypassing

SSL Insight technology includes an optional paid subscription service called A10 URL Classification Service. With this service, you can 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 license (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 ssli-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 is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: **www.a10networks.com**

Corporate Headquarters

A10 Networks, Inc
3 West Plumeria Ave.
San Jose, CA 95134 USA
Tel: +1 408 325-8668
Fax: +1 408 325-8666
www.a10networks.com

Part Number: A10-DG-16162-EN-01
May 2017

Worldwide Offices

North America
sales@a10networks.com
Europe
emea_sales@a10networks.com
South America
latam_sales@a10networks.com
Japan
jinfo@a10networks.com
China
china_sales@a10networks.com
Hong Kong
hongkong@a10networks.com
Taiwan
taiwan@a10networks.com
Korea
korea@a10networks.com
South Asia
southasia@a10networks.com
Australia/New Zealand
anz_sales@a10networks.com

To discover how A10 Networks products will enhance, accelerate and secure your business, contact us at a10networks.com/contact or call to speak with an A10 sales representative.