A10 Networks

Thunder Series

RSA Ready Implementation Guide for RSA Security Analytics

Last Modified: February 19th, 2015

Partner Information

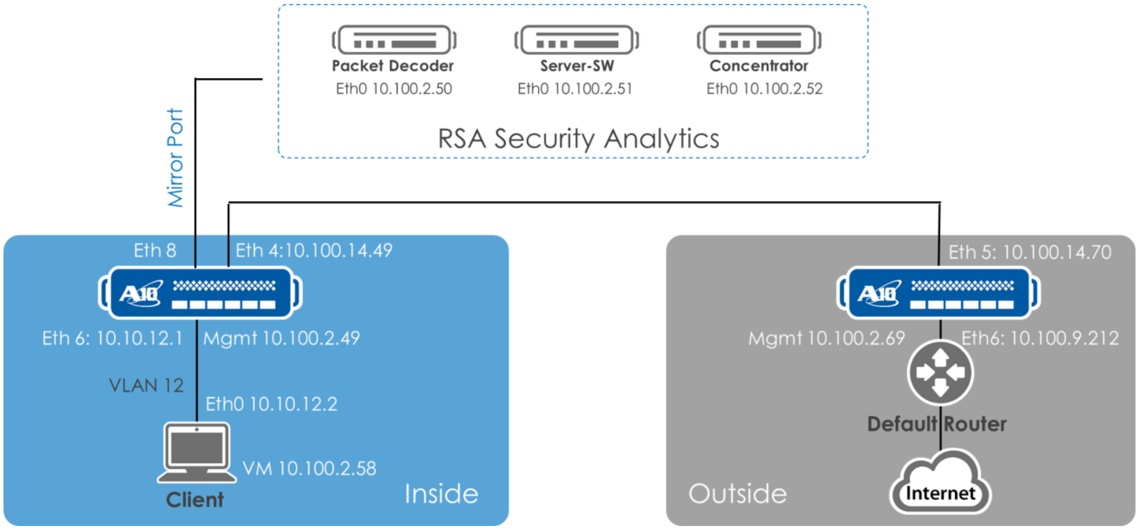
Product Information	
Partner Name	A10 Networks
Web Site	www.a10networks.com
Product Name	Thunder Series
Version & Platform	ACOS 2.7.2 P2-SP1 or higher
Product Description	A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure.

Solution Summary

A wide range of security devices require visibility into network traffic—including encrypted traffic--to discover attacks, intrusions, and data exfiltration. Growing SSL bandwidth, coupled with increasing SSL key lengths and more computationally complex SSL ciphers, make it difficult for even the most powerful inline security devices to decrypt SSL traffic. On top of today's SSL performance challenges, many types of security devices are deployed non-inline to monitor network traffic. Often, these devices cannot decrypt outbound SSL traffic. To eliminate the SSL blind spot in corporate defenses, A10 Networks® has introduced SSL Insight™, a feature included in the A10 Thunder® Application Delivery Controller (ADC) product line. A10 Networks SSL Insight decrypts SSL traffic and enables third party security products to inspect the unencrypted traffic. When configured for SSL Insight, the Thunder ADC intercepts SSL traffic, decrypts it and forwards it to a security device such as a firewall, an Intrusion Prevention System (IPS) or an advanced threat prevention platform. Thunder ADC can also mirror the unencrypted traffic to non-inline security devices such as analytics or forensics products. A second Thunder ADC appliance then takes this traffic and encrypts it again, and sends it to the remote destination. Using A10's Application Delivery Partitions (ADPs), SSL Insight can be configured with a single Thunder ADC appliance for encryption, decryption, and load balancing.

A10 Thunder ADC empowers customers to gain SSL visibility by intercepting SSL traffic and sending unencrypted traffic for inspection and analysis.

- Uncover threats concealed in encrypted traffic by decrypting SSL traffic at high speeds
- Investigate, prioritize and remediate incidents with unprecedented precision and speed
- Detect and analyze even the most advanced attacks before they can impact the business
- Scale RSA Security Analytics deployments with load balancing



Graphic 1: Security Analytics and Thunder Lab Topology

Partner Product Configuration

Introduction

This section illustrates a joint solution of A10 Networks Thunder ADCs and RSA Security Analytics for SSL Insight. The SSL Insight services are provided by the Thunder ADC appliances while the packet inspection and classification services are provided by the RSA Security Analytics devices.

SSL Insight (aka SSL Intercept) is an important technology that enables the A10 Thunder Application Delivery Controller (ADC) to intercept and decrypt SSL traffic sent between users and web servers, allowing third-party security devices to gain full visibility into encrypted traffic. By decrypting enterprise traffic, SSL Insight eliminates the SSL blind spot in corporate defenses.

Note: For HTTP content that is gzip encoded, some of the associated metadata may not be available in Security Analytics. It is possible however to fully reconstitute the decrypted TCP session when performing an investigation.

Before You Begin

This section provides instructions for configuring the A10 Networks with RSA Security Analytics. This document does not intend to suggest optimum installations or configurations for RSA and A10 devices. The details provided in this implementation are in working order as long as the assumed requirements are followed by the administrator.

It is assumed that administrator has a working knowledge of RSA Security Analytics and A10 Networks ADC, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

It is strongly suggested that all the RSA Security Analytics systems are installed first and are fully tested prior to the SSL insight integration with A10 ADC.

Configuring the A10 Thunder Series Device

This section describes how to log into the Thunder Series device. The Thunder device can be accessed either from a Command Line Interface (CLI) or 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 over the network using either of the following protocols:
  - **Secure protocol** – Secure Shell (SSH) version 2
  - **Unsecure protocol** – Telnet (if enabled)
- **GUI** – Web-based interface in which you click to access configuration or management pages and type or select values to configure or manage the device. You can access the GUI using the following protocol:
  - **Secure protocol** – Hypertext Transfer Protocol over Secure Socket Layer (HTTPS)

Default Access Information:

- Default Username: “*admin”*
- Default password: “*a10*”

- Default IP Address of the device: “*172.31.31.31*”

> **Note: HTTP requests are redirected to HTTPS by default on the Thunder device. For detailed information on how to access the Thunder Series device, refer to document *A10 Networks Thunder Series System Configuration and Administration Guide*.**

SSL Insight with an Inline Security Deployment

The objective of the SSL Insight feature is to transparently intercept SSL traffic, decrypt it and send it through the security device(s) in clear text. After the security device has inspected the intercepted traffic, it is re-encapsulated in SSL and sent to the destination.

There are three distinct stages for traffic in such a solution, depicted in **Error! Reference source not found.**:

1) From client to the internal Thunder ADC appliance, where traffic is encrypted

2) From the internal Thunder ADC appliance to the external Thunder ADC appliance, through the security device. Traffic is in clear text in this segment

3) Traffic from the external Thunder ADC appliance to the remote server, where traffic is encrypted again.

Configuration Overview

CA Certification

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

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

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

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

```
openssl genrsa -out <name>.key

openssl req -new -x509 -days 3650 -key <name>.key -out <name>.crt
```

Once generated, the certificate can be imported onto the Thunder ADC appliances in the internal zone using SFTP or SCP.

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

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

Note: Further details for Group Policy Manager can be found at:
http://technet.microsoft.com/en-us/library/cc772491.aspx

SSL Insight Configuration

One of the primary requirements to enable SSL Insight with A10 is that client-SSL and server-SSL templates are required on the internal (depcryptor) and the external(encryptor) Thunder ADC appliances respectively and SSL traffic is intercepted.

This guide discusses the configuration of only one external Thunder ADC Appliance and one internal Thunder ADC Appliance. The internal Thunder ADC has a mirrored port configured to send traffic to the RSA Security Analytics. The outside Thunder accepts all the unencrypted traffic from the inside Thunder and sends the requested URL to the internet.

SSL Insight Configuration on Internal Thunder ADC Appliance

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

- SSL traffic entering on port 443 is intercepted.
  - ♦ Port 443 is defined under a wildcard VIP to achieve this.
- The SSL server certificate is captured during the SSL handshake; all X.509 DN attributes are duplicated, except for the issuer and base64 encoded public key.
  - ♦ Client-SSL template is used for this. The Client-SSL template includes the required command **forward-proxy-enabled**, along with the local CA certificate and its private key which is used for signing dynamically forged certificates.
- Along with the protocol (HTTPS to HTTP), the destination port also gets changed from 443 to 8080.
  - ♦ Service group is defined with port 8080 and bound to the virtual port.
- However, the destination IP (i.e. Internet Server IP) remains unchanged.
  - ♦ The command no-dest-nat port-translation achieves this.
- The incoming SSL traffic is intercepted and decrypted, and is then forwarded in clear text over HTTP on port 8080 through the security device.
- The inside Thunder interface that connects to the outside Thunder has to have a mirrored configuration. The mirror port configuration can be achieve with the following commands:
  - ♦ “mirror-port 1 ethernet 8” (configured on the enable on config mode)
  - ♦ Monitor both 1 (configured on the outgoing interface)

SSL Insight Configuration on External Thunder ADC Appliance

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

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

Configuration Steps for Thunder ADC Appliance

L2/L3 and High Availability on the Thunder ADC Appliances

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

- VLANs and their router interfaces
- Virtual Ethernet (VE) interfaces, which are IP addresses assigned to VLAN router interfaces

Configure the VLANs and add Ethernet and Router Interfaces

Configure the following VLAN parameters:

- VLAN-12: This is the uplink to the client network. Add **router-interface ve 12** along with the Ethernet interface.

- VLAN-1014: This is the path to the outside Thunder ADC Appliances. Add **router-interface ve 1014** along with the Ethernet interface.

- Management interface is separate which is configure as:

```
interface management
ip address 10.100.2.49 255.255.255.0
ip default-gateway 10.100.2.1
```

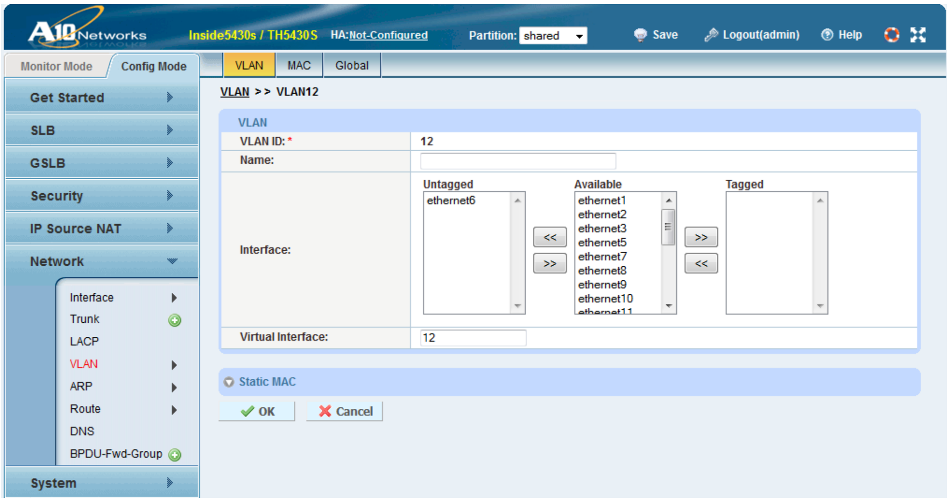
Note: Make sure every interface are reachable before moving forward.

Using the CLI:

```
ACOS(config)#vlan 12
ACOS(config-vlan:10)#untagged ethernet 6
ACOS(config-vlan:10)#router-interface ve 10
ACOS(config-vlan:10)#exit
ACOS(config)#vlan 1014
ACOS(config-vlan:15)#untagged ethernet 4
ACOS(config-vlan:15)#router-interface ve 1014
ACOS(config-vlan:15)#exit
```

Using the GUI:

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



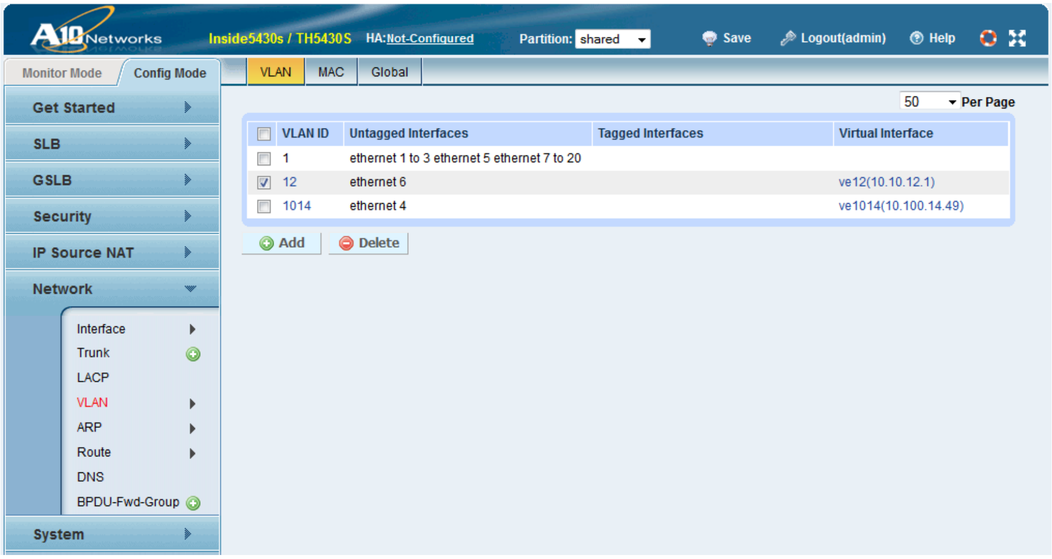
VLAN >> VLAN12

VLAN

VLAN ID: *	12
Name:	
Interface:	Untagged: ethernet6 Available: ethernet1, ethernet2, ethernet3, ethernet5, ethernet7, ethernet8, ethernet9, ethernet10, ethernet11 Tagged:
Virtual Interface:	12

Figure 1. VLAN configuration

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



	VLAN ID	Untagged Interfaces	Tagged Interfaces	Virtual Interface
□	1	ethernet 1 to 3 ethernet 5 ethernet 7 to 20		
☑	12	ethernet 6		ve12(10.10.12.1)
□	1014	ethernet 4		ve1014(10.100.14.49)

Figure 2. VLAN settings

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

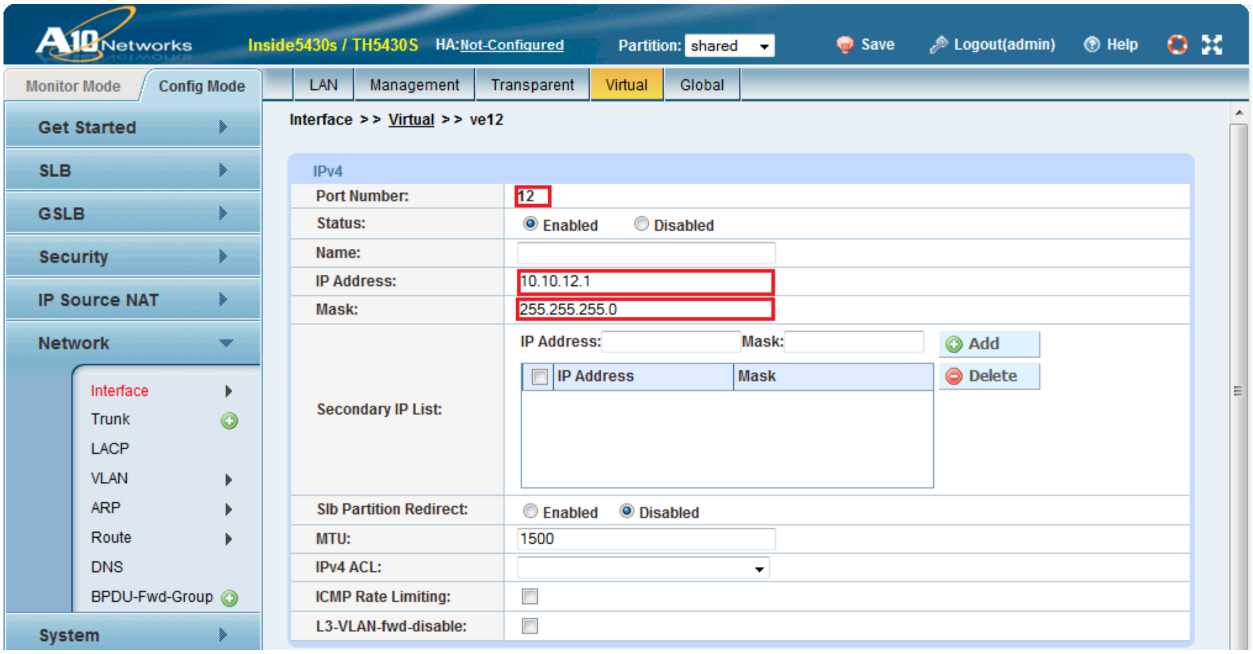
Figure 3. Using the CLI:

```
ACOS(config)#interface ve 12
ACOS(config-if:ve12)#ip address 10.10.12.1 /24
ACOS(config-if:ve12)#ip allow-promiscuous-vip
ACOS(config)#interface ve 1014
```

```
        ACOS(config-if:ve1014)#ip address 10.10.14.49 /24
```

Using the GUI:

1. Navigate to **Config Mode > Interface > Virtual**. The interfaces configured above should be visible.
2. Click on “ve-12” and configure the IPv4 address and mask.
3. Click on **VIP** to display the configuration options.
4. Select Allow Promiscuous VIP.
5. Click **OK** when done.
6. Repeat for each VE.



Interface >> Virtual >> ve12

IPv4

Port Number:	12
Status:	● Enabled ○ Disabled
Name:	
IP Address:	10.10.12.1
Mask:	255.255.255.0
Secondary IP List:	IP Address: Mask: □ IP Address / Mask
Slb Partition Redirect:	○ Enabled ● Disabled
MTU:	1500
IPv4 ACL:	
ICMP Rate Limiting:	□
L3-VLAN-fwd-disable:	□

SSL Insight Configuration on the Thunder ADC Appliances

For SSL Insight deployment the internal Thunder ADC will intercept traffic on TCP port 443, decrypt it, and send it in clear text over TCP port 8080 to the security devices via mirrored port. Consequently, the external Thunder ADC will intercept clear text traffic arriving on TCP port 8080 and encrypt it back before sending it to the remote hosts.

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

Internal Thunder ADC Appliance

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

These steps configure TCP port 8080 and port 0 (TCP/UDP), Under the slb servers configured in FWLB configuration

Using the CLI:

```
ACOS(config)#slb server Externalroute 10.10.100.14.70
ACOS(config-real server)#port 8080 tcp
ACOS(config-real server-node port)#no health-check
ACOS(config-real server)#port 0 tcp
ACOS(config-real server-node port)#no health-check
ACOS(config-real server)#port 0 udp
ACOS(config-real server-node port)#no health-check
```

Using the GUI:

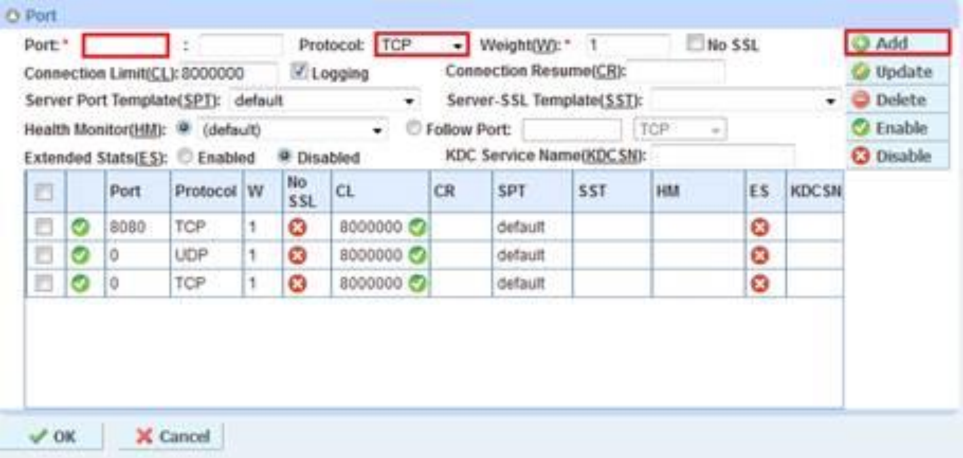
1. Navigate to **Config Mode > SLB > Service > Server**.
2. Select slb server “Externalroute” and click Edit
3. Enter Port parameters:
   - **Port:** "8080"
   - **Protocol:** "TCP"
   - **Health Monitor:** Select blank (disabled).
   - Click **Add**.
4. Enter Port parameters:
   - **Port:** "0"
   - **Protocol:** "TCP"
   - **Health Monitor:** Select blank (disabled).
   - Click **Add**.
5. Enter Port parameters:
   - **Port:** "0"
   - **Protocol:** "UDP"
   - **Health Monitor:** Select blank (disabled).

- Click **Add**.

Note: you can add Port 0/Protocol: Other for ICMP traffic. This is an optional configuration.

Using the GUI:

1. Navigate to **Config Mode > SLB > Service > Server**.
2. Select slb server “Externalroute” and click Edit
3. Enter Port parameters:
    - **Port:** "8080"
    - **Protocol:** "TCP"
    - **Health Monitor:** Select blank (disabled).
    - Click **Add**.
    - **Port:** "0"
    - **Protocol:** "TCP"
    - **Health Monitor:** Select blank (disabled).
    - Click **Add**.
    - **Port:** "0"
    - **Protocol:** "UDP"
    - **Health Monitor:** Select blank (disabled).
    - Click **Add**.
4. Click **OK**.



Port

Port: * ____ : ____ Protocol: TCP Weight(W): * 1 □ No SSL

Connection Limit(CL): 8000000 ☑ Logging Connection Resume(CR):

Server Port Template(SPT): default Server-SSL Template(SST):

Health Monitor(HM): ● (default) ○ Follow Port: TCP

Extended Stats(ES): ○ Enabled ● Disabled KDC Service Name(KDCSN):

□		Port	Protocol	W	No SSL	CL	CR	SPT	SST	HM	ES	KDCSN
□	✓	8080	TCP	1	☒	8000000 ✓		default			☒	
□	✓	0	UDP	1	☒	8000000 ✓		default			☒	
□	✓	0	TCP	1	☒	8000000 ✓		default			☒	

Configure a Service Group

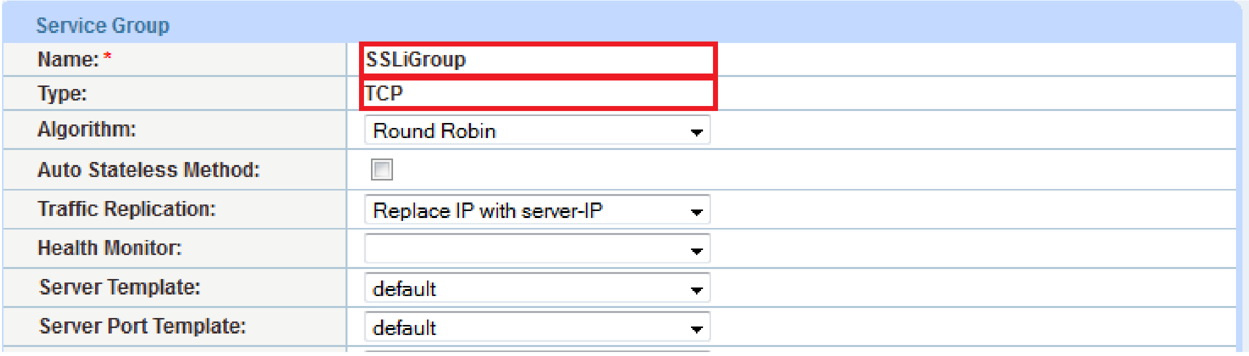
These steps add the servers to a service group.

Using the CLI:

```
ACOS(config)#slb service-group SSLiGroup tcp
ACOS(config-slb svc group)#member SecurityDevice1_Path:8080
ACOS(config-slb svc group)#exit
```

Using the GUI:

1. Navigate to **Config Mode > SLB > Service > Service Group**.
2. Click Add.
3. Enter the following parameters:
   - **Name**: "SSLiGroup"
   - **Type**: "TCP"
4. Click on **Server**.
5. Select the **Server**, "Externalroute", from the drop-down list.
6. Select the **Port**, "8080".
7. Click **OK**.



Service Group

Name: *	SSLiGroup
Type:	TCP
Algorithm:	Round Robin
Auto Stateless Method:	□
Traffic Replication:	Replace IP with server-IP
Health Monitor:	
Server Template:	default
Server Port Template:	default

Figure 4. Service group configuration (internal)

Note: Create service-groups for Port 0 TCP and Port 0 UDP. Make sure you add the server to the service-group by following the same instructions from port 8080. Sample configurations are available in the Appendix.

Configure the Client-SSL Template

These steps configure the client-SSL template. The command **forward-proxy-enable** essentially enables SSL Insight on the client-ssl template.

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

Using the CLI:

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

Using the GUI:

1. Navigate to **Config Mode > SLB > Template > SSL > Client SSL**.

2. Click **Add**.

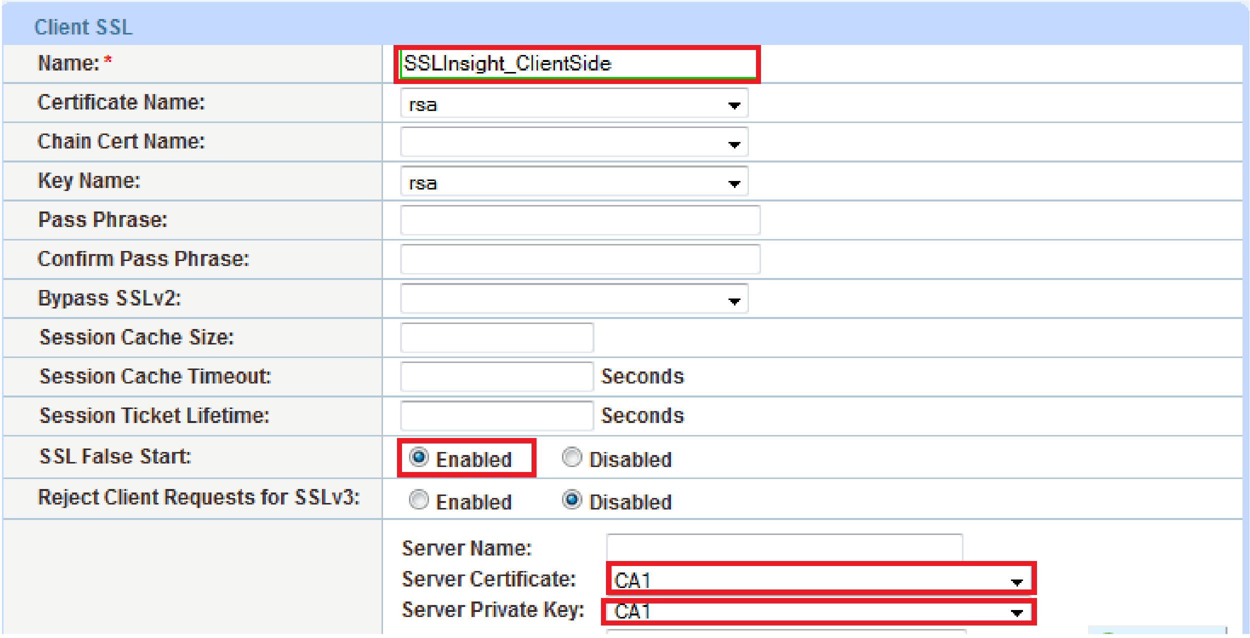
3. Enter a **Name**, "SSLInsight_ClientSide".

4. Select Enabled next to **SSL Forward Proxy**.

5. Select the CA certificate from the **CA Certificate** drop-down list.

6. Select the private key from the **CA Private Key** drop-down list.

7. Click **OK**.



Client SSL

Name: *	SSLInsight_ClientSide
Certificate Name:	rsa
Chain Cert Name:	
Key Name:	rsa
Pass Phrase:	
Confirm Pass Phrase:	
Bypass SSLv2:	
Session Cache Size:	
Session Cache Timeout:	Seconds
Session Ticket Lifetime:	Seconds
SSL False Start:	● Enabled ○ Disabled
Reject Client Requests for SSLv3:	○ Enabled ● Disabled
	Server Name: Server Certificate: CA1 Server Private Key: CA1

Figure 5. Client-SSL configuration (internal)

Configure the Wildcard VIP

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

Using the CLI:

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

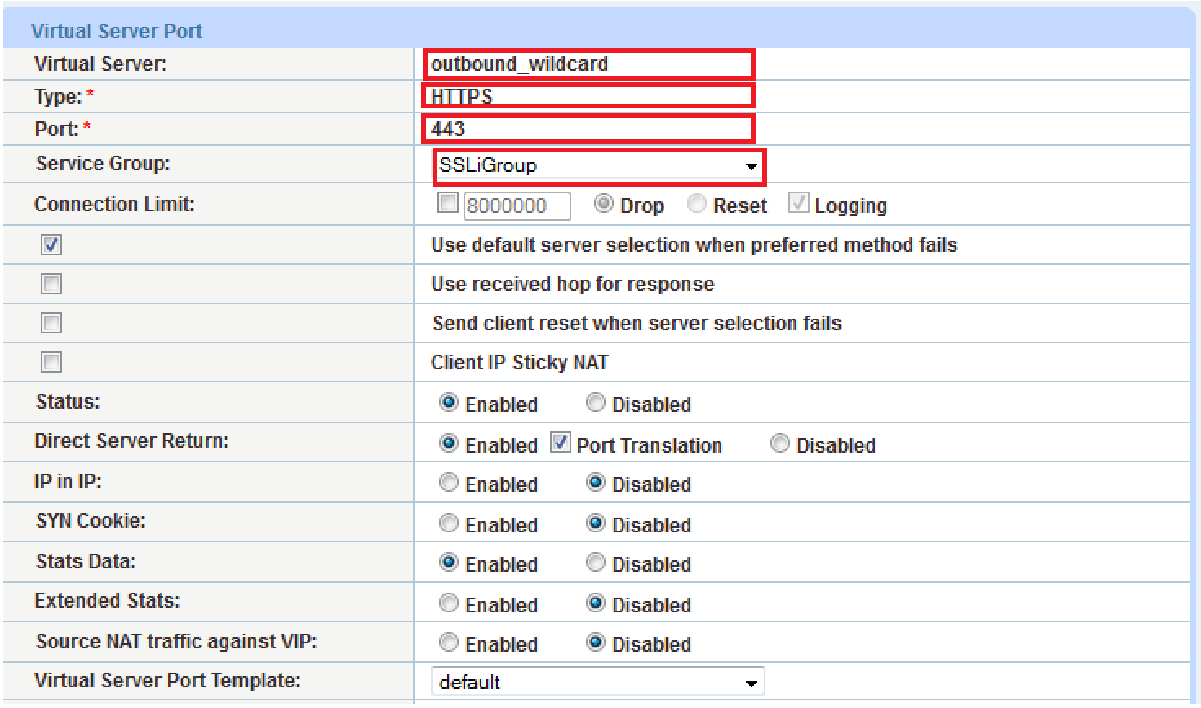
Using the GUI:

1. Navigate to **Config Mode > SLB > Service > Virtual Server**.
2. Select the “Outbound_Wildcard_VIP” and click **Edit**
3. Click **Add** in the **Port** section.
4. Enter or select the following settings:

- **Type:** "HTTPS"
- **Port:** "443"
- **Service Group:** "SSLi"
- **Direct Server Return:** Select Enabled, and select the **Port Translation** checkbox.
- **Client-SSL Template:** “SSLInsight_ClientSide”

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

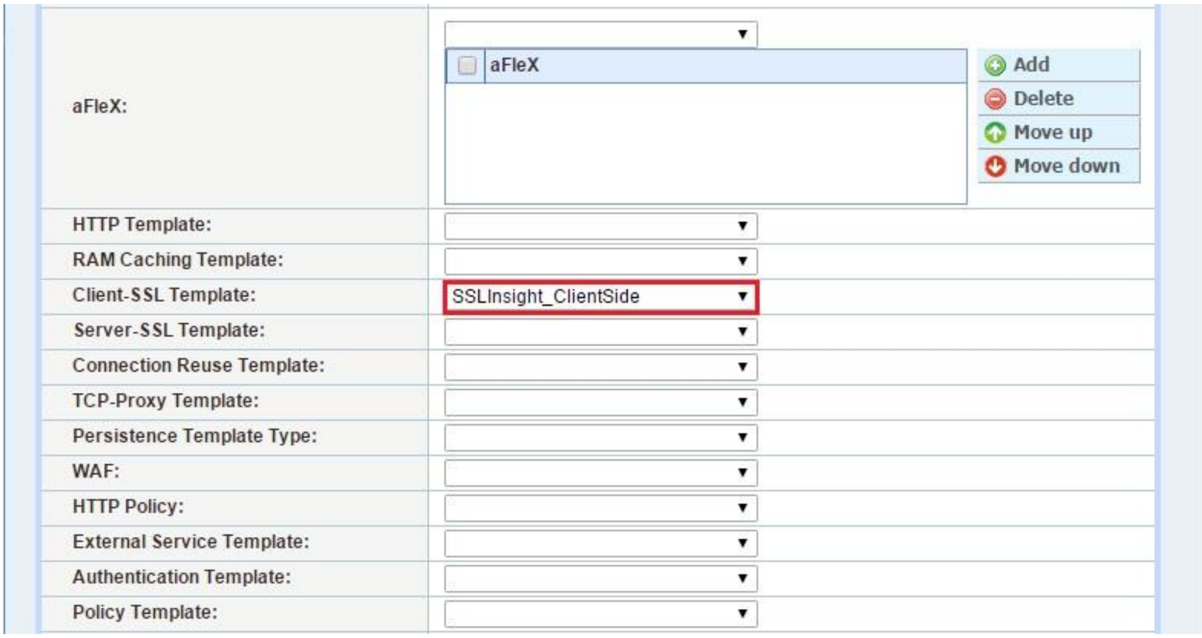
6. Click **OK** to exit the Virtual Server configuration page.



Virtual Server Port

Virtual Server:	outbound_wildcard
Type: *	HTTPS
Port: *	443
Service Group:	SSLiGroup
Connection Limit:	□ 8000000 ● Drop ○ Reset ☑ Logging
☑	Use default server selection when preferred method fails
□	Use received hop for response
□	Send client reset when server selection fails
□	Client IP Sticky NAT
Status:	● Enabled ○ Disabled
Direct Server Return:	● Enabled ☑ Port Translation ○ Disabled
IP in IP:	○ Enabled ● Disabled
SYN Cookie:	○ Enabled ● Disabled
Stats Data:	● Enabled ○ Disabled
Extended Stats:	○ Enabled ● Disabled
Source NAT traffic against VIP:	○ Enabled ● Disabled
Virtual Server Port Template:	default

From the drop down select the Client-SSL Template “SSLInsight_ClientSide”



aFleX:	□ aFleX
HTTP Template:	
RAM Caching Template:	
Client-SSL Template:	SSLInsight_ClientSide
Server-SSL Template:	
Connection Reuse Template:	
TCP-Proxy Template:	
Persistence Template Type:	
WAF:	
HTTP Policy:	
External Service Template:	
Authentication Template:	
Policy Template:	

Figure 6. *Virtual server port configuration (internal)*

Outside Thunder ADC Appliance

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

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

Add TCP Port 443 to the FWLB Gateway Path

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

Using the CLI:

```
ACOS(config)#slb server server-gateway1 10.100.9.1
ACOS(config-real server)#port 443 tcp
ACOS(config-real server-node port)#no health-check
ACOS(config-real server-node port)#exit
ACOS(config-real server)#exit
```

Add the Server Port Configuration to a Service Group

These steps add the server port to a service group.

Using the CLI:

```
ACOS(config)#slb service-group SG_443 tcp
ACOS(config-slb svc group)#member server-gateway1:443
ACOS(config-slb svc group)#exit
```

Configure the Server-SSL Template

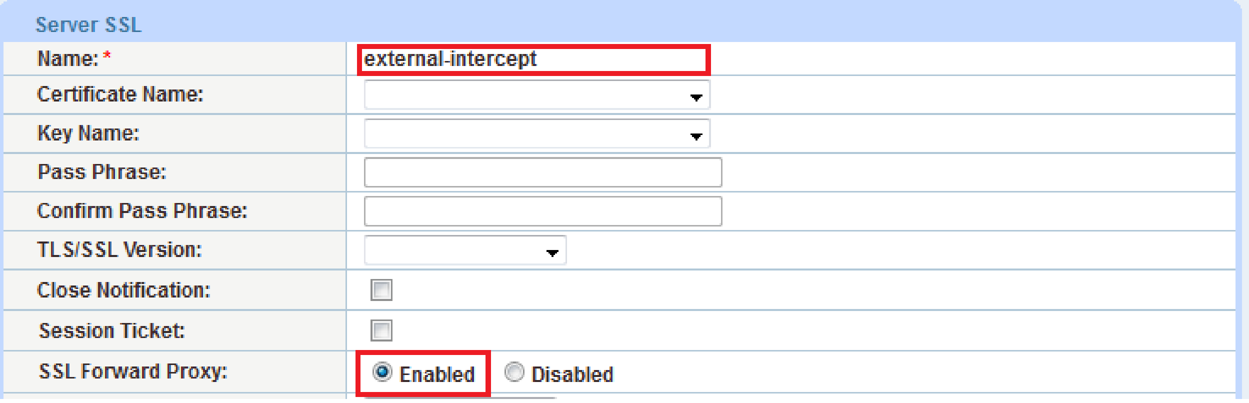
These steps configure the server-SSL template.

Using the CLI:

```
ACOS(config)#slb template server-ssl external-intercept
ACOS(config-server ssl)#forward-proxy-enable
ACOS(config-server ssl)#exit
```

Using the GUI:

1. Navigate to **Config Mode > SLB > Template > SSL > Server SSL**
2. Click **Add**.
3. Enter a **Name**, "**external-intercept**".
4. Select Enabled next to **SSL Forward Proxy**.
5. Leave other fields blank.
6. Click **OK**.



Server SSL

Name: *	external-intercept
Certificate Name:	
Key Name:	
Pass Phrase:	
Confirm Pass Phrase:	
TLS/SSL Version:	
Close Notification:	□
Session Ticket:	□
SSL Forward Proxy:	● Enabled ○ Disabled

Figure 7. *Server-SSL configuration (external)*

Configure the Wildcard VIP

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

Using the CLI:

```
ACOS(config)#slb virtual-server external_in_to_out 0.0.0.0 acl 100
ACOS(config-slb vserver)#port 8080 http
ACOS(config-slb vserver-vport)#service-group SG_443
ACOS(config-slb vserver-vport)#template server-ssl external-intercept
ACOS(config-slb vserver-vport)#no-dest-nat port-translation
ACOS(config-slb vserver-vport)#use-rcv-hop-for-resp
ACOS(config-slb vserver-vport)#exit
ACOS(config-slb vserver)#exit
```

Other Configuration

Below are the instructions required to export self-signed certifcates from Thunder ADC.

From the Thunder ADC Web User Interface (in ACOS version 2.7.2):

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

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

  - Click **Save**.
  - Navigate to the save location.
  - Click **Save** again.
- To export a key:
  - Select the SSL key.
  - Click **Export**.
  - Click **Save**. Navigate to the save location.
  - Click **Save** again.

Summary

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

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

For more information about Thunder ADC products:

- http://www.a10networks.com/products/thunder-series-appliances.php
- http://www.a10networks.com/resources/solutionsheets.php
- http:/www.a10networks.com/resources/casestudies.php

Certification Checklist for RSA Security Analytics

Date Tested: December 18th, 2014

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Security Analytics	10.4	Virtual Appliance
A10 Thunder Series	2.7.2 SP1 P2 or higher	Appliance/Virtual Appliance *
*SSL Insight requires hardware appliance for high performance and better SSL throughput		

Security Analytics Test Case	Result
Outbound SSL Decryption	
HTTPS	
Google Search	✓
Bing Search	✓
Facebook	✓
YouTube	✓
Twitter	✓
LinkedIn	✓
Reddit	✓
WEBMAIL	
GMail	✓
Yahoo	✓
Live	✓
AOL	✓
Inbound SSL Decryption	
HTTPS	
Web Server	✓

JEC/PAR ✓ = Pass ✗ = Fail N/A = Non-Available Function

Known Issues

1. SSL Insight is supported on ACOS versions 2.7.0 and greater. The only version not recommended is ACOS version 2.7.2 P2 because of compatibility issues with SSL Insight. But all other versions greater are supported and the latest version currently available, 2.7.2 P3, is recommended.
2. Based on A10 and RSA integration, Security Analytics can only support in-line/tap-mode using port mirroring configuration from A10.

Appendix

The attached configurations below are quick cli templates that you can use for quick CLI implementations.

Internal ADC Configuration	**External ADC Configuration**
slb server Externalroute 10.100.14.70 port 0 tcp no health-check port 0 udp no health-check port 8080 tcp no health-check ! slb service-group LB_Paths_UDP udp member Externalroute:0 ! slb service-group LB_Paths_TCP tcp member Externalroute:0 ! slb service-group SSLi tcp member Externalroute:8080 ! slb template client-ssl SSLInsight_ClientSide forward-proxy-enable forward-proxy-ca-cert SSLi-CA forward-proxy-ca-key SSLi-CA ! slb virtual-server Outbound_Wildcard_VIP 0.0.0.0 acl 100 port 0 tcp service-group LB_Paths_TCP no-dest-nat port 0 udp service-group LB_Paths_UDP no-dest-nat port 443 https service-group SSLi template client-ssl SSLInsight_ClientSide no-dest-nat port-translation ! end	slb server server-gateway1 10.100.9.1 port 0 tcp no health-check port 0 udp no health-check port 8080 tcp no health-check slb service-group SG_UDP udp member server-gateway1:0 ! slb service-group LB_Paths_TCP tcp member server-gateway1:0 ! slb service-group SSLi tcp member server-gateway1:8080 ! slb template client-ssl SSLInsight_ClientSide forward-proxy-enable forward-proxy-ca-cert SSLi-CA forward-proxy-ca-key SSLi-CA ! slb virtual-server external_in_to_out 0.0.0.0 acl 100 port 0 tcp service-group SG_TCP no-dest-nat port 0 udp service-group SG_UDP no-dest-nat port 8080 http service-group SG_443 template server-ssl external-intercept no-dest-nat port-translation ! End