DEPLOYMENT GUIDE

HOW TO DEPLOY A10 NETWORKS SSLI AND DIGITAL GUARDIAN NETWORK DLP APPLIANCE

A COMPREHENSIVE WEB MONITORING AND CONTROL SOLUTION

OVERVIEW

Digital Guardian provides a threat-aware data protection platform to monitor and prevent the misuse, accidental disclosure, or theft of sensitive data throughout the extended enterprise. This threat-aware platform provides comprehensive data protection solutions and controls for both insider and outsider risks. Whether data is stored and used at the endpoint, accessed remotely from a shared server, stored in a database repository, copied to removable media, attached to an email, or in the cloud, Digital Guardian provides solutions for your sensitive data challenges.

A10 Networks has partnered with Digital Guardian to provide comprehensive web monitoring and control solution. Digital Guardian appliances incorporate inline web inspection that integrates with the A10 Networks proxy to provide policy-based web monitoring and control. All traffic is inspected for sensitive content, and administrators can set up incident management workflow to automate response actions in the event policy violations occur.

TALK
WITH A10

CONTACT US
a10networks.com/contact

TABLE OF CONTENTS

OVERVIEW 2

DEPLOYMENT PREREQUISITES 4

ARCHITECTURE OVERVIEW 4

SSLi 4

SSLi with ICAP 5

SSLi with AAM 6

ACCESSING THUNDER SSLI 6

CONFIGURATION OVERVIEW 7

Basic SSLi Configuration 8

ICAP Client Configuration 14

AAM Authentication Relay Configuration 16

Configuration Steps for the Digital Guardian Network DLP System 17

SUMMARY 20

APPENDIX A 21

APPENDIX B – APPCENTRIC TEMPLATES UPGRADE 26

ABOUT A10 NETWORKS 26

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.

DEPLOYMENT PREREQUISITES

Requirements for A10 Thunder® SSLi® (SSL Insight®) + Digital Guardian DLP solution:

- Thunder SSLi appliance with Advanced Core Operating System (ACOS®) version 4.1.1-P3 or later
- A10 Networks AppCentric Templates (ACT) version act-0911-17 (see Appendix B for details on upgrading ACT)
- Digital Guardian Network DLP – DG Appliance (can be deployed as physical or VM)
- Microsoft Active Directory-based user authentication system

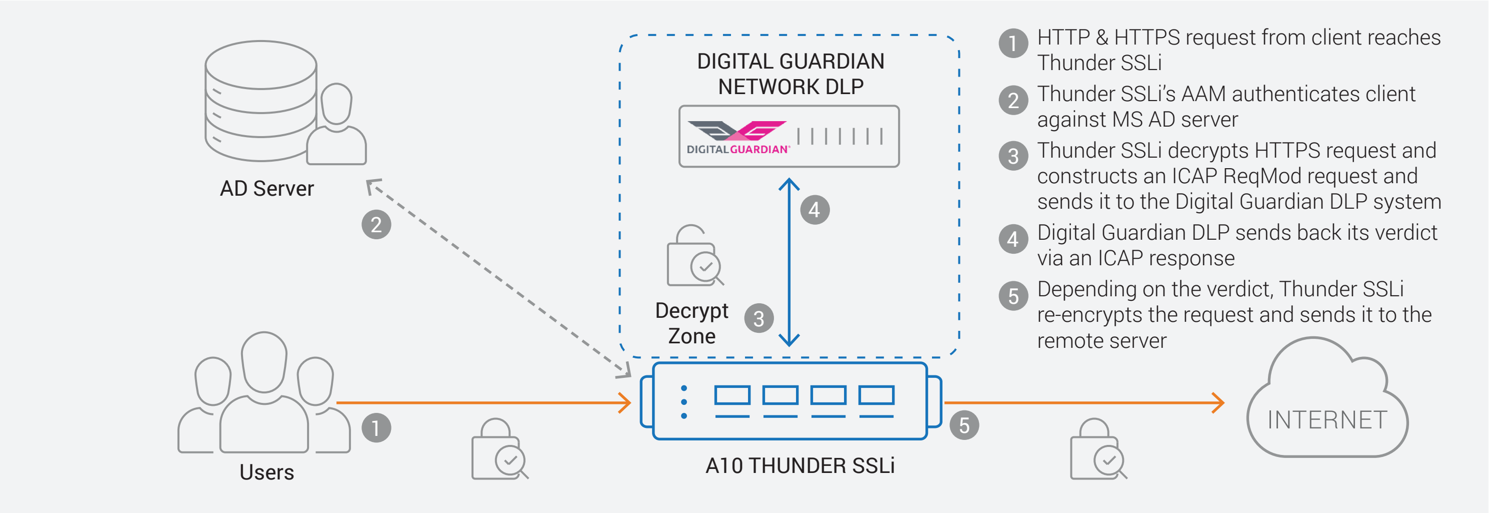
__NOTE__: The CLI commands presented in this guide are based on ACOS version 4.1.1-P3.

ARCHITECTURE OVERVIEW

This section illustrates a joint solution with A10 Networks Thunder SSLi and Digital Guardian Network DLP. Thunder SSLi provides SSL-decryption, ICAP client agent, and user-authentication relay services and the Digital Guardian DLP provides ICAP-based advanced data loss prevention services. This deployment excludes high-availability features, though the solution can be easily extended to an active-standby, redundant setup.

NOTES:

- *Tested Microsoft Active Directory-based LDAP client authentication for this setup, though any authentication service supported by the A10 Application Access Management (AAM) module will work.*
- *Digital Guardian DLP system uses ICAP REQMOD-based service only.*



1. HTTP & HTTPS request from client reaches Thunder SSLi
2. Thunder SSLi's AAM authenticates client against MS AD server
3. Thunder SSLi decrypts HTTPS request and constructs an ICAP ReqMod request and sends it to the Digital Guardian DLP system
4. Digital Guardian DLP sends back its verdict via an ICAP response
5. Depending on the verdict, Thunder SSLi re-encrypts the request and sends it to the remote server

Figure 1: A10 Thunder SSLi + Digital Guardian DLP solution high-level traffic flow

SSLI

A10 Networks SSLi solution consists of two processes, as shown in Figure 2:

- A decryption process that operates on the secure/private side of an inline security device takes encrypted traffic from the clients and decrypts it for the security device(s).
- A re-encryption process which operates on the insecure/public side of an inline security device takes traffic from the security device(s) and re-encrypts it before sending it off to the internet gateway.

These decryption and re-encryption processes can run on a single Thunder SSLi appliance, split into two logical network partitions (presented in this document), or they can be split out between two Thunder SSLi appliances: one dedicated for decryption, and the other for re-encryption.

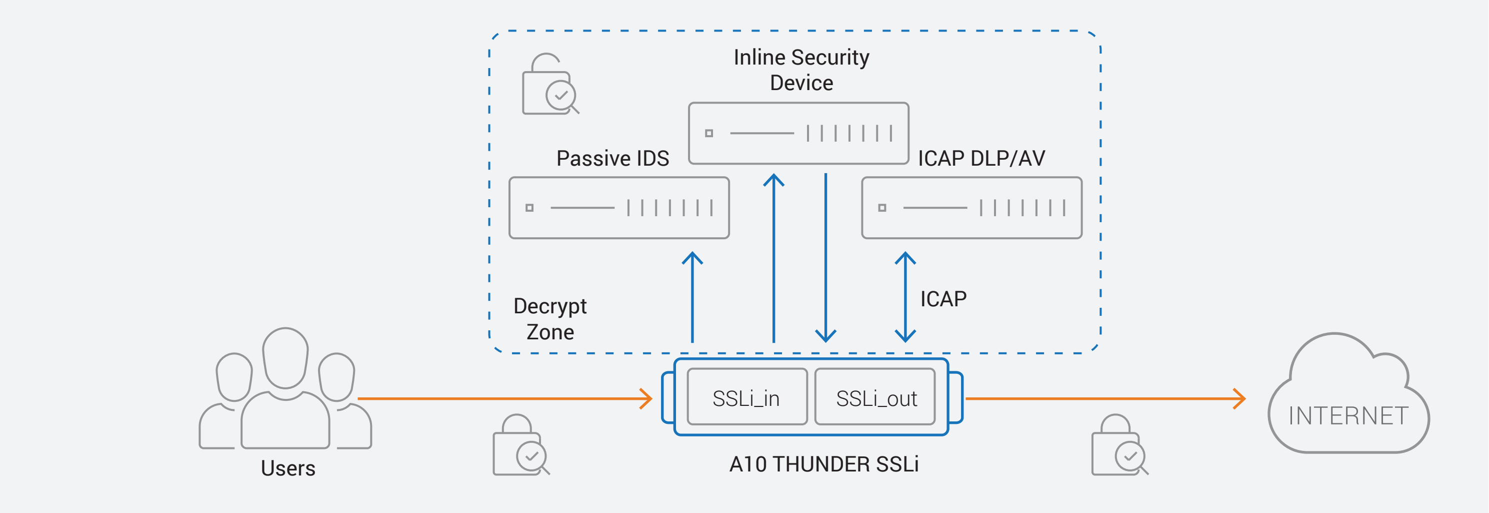


Figure 2: A10 Thunder SSLi feature overview

__NOTE__: Please refer to the ACOS SSL Insight Configuration Guide for additional details on the SSLi feature.

__NOTE__: This deployment is focused on the ICAP-based Digital Guardian DLP only. A straight wire is connected between the SSLi_in and SSLi_out network partitions to simulate a virtual firewall in vWire mode, which permits everything through.

SSLI WITH ICAP

Internet Content Adaptation Protocol or ICAP is a lightweight HTTP-like protocol described in RFC 3507, which is used by proxy servers to deliver HTTP content to external DLP or AV servers. A10 Thunder SSLi provides an RFC-compliant REQMOD and RESPMOD based ICAP client service which provides SSL visibility to an ICAP-enabled DLP/AV appliance. For the scope of this deployment, we will focus on REQMOD-based ICAP requests only, which are used to facilitate data loss prevention (DLP) services (such as Digital Guardian Network DLP) as shown in Figure 1.

- A10 sends decrypted request in an ICAP REQMOD message to the ICAP server
- ICAP REQMOD response elicits the following actions:
  - Status code 200 and modified HTTP request:
    - The modified HTTP request is re-encrypted and forwarded out to the remote server
  - Status code 200 and HTTP response:
    - The HTTP request is NOT re-encrypted and forwarded out. Instead, the response is encrypted, and sent back to the client
  - Status code 204:
    - The original HTTP request is re-encrypted and forwarded out to the remote server
  - Status code 100:
    - More data is sent to the ICAP server
  - Other:
    - Treated as status code 204

SSLI WITH AAM

A10 Networks Application Access Management (AAM) is designed to optimize authentication, authorization, and accounting (AAA) for client-to-server traffic. AAM centralizes control for managing access, eliminates the need to manage individual services on multiple servers, and simplifies login through single sign-on (SSO) technology. AAM integration with SSLi adds the capability to relay and maintain client authentication sessions with backend authentication services, while embedding the client's user-ID into ICAP requests fed to DLP/AV systems.

ACCESSING THUNDER SSLI

This section describes how to access Thunder SSLi from a command line interface (CLI), graphical user interface (GUI) or AppCentric Templates (ACT):

- CLI – The CLI 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 over the network using either of the following protocols:
  - Secure protocol – Secure Shell (SSH) version 2
  - Unsecure protocol – Telnet (if enabled)
- GUI – This is a web-based interface in which you click buttons, menus and other graphical icons to access the configuration or management pages. From these pages, you can 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)
- AppCentric Templates (ACT) - A10 ACOS GUI plug-in module that enhances the user experience to deploy, monitor and troubleshoot applications in a frictionless manner. Obtain the latest ACT file and import it into Thunder SSLi. Refer to Appendix B for details on how to acquire and import the file. The AppCentric Templates can be accessed by opening the GUI by entering the Management IP in the browser's address bar (e.g. https://172.31.31.31/) and navigating to System > App Template.

__NOTE__: HTTP requests are redirected to HTTPS by default on Thunder SSLi.

Default Access Information:

- Default username: “admin”
- Default password: “a10”
- Default IP address of the device: “172.31.31.31”

CONFIGURATION OVERVIEW

In this guide, we will use a basic network topology described in Figure 3 as a starting point. A Windows client gets internet access through a gateway router, while authenticating against a Microsoft Active Directory server in the same network segment/domain.

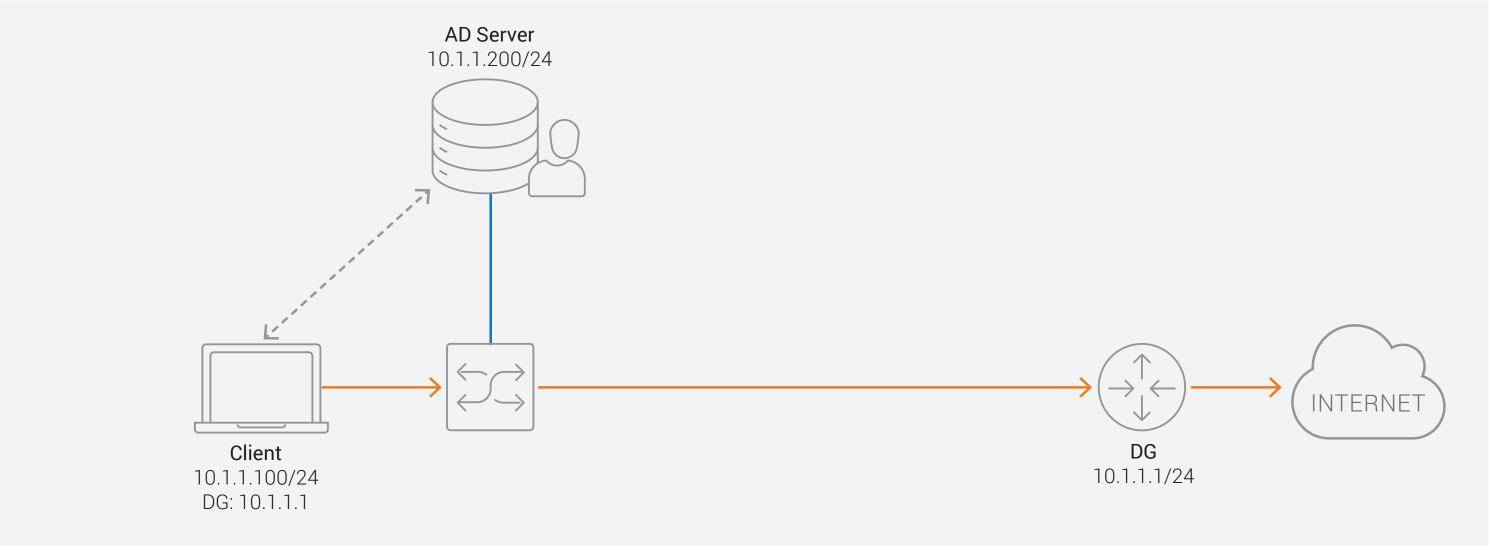


Figure 3: Sample network topology prior to solution deployment

Once the Thunder SSLi and Digital Guardian DLP are brought in, the client continues to operate in the same way as before, pointing to the gateway router as its default gateway, as shown in Figure 4.

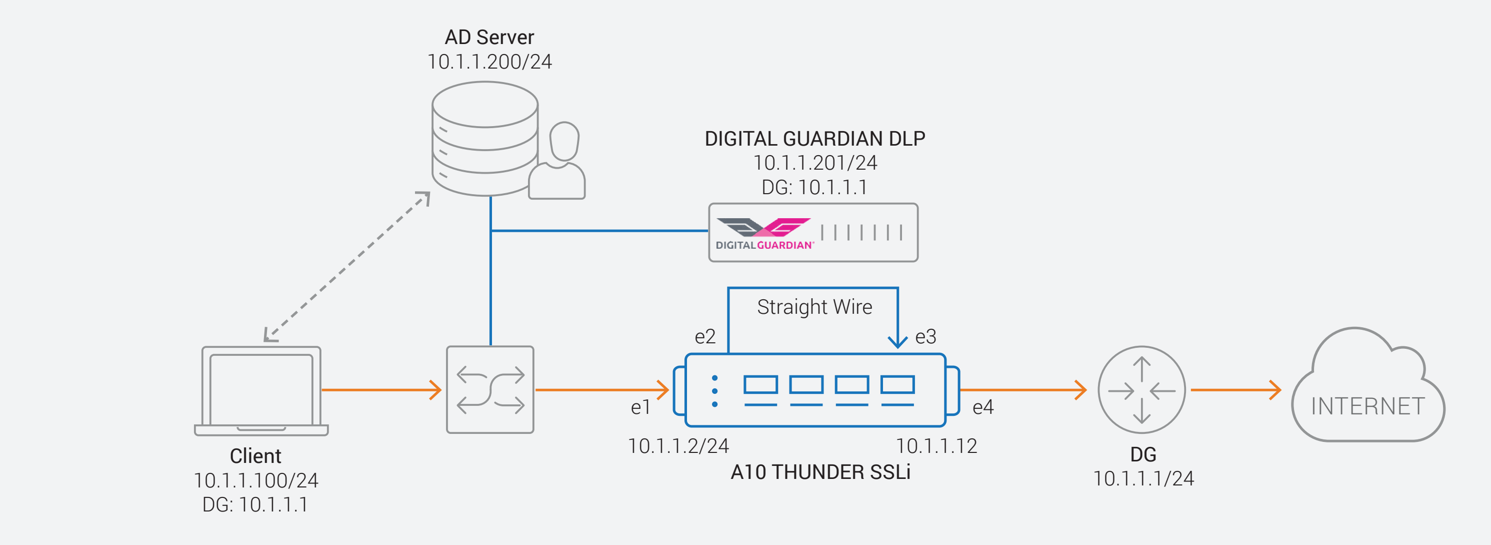


Figure 4: Sample network topology after solution deployment

Deployment configuration can be divided into the following portions:

- Basic SSLi configuration
- ICAP client configuration
- AAM authentication relay configuration
- Digital Guardian Network DLP configuration

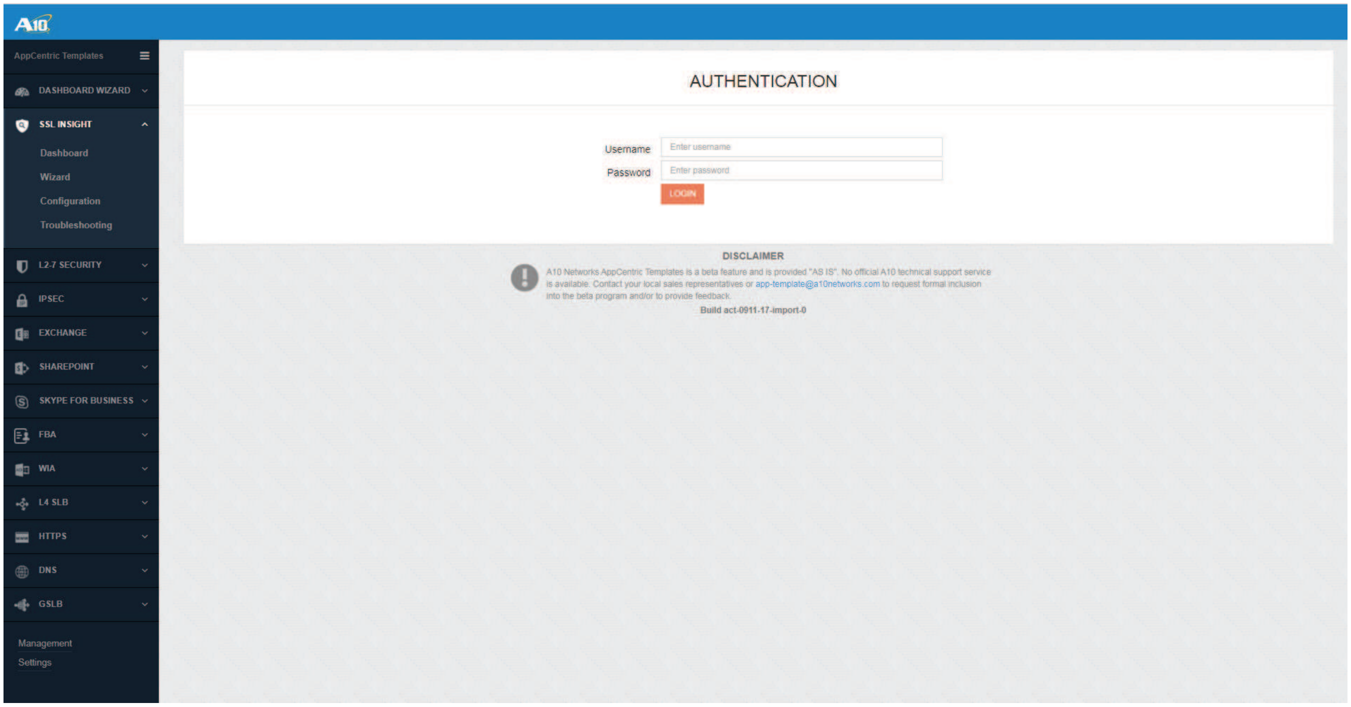
BASIC SSLI CONFIGURATION

SSLi configuration encompasses the basic L2/L3 configuration on the Thunder SSLi appliance along with virtual services for HTTP and HTTPS traffic. This deployment document only covers the most basic SSLi configuration applied through the "SSLi AppCentric Template (ACT)," which works with the Digital Guardian appliance. For a thorough configuration overview for SSLi, refer to the A10 SSLi Deployment Guide[1].

> ***NOTE***: *ACT build 0911-17 was used at the time of this writing.*

The following steps summarize the SSLi configuration process with the SSLi ACT:

1. From the A10 Thunder SSLi GUI, navigate to System > App Template. This launches the AppCentric Templates (ACT) Authentication page.



DISCLAIMER

A10 Networks AppCentric Templates is a beta feature and is provided "AS IS". No official A10 technical support service is available. Contact your local sales representatives or app-template@a10networks.com to request formal inclusion into the beta program and/or to provide feedback.

Build act-0911-17-import-0

Figure 5: SSLi ACT login page

2. Login with the same credentials used to access the A10 Thunder SSLi GUI.
3. From the menu on the left, navigate to SSL INSIGHT > Wizard.
4. Select your SSLi deployment topology. For this deployment exercise, we will keep the default "L2, Single Path" topology and select "Next."

[1] https://www.a10networks.com/sites/default/files/A10-DG-16160-EN.pdf

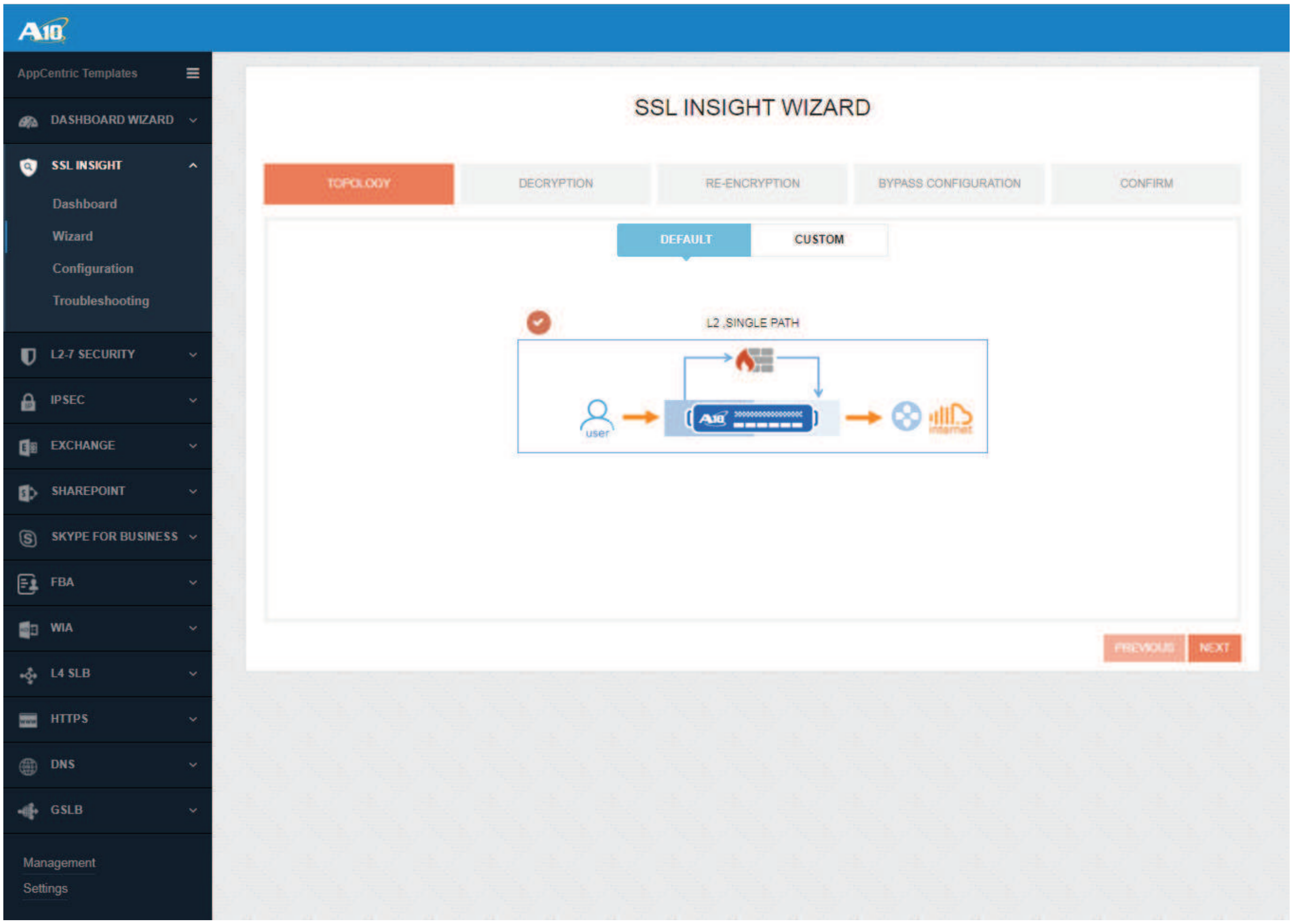
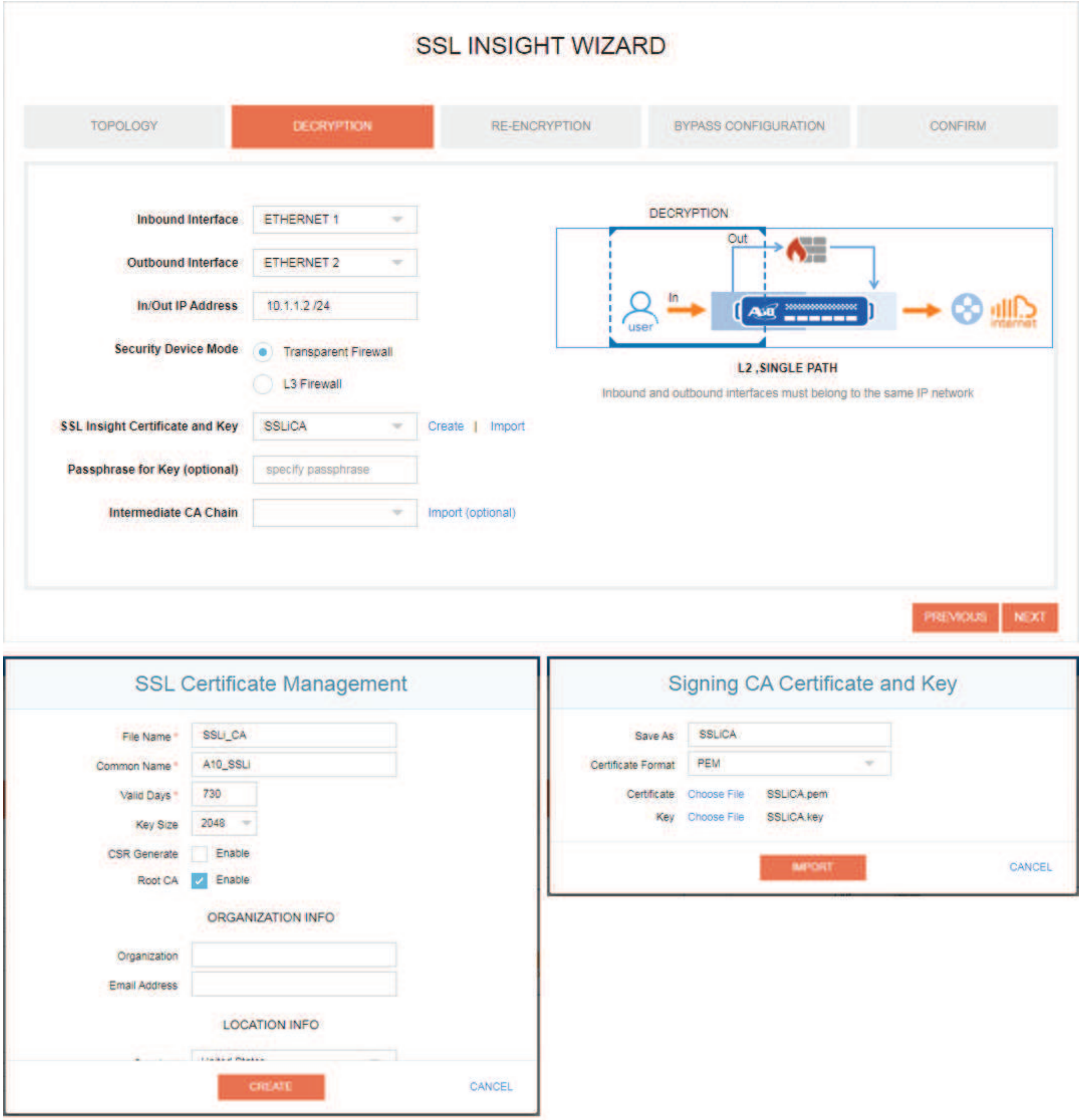


Figure 6: SSLi ACT Wizard topology tab

5. Enter all the configuration data as shown below and select "Next." For the SSL Insight Certificate and Key, choose either "Create" to generate a self-signed CA certificate-key pair, or choose "Import" to import a CA certificate-key pair from your computer. For this exercise, the certificate-key pair was imported.

   This creates the necessary minimum configuration on the decryption partition, aka "ssli_in."

   ***NOTE**: The "In/Out IP address" is an IP address assigned to the ssli_in partition from the network segment in which it resides. The IP address is used for internal communication between the decryption and re-encryption processes and has no bearing on the traffic that is passed through it.*



Inbound Interface	ETHERNET 1
Outbound Interface	ETHERNET 2
In/Out IP Address	10.1.1.2 /24
Security Device Mode	● Transparent Firewall ○ L3 Firewall
SSL Insight Certificate and Key	SSLiCA
Passphrase for Key (optional)	specify passphrase
Intermediate CA Chain	

File Name *	SSLi_CA
Common Name *	A10_SSLi
Valid Days *	730
Key Size	2048
CSR Generate	□ Enable
Root CA	☑ Enable
Organization	
Email Address	

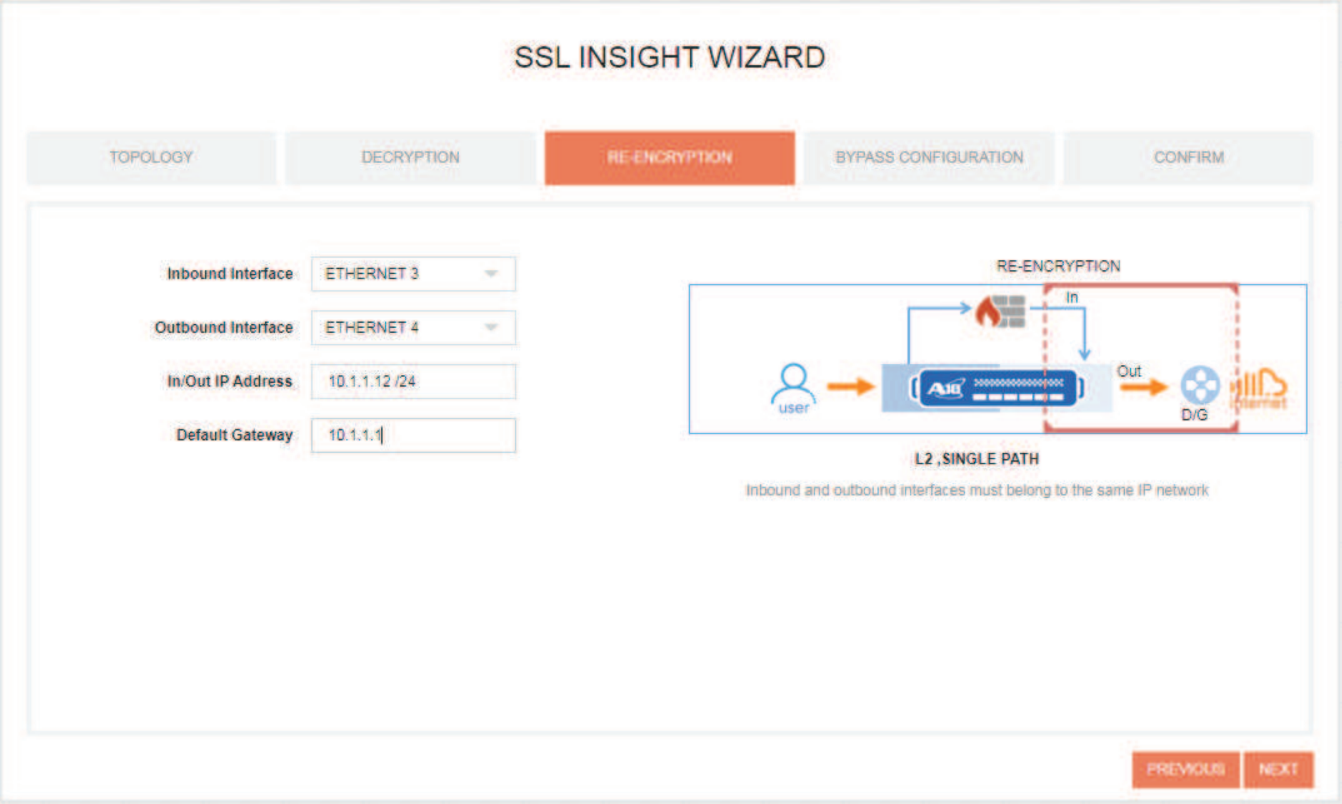
Save As	SSLiCA
Certificate Format	PEM
Certificate	SSLiCA.pem
Key	SSLiCA.key

Figure 7: SSLi ACT Wizard decryption tab (top) / SSL certificate create pop-up (left) / SSL certificate import pop-up (right)

6. Enter all the configuration information as shown below and select 'Next."

This creates the necessary minimum configuration on the re-encrypt partition, aka "ssli_out."

> ***NOTE***: *The "In/Out IP address" is an IP address assigned to the ssli_out partition from the network segment in which it resides. The IP address is used for internal communication between the decryption and re-encryption processes and has no bearing on the traffic that is passed through it.*



SSL INSIGHT WIZARD

Inbound Interface: ETHERNET 3

Outbound Interface: ETHERNET 4

In/Out IP Address: 10.1.1.12 /24

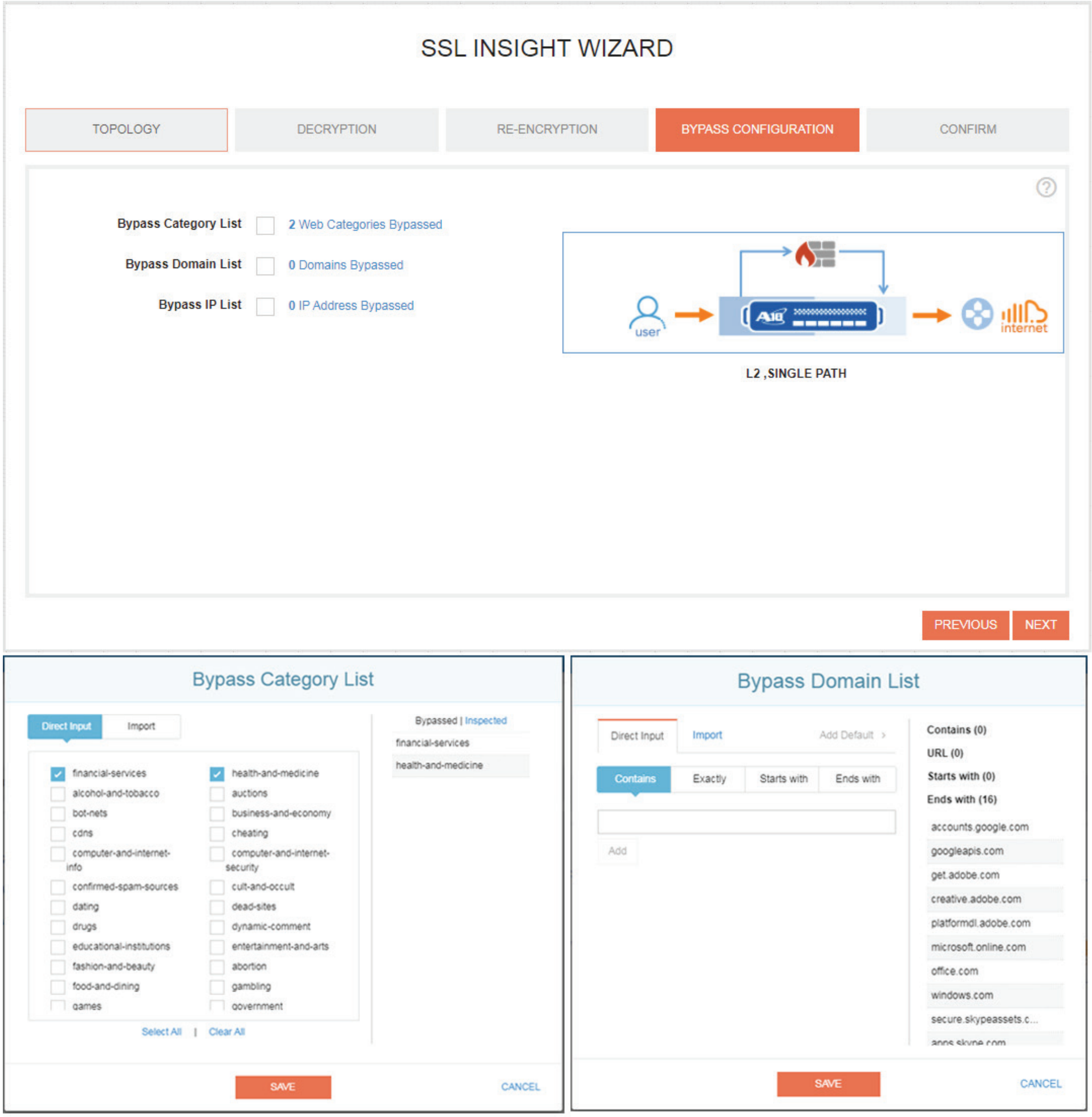
Default Gateway: 10.1.1.1

Inbound and outbound interfaces must belong to the same IP network

Figure 8: SSLi ACT Wizard re-encryption tab

7. This tab is optional, but recommended.
   a. Select the “Bypass Category List” check box to bypass the two default web categories from SSL inspection: “financial-services” and “health-and-medicine”. You can click the “Web Categories Bypassed” link to choose additional categories as needed from the pop-up window.
   b. Select the “Bypass Domain List” check box, and click the “Domains Bypassed” link. A pop-up window appears. Select the “Add Default >” link to auto-populate a list of known certificate-pinning apps that do not work with SSL inspection solutions.
   c. Click “Next” when done.

***NOTE**: The “Bypass Category List” option requires a web category add-on license on the Thunder SSLi.*



SSL INSIGHT WIZARD

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

Bypass Category List □ 2 Web Categories Bypassed

Bypass Domain List □ 0 Domains Bypassed

Bypass IP List □ 0 IP Address Bypassed

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 | Inspected

financial-services

health-and-medicine

Bypass Domain List

Contains (0)

URL (0)

Starts with (0)

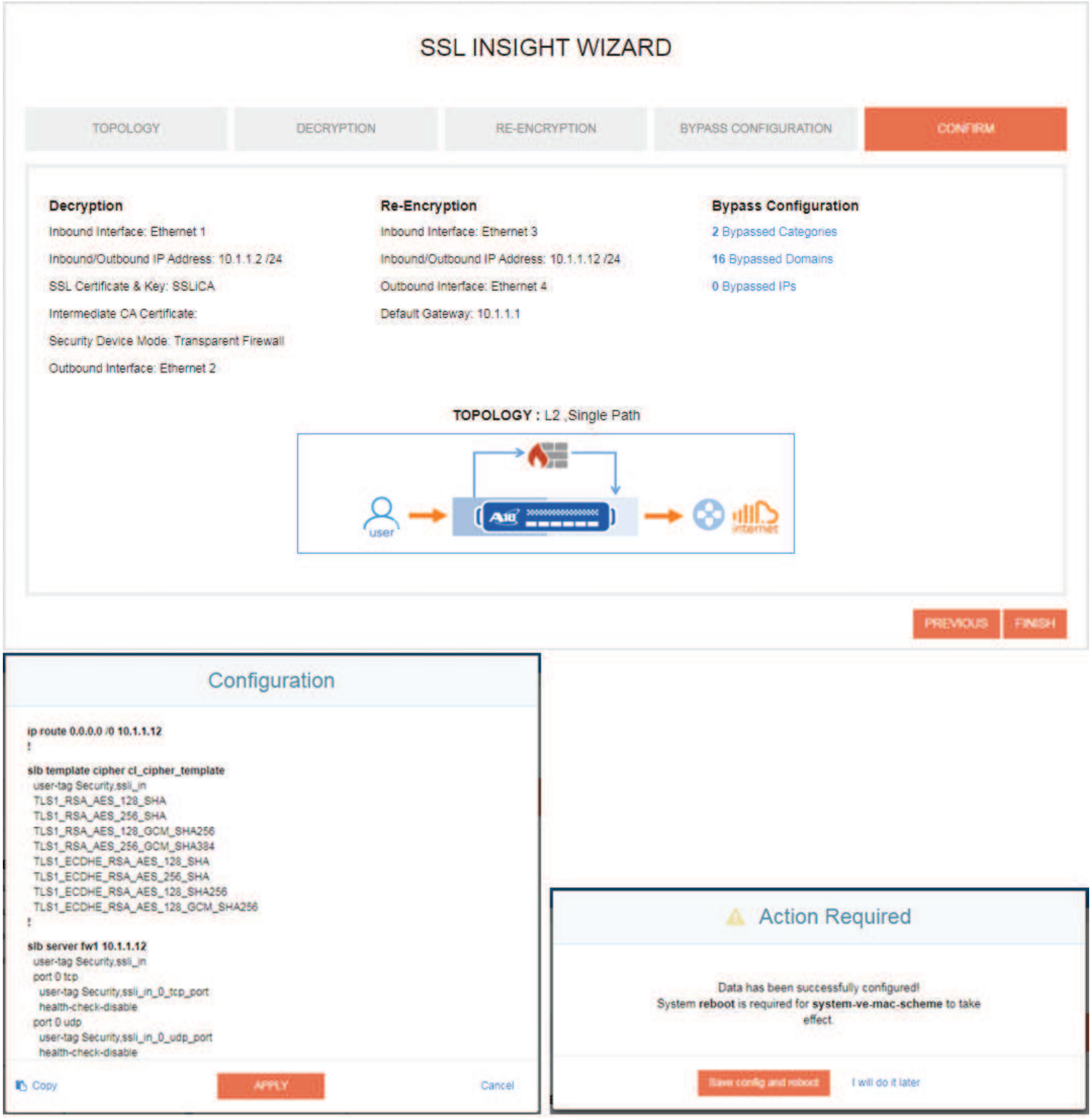
Ends with (16)

accounts.google.com
googleapis.com
get.adobe.com
creative.adobe.com
platformdl.adobe.com
microsoft.online.com
office.com
windows.com
secure.skypeassets.c...
apps.skype.com

Figure 9: SSLi ACT Wizard Bypass Configuration tab (top) / Bypass Category List pop-up (left) / Bypass Domain List pop-up (right)

8. Verify all configuration changes and Click “Finish.” Next, review configuration and click “Apply.”

__NOTE__: If the SSLi configuration is being applied for the first time, you may be prompted to save changes and reboot. Proceed as directed.



SSL INSIGHT WIZARD

Decryption

Inbound Interface: Ethernet 1

Inbound/Outbound IP Address: 10.1.1.2 /24

SSL Certificate & Key: SSLiCA

Intermediate CA Certificate:

Security Device Mode: Transparent Firewall

Outbound Interface: Ethernet 2

Re-Encryption

Inbound Interface: Ethernet 3

Inbound/Outbound IP Address: 10.1.1.12 /24

Outbound Interface: Ethernet 4

Default Gateway: 10.1.1.1

Bypass Configuration

2 Bypassed Categories

16 Bypassed Domains

0 Bypassed IPs

TOPOLOGY : L2 ,Single Path

Configuration

```
ip route 0.0.0.0 /0 10.1.1.12
!
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 10.1.1.12
 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
```

Action Required

Data has been successfully configured!
System **reboot** is required for **system-ve-mac-scheme** to take effect.

Figure 10: SSLi ACT Wizard Confirmation tab (top) / CLI Configuration preview pop-up (left) / Pop-up if reboot is required (right)

This will apply the configuration to the Thunder SSLi device. Refer to Appendix A for the complete CLI configuration.

ICAP CLIENT CONFIGURATION

The ICAP configuration is added manually in the Thunder SSLi CLI, on top of the preexisting SSLi configuration presented in the previous section. This involves the following steps:

- Configure ICAP server IP address and listening ports as SLB servers
- Create service group for the ICAP servers
- Create the ICAP REQMOD template which includes:
  - The ICAP service group
  - The URL of the ICAP REQMOD server
  - Optional configuration
- Apply the SLB REQMOD templates under HTTP and HTTPS vPorts
  - Since the SSLi ACT does not add an HTTP vPort, the HTTP vPort is added manually

1. Configure the Digital Guardian DLP as an SLB server.

```
slb server DG_icap_1 10.1.1.201
  port 1344 tcp
    health-check-disable
!
```

Where 10.1.1.201 and port 1344 are the IP address and listening port on the Digital Guardian DLP.

2. Define an slb service-group for the Digital Guardian DLP

```
slb service-group SG_ICAP tcp
  member DG_icap_1 1344
!
```

3. If you intend to log all ICAP exchanges between the Thunder SSLi and the Digital Guardian DLP, then you may enter the following sample configuration:

```
slb server Syslog 192.168.1.2
  port 514 udp
!
slb service-group SG_Syslog udp
  member Syslog 514
!
slb template logging log
  service-group SG_Syslog
  local-logging 1
!
```

Where 192.168.1.2 and port 514 are the IP address and listening port on a remote syslog server and the command local-logging 1 enables logging to the local syslog on the Thunder SSLi. Syslog configuration using the SLB template logging method is not very common in ACOS. For ICAP client configuration, this implements a CEF logging format for the ICAP syslog logging destinations.

4. Create the ICAP REQMOD SLB template and bind the Digital Guardian DLP Service group and ICAP logging template under it as follows:

```
slb template reqmod-icap reqmod
  service-url icap://10.1.1.201:1344/request
  service-group SG_ICAP
  template logging log
!
```

   Where icap://10.1.1.201:1344/request is the ICAP service URL on the Digital Guardian DLP at 10.1.1.201.

5. Since the SSLi ACT only created an HTTPS vPort 443 for inspecting SSL traffic, you will need to add a new vPort for port 80 HTTP traffic manually as follows:

```
slb server fw1 10.1.1.12
  port 80 tcp
    health-check-disable
!
slb service-group SG_HTTP tcp
  member fw1 80
!
slb virtual-server SSLi_in_ingress 0.0.0.0 acl 190
  port 80 http
    service-group SG_SSLi_TCP
    no-dest-nat
!
```

6. Lastly, bind the ICAP REQMOD SLB template under both HTTP vPort 80 as well as HTTPS vPort 443

```
slb virtual-server SSLi_in_ingress 0.0.0.0 acl 190
  port 80 http
    template reqmod-icap reqmod
  port 443 https
    template reqmod-icap reqmod
!
```

AAM AUTHENTICATION RELAY CONFIGURATION

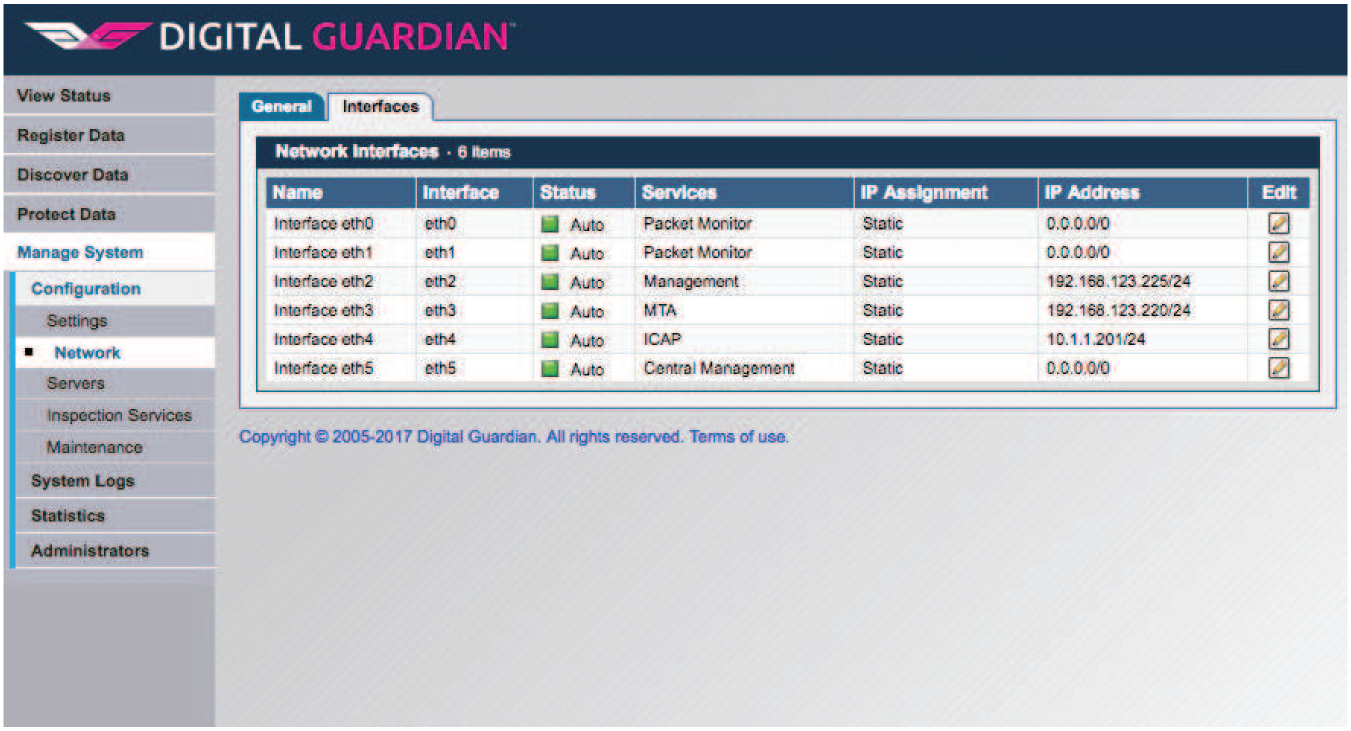
The AAM Authentication Relay configuration is added in the end in order to allow the user identification data to get embedded into the ICAP requests to the Digital Guardian DLP. The following configuration was added for this solution in order to relay user identification data from Microsoft Active Directory server at 10.1.1.200:

```
aam authentication portal default-portal
  logo def_logo.png
!
aam authentication logon form-based aam-logon
  portal default-portal
!
!
aam authentication server ldap ldap-server
  host 10.1.1.200
  base CN=users,DC=panam,DC=org
  admin-dn CN=administrator,CN=Users,DC=panam,DC=org
  admin-secret <password>
!
aam authentication template aam-template
  auth-sess-mode ip-based
  logon aam-logon
  logout-idle-timeout 1800
  server ldap-server
!
aam aaa-policy aam-policy
  aaa-rule 1
    action allow
    authentication-template aam-template
!
slb virtual-server SSLi_in_ingress 0.0.0.0 acl 190
  port 80 http
    aaa-policy aam-policy
  port 443 https
    aaa-policy aam-policy
!
```

CONFIGURATION STEPS FOR THE DIGITAL GUARDIAN NETWORK DLP SYSTEM

Digital Guardian appliance configuration steps are limited to connecting the DLP via ICAP to the Thunder SSLi appliance. DLP policy configuration and incident management can be found in Digital Guardian appliance administration guide.

1. Enable network interface on the Digital Guardian appliance:
   This step will vary based on how the Digital Guardian appliance is deployed:
   Physical appliance or local VM deployment – multiple network interfaces can be configured. Go to Manage System -> Network -> Interfaces tab to configure ICAP IP (click on edit button for ICAP services). Use IP defined under **ICAP Client Configuration when configured A10 Network appliance**.



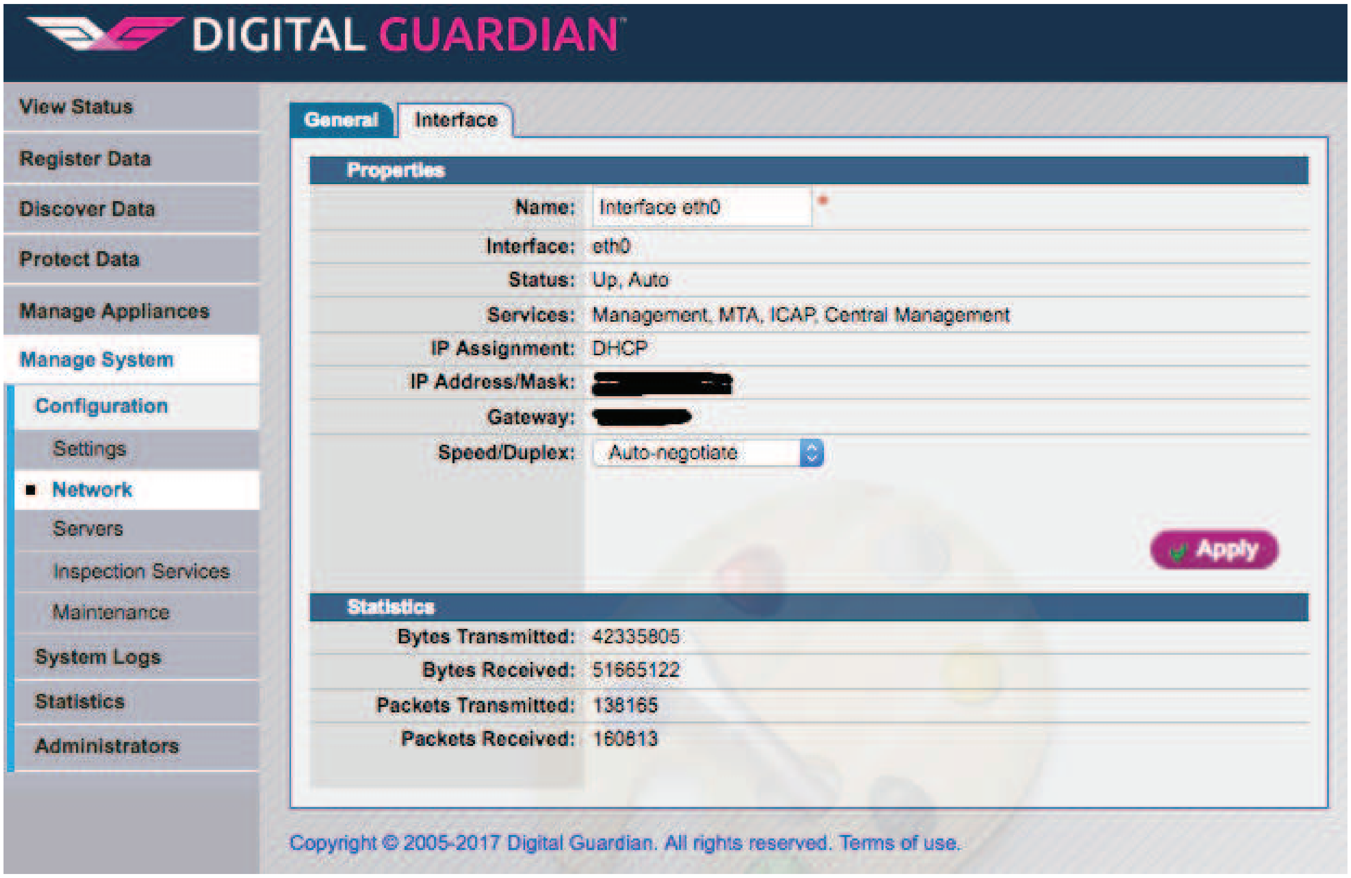
Network Interfaces · 6 items

Name	Interface	Status	Services	IP Assignment	IP Address	Edit
Interface eth0	eth0	🟩 Auto	Packet Monitor	Static	0.0.0.0/0	✎
Interface eth1	eth1	🟩 Auto	Packet Monitor	Static	0.0.0.0/0	✎
Interface eth2	eth2	🟩 Auto	Management	Static	192.168.123.225/24	✎
Interface eth3	eth3	🟩 Auto	MTA	Static	192.168.123.220/24	✎
Interface eth4	eth4	🟩 Auto	ICAP	Static	10.1.1.201/24	✎
Interface eth5	eth5	🟩 Auto	Central Management	Static	0.0.0.0/0	✎

Copyright © 2005-2017 Digital Guardian. All rights reserved. Terms of use.

Figure 11: Configuring DG appliance network interfaces configuration summary

Azure and/or AWS cloud deployment – single network interface only. When deployed via cloud provider, IP gets assigned automatically by DHCP server. Record this IP and use under **ICAP Client Configuration** when configuring A10 Network appliance.



Properties

Name: Interface eth0 *
Interface: eth0
Status: Up, Auto
Services: Management, MTA, ICAP, Central Management
IP Assignment: DHCP
IP Address/Mask: [redacted]
Gateway: [redacted]
Speed/Duplex: Auto-negotiate

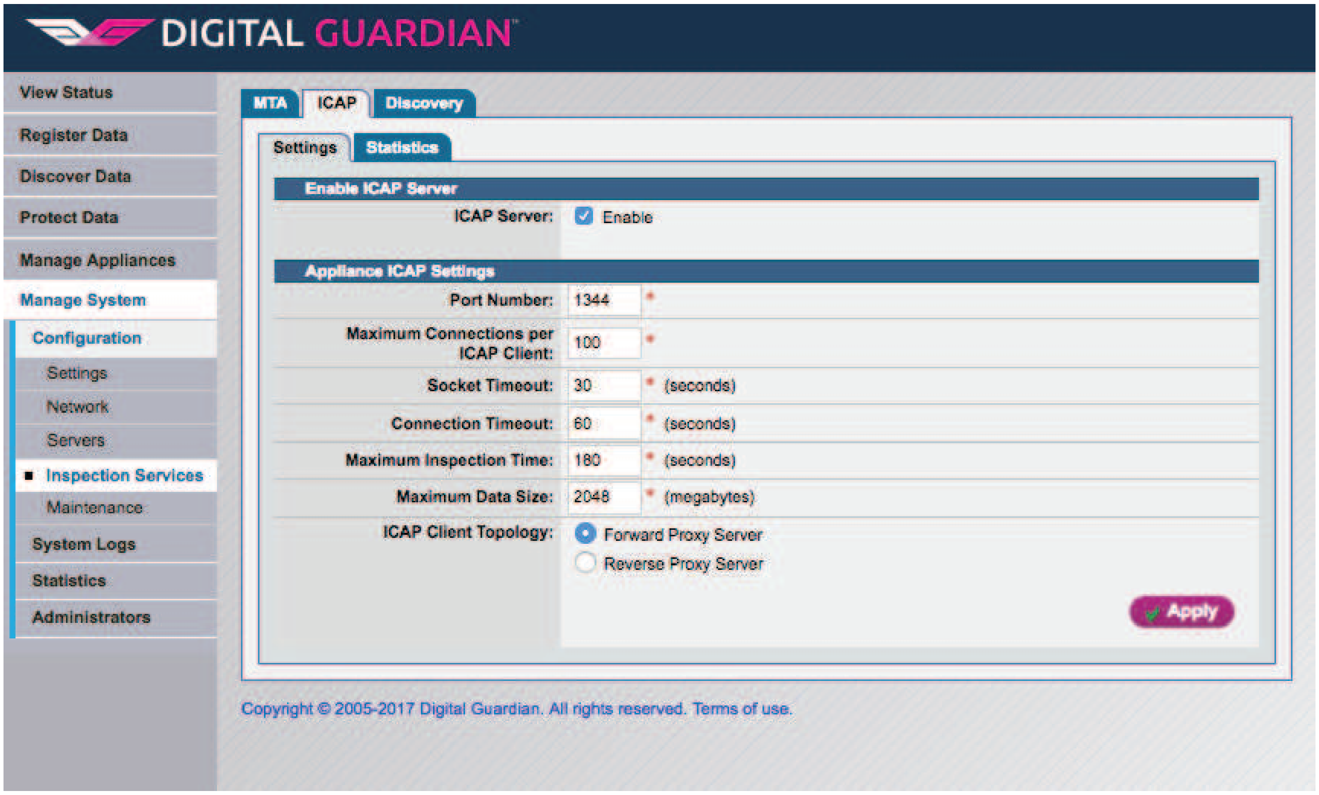
Statistics

Bytes Transmitted: 42335805
Bytes Received: 51665122
Packets Transmitted: 138165
Packets Received: 160813

Copyright © 2005-2017 Digital Guardian. All rights reserved. Terms of use.

Figure 12: DG appliance network interface configuration

2. Enabling ICAP service:
   Go to Manage System -> Inspection Services -> ICAP and enable ICAP server. In addition, other ICAP configuration options are available. Click “Apply” when finished with ICAP configuration. Once configuration is applied the Digital Guardian appliance will be able to accept ICAP traffic from the A10 Networks appliance. An administrator must define data protection policies to protect sensitive information from leaving an organization.



Enable ICAP Server

ICAP Server: ☑ Enable

Appliance ICAP Settings

Port Number: 1344 *

Maximum Connections per ICAP Client: 100 *

Socket Timeout: 30 * (seconds)

Connection Timeout: 60 * (seconds)

Maximum Inspection Time: 180 * (seconds)

Maximum Data Size: 2048 * (megabytes)

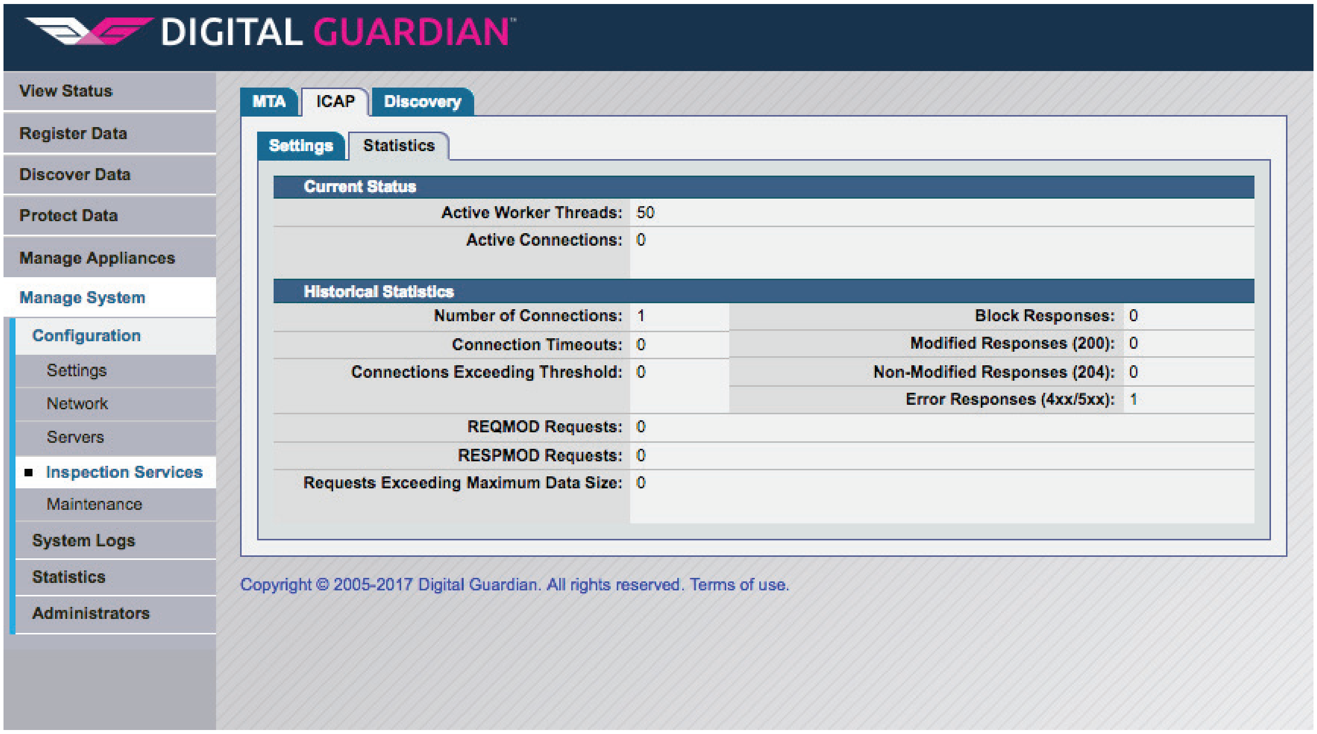
ICAP Client Topology: ● Forward Proxy Server ○ Reverse Proxy Server

Copyright © 2005-2017 Digital Guardian. All rights reserved. Terms of use.

Figure 13: Enabling ICAP service on the DG appliance

3. Validating configuration:

   Go to Manage System -> Inspection Services ->ICAP -> Statistics to validate if traffic from the A10 appliance is seen by the Digital Guardian appliance.



Current Status

Active Worker Threads: 50

Active Connections: 0

Historical Statistics

Number of Connections:	1	Block Responses:	0
Connection Timeouts:	0	Modified Responses (200):	0
Connections Exceeding Threshold:	0	Non-Modified Responses (204):	0
		Error Responses (4xx/5xx):	1
REQMOD Requests:	0		
RESPMOD Requests:	0		
Requests Exceeding Maximum Data Size:	0		

Copyright © 2005-2017 Digital Guardian. All rights reserved. Terms of use.

Figure 14: Viewing ICAP statistics on the DG appliance

SUMMARY

Digital Guardian together with A10 Networks delivers threat-aware data protection to stop both insider and outsider threats. We do this through the deepest visibility, real-time analytics and flexible controls, all of which can be delivered via multiple deployment options.

- Deepest Visibility: The deepest view into your data to show where it is, what it is, and when it is at risk through system, user and data level events. To go from reactive to proactive you need comprehensive visibility across the extended enterprise.
- Real-Time Analytics: Real-time analytics cut through the noise that slows most data security efforts, speeding both the discovery and investigation of incidents.
- Flexible Controls: Flexible controls adapt to your business and business processes, not the other way around. These controls are everywhere your data lives.
- Multiple Deployment Options: Organizations have different priorities when it comes to their data security program. For those investing in their information security team and infrastructure an on-premise deployment helps further leverage that investment. For organizations looking to have a team of security experts manage it for them, our industry first Managed DLP provides an instant InfoSec team. For organizations that have the infrastructure, but need the expertise, our hybrid approach fills the gap.

APPENDIX A

Full configuration on ‘shared’ partition

```
!Current configuration: 579 bytes
!Configuration last updated at 06:46:00 IST Tue Sep 19 2017
!Configuration last saved at 06:46:00 IST Tue Sep 19 2017
!64-bit Advanced Core OS (ACOS) version 4.1.1-P5, build 20 (Sep-12-2017,18:18)
!
multi-config enable
!
monitor buffer-usage 711760
!
!
system ve-mac-scheme system-mac
!
terminal idle-timeout 0
!
ip dns primary 8.8.8.8
!
partition ssli_in id 3
!
partition ssli_out id 4
!
interface management
  flow-control
  ip address 10.101.6.61 255.255.252.0
  ip default-gateway 10.101.4.1
!
interface ethernet 1
!
interface ethernet 2
!
interface ethernet 3
!
interface ethernet 4
  enable
!
interface ethernet 5
  enable
!
interface ethernet 6
!
interface ethernet 7
!
interface ethernet 8
!
interface ethernet 9
!
```

```
interface ethernet 10
!
interface ethernet 11
!
interface ethernet 12
!
!
web-category
  use-mgmt-port
  enable
!
end
```

Full configuration on ‘ssli_in’ partition

```
active-partition ssli_in
!
!
access-list 190 remark ssli_in
!
access-list 190 permit ip any any vlan 850
!
access-list 191 remark block_quic
!
access-list 191 deny udp any any eq 80
!
access-list 191 deny udp any any eq 443
!
access-list 191 permit ip any any
!
class-list bypass_domains ac
  ends-with accounts.google.com
  ends-with googleapis.com
  ends-with get.adobe.com
  ends-with creative.adobe.com
  ends-with platformdl.adobe.com
  ends-with microsoft.online.com
  ends-with office.com
  ends-with windows.com
  ends-with secure.skypeassets.com
  ends-with apps.skype.com
  ends-with api.skype.com
  ends-with webex.com
  ends-with api.quora.com
  ends-with update.microsoft.com
  ends-with roaming.officeapps.live.com
  ends-with ui.skype.com
  user-tag Security,ssli_in
!
```

Full configuration on ‘ssli_out’ partition

```
active-partition ssli_out
!
!
access-list 191 remark ssli_out
!
access-list 191 permit ip any any vlan 860
!
vlan 860
  untagged ethernet 3 to 4
  router-interface ve 860
  name ssli_out_ingress_egress
  user-tag Security,ssli_out_ingress_egress
!
interface ethernet 3
  name ssli_out_ingress
  enable
  user-tag Security,ssli_out_ingress
!
interface ethernet 4
  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 10.1.1.12 255.255.255.0
  ip allow-promiscuous-vip
!
!
ip route 0.0.0.0 /0 10.1.1.1
!
slb template cipher sr_cipher_template
  TLS1_RSA_AES_128_SHA
```

```
vlan 850
  untagged ethernet 1 to 2
  router-interface ve 850
  name ssli_in_ingress_egress
  user-tag Security,ssli_in_ingress_egress
!
interface ethernet 1
  name ssli_in_ingress
 enable
  user-tag Security,ssli_in_ingress
!
interface ethernet 2
  name ssli_in_egress
  enable
  user-tag Security,ssli_in_egress
!
interface ve 850
  name ssli_in_ingress_egress
  access-list 191 in
  user-tag Security,ssli_in_ingress_egress
  ip address 10.1.1.2 255.255.255.0
  ip allow-promiscuous-vip
!
!
ip route 0.0.0.0 /0 10.1.1.12
!
aam authentication portal default-portal
  logo def_logo.png
!
aam authentication logon form-based aam-logon
  portal default-portal
!
!
aam authentication server ldap ldap-server
  host 10.1.1.200
  base CN=users,DC=panam,DC=org
  admin-dn CN=administrator,CN=Users,DC=pan-
am,DC=org
  admin-secret <password>
!
aam authentication template aam-template
  auth-sess-mode ip-based
  logon aam-logon
  logout-idle-timeout 1800
  server ldap-server
!
aam aaa-policy aam-policy
  aaa-rule 1
    action allow
```

```
  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 10.1.1.1
  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
    authentication-template aam-template
!
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 10.1.1.12
  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
  port 80 tcp
    health-check-disable
!
slb server icap_1 10.1.1.201
  port 1344 tcp
    health-check-disable
!
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 service-group SG_HTTP tcp
  member fw1 80
!
slb service-group SG_ICAP tcp
  member icap_1 1344
    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_decrypted_
port_8080http
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
!
end
!
```

```
!
slb template client-ssl cl_ssl
  forward-proxy-ca-cert SSLiCA
  forward-proxy-ca-key SSLiCA
  forward-proxy-ocsp-disable
  forward-proxy-crl-disable
  forward-proxy-cert-expiry hours 168
  forward-proxy-enable
  forward-proxy-failsafe-disable
  forward-proxy-bypass class-list bypass_domains
  forward-proxy-bypass web-category financial-services
 forward-proxy-bypass web-category health-and-medicine
  template cipher cl_cipher_template
  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 template logging log
  local-logging 1
!
slb template reqmod-icap reqmod
  service-url icap://10.1.1.201:1344/request
  service-group SG_ICAP
  template logging log
!
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
    use-rcv-hop-for-resp
    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
    use-rcv-hop-for-resp
    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
    use-rcv-hop-for-resp
    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
    use-rcv-hop-for-resp
    aaa-policy aam-policy
    template reqmod-icap reqmod
    template http insertHeaders
```

APPENDIX B – APPCENTRIC TEMPLATES UPGRADE

AppCentric Templates (ACT) is available in ACOS release 4.1.0-P9 and later. Please make sure that the ACT version on your Thunder SSLi device is up to date.

1. Obtain the latest version of ACT by sending an e-mail to app-template@a10networks.com
2. Log into the Thunder SSLi GUI
3. Ensure that the clock and time zone of your Thunder SSLi device are set correctly
4. Click System > App Template Import and follow instructions

The upgrade is achieved seamlessly without disrupting any Thunder SSLi operations.

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) is a Secure Application Services™ company, 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, Calif., and serves customers globally with offices worldwide.

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

LEARN MORE
ABOUT A10 NETWORKS

CONTACT US
a10networks.com/contact

Part Number: A10-DG-19168-EN-01   NOV 2017