Agility 2018 Hands-on Lab Guide

Contents:

1	Welc	ome		5	
2	Class 1: SSL Orchestration				
	2.1	Lab To	pology	8	
	2.2	Module	1: Outbound SSLO	9	
		2.2.1	Lab 1.1: Deployment Settings	9	
		2.2.2	Lab 1.2: HTTP Service	12	
		2.2.3	Lab 1.3: ICAP Service	16	
		2.2.4	Lab 1.4: L2 Service	17	
		2.2.5	Lab 1.5: L3 Service	19	
		2.2.6	Lab 1.6: TAP Service	21	
		2.2.7	Lab 1.7: Outbound Interception Rules	23	
		2.2.8	Lab 1.8: Testing	27	
	2.3	Module	e 2: Inbound SSLO	29	
		2.3.1	Lab 2.1: Inbound Interception Rules	29	
		2.3.2	Lab 2.2: Testing	34	
	2.4	Module	3: Service Policies	35	
		2.4.1	Lab 3.1: Reviewing the Policies	35	

Welcome

Welcome to F5's SSL Orchestration Training series. The intended audience for these labs are security engineers that would like to leverage the SSL Orchestration tools offered by the F5 platform and gain regulatory visibility into the encrypted traffic on their networks. If you require a pre-built lab environment, please contact your F5 account team and they can provide access to environments on an as-needed basis.

The content contained here adheres to a DevOps methodology and automation pipeline. All content contained here is sourced from the following GitHub repository:

https://github.com/f5devcentral/f5-agility-labs-sslviz

Bugs and Requests for enhancements are handled in two ways:

- · Fork the Github Repo, fix or enhance as required, and submit a Pull Request
 - https://help.github.com/articles/creating-a-pull-request-from-a-fork/
- Open an Issue within the repository.

Class 1: SSL Orchestration

2

F5 SSL Orchestrator provides high-performance decryption of inbound and outbound SSL/TLS traffic, enabling security inspection to expose threats and stop attacks. Dynamic service chaining and policy-based traffic steering allow organizations to intelligently manage encrypted traffic flows across the entire security chain with optimal availability.

SSL Orchestrator ensures encrypted traffic can be decrypted, inspected by security controls, then reencrypted, delivering enhanced visibility to mitigate threats traversing the network. As a result, organizations maximize their security services investment for malware, data loss prevention (DLP), ransomware, and next-generation firewalls (NGFW), thereby preventing inbound and outbound threats, including exploitation, callback, and data exfiltration.

This class covers the following topics:

- SSLO Deployment Settings
- · Security Services Creation
- · Classification and Interception Rules
- · Outbound and Inbound Use cases

Expected time to complete: 4 hours

To continue please review the information about the Lab Environment.

2.1 Lab Topology



The credentials used to access the resources are:

Environment	Username	Password
Window(s) RDP	student	agility
Ubuntu(s)	student	agility
BIG-IP SSH	root	F5agility!2
BIG-IP GUI	admin	F5agility!2

And the networking information is as follows:

VLAN	Interface (tag)	Self-IP
client-net	1.1	10.20.0.100
HTTP_in	1.3 (110)	SSLO managed
HTTP_out	1.3 (120)	SSLO managed
ICAP	admin	10.70.0.10
L2_in	1.6	SSLO managed
L2_out	1.7	SSLO managed
L3_in	1.3 (50)	SSLO managed
L3_out	1.3 (60)	SSLO managed
Тар	1.4	SSLO managed
outbound-net	1.2	10.30.0.100

2.2 Module 1: Outbound SSLO



In this module we will learn the basic concepts required to deploy Outbound SSLO. Additionally, we will walk through creating services and interception rules. It's important to note that this module will focus on demonstrating an **Outbound** SSLO.

We will be following the workflow in the following diagram for the SSLO configuration:



2.2.1 Lab 1.1: Deployment Settings

Task 1 - Create Outbound SSLO Deployment

In this lab, we will explore the settings required to deploy Outbound SSLO. First, we will cover the *General Properties* of the deployment. We will then configure the *Egress*, *DNS*, and *Logging* settings.

Note: This guide may require you to Copy/Paste information from the guide to your jumphost. To make this easier you can open a copy of the guide by using the **Lab Guide** bookmark in Firefox.

1. Open Firefox and navigate to the following bookmark: *f5 BIG-IP*. Bypass any SSL errors that appear and ensure you see the login screen for each bookmark:

BIG-IP® - bigip40.f5demol	× +	
← ▲ https://10.10.0.110/tmui/	/login.jsp	C
📙 Regular Tests 📄 Malware Tests	🚯 f5 BIG-IP	

Warning: We are using a self-signed certificate in this lab. In your environment you must make sure that you use certificates issued by your certificate authority for both production and lab equipment. Not doing so would make it possible for an attacker to do a man-in-the-middle attack and allow him the ability to steal passwords and tokens.

- 2. Authenticate to the interface using the default credentials as defined in the lab topology.
- 3. Navigate to SSL Orchestrator \rightarrow Deployment \rightarrow Deployment Settings and click:



4. In General Properties change the Deployment Name to sslo_agility_lab

General Properties			
Deployment Name	sslo_agility_lab		
Description	SSL Orchestrator		
Strict Update			
Deployed Network	L3 Network 💌		
IP Family	IPv4		

- 5. In the Egress Configuration section set the following:
 - (a) Manage SNAT Settings -> Auto Map
 - (b) Gateways -> Specific gateways
 - (c) Add IPv4 gateway address 10.30.0.1

Egress Configuration				
Manage SNAT Settings	Auto Map	•		
Gateways	Specific ga	ateways 💌		
IPv4 Outbound Gateway	Ratio	IPv4 gateway addres	s	
	1	10.30.0.1	+ -	

- 6. Leave the DNS settings at their defaults.
- 7. Change Logging level -> Debug

Logging Configuration		
Logging Level	Debug 🖵	

Note: The Debug log level should not be used in production unless recommended by f5 Support.

This completes the Deployment Settings setup. When your screen looks like the following, click Finished:

sslo_agility_lab
SSL Orchestrator
· · · · · · · · · · · · · · · · · · ·
L3 Network
IPv4
Auto Map
Specific gateways
Ratio IPv4 gateway address 1 Image: Second
Internet authoritative Name Server
Forward Zones: Nameservers:
+ -
Debug -

Note: The *Strict Updates* option protects against accidental changes to an application service's configuration. The *Strict Updates* setting is *checked* by default.

Unless you have a specific reason to turn off strict updates, F5 recommends that you leave the setting enabled.

2.2.2 Lab 1.2: HTTP Service

Task 1 - Create SSLO HTTP Service

A service is a collection of security devices that will receive decrypted traffic from the SSLO solution. In this section, the HTTP Service will be created. An HTTP Service would typically be a Secure Web Proxy. The proxy could explicit or transparent.

- 1. Login to the BIG-IP with Firefox
- 2. Navigate to SSL Orchestrator \rightarrow Deployment \rightarrow Deployment Settings and click:

Ma	in Help	About	SSL Orchestrator » Deplo
<u>h</u>	Statistics		🚓 👻 Deployment Settings
iApps			
Ê v	Vizards		My Network
S DNS			Clie
6	SL Orchestrator		
	Deployment	Þ	Deployment Settings
	SSL Managemer	nt 🕨	Interception Rules
	Services	Þ	
	Policies	ŀ	

3. On the menu across the top of the main window pane, navigate to Services \rightarrow HTTP Services and click:



4. Click Create on the far right:

General Properties				
Name	ssloS_HTTP_service			
Description				
Strict Update				
IP Family	IPv4 only			
Service Definition				
Auto Manage				
Ргоху Туре	Explicit			
To Service	198.19.96.7/25 🚽 Create New			
VLAN	ssloN_HTTP_in.app/ssloN_HTTP_in Create New			
Node	IP Address Port 198.19.96.66 3128			
	3128 Add			
From Service	198.19.96.245/25 Create New			
VLAN	ssioN_HTTP_out.app/ssioN_HTTP_out Create New			
Service Down Action	Ignore 🗨			
Authentication Offload				
Resources				
iRules	Selected Available Filter No available items No available items <			
Cancel Finished				

5. Enter the following information:

Property	Value
Name	ssloS_HTTP_service
Ргоху Туре	Explicit
To Service VLAN	ssloN_HTTP_in.app/ssloN_HTTP_in
Node -> IP Address	198.19.96.66 (click Add)
From Service VLAN	ssloN_HTTP_out.app/ssloN_HTTP_out

Note: For *To Service VLAN* and *From Service VLAN*, use the drop-down menu to select the correct value.

6. Once your settings look like the following screenshot, click *Finish*:

General Properties				
Name	ssloS_HTTP_service			
Description				
Strict Update	V			
IP Family	IPv4 only 💌			
Service Definition				
Auto Manage				
Ргоху Туре	Explicit 💌			
To Service	198.19.96.7/25 🐷 Create New			
VLAN	ssloN_HTTP_in.app/ssloN_HTTP_in Create New			
Node	IP Address Port			
	3128 Add			
From Service	198.19.96.245/25 - Create New			
VLAN	ssloN_HTTP_out.app/ssloN_HTTP_out Create New			
Service Down Action	Ignore 🗨			
Authentication Offload				
Resources				
iRules	Selected Available			
	No available items /Common			
Cancel Finished	Common			

2.2.3 Lab 1.3: ICAP Service

Task 1 - Create SSLO ICAP Service

A Service is a collection of security devices that will receive decrypted traffic from the SSLO solution. In this section, an *ICAP Service* will be created. An ICAP Service would typically be an Anti-Virus or DLP solution. It is important to have the correct *Request* and *Response* URIs for the solution and the appropriate *Preview Max Length*.

- 1. Login to the BIG-IP with Firefox
- 2. Navigate to SSL Orchestrator \rightarrow Deployment \rightarrow Deployment Settings and click:

Mai	in	Help	About		SSL O	rchestrator »	Deplo	
Statistics					\$ -	Deployment Se	ettings	
iApps								
😰 Wizards					My Network			
() D	NS						Clie	
🛱 s	SL Orch	estrator						
	Deploy	rment		×	Deployr	nent Settings	I.	
	SSL Management >			F	Interception Rules			
	Service	es		F				
	Policie	s		F.				

3. On the menu across the top of the main window pane, navigate to Services \rightarrow ICAP Services and click:

SSL Orchestrator » Services : HTTP Services								
* *	Deployment Settings	SSL Management 👻	Services 👻	Policies -	Interception Rules			
нтт	P Services		HTTP Services					
•		Search	ICAP Services					
			L2 Services					
	Strictne Name		L3 Services		To Service N			
	SSIOS H	TTP service	TAP Services		198.19.2.100			
Del	ete		·r					

4. Click Create on the far right

SI Orchestrator y Services - ICAP Services							
🔅 🗸 Deployment Settings	SSL Management	- Services			s		
ICAP Services							
•	Search						
						Create	
Strictne Name	Headers	OneConnect	Request		Response	Service Down Action	
No records to display							

5. Enter the following values:

Property	Value
Name	ssloS_ICAP_service
ICAP Devices -> IP Address	10.70.0.10 (click <i>Add</i>)
Request	Replace /req with /squidclamav
Response	Replace /res with /squidclamav
Preview Max Length	1048576

6. Once your settings look like the following screenshot, click Finish:

SSL (SSL Orchestrator » Services : ICAP Services » New ICAP Service								
* -	Deployment Settings	SSL Manageme		Services	-			Interception Rules	
Gen	General Properties								
Na	ime	S	loS_l	CAP_service					
De	scription								
Stri	Strict Update								
ICA	ICAP Services								
IP F	amily	IP	v4 only	/					
IC,	AP Devices	10.	Addres 70.0.10	5)	Port 1344				
		10	.70.0.1	D	1344	Add			
Не	aders Mode	D	efault	-					
On	eConnect	V							
Re	quest	ic	ap://\${S	ERVER_IP}:\${	SERVER_PO	DRT}/squidclamav			
Re	sponse	ic	ap://\${S	ERVER_IP}:\$	SERVER_PO	DRT}/squidclamav			
Pr	eview Max Length(byte	s) 10	48576						
Ser	vice Down Action	Ig	nore						
Ser	Send HTTP/1.0 Requests to ICAP		HTTP/1.0 & HTTP/1.1						
IC.A	P Policy	[-	choose	option - 🕌					
C	ancel Finished								

2.2.4 Lab 1.4: L2 Service

Task 1 - Create SSLO L2 Service

A *Service* is a collection of security devices that will receive decrypted traffic from the SSLO solution. In this section an *L2 Service* will be created. An L2 Service could be an IDS/IPS or DLP solution. Some refer

to this as a "Bump in the Wire."

- 1. Login to the BIG-IP with Firefox
- 2. Navigate to SSL Orchestrator \rightarrow Deployment \rightarrow Deployment Settings and click:

Mai	in	Help	About		SSL C	Orchestrator » Deplo
Statistics					* -	Deployment Settings
iApps					11.1	latuark
🖻 v	🔨 Wizards				My I	Network
()	NS					Clie
🛱 s	SL Or	chestrator				
	Depl	loyment			Deploy	ment Settings
	SSL Management				Interce	ption Rules
	Serv	ices				
	Polic	ies				

3. On the menu across the top of the main window pane, navigate to Services \rightarrow L2 Services and click:

SSL Orchestrator » Services : ICAP Services								
🚓 👻 Deployment Settings	SSL Management 👻	Services -	Policies 👻	Interception Rules				
ICAP Services		HTTP Services						
•	Search	ICAP Services						
		L2 Services						
Strictne Name	Headers	L3 Services	juest	Res				
SsloS I	CA false t	TAP Services	://\${SERVER_IP}:\${SERV	ER_PORT}/sq icap				
Delete		1						

4. Click Create on the far right:

SSL (SSL Orchestrator » Services : L2 Services						
* -	Deployment Settings	SSL Management 👻	Services -		Interception Rules		
L2 lr	L2 Inline Services						
	Strictne Name		Service Down Action	1			
No records to display							
Del	ete						

5. Enter the following values:

Property	Value
Name	ssloS_L2_service
Paths –> From BIGIP VLAN	ssloN_L2_in.app/ssloN_L2_in
Paths -> To BIGIP VLAN	ssloN_L2_out.app/ssloN_L2_out (click Add)

6. Once your settings look like the following screenshot, click *Finished*:

Manag		
Name	ssloS_L2_service	
Description		
Strict Update		
P Family	IPv4 only 🕌	
Service Subnet	198.19.32.0 A The L2-s out on the VLAN where the L2-service	ervice's internally assigned IP Ado e resides.
2 Service		
Paths	Ratio From BIGIP VLAN To	BIGIP VLAN
	1 - choose option -	- choose option - Add
	1 ssloN_L2_in.app/ssloN_L2_inssloN	N_L2_out.app/ssloN_L2_out
		-
Service Down Action	Ignore 💌	
Service Down Action Port Remap	Ignore Enabled	
Service Down Action Port Remap esources	Ignore 💌	-
Service Down Action Port Remap esources iRules	Ignore Enabled Selected	Available
Service Down Action Port Remap esources Rules	Ignore Ignore Enabled Selected Filter No available items	Available Common/_sys Common/_sys /Common/_sys /Common/_sys

2.2.5 Lab 1.5: L3 Service

Task 1 - Create SSLO L3 Service

A *Service* is a collection of security devices that will receive decrypted traffic from the SSLO solution. In this section, an *L3 Service* will be created. An L3 Service would typically be an IDS/IPS, DLP, or Next-Gen Firewall (NGFW).

- 1. Login to the BIG-IP with Firefox
- 2. Navigate to SSL Orchestrator \rightarrow Deployment \rightarrow Deployment Settings and click:

Ma	ain Help	About	SSL Orchestrator » Deplo
~	Statistics		🔅 👻 Deployment Settings
i 🧔	Apps		
Ê I	Wizards		My Network
()	DNS		Clie
	SSL Orchestrator		
	Deployment	•	Deployment Settings
	SSL Management	Þ	Interception Rules
	Services	Þ	
	Policies	F	

3. On the menu across the top of the main window pane navigate to Services \rightarrow L3 Services and click:

SSL Orchestrator » Services : L2 Services » New L2 Service								
* -	Deployment Settings	SSL Management 👻	Services ·	Ŧ	Policies 👻	Interception Rules		
L2 li	nline Services		HTTP Services					
•	• Search		ICAP Services	ICAP Services				
			L2 Services					
	Strictne Name		L3 Services	on	1			
	SSIOS L	2 service	TAP Services					
			1					

4. Click *Create* on the far right:

SSL Orchestrator » Services :L3 Services								
÷ •	Deployment Settings	SSL Management 👻	Services -			Rules		
L3 Inline Services • Search Create								
	Strictne Name To Service Network From Servic Service Down Action							
No records to display								
Del	Delete							

5. Enter the following values:

Property	Value
Name	ssloS_L3_service
To Service VLAN	ssloN_L3_in.app/ssloN_L3_in
Node -> IP Address	198.19.64.64 (click Add)
From Service VLAN	ssloN_L3_out.app/ssloN_L3_out

Note: For *To Service VLAN* and *From Service VLAN*, use the drop-down menu to select the correct value.

6. Once your settings look like the following screenshot, click *Finished*:

V4 only 8.19.64.7/25 Create New loN_L3_in.app/ssloN_L3_in Create New Add Add
v4 only 8.19.84.7/25 Create New loN_L3_in.app/ssloN_L3_in Create New kddress .19.84.84 Add Add
v4 only 8.19.64.7/25 Create New loN_L3_in.app/ssloN_L3_in Create New kddress 19.64.64 Add
8.19.84.7/25 Create New loN_L3_in.app/ssloN_L3_in Create New
8.19.84.7/25 Create New loN_L3_in.app/ssloN_L3_in Create New Address .19.84.84 Add Add
8.19.84.7/25 Create New loN_L3_in.app/ssloN_L3_in Create New kddress 19.64.64 Add Add
8.19.64.7/25 Create New loN_L3_in.app/ssloN_L3_in Create New
IoN_L3_in.app/ssIoN_L3_in Create New
Address .19.84.84 Add
8.19.64.245/25 🐷 Create New
loN_L3_out.app/ssloN_L3_out
nore 💌
Enabled
elected Availa ter //comr No available items //comr

2.2.6 Lab 1.6: TAP Service

Task 1 - Create SSLO TAP Service

A *Service* is a collection of security devices that will receive decrypted traffic from the SSLO solution. In this section, a *TAP Service* will be created. A TAP Service would typically be an IDS/IPS.

- 1. Login to the BIG-IP with Firefox
- 2. Navigate to SSL Orchestrator \rightarrow Deployment \rightarrow Deployment Settings and click:

Ma	in	Help	About		SSL C	orchestrator » De	eplo
<u>h</u>	Statistic	s		* -	Deployment Setti	ings	
ii 🔊	Apps Vizards	3		My N	letwork		
())N S					Clie	
6	SSL Ord	chestrator					
	Depl	oyment			Deploy	ment Settings	F
	SSL Management				Interception Rules		
	Services >						
	Polic	ies		E.			

3. On the menu across the top of the main window pane navigate to Services \rightarrow TAP Services and click:

SSL Orchestrator » Services : L3 Services							
🚓 🗸 Deployment Settings SSL Management 👻	Services 👻	Policies 👻	Interception Rules				
L3 Inline Services	HTTP Services						
• Search	ICAP Services						
	L2 Services						
Strictne Name	L3 Services		To Servio				
ssloS L3 service	TAP Services		198.19.1				
Delete							

4. Click Create on the far right:

SSL Orchestrator >> Services : TAP Services									
* -	Deployment Settings	SSL Management 👻	Services 👻	Polic		Interception Rules			
TAP Services									
Strictne Name					VLAN			Interface	
No	No records to display								

5. Enter the following values:

Property	Value
Name	ssloS_TAP_service
MAC Address	2c:c2:60:22:e4:23
VLAN	ssloN_TAP_in.app/ssloN_TAP_in
Interface	1.4

Note: For *VLAN*, use the drop-down menu to select the correct value.

6. Once your settings look like the following screenshot, click Finished:

General Properties	
Name	ssloS_TAP_service
Description	
Strict Update	
TAP Services	
IP Family	IPv4 only
MAC Address	20:02:60:22:e4:23
VLAN	/Common/ssloN_TAP_in_app/ssloN_TAP_in Create New
Interface	1.4 💌
Service Down Action	Ignore 💌
Port Remap	Enabled
IP Address	198.19.0.10
	out on the VLAN where the TAP-service resides.
Cancel Finished	

2.2.7 Lab 1.7: Outbound Interception Rules

Task 1 - Interception Rules

- 1. Login to the BIG-IP with Firefox
- 2. Navigate to SSL Orchestrator \rightarrow Deployment \rightarrow Interception Rules and click:

6	SSL Orchestrator	
	Deployment >	Deployment Settings
	SSL Management	Interception Rules

3. Click Install Default Rules...

Interception Rules							
						Install Default Rules Create	Outbound Rule Create Inbound Rule
	Destination Addre	Service Port	Protocol	VLAN	Partition	Policy	SSL

4. Under *Proxy Settings*, configure these options:

Property	Value
Proxy Scheme	Transparent and Explicit
Proxy Server : Port	10.20.0.150 : 3128

Proxy Settings						
IP Family	IPv4 🗘					
Proxy Scheme	Transparent and Explicit Proxies \$					
Proxy Server	IPV4 Address : 10.20.0.150 Port : 3128					
Classify UDP						
Allow non-UDP/non-TCP						

5. Under Security \rightarrow SSL, select Create New. This will redirect to a separate page for configuring SSL settings.

S	e	С	u	r	ľ	tν	
-	-	-	-			- 7	

SSL	choose option 🖨 Create New
Per Request Policy	choose option -

6. Name the configuration *ssloT_ob_ssl*

Name	ssloT_ob_ssl
Description	
Strict Update	
Proxy Section	

7. In the Client section, for Certificate Key Chains, select default.crt and default.key, and then click Add

Client					
Cipher Type	Cipher Group O Cipher S	itring			
Ciphers	DEFAULT				
Certificate Key Chains	Certificate //Common/default.crt	Key /Common/default.key	Chain	PassPhrase	Add
	/Common/default.crt	Common/default.key	♦ None	¢	Add

8. Under CA Certificate Key Chains, select subca.f5demolabs.com.cer and subca.f5demolabs.com.key, and then click Add.

Certificate Key Chains	Certificate /Common/default.crt	Key /Common/default.key	Chain	PassPhrase	
	/Common/default.crt	Common/default.key	¢ None	¢	Add
CA Certificate Key Chains	Certificate /Common/subca.f5demolabs.com	Key /Common/subca.f5demolabs.com	Chain	PassPhrase	
	/Common/subca.f5demolabs.com	Common/subca.f5demolabs.cc	om 🗘 None	\$	Add Add

9. In the *Server* section, select *ca-bundle.crt* for *Trusted Certificate Authority*. Leave all other settings at the defaults. Click *Finished*.

Server

Cipher Type	Cipher Group Cipher String
Ciphers	DEFAULT
Trusted Certificate Authority	/Common/ca-bundle.crt
Expire Certificate Response Control	drop 🗘
Untrusted Certificate Response Control	drop 🖨
OCSP	choose option \$
CRL	choose option \$ Create New

10. The screen should have returned to the original *Install Default Rules* page. Under the *Security* section, from the *Per Request Policy* drop-down select *Create New*

	Security					
l	SSL	ssloT_outbound_ssl 🖨 Create Ne	ew			
l	Per Request Policy	choose option 🔻				
I	ngress Network	Create New				
	VLANs	Selected	Availab			

11. Name the policy *ssloP_ob_pol*

(General Properties						
	Name	ssloP_ob_pol					
1	TCP Service Chain						

12. Under *TCP Service Chain*, add and order the available services to both the *Intercept Chain* and *Non Intercept Chain*:

TCP Service Chain			
Non Intercept Chain	Selected	Available	
	Filter	*	
	ssloS_ICAP_service ssloS_HTTP_service ssloS_L3_service	*	
	ssloS_L2_service ssloS_Tap_service	*	
		*	
Intercept Chain	Selected	Available	
	Filter	*	
	ssloS_ICAP_service ssloS_HTTP_service	»	
	ssloS_L2_service ssloS_Tap_service	*	
		*	1
JDP Service Chain			
Service Chain Sequence	Selected	Available	
	Filter	«	
	ssloS_L3_service ssloS_L2_service	*	
	ssios_lap_service	*	
		*	
		"	4

- 13. Repeat step (12) for UDP Service Chain
- 14. Click Finish.
- 15. Under *Ingress Network* → *VLANs*, choose */Common/client-net* from the *Available VLANs* and add to the *Selected* section.

ngress Network		
VLANs	Selected	Available
	Filter	/Common/ssloN tap service out.app/ssloN tap service out
	/Common/client-net	/Common/ssloN_I3_service_out.app/ssloN_I3_service_out /Common/ssloN_I3_service_in.app/ssloN_I3_service_in /Common/ssloN_I2_service_out.app/ssloN_I2_service_out
		/Common/ssloN_I2_service_in.app/ssloN_I2_service_in /Common/ssloN_http_service_out.app/ssloN_http_service_out
	Create New	

16. Click Finish.

2.2.8 Lab 1.8: Testing

In order to test the configuration, we will open an HTTPS website and observe plain text traffic within the inspection zone.

Task 1 - Issuing Requests

- 1. Open a remote desktop (RDP) session to the Windows 7 Outbound Client and log in with the credentials referenced in the lab topology.
- 2. Open a web browser and navigate to some HTTPS URLs.
- 3. Observe the resigned certificate. (Pay attention to the Issued By line.)

7 Certificate	×
General Details Certification Path	_
Certificate Information	
This certificate is intended for the following purpose(s): • Ensures the identity of a remote computer	
Issued to: www.google.com	2776
Issued by: subca.f5demolabs.com	
Valid from 6/ 19/ 2018 to 8/ 16/ 2018	
Learn more about certificates	
ОК	Search

4. SSH into the Layer 3 Security device with the credentials in the topology. Run a *tcpdump* with the following parameters:

sudo tcpdump -i eth5.60 -X

Observe the plain text HTTP traffic.

0x0040:	2†3†	7069	643d	3638	3833	2673	3d31	2675	/?pid=6883&s=1&u
0x0050:	726c	3d68	7474	7073	2533	4125	3246	2532	rl=https%3A%2F%2
0x0060:	4666	352e	636f	6d25	3246	2670	6167	6555	Ff5.com%2F&pageU
0x0070:	726c	3d68	7474	7073	2533	4125	3246	2532	rl=https%3A%2F%2
0x0080:	4666	352e	636f	6d25	3246	2672	6566	3d26	Ff5.com%2F&ref=&
0x0090:	636f	6f6b	6965	7354	6573	743d	7472	7565	cookiesTest=true
0x00a0:	266f	7069	643d	3831	3632	2666	6d74	3d6a	&opid=8162&fmt=j
0x00b0:	7326	7469	6d65	3d31	3533	3139	3032	3736	s&time=153190276
0x00c0:	3938	3334	2048	5454	502f	312e	310d	0a55	9834.HTTP/1.1U
0x00d0:	7365	722d	4167	656e	743a	204d	6f7a	696c	<pre>ser-Agent:.Mozil</pre>
0x00e0:	6c61	2f35	2e30	2028	5769	6e64	6f77	7320	la/5.0.(Windows.
0x00f0:	4e54	2036	2e31	2920	4170	706c	6557	6562	NT.6.1).AppleWeb
0x0100:	4b69	742f	3533	372e	3336	2028	4b48	544d	Kit/537.36.(KHTM
0x0110:	4c2c	206c	696b	6520	4765	636b	6f29	2043	L,.like.Gecko).C

2.3 Module 2: Inbound SSLO

In this lab, we will explore the settings required to deploy **Inbound SSLO**. We will be deploying SSLO in *Transparent Proxy* mode. This single rule will provide visibility for all SSL sites behind the SSLO solution.

2.3.1 Lab 2.1: Inbound Interception Rules

Task 1 - Create a new Interception Rule

1. Navigate to SSL Orchestrator \rightarrow Deployment \rightarrow Interception Rules



2. In the top, right hand corner, click Create Inbound Rule...

Edit Default Outbound Rules	Create Outbound Rule	. Create Inbound Rule
Policy	SSL	
ssloP_outbound_ssl_prpTc	p ssloT_ob_s	sl
ssloP outbound ssl proUc	dp	

Task 2 - Create Wildcard Listener

In this step we will create a listener to intercept all inbound HTTPS traffic. After the configuration steps, this will be saved as a wildcard virtual server listening on port 443.

1. Under the *General Properties* section, configure the following values:

Property	Value
Name	ssl_inbound_listener
Destination Address/Mask	0.0.0/0
Service Port	443

Name	ssl_inbound_listener
Description	
Configuration	Basic 🗘
Label	Inbound
Protocol	TCP 🖨
Source Address	0.0.0/0
Destination Address/Mask	0.0.0/0
Service Port	443

Under the Security Policy section, select Create New.

Security Policy	
SSL settings	None Create New
L7 Profile Type	None ¢

General Properties

The configuration GUI will redirect to the SSL settings configuration page.

3. In the General Settings section of the Security Policy, set the name to ssloT_inbound_ssl.

Note: For Inbound configurations the Forward Proxy option should be disabled

General Properties	
Name	ssloT_inbound_ssl
Description	
Strict Update	
Proxy Section	
Forward Proxy	Enabled

4. Under the *Client-side SSL* section, choose *wildcard.f5demolabs.com.crt* and *wild-card.f5demolabs.com.key* from the respective drop-down menus and click *Add*.

Client-side SSL					
Cipher Type	Cipher Group 📀 Cipher String				
Ciphers	DEFAULT				
Certificate Key Chains	Certificate /Common/wildcard.f5demolabs.com /Common/wildcard.f5demolabs.com	Key /Common/wildcard.f5demolabs.com	Chain n 	PassPhrase	Add

5. Under the section *Server-side SSL*, configure the following values:

Property	Value
Expire Certificate Response Control	ignore
Untrusted Certificate Response Control	ignore

General Properties	
Name	ssloT_inbound_ssl
Description	
Strict Update	
Proxy Section	
Forward Proxy	Enabled
Client-side SSL	
Cipher Type	Cipher Group Scipher String
Ciphers	DEFAULT
Certificate Key Chains	Certificate Key Chain PassPhrase
	/Common/wildcard.f5demolabs.com /Common/wildcard.f5demolabs.com
Server-side SSL	
Cipher Type	Cipher Group Cipher String
Ciphers	DEFAULT
Trusted Certificate Authority	/Common/ca-bundle.crt
Expire Certificate Response Control	ignore 🛊
Untrusted Certificate Response Control	ignore 🛊
OCSP	-choose option \$
CRL	-choose option \$ Create New

6. Review the settings and click *Finished*. This will redirect back to the original *Inbound Listener* configuration screen.

Task 3 - Configure VLAN Settings

In this step, we will define which VLAN interface that our listener will accept connections.

Note: Since we are configuring only for inbound traffic, it is important that the wildcard listener only accept connections on the incoming interface. In this case, the VLAN labeled *outbound*.

1. In the VLANs section, choose the /Common/outbound VLAN from the Available List and click the left arrow to move it into Selected.

VLANs	Selected	Available
	Filter	/Common/ssloN_L3_out.app/ssloN_L3_out
	/Common/outbound	<pre>//Common/ssloN_L3_in.app/ssloN_L3_in //Common/ssloN_L2_out.app/ssloN_L2_out //Common/ssloN_L2_in.app/ssloN_L2_in //Common/ssloN_HTTP_out.app/ssloN_HTTP_out //Common/ssloN_HTTP_in.app/ssloN_HTTP_in //Common/dlp-net</pre>
	Create New	

2. Under the Security Policy section, configure these values:

Property	Value	
L7 Profile Type	HTTP	
L7 Profile	/Common/http	
Access Profile	/Common/ssloP_outbound_ssl.app/ssloP_outbou	ind_ssl_access
Per Request Policy	Create New	

Security Policy

SSL settings	ssloT_inbound_ssl Create New
L7 Profile Type	HTTP \$
L7 Profile	Common/http
Access Profile	/Common/ssloP_outbound_ssl.app/ssloP_outbound_ssl_accessProfile \$
Per Request Policy	None Edit
Ingress Network VLANs	None /Common/ssloP_inbound_pol.app/ssloP_inbound_pol_prpTcp /Common/ssloP_outbound_ssl.app/ssloP_outbound_ssl_prpTcp /Common/ssloP_outbound_ssl.app/ssloP_outbound_ssl_prpUdp
	Create New

- 3. Once redirected to the New Inbound Rule configuration:
 - (a) Create a name for the rule
 - (b) Add ICAP, TAP, and L2 services to the Intercept Chain section
 - (c) Repeat step (ii) for the Non Intercept Chain
 - (d) Click Finished

Name	ssloP_inbound_pol			
CP Service Chain				
ntercept Chain	Selected Services		Available Services	
	Filter	"	ssloS HTTP service	
	ssloS_ICAP_service ssloS_TAP_service ssloS_L2_service	*	ssloS_L3_service	
		*		
Non Intercept Chain	Selected Services		Available Services	
	Filter	«	ssloS_HTTP_service	
	ssloS_ICAP_service ssloS_TAP_service ssloS_L2_service	»	ssio5_L3_service	
		*		
		*		

4. Verify the settings under *Security Policy*.

Security Policy	
SSL settings	ssloT_inbound_ssl \$ Create New
L7 Profile Type	HTTP \$
L7 Profile	/Common/http Create New
Access Profile	/Common/ssloP_outbound_ssl.app/ssloP_outbound_ssl_accessProfile \$
Per Request Policy	/Common/ssloP_inbound_pol.app/ssloP_inbound_pol_prpTop Edit

5. Click Finish

2.3.2 Lab 2.2: Testing

- 1. Open up a RDP session to the Inbound Win7 Client and log using the documented credentials.
- 2. Launch Firefox and expand the Inbound Testing' Bookmarks
- 3. Use SSH or the console to the Layer 2 Security device and log in using the documented credentials.

👼 New Tab	×
$\langle \cdot \rangle \mathbf{G}$ \triangleleft	
📙 Inbound Testing	
📙 Links 🕨 📙 Inbound Testing	Test0
	🗋 Test1
	🗋 Test2
	🗋 Test3

- 4. Choose one of the Test websites and open the page.
- 5. Run a *tcpdump* with the following parameters:

sudo tcpdump -i eth5.60 -X

Refresh the web page in the browser and observe the plain text HTTP traffic in the Layer 2 Security device console.

11.11.11.1.1.	11 × 11 ×	7070	6 / 1 0	114 110	******	94.79	1101110	9475	
0X0040:	2131	1009	043û	3038	3833	20/3	3031	20/5	/:pid=0883&S=1&U
0x0050:	726c	3d68	7474	7073	2533	4125	3246	2532	rl=https%3A%2F%2
0x0060:	4666	352e	636f	6d25	3246	2670	6167	6555	Ff5.com%2F&pageU
0x0070:	726c	3d68	7474	7073	2533	4125	3246	2532	rl=https%3A%2F%2
0x0080:	4666	352e	636f	6d25	3246	2672	6566	3d26	Ff5.com%2F&ref=&
0x0090:	636f	6f6b	6965	7354	6573	743d	7472	7565	cookiesTest=true
0x00a0:	266f	7069	643d	3831	3632	2666	6d74	3d6a	&opid=8162&fmt=j
0x00b0:	7326	7469	6d65	3d31	3533	3139	3032	3736	s&time=153190276
0x00c0:	3938	3334	2048	5454	502f	312e	310d	0a55	9834.HTTP/1.1U
0x00d0:	7365	722d	4167	656e	743a	204d	6f7a	696c	<pre>ser-Agent:.Mozil</pre>
0x00e0:	6c61	2f35	2e30	2028	5769	6e64	6f77	7320	la/5.0.(Windows.
0x00f0:	4e54	2036	2e31	2920	4170	706c	6557	6562	NT.6.1).AppleWeb
0x0100:	4b69	742f	3533	372e	3336	2028	4b48	544d	Kit/537.36.(KHTM
0x0110:	4c2c	206c	696b	6520	4765	636b	6f29	2043	L,.like.Gecko).C

2.4 Module 3: Service Policies

In this lab, we will review and modify the *Service Policies* that are created by the **Inbound** and **Outbound** SSLO templates. Service Polices provide the classification to provide Dynamic Service chaining.

2.4.1 Lab 3.1: Reviewing the Policies

Task 1 - View the Per-Request Policies

- 1. Login to the BIG-IP with Firefox
- 2. Navigate to SSL Orchestrator \rightarrow Policies \rightarrow Access Per-Request Policies

S	SL 0	rchestrator » Policies	s : Access Per-Reques	t Policies			
1	¢:				Policies 👻	lules	
	Per-f	Request Policies	Searc	ch			
		Name				Policy Type	Per-Request Policy
		ssloP outbound ssl				per-rq-policy	+ Show All
		ssloP inbound				per-rq-policy	+ Show All
		ssloP inbound pol				per-rq-policy	ssloP inbound pol prpTcp
	Dele	te					

- 3. Click the plus sign next to Show all for the ssloP_outbound_ssl row
- 4. Select the *ssloP_outbound_ssl_prpTcp* Per-Request policy

SSL Orchestrator » Policies : Access Per-Request Policie			
🚓 🗸 Deployment Settings SSL Management 👻 Service	s 👻 Policies 👻 Interception Rule	es	
Per-Request Policies		_	
Name	P	Policy Type	Per-Request Policy
ssloP outbound ssl	р	er-rq-policy	= Hide All
			ssioP outbound ssi prpTcp
			ssloP outbound ssl prpUdp
ssloP inbound	p	er-rq-policy	Show All
ssloP inbound pol	р	er-rq-policy	ssloP inbound pol prpTcp
Delete			

5. Review the general flow from categorization through Intercept policy to Service Chain

SSL Orchestrator » Policies : Access Per-Request Policies	
	Close
SSL-Orchestrator Policy: /Common/ssloP_outbound_ssl.app/ssloP_outbound_ssl_prpTcp Edit Endings (Endings: Reject, Allow (default))	
Start falback + Categorization Out + Alow Start Ss. Intercept Policy Not intercepted + Service Chain Not intercepted Out + Alow	
Add New Macro	
E H Macro: Categorization (Terminals: Cut [default])	Use Count: 1 🛛 🕅
H Macro: IP Policy (Terminals: Passed [default], Failed)	Use Count: 0 🛛 🗙
* Macro: Proxy Chaining(Connect) (Terminals: Out [default])	Use Count: 0 🔀
*Macro: Proxy Chaining(URI Rewrite) (Terminals: Out [default])	Use Count: 0 🛛 🗙
E Macro: SSL Intercept Policy (Terminals: Intercepted (default), Not Intercepted)	Use Count: 1 🔀
🗄 🗄 Macro: Service Chain Intercepted (Terminals: Out [default])	Use Count: 1 🔀
🗄 🕂 Macro: Service Chain Not Intercepted (Terminals: Out [default])	Use Count: 1 🛛 🖂

6. Expand the *Macro: Categorization* macro by clicking on *Categorization* in the boxed area or the plus symbol in the macro section.

SSL Orchestrator » Policies : Access Per-Request Policies	
	Close
SSL-Orchestrator Policy: /Common/ssloP_outbound_ssl.app/ssloP_outbound_ssl_prpTcp Edit Endings (Endings: Reject, Allow (default))	
Start - Gategorization Out +	
Add New Macro	
문 I Macro: Categorization (Terminals: Cut [default])	Use Count: 1 🛛 🔀
Hacro: IP Policy (Terminals: Passed (default), Falled)	Use Count: 0 🛛 🗙
*Macro: Proxy Chaining(Connect) (Terminals: Out [default])	Use Count: 0 🛛 🗙
+ *Macro: Proxy Chaining(URI Rewrite) (Terminals: Out [default])	Use Count: 0 🛛 🗙
Terminals: Intercepted [default], Not Intercepted]	Use Count: 1 🛛 🔀
E Macro: Service Chain Intercepted (Terminals: Out [default])	Use Count: 1 🔀
E Macro: Service Chain Not Intercepted (Terminals: Out [default])	Use Count: 1 🔀

7. Explore the SSL Check advanced Action Properties



SSL Found	Add Branch Rule		Insert Before:
SSL Check fallback +	Name: SSL Found Expression: SSL is Name: failback	Simple Advanced expr { [mcget {perflow.ssl_check.ssl_found}] == 1 }	X
IP Policy (Terminals: Passed [default],			
o: Proxy Chaining(Connect)		//	
o: Proxy Chaining(URI Rewr			
ro: SSL Intercept Policy Mac			
Sites with Pinned Certi Category Branching Finance and Healthcard fallback			
o: Service Chain Intercepte			
o: Service Chain Not Interce		Cancel Finished Help	
	Cancel Save		Help

8. Expand the *SSL Intercept Policy* macro. Notice that the *Not Intercepted* and *Intercepted* terminal endings differ based on the category and setting interception.

SSL Orchestrator » Policies : Access Per-Request Policies
<u>f5</u>
SSL-Orchestrator Policy: /Common/ssloP_outbound_ssl.app/ssloP_outbound_ssl_prpTcp Edit Endings (Endings: Reject, Allow (default])
Start -fallback +
Add New Macro
Terminals: Out [default])
H Macro: IP Policy (Terminals: Passed [default], Failed)
+ *Macro: Proxy Chaining(Connect) (Terminals: Out [default])
*Macro: Proxy Chaining(URI Rewrite) (Terminals: Out [default])
Edit Terminals: Intercepted [default], Not Intercepted)
In Sites with Pinned Certificates Sites with Pinned Certificates +> Not Intercepted > Finance and Healthcare +> Sites Set > Fallback > Sites Set > Sites Set > Not Intercepted > Sites > Sites

9. Explore the Category Branching Action Property

SSL Orchestrator » Policies : Access Per-Request Policies	ies	
<u>65</u>		
SSL-Orchestrator Policy: /Common/sslol	P_outbound_ssl.app/ssloP_outbound_ssl_prpTcp Edit Endings (Endings: Reject, Allow (defi	āult])
Start fallback + - <u>Categorization</u> Out +	Intercepted +> Service Chain Intercepted Out +> Allow Not Intercepted +> Service Chain Not Intercepted Out +> Allow	
Add New Macro		1
📇 🛨 Macro: Categorization (Terminals: Out	Properties Branch Rules	
+ Macro: IP Policy (Terminals: Passed [default],	Add Branch Rule Insert Before: 1: Sites with Pinned Certificates 🔻	
+ *Macro: Proxy Chaining(Connect)	Name: Sites with Pinned Certificates	
🛨 *Macro: Proxy Chaining(URI Rewr	Expression: Category is -Custom- Pinners change	
📇 🖃 Macro: SSL Intercept Policy Mac	Name: Finance and Healthcare	
Fallback	OR Category is Health and Medicine change	
In Hanback +-	Name: failback	
Category Branching		
+->>		
🗄 🛨 Macro: Service Chain Intercepte		
🗄 🛨 Macro: Service Chain Not Interce		

10. Expand the macros Service Chain Intercepted and Service Chain Not Intercepted

SSL Orchestrator » Policies : Access Per-Request Policies
<u>6</u>
SSL-Orchestrator Policy: /Common/ssloP_outbound_ssl.app/ssloP_outbound_ssl_prpTcp Edit Endings (Endings: Reject, Allow [default])
Start fallback + Categorization Out + Service Chain Intercepted SSL Intercept Policy Not Intercepted + Service Chain Not Intercepted Out Not Intercepted + Service Chain Not Intercepted Out
Add New Macro
Terminals: Out [default])
+ Macro: IP Policy (Terminals: Passed [default], Failed)
+ *Macro: Proxy Chaining(Connect) (Terminals: Out [default])
+ *Macro: Proxy Chaining(URI Rewrite) (Terminals: Out [default])
E Macro: SSL Intercept Policy (Terminals: Intercepted [default], Not Intercepted)
Edit Terminals: Out [default])
$\boxed{\text{In}}_{\text{fallback}} + - \boxed{\text{ICAP service}}_{\text{fallback}} + \rightarrow - \boxed{\text{TAP service}}_{\text{fallback}} + \rightarrow - \boxed{\text{L3 service}}_{\text{fallback}} + \rightarrow - \boxed{\text{L2 service}}$
Edit Terminals: Out [default])
$\frac{x}{\text{In}} + \frac{x}{\text{ICAP service}} + \rightarrow -\frac{x}{\text{TAP service}} + \rightarrow -\frac{x}{\text{HTTP service}} + \rightarrow -\frac{x}{\text{HTTP service}} + \rightarrow -\frac{x}{\text{L3 service}} + \rightarrow -\frac{x}{\text{L3 service}} + \rightarrow -\frac{x}{\text{L2 service}} + \rightarrow$

11. Explore the Action Properties in the Service Chains and notice the Connector Profiles

Add New Macro	Properties Branch Rules		_
📇 🛨 Macro: Categoriza	Name: ICAP_service		
H Macro: IP Policy (Te	Service Connect Connector Profile	/Common/ssloS_ICAP_service.app/ssloS_ICAP_service-t-connector	
🛨 *Macro: Proxy Chai			
🕂 *Macro: Proxy Chai			
🗄 🛨 Macro: SSL Interd			
🗄 🖃 Macro: Service Ch			
In fallback + ICAP_service falls			
🗄 🖃 Macro: Service Ch			
	Cancel Save	Не	:lp

Task 2 - Modify the Intercept Policy

1. Expand the macro SSL Intercept Policy and click the Intercepted terminal ending

Edit Terminals: Intercepted [default], Not Intercepted)			
In fallback +	Sites with Pinned Certificates + ->- SSL Bypass Set fallback + ->- Not Intercepted Finance and Healthcare + ->- SSL Bypass Set fallback + ->- Not Intercepted fallback + ->- SSL Bypass Set fallback + ->- Not Intercepted fallback + ->- SSL Intercept Set fallback + ->- Intercepted		

2. Select the Not Intercepted radio button, then Save

1			ล	
	Select Terminal:			
яL	۲	Intercepted 🗖		
	\bigcirc	Not Intercepted 🗖		
it				
-			-	
_				
56				
_				
56				
-2				
1				
16				
	Са	ncel Save Help		

Note: Notice that now all traffic is bypassed and therefore not decrypted

In fallback +	Sites with Pinned Certificates $+ \rightarrow - SSL Bypass Set$ fallback $+ \rightarrow - Not Intercepted$
Category Branching	Finance and Healthcare +
	fallback +

- 3. Repeat the test from Lab 1.8 and notice that traffic is not decrypted. Notice that this had the impact of all traffic bypassing inspection zone.
- 4. Undo the change by setting the terminal ending back to *Intercepted* and repeat test.

Task 3 - Modify Service Chain

1. Expand the macro named *Service Chain Not Intercepted* and remove the *HTTP Service* node by selecting the *X* in the corner. The *X* will turn red when you hover over it.



2. Click the *Delete* button in the Item delete confirmation dialogue box

Item deletion confirmation	
Do you really want to delete action 'HTTP_service'	
● Connect previous node to fallback ▼ branch	
Delete all branches	
Cancel Delete	Help

3. View your results



4. Add the HTTP Service node back by selecting the plus key between TAP and L3 services

\blacksquare \square Macro: Service Chain Not Intercepted	Macro Settings / Rename Edit Terminals (Terminals: Out [default])
In fallback + ICAP service fallback +	+

5. Select the Traffic Management tab, then the Service Connect item and click Add Item

Beg	in typing to search		Q
Assi	gnment Endpoint Security (Security)	Server-Side) Classification General Purpose Traffic Management SSLO Macros	
0	Proxy Select	Proxy Select	
	Service Connect	Service Connect	
0	Session Check	Session Check	
Cano	Add Item		Help

6. Change the *Name* to *HTTP Service*, choose the HTTP Service item from the *Connector Profile* drop down menu named /*Common/ssloS_HTTP_server.app/ssloS_HTTP_service-t-connector* and then click *Save* at the bottom

1			
	Properties* Branch Rules		
	Name: HTTP Service		
	Corruico Coppost		
service Connect			
	Connector Profile	/Common/ssloS_HTTP_service.app/ssloS_HTTP_service-t-connector 🔻	
],		None	
		/Common/connector /Common/cdoS_ICIR_convice_app/cdoS_ICIR_convice_t_connector	
		/Common/sslo5_texp_service.app/sslo5_texp_service-u-connector	
-		/Common/ssloS_TAP_service.app/ssloS_TAP_service-t-connector	
ri		/Common/ssloS_HTTP_service.app/ssloS_HTTP_service-t-connector	
-		/Common/ssloS_L3_service.app/ssloS_L3_service-t-connector	-
n		/common/sslo5_L3_service.app/sslo5_L3_service-u-connector /Common/sslo5_L2_service.app/sslo5_L2_service-u-connector	
		/Common/ssloS_L2_service.app/ssloS_L2_service-t-connector	
30			
n			
_			
_			
a,			
-			
	Cancel Save (*Data in tab has	been changed, please don't forget to save)	Help