
SSLO v17.1 セットアップガイド

F5 ネットワークスジャパン合同会社

2024 年 01 月 23 日

目次:

第 1 章	はじめに	3
第 2 章	コンテンツ	5
2.1	SSLO (L3 Explicit Proxy) の設定	5

最終更新日: 2023 年 9 月 20 日

第 1 章

はじめに

このページでは、これらのオフィシャルなドキュメントの補足となる資料や、複数の機能を組合せてソリューションを実現する方法をご紹介します。F5 のオフィシャルなドキュメントはこちらにございます。

- F5: <https://my.f5.com/manage/s/>
- F5 Cloud Docs: <https://clouddocs.f5.com/>
- F5 DevCentral (コミュニティ) : <https://devcentral.f5.com/>

第 2 章

コンテンツ

こちらのページでは、以下の内容をご紹介します。

- 本セットアップガイドにて、F5 SSL Orchestrator (以下、SSLO) の基本設定方法についてご案内します。
- SSLO は、SSL 可視化製品です。
- 本ガイドでは、SSLO をご購入いただいてすぐに SSL 可視化を導入頂けるように、必要となる典型的なセットアップ手法を、豊富なスクリーンショットを交えて解説します。(実際は環境構成にあった設定値を設定して下さい。)
- 本ガイドでは、F5 Japan におけるハンズオントレーニングのコースでも利用しております。

2.1 SSLO (L3 Explicit Proxy) の設定

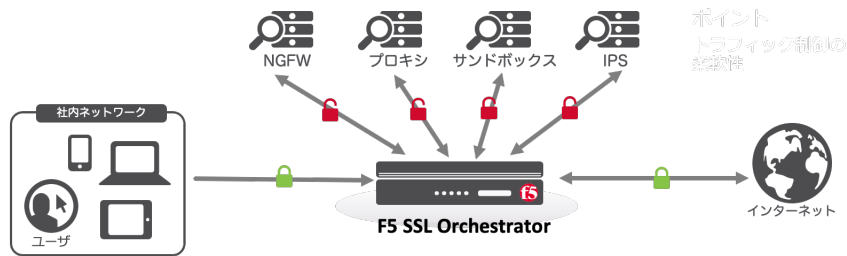
本章では、以下の組合せのケースの設定概要をご紹介します。

- SSLO : L3 Explicit Proxy
- 可視化セキュリティデバイス : L2

2.1.1 F5 SSL Orchestrator(SSLO) とは

F5 SSL Orchestrator(SSLO) は、社内ネットワークからのアウトバウンド通信を復号し、その通信を各セキュリティ製品にポリシーに従って転送し、最後に SSL 再暗号化することができる製品です。アーキテクチャとしては BIG-IP 同様にフルプロキシアーキテクチャを採用し、クライアントサイド、サーバサイドで TCP コネクションをはり直しますので、柔軟にトラフィック制御が可能です。

特長としては以下のようなポイントがあります。



- セキュリティ機器での SSL 処理負荷を代行することが可能
- SSL 可視化トラフィックを柔軟に制御可能
- サービスチェーンによる柔軟なポリシー作成
- 最新の SSL プロトコルに対応
- L3 Explicit Proxy 構成, L3 Transparent Proxy 構成, L2 構成, リバースプロキシ構成が可能
- 様々な機器 (L2、L3、ICAP、TAP、HTTP) との連携が可能
- 専用 GUI によるポリシー設定が容易に可能
- SSL 可視化状況の見える化が可能

2.1.2 本ガイドの利用バージョンと構成イメージ

本手順書では以下のサンプルネットワーク構成で設定を行います。(F5 ハンズオン環境でも同様のネットワーク構成を利用しています。)

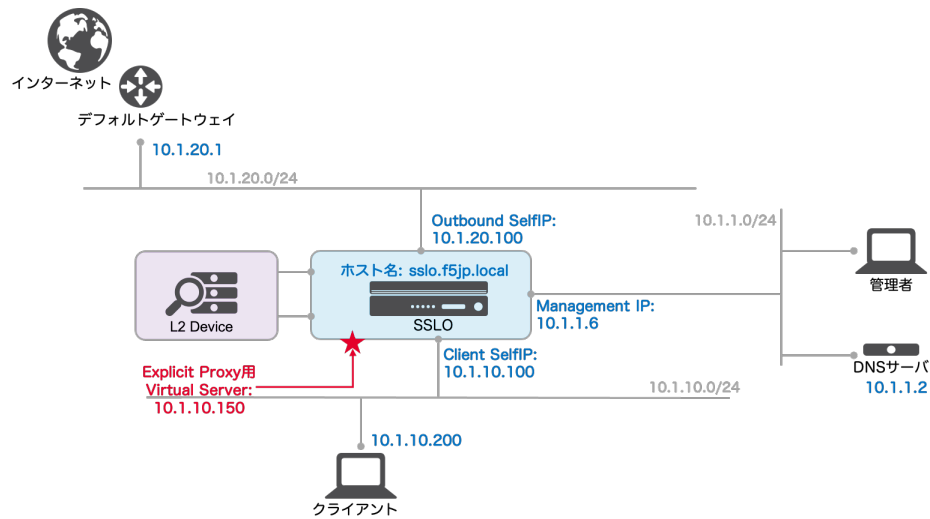
1. 利用バージョン

製品名	バージョン
TMOS	v17.10.2
F5 SSL Orchestrator(RPM)	11.0.31

注釈:

- **TMOS v17.1.0.2** 以上のバージョンをご利用下さい。
- (各 F5 代理店でサポート可能な範囲において、) 極力最新のバージョンを適用頂くことをおすすめ致します。最新のバージョンは AskF5 でご確認ください。
- Proxy 認証を行いたい場合、可視化ゾーンの機器に AD ユーザ名を転送したい場合は、APM のライセンスが必要となります。

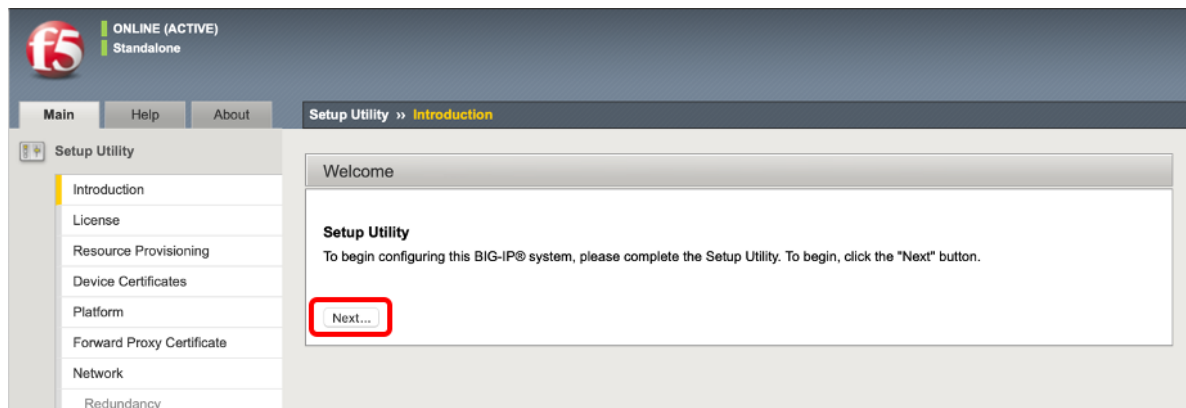
2. 本ガイドにおける構成イメージ



2.1.3 ライセンスアクティベーション、プロビジョニング、CA 証明書 / 鍵登録

(F5 ハンズオンでは以下設定済みです。)

1. *Next* ボタンを押します。



2. ライセンスをアクティベーションします。

3. 以下のモジュール（SSL 復号 / 再暗号化：SSLO）をプロビジョニングします。（F5 ハンズオンでは、1.9 章で利用する URL Filtering のカテゴリ利用のために、URLDB、現在手順にはありませんがプロキシ認証を行うための APM もプロビジョニングしています。ライセンスは SSLO と APM の 2 つと、URL Filtering サブスクリプションを利用しています。）

System » Resource Provisioning

Module Allocation License

Current Resource Allocation

CPU	MGMT TMM(87%)
Disk (122GB)	MGMT URLDB
Memory (15.6GB)	MGMT TMM URLDB

Module	Provisioning	License Status	Required Disk (GB)	Required Memory (MB)
Management (MGMT)	Small	N/A	0	1564
Local Traffic (LTM)	<input type="checkbox"/> None	Unlicensed	0	1856
Application Security (ASM)	<input type="checkbox"/> None	Unlicensed	20	1492
Fraud Protection Service (FPS)	<input type="checkbox"/> None	N/A	12	544
Global Traffic (DNS)	<input type="checkbox"/> None	Unlicensed	0	148
Link Controller (LC)	<input type="checkbox"/> None	Unlicensed	0	148
Access Policy (APM)	<input checked="" type="checkbox"/> Minimum	Licensed	12	494
Application Visibility and Reporting (AVR)	<input type="checkbox"/> None	Licensed	16	576
Policy Enforcement (PEM)	<input type="checkbox"/> None	Unlicensed	16	1223
Advanced Firewall (AFM)	<input type="checkbox"/> None	Unlicensed	16	1058
Application Acceleration Manager (AAM)	<input type="checkbox"/> None	Unlicensed	32	2050
Secure Web Gateway (SWG)	<input type="checkbox"/> None	Licensed	24	4096
iRules Language Extensions (iRulesLX)	<input type="checkbox"/> None	Licensed	0	748
URLDB Minimal (URLDB)	<input checked="" type="checkbox"/> Nominal	Licensed	36	2048
SSL Orchestrator (SSLO)	<input checked="" type="checkbox"/> Nominal	Licensed	0	128
Carrier Grade NAT (CGNAT)	<input type="checkbox"/> None	Unlicensed	16	336

Revert Submit

4. Next ボタンを押します。

ONLINE (ACTIVE)
Standalone

Main Help About Setup Utility » Device Certificates

Setup Utility

- Introduction
- License
- Resource Provisioning
- Device Certificates
- Platform
- Forward Proxy Certificate
- Network
- Redundancy
- HA VLAN
- NTP
- DNS
- ConfigSync
- Failover
- Mirroring
- Active/Standby Pair
- Discover Peer

General Properties

Name	server.crt
Certificate Subject(s)	localhost.localdomain, MyCompany

Certificate Properties

Public Key Type	RSA
Public Key Size	2048 bits
Expires	Mar 28 2030 00:11:33 PDT
Version	3
Serial Number	fc:dd:d8:33:bc:8b:c5:73
Fingerprint	SHA256:66:29:AE:E7:69:88:94:C9:4F:65:64:B6:E8:87:92:9B:4F:F7:FA:29:D7:E2:E9:E7:64:F5:73:8B:C5:52:9B:D3
Subject	Common Name: localhost.localdomain Organization: MyCompany Division: MyOrg Locality: Seattle State Or Province: WA Country: --
Issuer	Self
Email	root@localhost.localdomain
Subject Alternative Name	

Back Renew... Import... **Next...**

5. ホスト名、タイムゾーン、**Root** パスワード を設定して、*Next* ボタンを押します。

ONLINE (ACTIVE)
Standalone

Main Help About Setup Utility » Platform

Setup Utility

- Introduction
- License
- Resource Provisioning
- Device Certificates
- Platform
- Forward Proxy Certificate
- Network
- Redundancy
- HA VLAN
- NTP
- DNS
- ConfigSync
- Failover
- Mirroring
- Active/Standby Pair
- Discover Peer

General Properties

Management Config IPv4 ☐ Automatic (DHCP) ☒ Manual

IP Address[/prefix]: 10.1.2.41
Network Mask: 255.255.255.0 /24
Management Route: 10.1.2.245

Management Config IPv6 ☐ Automatic (DHCP) ☒ Manual

Host Name: sslo1.f5jplab.local
Host IP Address: Use Management Port IP Address
Time Zone: Japan

User Administration

Root Account ☐ Disable login
Password: *****
Confirm: *****

SSH Access: ☒ Enabled
SSH IP Allow: * All Addresses

Back **Next...**

6. SSLO でサーバ証明書を書き換える際に利用する CA 証明書、CA 鍵 を選択し、任意の名前 を設定し、

Next ボタンを押します。

The screenshot shows the F5 Setup Utility interface. On the left is a sidebar with a tree view containing: Introduction, License, Resource Provisioning, Device Certificates, Platform, Forward Proxy Certificate (highlighted), Network, Redundancy, HA VLAN, NTP, and DNS. The main area is titled 'Forward Proxy Certificate/Key Source'. It contains several fields: 'Import Type' is set to 'Certificate and Key'; 'Certificate and Key Name' is 'f5jplabCA'; 'Certificate Source' has 'Upload File' selected with 'Choose File' and 'f5jplabCA.crt' below it; 'Key Source' has 'Upload File' selected with 'Choose File' and 'f5jplabCA.key' below it; 'Security Type' is 'Normal'; and 'Free Space on Disk' is '3990 MB'. At the bottom left of the main area are 'Back' and 'Next' buttons, with the 'Next' button highlighted by a red rectangle.

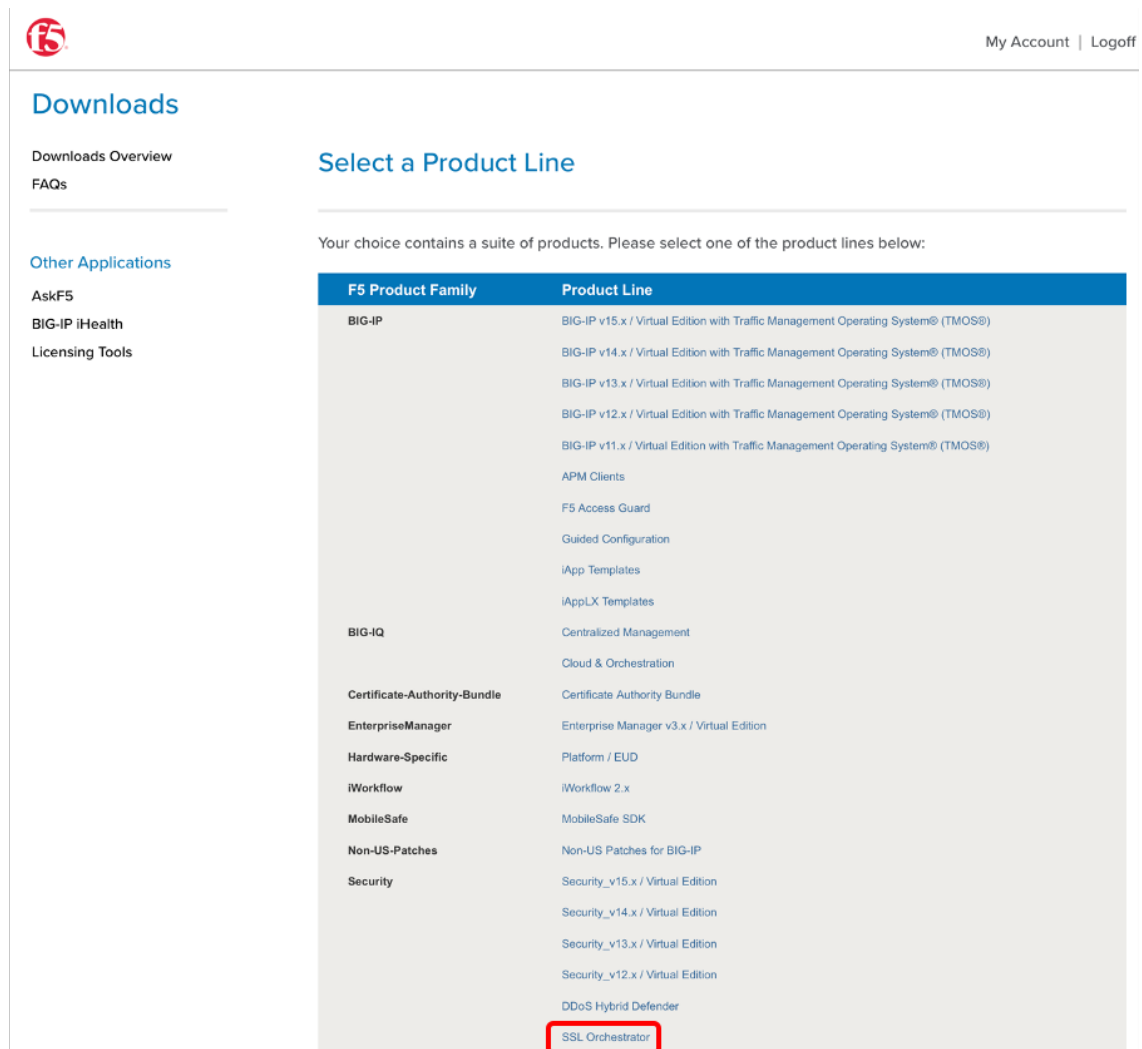
7. Finished ボタンを押します。

The screenshot shows the F5 Setup Utility interface with the 'Network' tab selected. The sidebar on the left is the same as in the previous screenshot, with 'Network' highlighted. The main area is titled 'Standard Network Configuration' and contains a list of features: Redundancy, VLANs, NTP, DNS, Config Sync, Failover, Mirroring, and Peer Device Discovery (for Redundant Configurations). Below this list is a 'Next...' button. Further down, there is a section titled 'Advanced Network Configuration' with a note: 'Create advanced device configurations by clicking **Finished** and navigating to the Main tab of the Configuration Utility.' At the bottom of this section is a 'Finished' button, which is highlighted by a red rectangle.

2.1.4 最新版の SSL Orchestrator RPM へのアップグレード

SSLO では、基本 OS である TMOS のバージョンの他に、SSLO の RPM のバージョンを考慮する必要があります。可能であれば、常に最新のバージョンにすることが好ましいです。以下の手順でアップグレードします。(F5 ハンズオンではバージョンの確認のみとなります。)

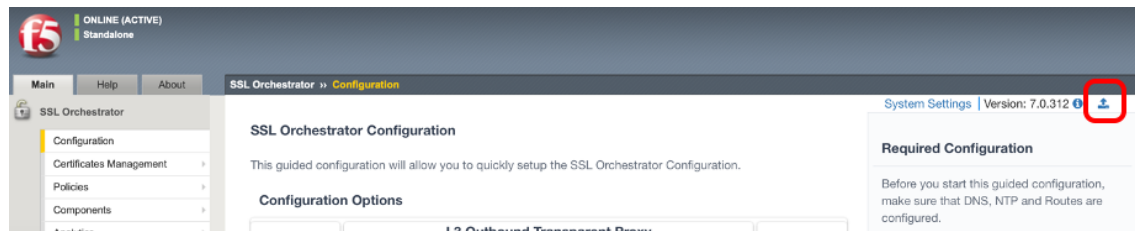
1. ASKF5 の [Download サイト](#) より最新版の SSLO RPM をダウンロードします。(ダウンロードには AskF5 のアカウント登録が必要となります。アカウント登録は数分で可能です。)



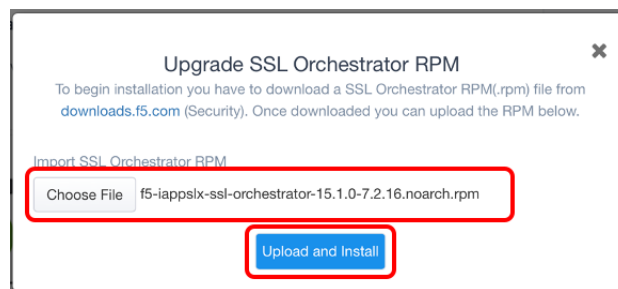
The screenshot shows the F5 Downloads page. On the left, there is a sidebar with links: Downloads Overview, FAQs, Other Applications, AskF5, BIG-IP iHealth, and Licensing Tools. The main content area is titled 'Select a Product Line' and contains the text: 'Your choice contains a suite of products. Please select one of the product lines below:'. Below this text is a table with two columns: 'F5 Product Family' and 'Product Line'. The table lists various product families and their corresponding product lines. The 'SSL Orchestrator' product line is highlighted with a red box.

F5 Product Family	Product Line
BIG-IP	BIG-IP v15.x / Virtual Edition with Traffic Management Operating System® (TMOS®)
	BIG-IP v14.x / Virtual Edition with Traffic Management Operating System® (TMOS®)
	BIG-IP v13.x / Virtual Edition with Traffic Management Operating System® (TMOS®)
	BIG-IP v12.x / Virtual Edition with Traffic Management Operating System® (TMOS®)
	BIG-IP v11.x / Virtual Edition with Traffic Management Operating System® (TMOS®)
	APM Clients
	F5 Access Guard
	Guided Configuration
	iApp Templates
	iAppLX Templates
BIG-IP	Centralized Management
	Cloud & Orchestration
Certificate-Authority-Bundle	Certificate Authority Bundle
EnterpriseManager	Enterprise Manager v3.x / Virtual Edition
Hardware-Specific	Platform / EUD
iWorkflow	iWorkflow 2.x
MobileSafe	MobileSafe SDK
Non-US-Patches	Non-US Patches for BIG-IP
Security	Security_v15.x / Virtual Edition
	Security_v14.x / Virtual Edition
	Security_v13.x / Virtual Edition
	Security_v12.x / Virtual Edition
	DDoS Hybrid Defender
	SSL Orchestrator

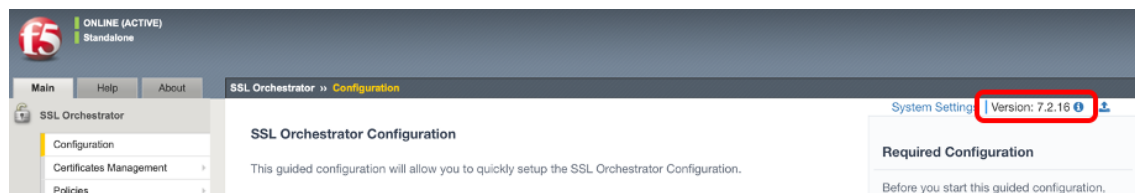
2. SSL Orchestrator >> Configuration の画面にて、右上の アップグレードボタン を押します。



3. *Choose File* にて、先程ダウンロードした RPM を選択し、*Upload and Install* を押します。

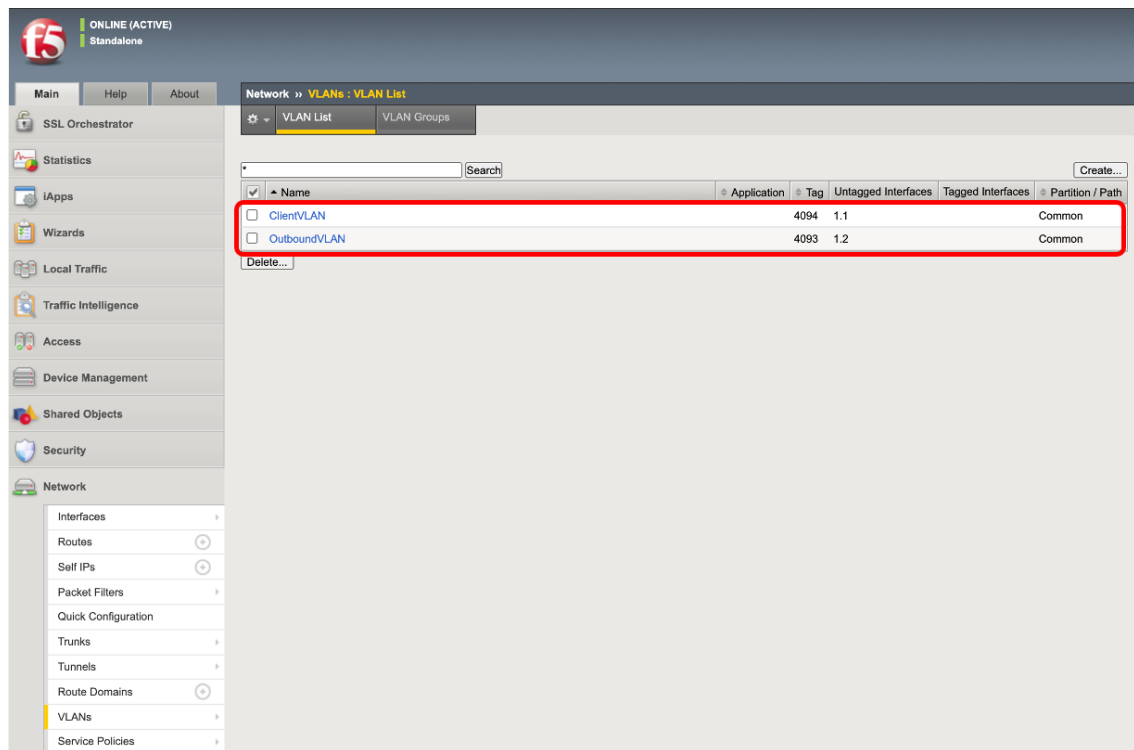


4. バージョンがアップグレードされていることを確認します。

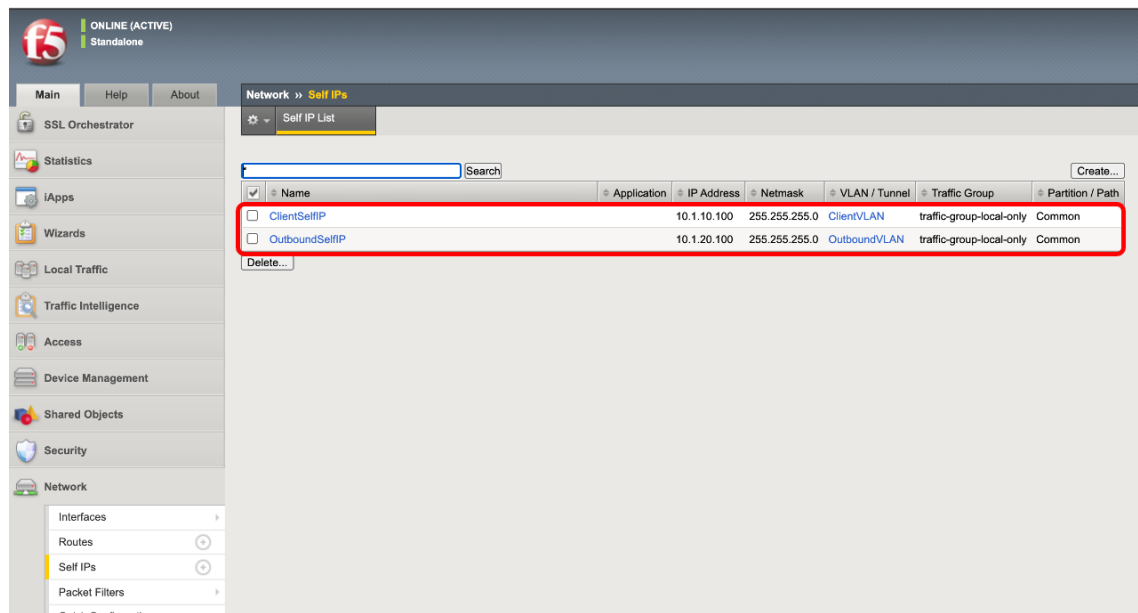


2.1.5 Network の基本設定

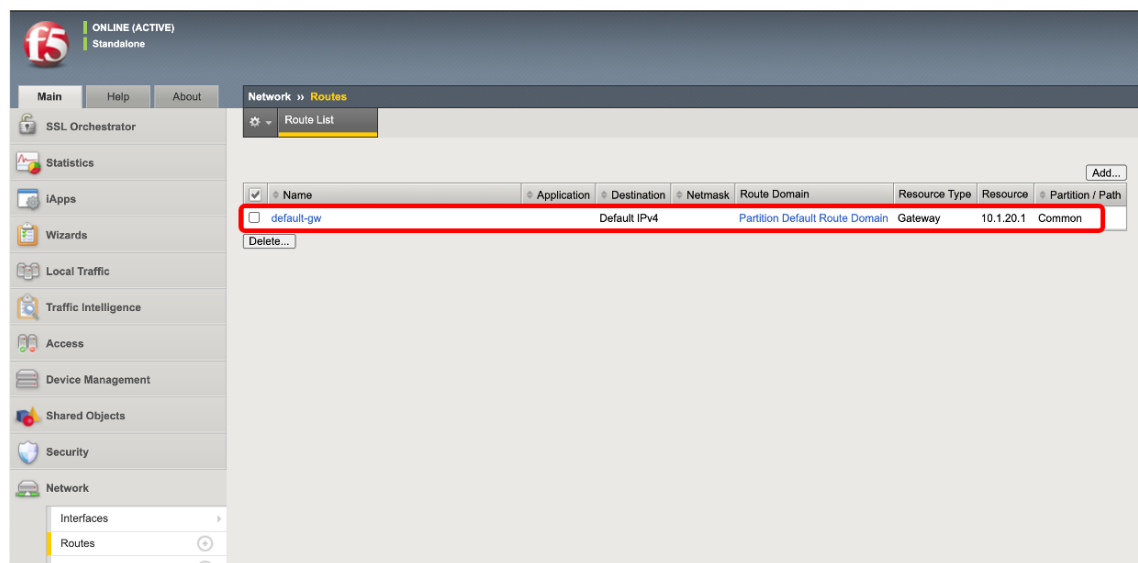
1. VLAN の設定を行います。(F5 ハンズオンでは設定済み)



2. Self IP の設定を行います。(F5 ハンズオンでは設定済み)



3. デフォルトゲートウェイの設定を行います。(F5 ハンズオンでは設定済み)



2.1.6 DNS, NTP の設定

1. DNS の設定を行います。(F5 ハンズオンでは設定済み)

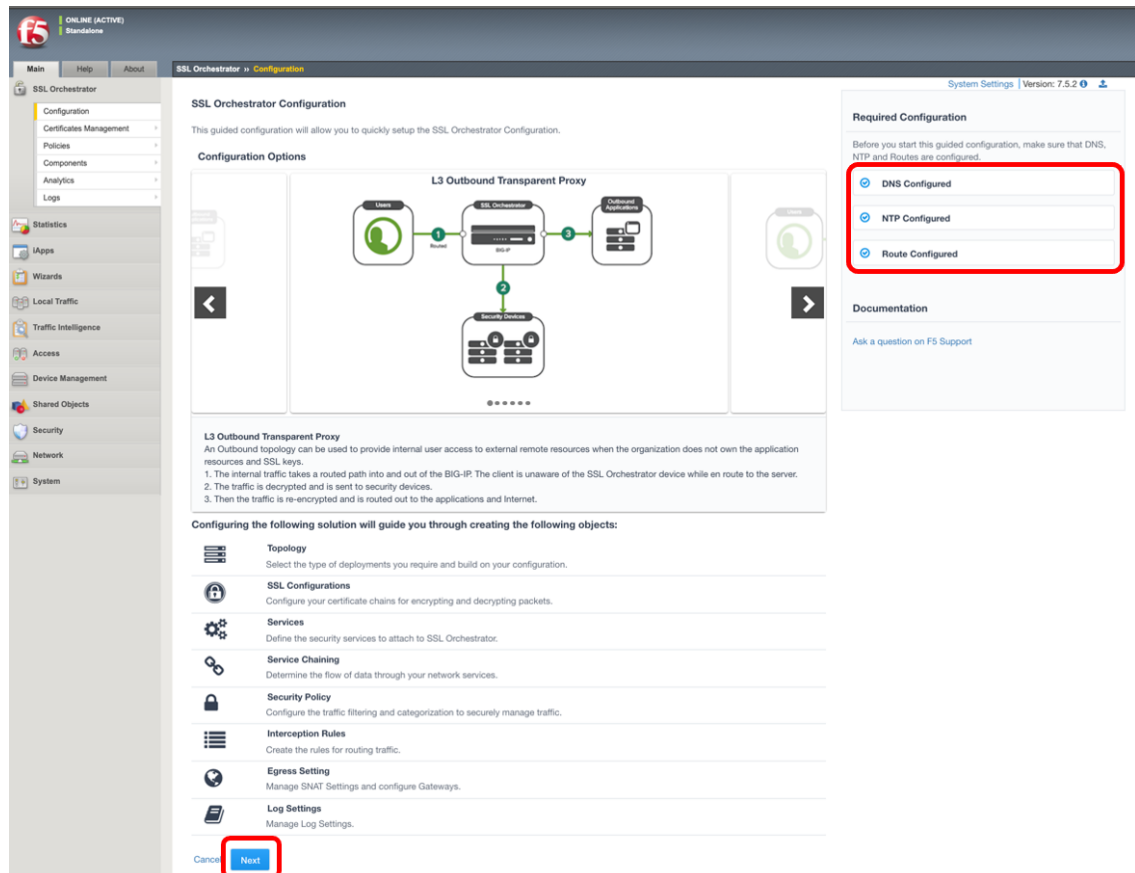
The screenshot shows the F5 Management Center interface for configuring DNS. The left sidebar contains a navigation menu with options like Main, Help, About, SSL Orchestrator, Statistics, iApps, Wizards, Local Traffic, Traffic Intelligence, Access, Device Management, Shared Objects, Security, Network, and System. The main content area is titled 'System >> Configuration : Device : DNS'. Below this, there are tabs for 'Device', 'Local Traffic', 'OVSDB', and 'App IQ'. The 'Device' tab is selected. The 'Properties' section on the right contains three main configuration areas: 'DNS Lookup Server List', 'BIND Forwarder Server List', and 'DNS Search Domain List'. Each area has an 'Address' field, an 'Add' button, and a list of addresses. The 'DNS Lookup Server List' has one address, '10.1.1.2', which is highlighted with a red box. The 'BIND Forwarder Server List' has one address, '10.1.1.2'. The 'DNS Search Domain List' has one address, 'localhost'. Below these lists are 'Edit', 'Delete', 'Up', and 'Down' buttons. At the bottom of the 'Properties' section, there are checkboxes for 'DNS Cache' and 'IP Version' (set to 'IPv4'), and an 'Update' button.

2. NTP の設定を行います。(F5 ハンズオンでは設定済み)

The screenshot shows the F5 Management Center interface for configuring NTP. The left sidebar is the same as in the previous screenshot. The main content area is titled 'System >> Configuration : Device : NTP'. Below this, there are tabs for 'Device', 'Local Traffic', 'OVSDB', and 'App IQ'. The 'Device' tab is selected. The 'Properties' section on the right contains a single configuration area: 'Time Server List'. It has an 'Address' field, an 'Add' button, and a list of addresses. The list contains one address, 'ntp.nict.jp', which is highlighted with a red box. Below the list are 'Edit' and 'Delete' buttons. At the bottom of the 'Properties' section, there is an 'Update' button.

2.1.7 SSLO Guided Configuration による SSLO の設定

1. **SSL Orchestrator >> Configuration** を選択します。DNS と NTP と Route が **Configure** となっているのを確認し、*Next* ボタンを押します。



2. 任意の名前を設定し、SSL Orchestrator Topologies として、**L3 Explicit Proxy** を選択し、*Save & Next* ボタンを押します。

SSL Orchestrator » Configuration

SSL Orchestrator Configuration Not Saved

Topology SSL Configuration Service Service Chain Security Policy Interception Rule Egress Setting Log Settings Summary

Topology Properties

Name
sslo: **L3Explicit**

In the topology Name field, type a name after the default prefix sslo_.

Description

Provide a description for this deployment.

Protocol i
TCP

IP Family i
IPv4

SSL Orchestrator Topologies i

L2 Outbound

L3 Outbound

L3 Explicit Proxy

L2 Inbound

L3 Inbound

Existing Application

*L2 Inbound and L2 Outbound topologies are only available on supported platforms. This platform does not support L2.

Cancel Save Draft **Save & Next**

3. **Create New** を選択し、右上の *Show Advanced Setting* をクリックします。

SSL Orchestrator » Configuration

SSL Orchestrator Configuration :sslo_L3Explicit Not Deployed

Topology SSL Configuration Service Service Chain Security Policy Interception Rule Egress Setting Log Settings Summary

SSL Configurations

SSL Profile i

☒ Create New ☐ Use Existing

Show Advanced Setting

4. **Client-side SSL** にて、利用したい TLS のバージョン を選択します。

Client-side SSL

Processing Options ⓘ

Enabled Options

Filter

TLSv1.1

TLSv1.2

TLSv1.3

Disabled Options

Cipher Type ⓘ

☒ Cipher Group ☐ Cipher String

Cipher

/Common/f5-default

Specify the ciphers that the system supports from the list. The default cipher list will display DEFAULT in the field.

5. **CA Certificate KeyChain** にて、既にインポート済みの CA ファイル (F 5 ハンズオンでは、証明書と秘密鍵に **f5jCA** を選択し、Passphrase に **f5demo** と入力します。) を選択して **Done** を押します。

CA Certificate Key Chain ⓘ

CA Certificate Key Chains

Certificate

/Common/f5jCA

Key

/Common/f5jCA

Chain

--Select--

Passphrase

.....

Cancel Done

No Cert Key Chains

☐ Bypass on Handshake Alert

☐ Bypass on Client Certificate Failure

6. Server-side SSL も同様に利用したい TLS バージョン を選択します。

Server-side SSL

Processing Options ⓘ

Enabled Options

Disabled Options

Filter

TLSv1.1

TLSv1.2

TLSv1.3

←

→

Cipher Type ⓘ

☒ Cipher Group ☐ Cipher String

Cipher

/Common/f5-default

Specify the ciphers that the system supports from the list. The default cipher list will display **DEFAULT** in the field.

7. 期限切れの証明書や自己署名証明書に対しての動作も確認し、*Save & Next* を押します。

Trusted Certificate Authority ⓘ

/Common/ca-bundle.crt

Expire Certificate Response ⓘ

drop

Untrusted Certificate Authority ⓘ

drop

OCSP ⓘ

--Select-- ↻

CRL ⓘ

--Select-- ↻

Cancel Save Draft Back **Save & Next**

8. OCSP を使用する場合、Authentication List 設定を追加することができます。本環境では使用しないため、*Save & Next* を押します。

Authentication List

Add

Delete

Items: 0

Filter Type by Name...

Name	Authentication Type
------	---------------------

Cancel

Save Draft

Back

Save & Next

9. サービス（ここでは L2 デバイス）を追加します。Add Service を押します。

SSL Orchestrator » **Configuration**

SSL Orchestrator Configuration :ssl0_L3Explicit NOT DEPLOYED

Topology

SSL Configuration

Service

Service Chain

Security Policy

Interception Rule

Egress Setting

Log Settings

Summary

Services List

Add Service

Delete Service

Items: 0

Filter Type by Name...

<input type="checkbox"/> Name	Service Type
-------------------------------	--------------

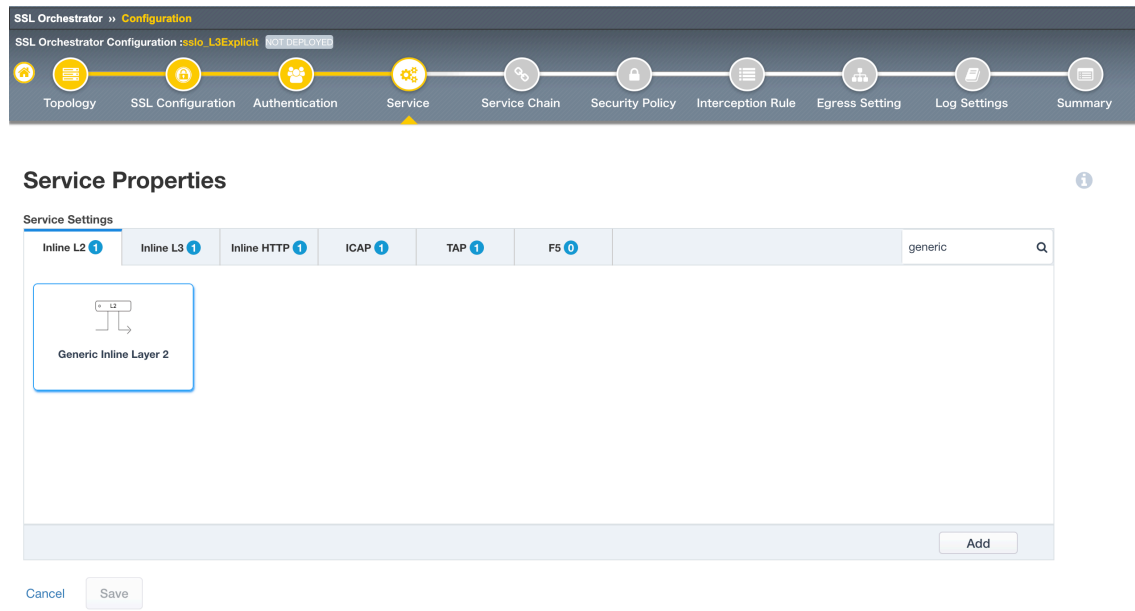
Cancel

Save Draft

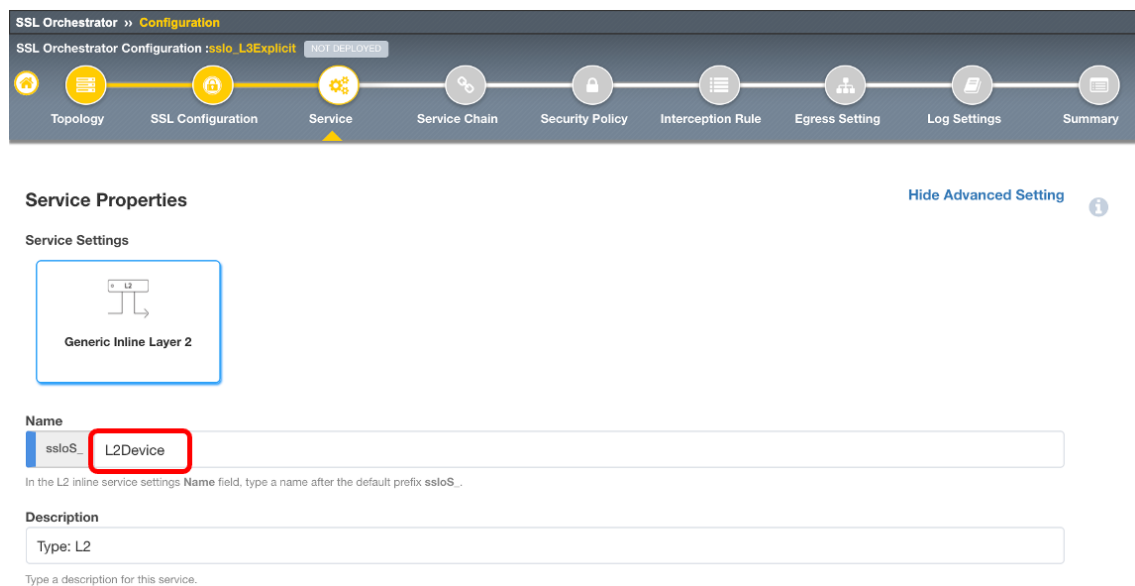
Back

Save & Next

10. **Generic Inline Layer2** を選択し、**Add** ボタンを押します。



11. 右上の **Show Advanced Setting** をクリックし、任意の名前 を設定します。



12. **Network Configuration** にて、**Add** ボタンを押します。 **From BIGIP VLAN** にて **Create New** を選択し、任意の名前を設定し、**Interface** を選択します。同様に、**To BIGIP VLAN** も設定します。(F5 ハンズオンでは、名称は任意で構いませんが、Interface はそれぞれ、**1.3** と **1.4** を選択します。) **Done** ボタンを押します。

Network Configuration

Ratio
1
Enter a valid ratio number in the range 1-65535.

From BIGIP VLAN ⓘ
☒ Create New ☐ Use Existing

Name
ssloN_ L2_In
In the From BIGIP VLAN Name field, type a name for the source BIGIP VLAN network after the default prefix ssloN_.

Interface
1.3
Select the associated BIG-IP system interface.

Tag

To BIGIP VLAN ⓘ
☒ Create New ☐ Use Existing

Name
ssloN_ L2_Out
In the To BIGIP VLAN Name field, type a name for the destination BIGIP VLAN network after the default prefix ssloN_.

Interface
1.4
Select the associated BIG-IP system interface.

Tag

Cancel Done

13. L2 デバイスが SSL 復号したトラフィックを HTTP トラフィックと同じようにセキュリティ検査するように、ポートリマップを行います。L2 デバイスによっては 443 ポートで接続すると、SSL トラフィックだと判断し、セキュリティ検査を正しく行わない場合があるためです。 **Enable Port Remap** にチェックをいれ、 **Remap Port** に必要なポート番号を設定し、 **Save** ボタンを押します。(L2 デバイスによって、仕様は異なります。F5 ハンズオンでは、**8080** と設定しておきます。)

Device Monitor ⓘ
/Common/gateway_icmp

Service Down Action ⓘ
Ignore

Internal IP Offset ⓘ
0

Internal IPv4 Address
198.19.32.0

Internal IPv6 Address
2001:0200:0:0200::

☒ Enable Port Remap

Specify whether you want to enable the Remap Port feature for inline services by selecting the Enable Port Remap check box.

Remap Port
8080

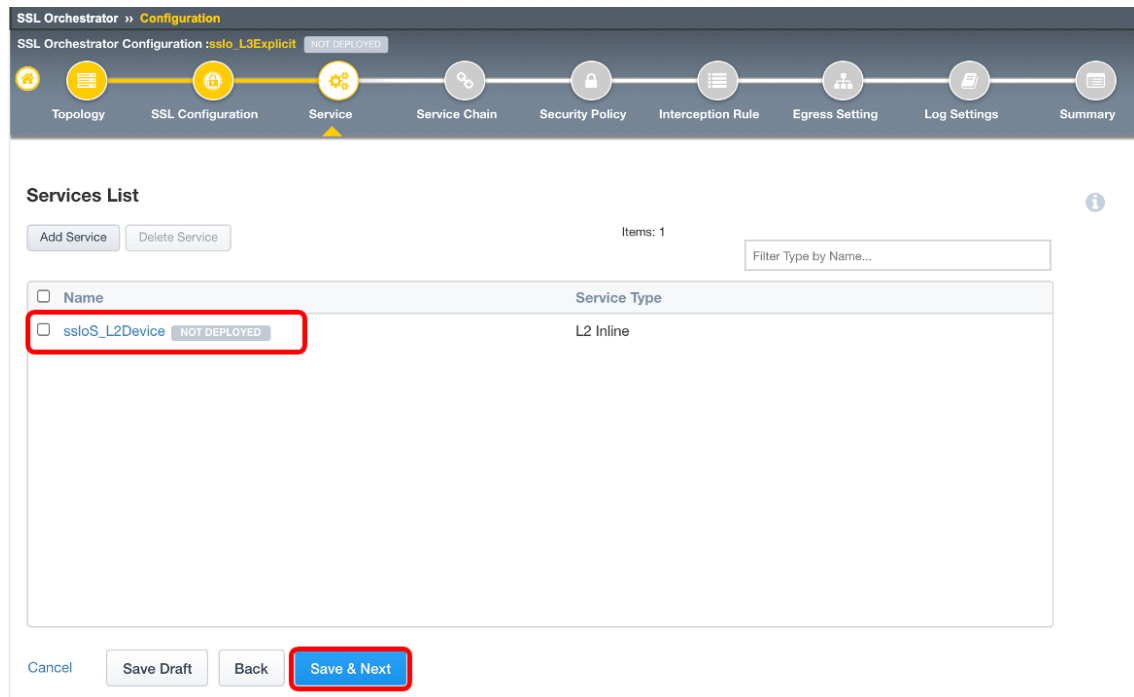
Specify the remap port number. The default is 80.

iRules ⓘ

Available		Selected
Filter		
No available items	<div>← → ↑ ↓</div>	

[Cancel](#) [Save](#)

14. 以下のようにサービスが追加されているのを確認したら、*Save* & *Next* を選択します。



- サービスチェーンを作成します。サービスチェーンを複数作成することで、可視化デバイスが複数ある場合に、条件に応じた可視化デバイスへの転送が可能となります。（この F5 ハンズオンでは可視化デバイスは 1 台ですが、サービスチェーンの作成は必要です。） **Service Chain List** で *Add* を押します。

SSL Orchestrator » Configuration

SSL Orchestrator Configuration :sslo_L3Explicit NOT DEPLOYED

Topology SSL Configuration Service Service Chain Security Policy Interception Rule Egress Setting Log Settings Summary

Services Chain List

Add Delete Items: 0 Filter Type by Name...

Name	Description
------	-------------

Cancel Save Draft Back Save & Next

16. 任意の名前を設定し、先程作成したサービスを右に移動させ、*Save* ボタンを押します。

SSL Orchestrator » Configuration

SSL Orchestrator Configuration :sslo_L3Explicit NOT DEPLOYED

Topology SSL Configuration Service Service Chain Security Policy Interception Rule Egress Setting Log Settings Summary

Services Chain Properties

Name
ssloSC_ MyServiceChain

In the services chain properties Name field, type a name after the default prefix ssloSC_.

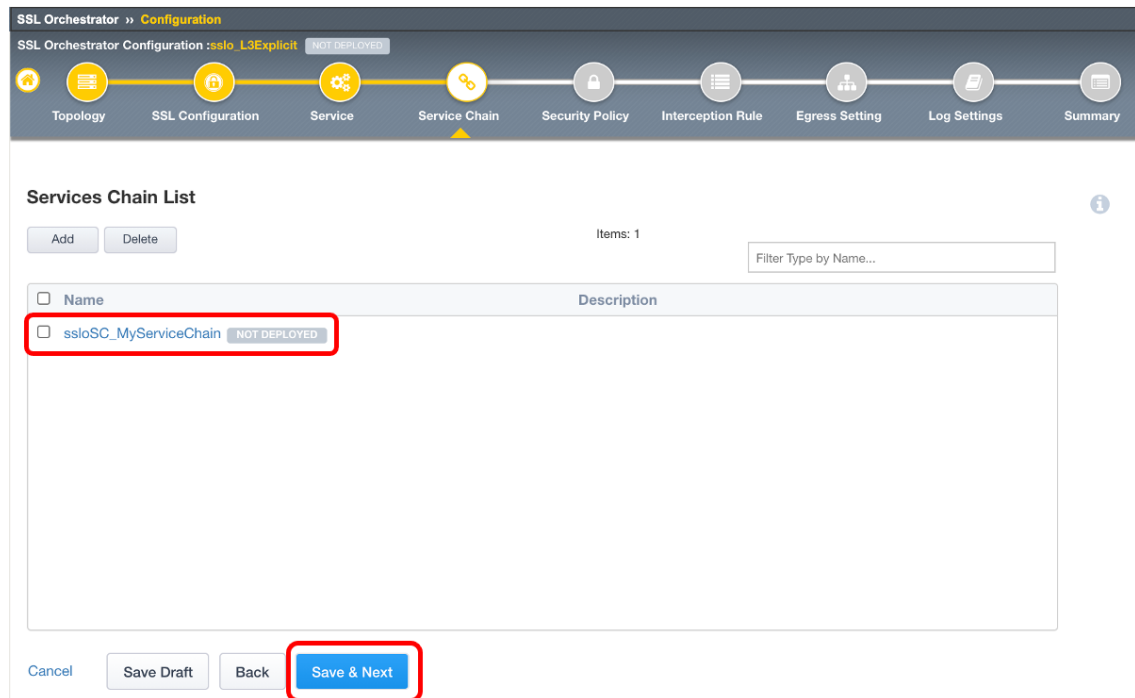
Description
Type a description for the service chain.

Services

Services Available	Selected Service Chain Order
Filter No available items	ssloS_L2Device

Cancel Save

17. **Service Chain** ができたことを確認し、*Save & Next* ボタンを押します。



18. セキュリティポリシーを設定します。All Traffic の ペンマーク をクリックします。

SSL Orchestrator >> Configuration

SSL Orchestrator Configuration :sslo_L3Explicit NOT DEPLOYED

Topology SSL Configuration Service Service Chain Security Policy Interception Rule Egress Setting Log Settings Summary

Security Policy

Type ⓘ

☒ Create New ☐ Use Existing ☐ None

Name

ssloP_ L3Explicit

In the security policy Name field, type a name after the default prefix ssloP_.

Description ⓘ

Rules

Name	Conditions	Action	SSL Forward Proxy Action	Service Chain
Pinner's_Rule	SSL Check is true and Category Lookup (SNI) is Pinner's	Allow	Bypass	-
All Traffic	All	Allow	Intercept	-

Add

19. 先程作成した **Service Chain** を選択し、**OK** ボタンを押します。

Rules

Name	Conditions	Action	SSL Forward Proxy Action	Service Chain
Pinner's_Rule	SSL Check is true and Category Lookup (SNI) is Pinner's	Allow	Bypass	-

Name

Default Rule

Type the name of your custom policy.

Action ⓘ

Allow

SSL Forward Proxy Action ⓘ

Intercept

Service Chain ⓘ

ssloSC_MyServiceChain

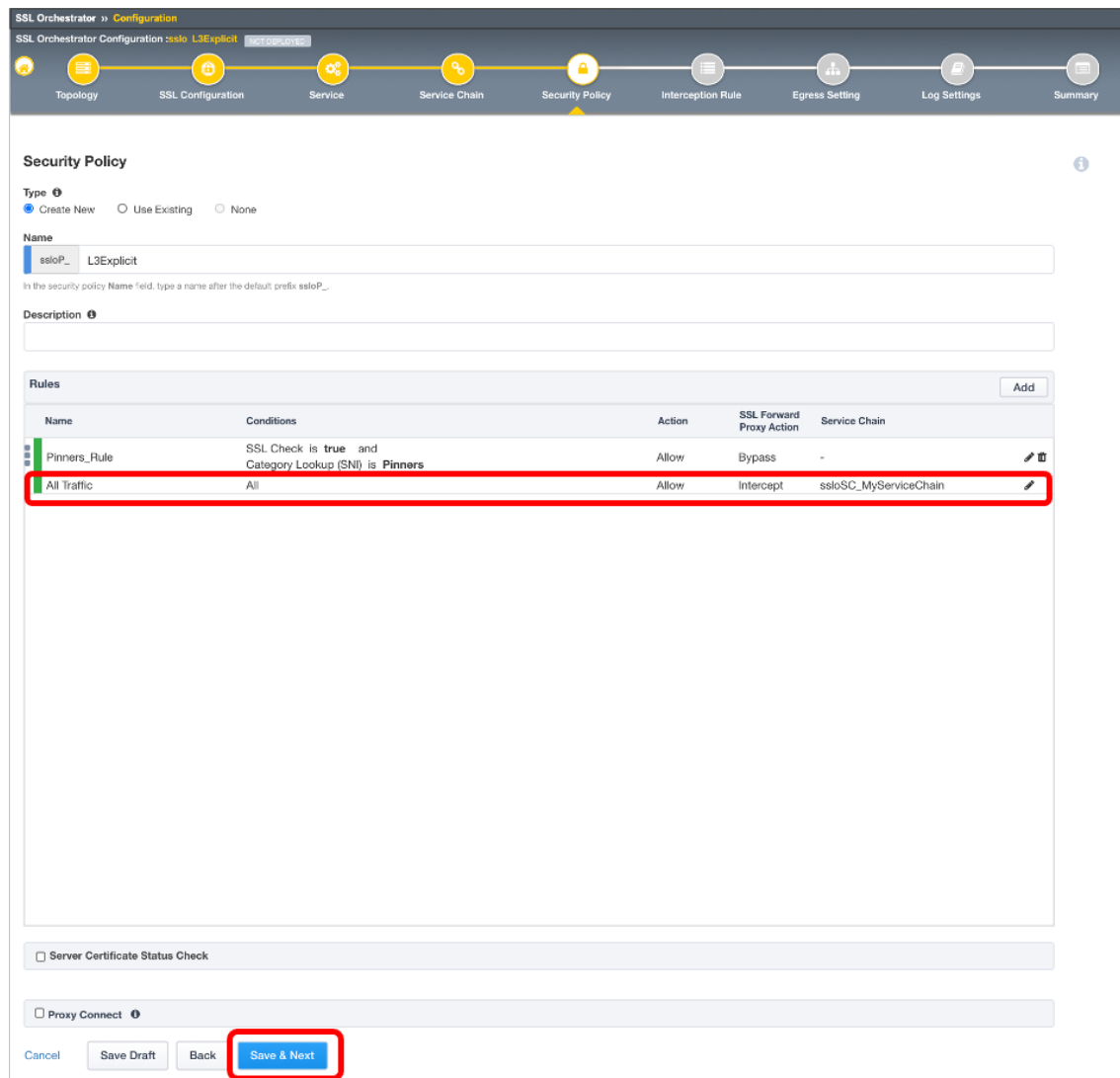
Search

None

ssloSC_MyServiceChain

Cancel OK

20. サービスチェーンが追加されたことを確認し、**Save & Next** ボタンを押します。



SSL Orchestrator » Configuration

SSL Orchestrator Configuration: sslo L3Explicit

Topology SSL Configuration Service Service Chain Security Policy Interception Rule Egress Setting Log Settings Summary

Security Policy

Type

☒ Create New ☐ Use Existing ☐ None

Name

ssloP_ L3Explicit

In the security policy Name field, type a name after the default prefix ssloP_

Description

Rules

Name	Conditions	Action	SSL Forward Proxy Action	Service Chain
Pinners_Rule	SSL Check is true and Category Lookup (SNI) is Pinners	Allow	Bypass	-
All Traffic	All	Allow	Intercept	ssloSC_MyServiceChain

☐ Server Certificate Status Check

☐ Proxy Connect

Cancel Save Draft Back **Save & Next**

21. **Proxy Server Settings** にクライアントからプロキシとしてアクセスさせる IP アドレス (F5 ハンズオンでは、10.1.10.150) を入力し、**DNS Resolver** をプルダウンメニューから選択します (F5 ハンズオンでは、ssloGS_global.app/ssloGS-net-resolver)。 **Ingress Network** として、クライアントからアクセス可能な **VLAN** (F5 ハンズオンでは、ClientVLAN) を選択し、*Save & Next* ボタンを押します。

Proxy Server Settings

IPv4 Address
10.1.10.150
Specify the IPv4 IP address.

Port
3128
Specify the service port number, 0 to 65535.

Access Profile ⓘ
None ▾

HTTP Profile ⓘ
/Common/sslo_L3Explicit.app/sslo_L3Explicit-xp-http ▾

DNS Resolver
/Common/ssloGS_global.app/ssloGS-net... ▾
You are required to select a DNS Resolver for a topology-based HTTP Profile.

Authentication

OCSP Responder ⓘ
None ▾

Ingress Network

VLANs

Available

Filter
/Common/OutboundVLAN

Selected

/Common/ClientVLAN

Create

Select one or more VLANs where transparent-proxy ingress traffic will arrive.

Protocol Settings

SSL Configurations

Available

Filter

Selected

ssloT_L3Explicit

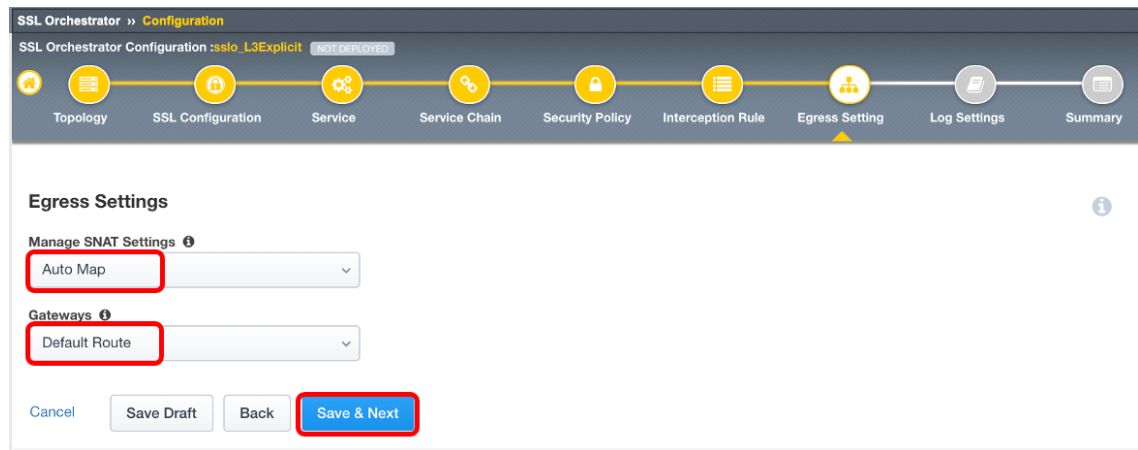
Specify the SSL setting.

Client TCP Profile
/Common/sslo_L3Explicit.app/sslo_L3Explicit-tcp-lan

☐ **Verified Accept** ⓘ
Specify the client TCP profile setting.

Cancel Save Draft Back **Save & Next**

22. **Manage SNAT Settings** で **Auto Map**、**Gateways** で **Default Route** を選択し、**Save & Next** ボタンを押します。(F5 ハンズオンではこのように設定しますが、環境に合わせてください。)



SSL Orchestrator >> Configuration

SSL Orchestrator Configuration :sslo_L3Explicit (NOT DEPLOYED)

Topology SSL Configuration Service Service Chain Security Policy Interception Rule Egress Setting Log Settings Summary

Egress Settings

Manage SNAT Settings ⓘ

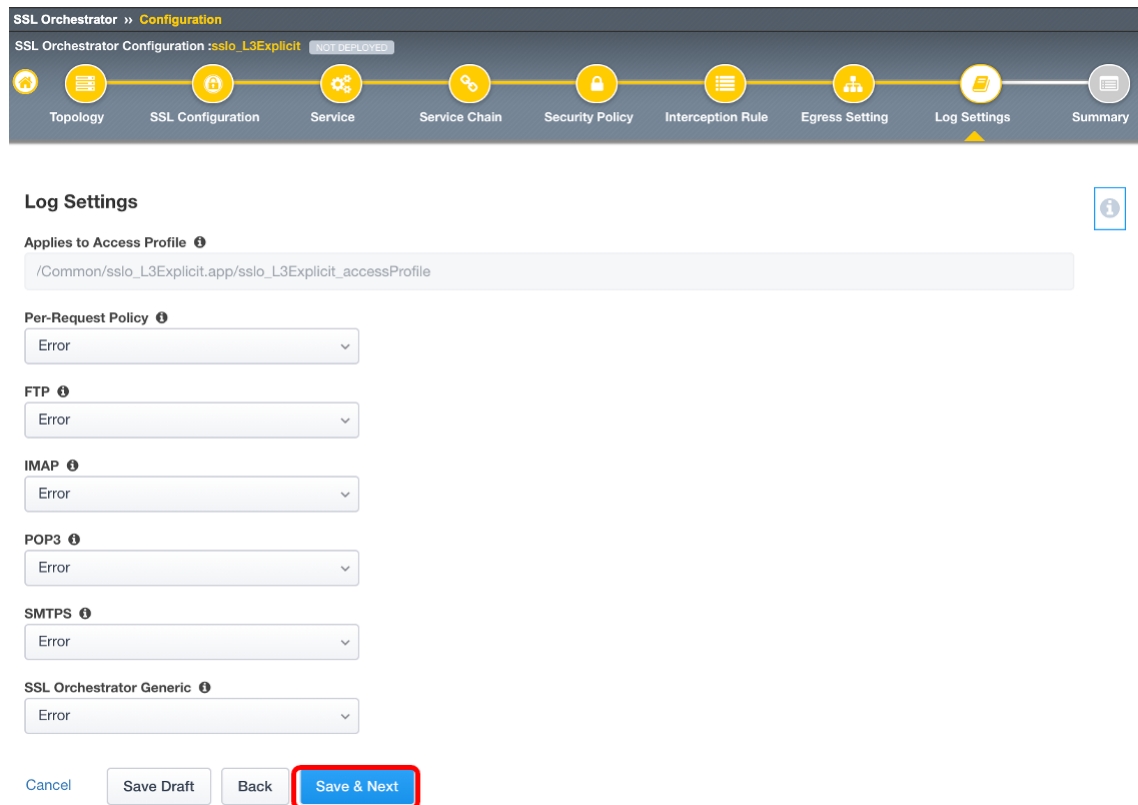
Auto Map

Gateways ⓘ

Default Route

Cancel Save Draft Back **Save & Next**

23. *Save & Next* ボタンを押します。



SSL Orchestrator >> Configuration

SSL Orchestrator Configuration :sslo_L3Explicit (NOT DEPLOYED)

Topology SSL Configuration Service Service Chain Security Policy Interception Rule Egress Setting Log Settings Summary

Log Settings

Applies to Access Profile ⓘ

/Common/sslo_L3Explicit.app/sslo_L3Explicit_accessProfile

Per-Request Policy ⓘ

Error

FTP ⓘ

Error

IMAP ⓘ

Error

POP3 ⓘ

Error

SMTPS ⓘ

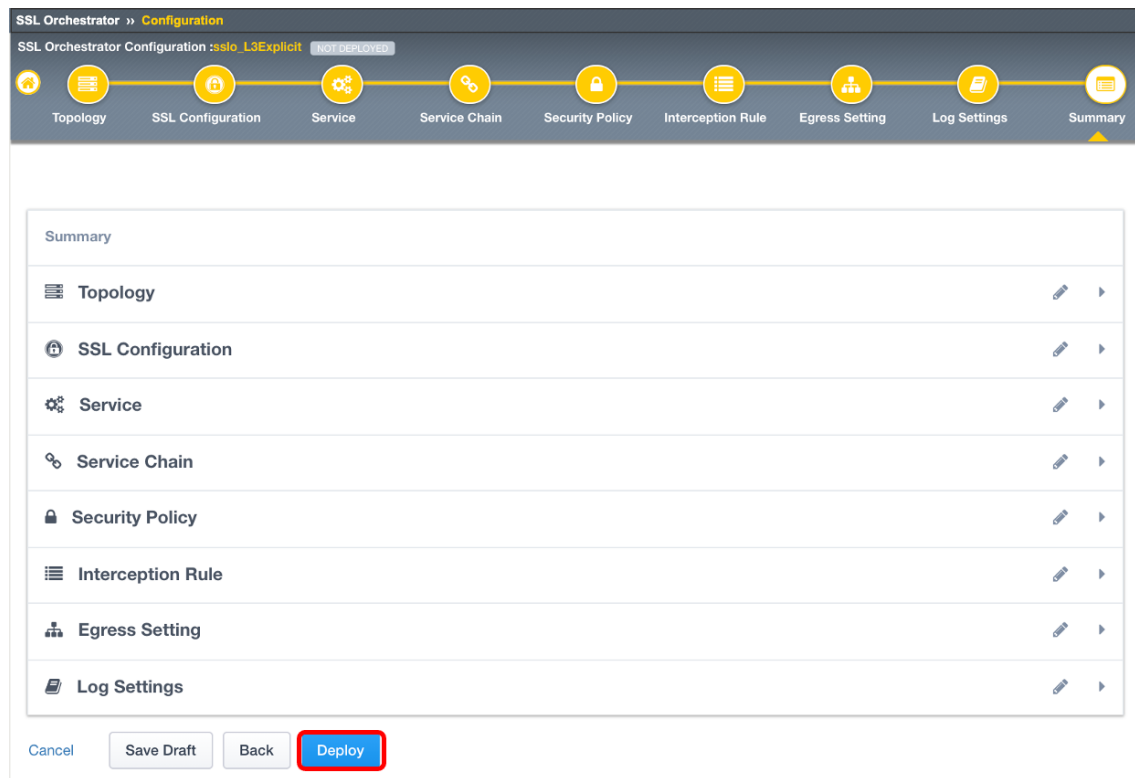
Error

SSL Orchestrator Generic ⓘ

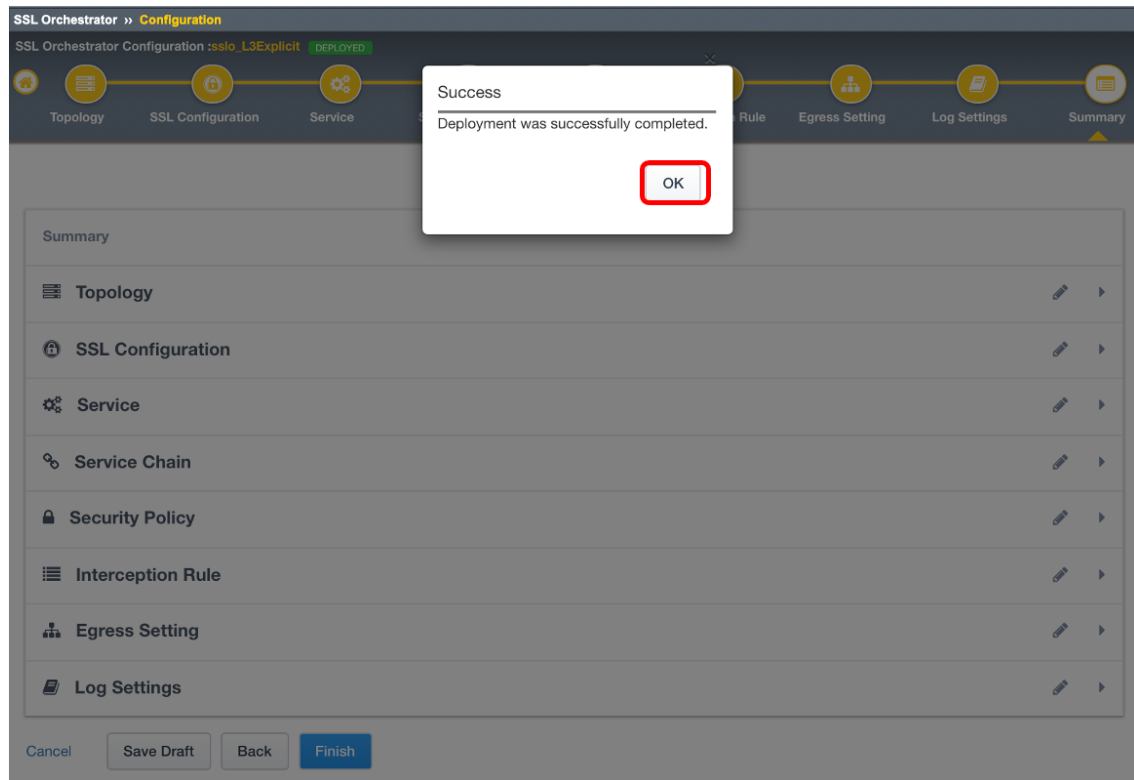
Error

Cancel Save Draft Back **Save & Next**

24. 必要に応じて、設定内容を見直し、*Save & Next* ボタンを押します。



25. Success ポップアップが表示されるまで待ち。OK ボタンを押します。

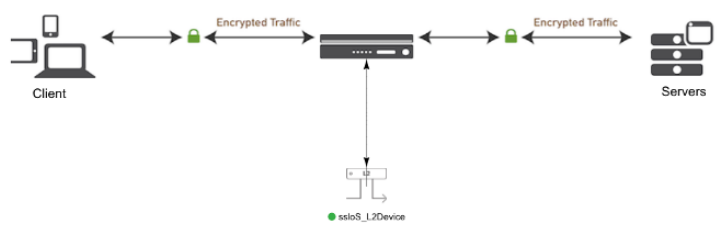


26. Deploy に成功すると以下のような緑色の **DEPLOYED** マークが表示されます。右上の **System Settings** アイコンを選択します。

SSL Orchestrator » Configuration

Configure Dashboard

Version: 7.5.2



Client Proxy Servers

ssloS_L2Device

Encrypted Traffic

Encrypted Traffic

Topologies Interception Rules Services Service Chains Security Policies SSL Configurations

Add Delete Items: 1

Name	Type	Security Policy	SSL Configuration...	Protected/Unprote...
sslo_L3Explicit DEPLOYED	L3 Explicit Proxy	ssloP_L3Explicit	ssloT_L3Explicit	

27. SSLO が Explicit Proxy として利用する **DNS** を設定し（F5 ハンズオンでは、10.1.1.2）、*Save & Next* を押します。

SSL Orchestrator » Configuration

System Settings : sslundefined NOT DEPLOYED

System Settings Summary

System Settings

IP Family ⓘ
IPv4

DNS Settings

DNS Query resolution ⓘ
Local Forwarding Nameserver

Local Forwarding NameServer(s)
Local DNS Nameserver*

10.1.1.2 + x

Type the IP addresses of local nameservers which will resolve all DNS queries from this solution. Click + to add additional nameservers.

Gateways Configuration

Gateways ⓘ
Default Route

Cancel Save Draft Save & Next

28. *Deploy* を押します。

SSL Orchestrator » Configuration

System Settings : sslundefined NOT DEPLOYED

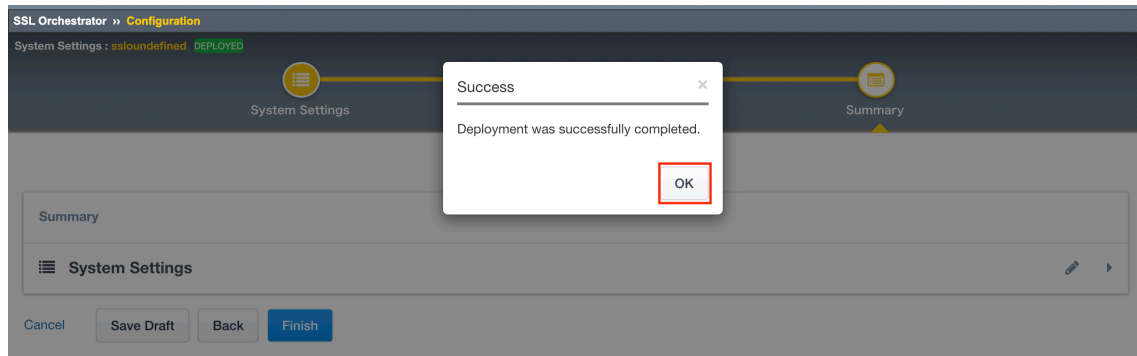
System Settings Summary

Summary

System Settings

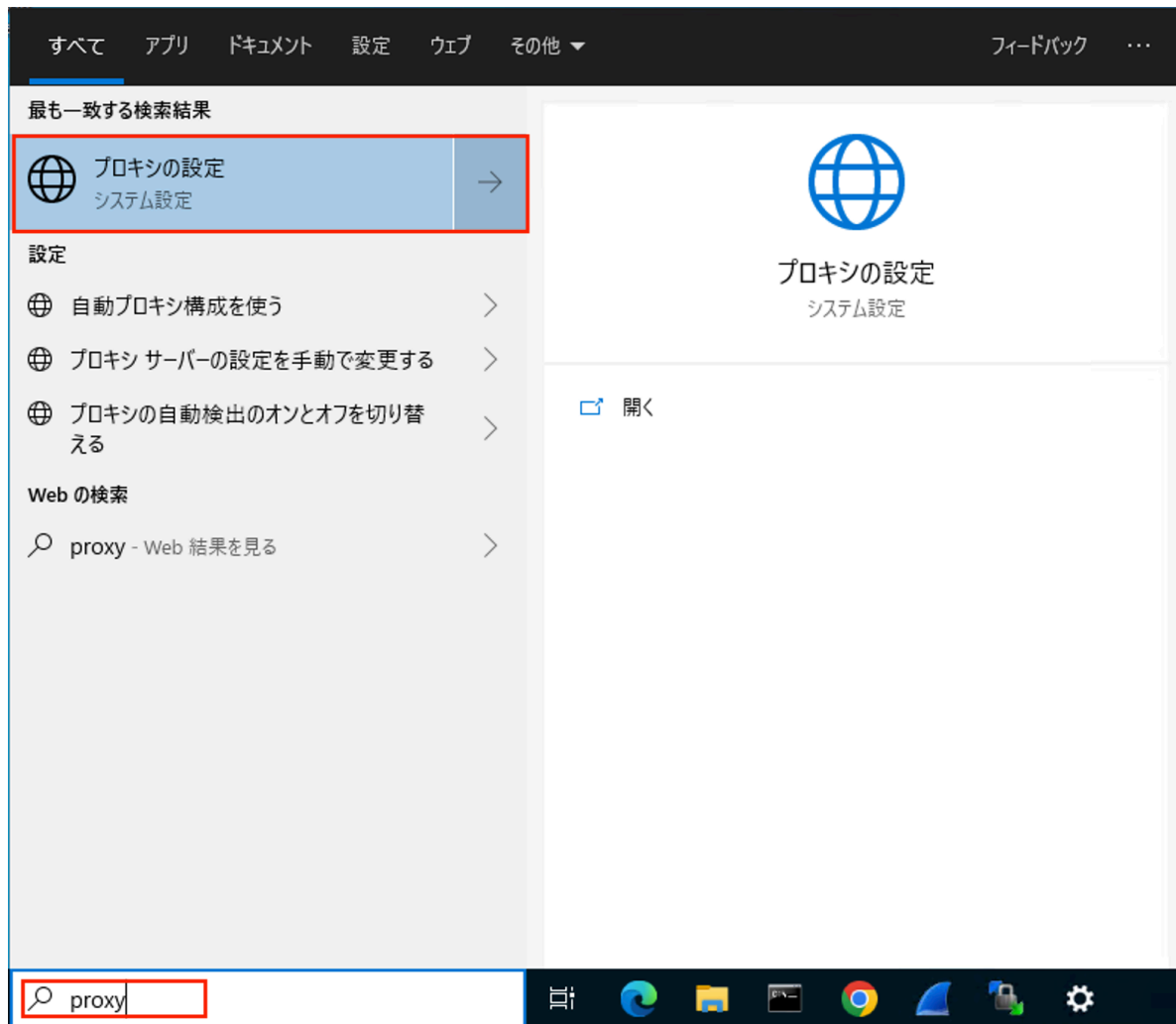
Cancel Save Draft Back Deploy

29. Success ポップアップが表示されるまで待ち、OK ボタンを押します。

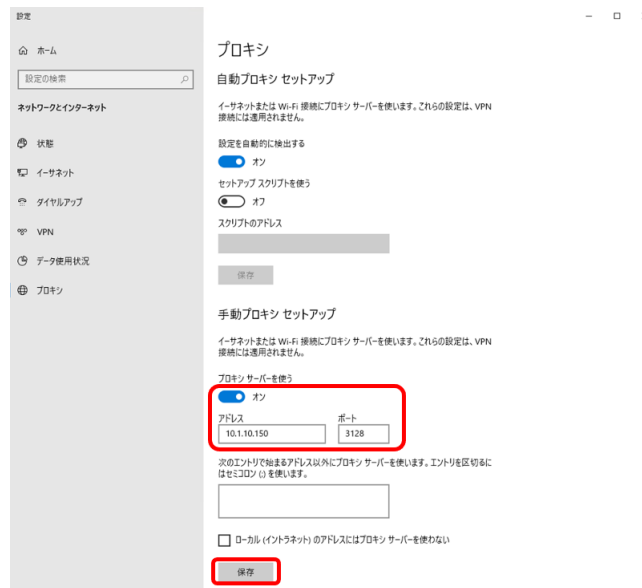


2.1.8 クライアントからの接続テスト

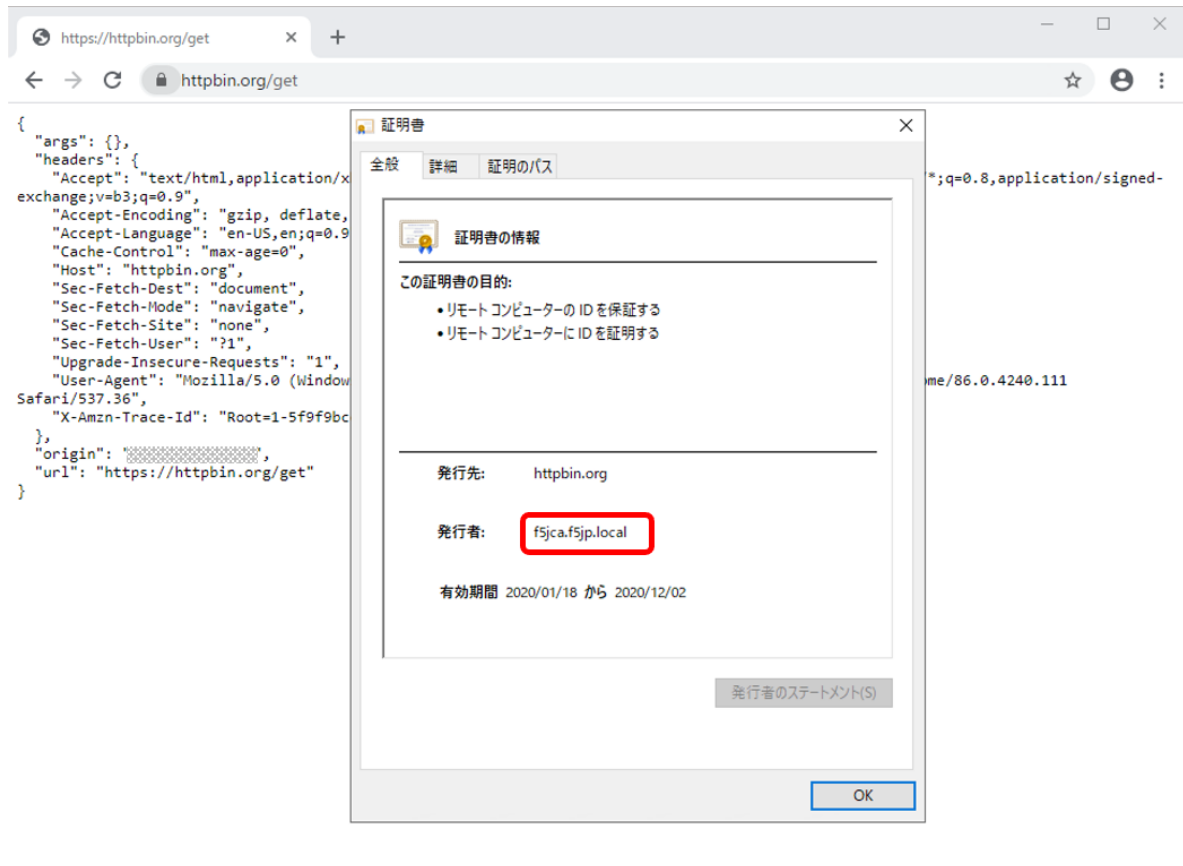
1. Windows クライアントを起動し、に SSLO に設定した CA 証明書をインポートします。(F5 ハンズオンでは、インポート済みです。)
2. プロキシ設定を行います。検索ボックスに proxy と入力し、プロキシの設定を開きます。



3. プロキシ設定として、SSLO で設定した Explicit Proxy のアドレスとポート番号を設定します。(F5 ハンズオンでは、アドレス:10.1.10.150、ポート:3128 が設定済みです。)



4. ブラウザを開き、任意の HTTPS サイトに接続し、そのサーバ証明書が SSLO で設定した CA 証明書によって書換えられていることを確認します。



5. curl コマンドで確認する場合は、`curl -vk --proxy 10.1.10.150:3128 https://httpbin.org/get` と入力し、確認します。(本ガイドからコピペすると、ハイフン (-) ハイフン (-)proxy が失敗する可能性がありますので、そこは入力し直してください。)

```

Administrator: コマンドプロンプト
C:\Users\Administrator>curl -vk --proxy 10.1.10.150:3128 https://httpbin.org/get
Trying 10.1.10.150...
TCP_NODELAY set
Connected to 10.1.10.150 (10.1.10.150) port 3128 (#0)
allocate connect buffer!
Establish HTTP proxy tunnel to httpbin.org:443
CONNECT httpbin.org:443 HTTP/1.1
Host: httpbin.org:443
User-Agent: curl/7.55.1
Proxy-Connection: Keep-Alive

HTTP/1.1 200 Connected

Proxy replied OK to CONNECT request
CONNECT phase completed!
schannel: SSL/TLS connection with httpbin.org port 443 (step 1/3)
schannel: disabled server certificate revocation checks
schannel: verifyhost setting prevents Schannel from comparing the supplied target name with the subject names in server certificates.
schannel: sending initial handshake data: sending 167 bytes...
schannel: sent initial handshake data: sent 167 bytes
schannel: SSL/TLS connection with httpbin.org port 443 (step 2/3)
schannel: encrypted data got 2278
schannel: encrypted data buffer: offset 2278 length 4096
schannel: sending next handshake data: sending 126 bytes...
CONNECT phase completed!
CONNECT phase completed!
schannel: SSL/TLS connection with httpbin.org port 443 (step 2/3)
schannel: encrypted data got 51
schannel: encrypted data buffer: offset 51 length 4096
schannel: SSL/TLS handshake complete
schannel: SSL/TLS connection with httpbin.org port 443 (step 3/3)
schannel: stored credential handle in session cache
GET /get HTTP/1.1
Host: httpbin.org
User-Agent: curl/7.55.1
Accept: */*

schannel: client wants to read 102400 bytes
schannel: encdata_buffer resized 103424
schannel: encrypted data buffer: offset 0 length 103424
schannel: encrypted data got 515
schannel: encrypted data buffer: offset 515 length 103424
schannel: decrypted data length: 486
schannel: decrypted data added: 486
schannel: decrypted data cached: offset 486 length 102400
schannel: encrypted data buffer: offset 0 length 103424
schannel: decrypted data buffer: offset 486 length 102400
schannel: schannel_recv cleanup
schannel: decrypted data returned 486
schannel: decrypted data buffer: offset 0 length 102400
HTTP/1.1 200 OK
Date: Mon, 02 Nov 2020 05:45:19 GMT
Content-Type: application/json
Content-Length: 256
Connection: keep-alive
Server: gunicorn/19.9.0
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true

{
  "args": {},
  "headers": {
    "Accept": "*/*",
    "Host": "httpbin.org",
    "User-Agent": "curl/7.55.1",
    "X-Amzn-Trace-Id": "Root=1-5f9f9cee-75647f114badcc2f5a0a2fdb"
  },
  "origin": "10.1.10.150",
  "url": "https://httpbin.org/get"
}
Connection #0 to host 10.1.10.150 left intact
C:\Users\Administrator>

```

6. (オプション) F5 ハンズオンでは L2 デバイスに SSH 接続し、tcpdump コマンドで通信の確認をします。
(F 5 ハンズオンでは、ネットワークブリッジ名は **L2PEOLD** となります。)

- ポート 8080 番のリクエストとレスポンスを確認するコマンド例 (本ガイドからコピペすると、シングルオーテーションが失敗する可能性がありますので、そこは入力し直してください。)
- (sudo) tcpdump -i L2PEOLD -A -s 0 'tcp port 8080 and (((ip[2:2] - ((ip[0]&0xf)<<2)) -

```
((tcp[12]&0xf0)>>2)) != 0)'
```

```
centos@18db2db7-8bfb-44d2-9ba8-0e273dde20b0:~$
[centos@18db2db7-8bfb-44d2-9ba8-0e273dde20b0 ~]$ sudo tcpdump -i L2PEOLD -A -s 0 'tcp port 8080 and (((ip[2:2] - ((ip[0]&0xf)<<2)) - ((tcp[12]&0xf)>>2)) != 0)'
tcpdump: no output suppressed, use -v or -vv
listening on L2PEOLD, link-type EN10MB (Ethernet), capture size 262144 bytes
15:07:26.612764 IP 10.1.10.200.10721 > ec2-52-6-34-179.compute-1.amazonaws.com.webcache: Flags [P.], seq 404915:87:26.612764 IP 10.1.10.200.10721 > ec2-52-6-34-179.compute-1.amazonaws.com.webcache: Flags [P.], seq 404915:87:26.612764 IP 10.1.10.200.10721 > ec2-52-6-34-179.compute-1.amazonaws.com.webcache: Flags [P.], seq 404915:87:26.612764 IP 10.1.10.200.10721 > ec2-52-6-34-179.compute-1.amazonaws.com.webcache: Flags [P.], seq 4049410915:4049410993, ack 1453561185, win 14600, options [nop,nop,TS val 274445203 ecr 2274445202], length 78: HTTP: GET /get HTTP/1.1
E...A.@....=
.
.4..)...].c.v..a..9.k.....
..G...G.GET /get HTTP/1.1
Host: httpbin.org
User-Agent: curl/7.55.1
Accept: */*

15:07:26.680874 IP ec2-52-6-34-179.compute-1.amazonaws.com.webcache > 10.1.10.200.10721: Flags [P.], seq 1:487, ack 78, win 23438, options [nop,nop,TS val 2274445270 ecr 2274445203], length 486: HTTP: HTTP/1.1 200 OK
E...A.@....4..".
.
...).V..a..)...[.m.....
..G...G.HTTP/1.1 200 OK
Date: Mon, 02 Nov 2020 06:07:26 GMT
Content-Type: application/json
Content-Length: 256
Connection: keep-alive
Server: gunicorn/19.9.0
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true

{
  "args": {},
  "headers": {
    "Accept": "*/*",
    "Host": "httpbin.org",
    "User-Agent": "curl/7.55.1",
    "X-Amzn-Trace-Id": "Root=1-5f9fa21e-3745ea4a49d7ed1a69da11c5"
  },
  "origin": "10.1.10.200",
  "url": "https://httpbin.org/get"
}
```

7. (オプション) NTOPNG でトラフィック確認した場合のイメージです。

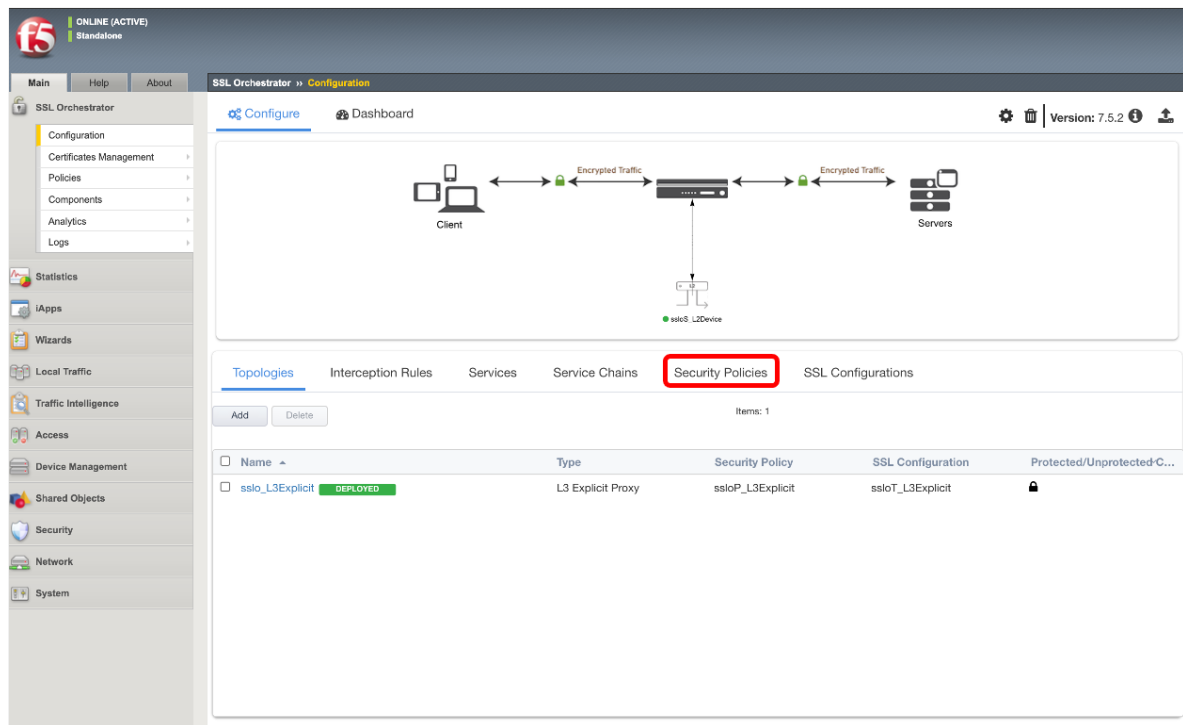


2.1.9 SSL 復号バイパスルールの設定 (URL Filtering カテゴリ)

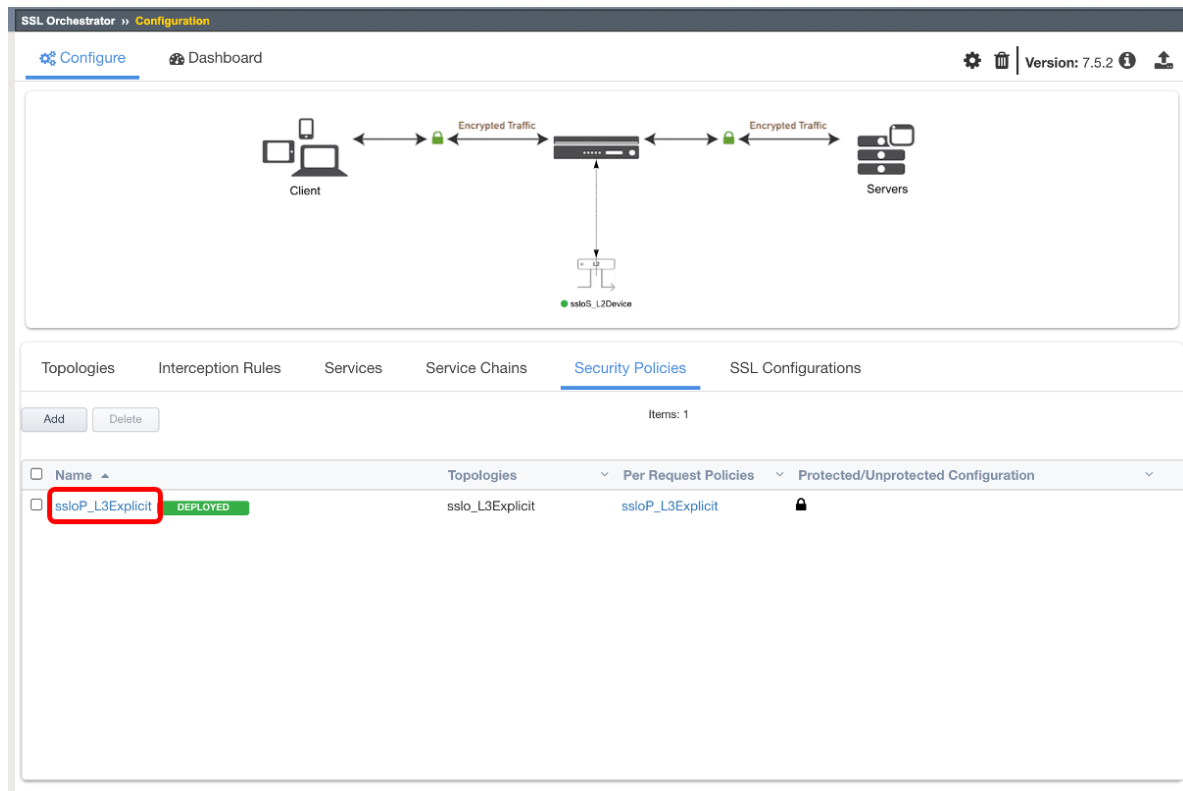
SSLO では、SSL 復号をバイパスするためのルールを柔軟に設定可能です。ここでは、特定カテゴリのサイト (例：金融、ヘルスケア) へのアクセスは、SSL 復号をバイパスする設定を行います。

注釈：管理者が設定した接続先でルールを設定することもできますが、一般的なカテゴリルールを利用したい場合、別途 URL Filtering のサブスクリプションライセンスが必要となります。また、URL Filtering のプロビジョニング、URL Filtering DB のダウンロードが必要です。(F5 ハンズオンでは予め、URL Filtering DB を設定、ダウンロードしてあります。)

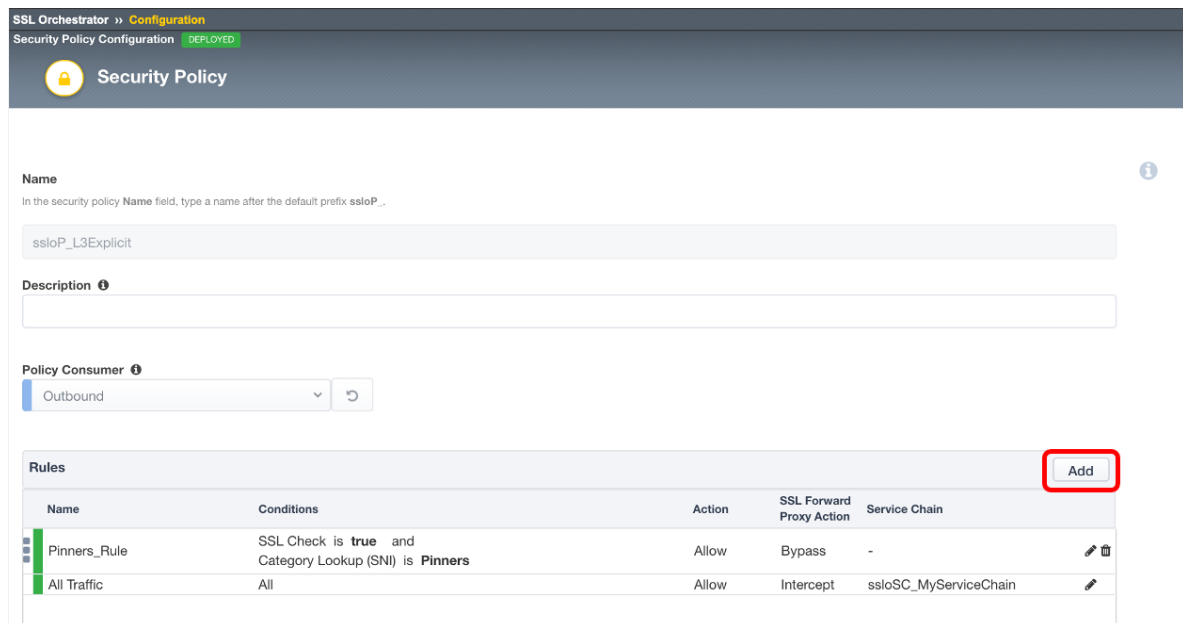
1. SSL Orchestrator >> Configuration にて、Security Policies を選択します。



2. 作成済みのポリシーを選択します。



3. Add を押します。



4. **Name** に任意の名前を設定し、**Conditions** にて **Category Lookup(All)** を選択し、バイパスさせたいカテゴリを選択し、**SSL Forward Proxy Action** にて **Bypass** を選択し、SSL 復号していないトラフィックもセキュリティデバイスに転送したい場合は、**Service Chain** も選択し、**OK** を押します。

Rules

Name	Conditions	Action	SSL Forward Proxy Action	Service Chain
Pinners_Rule	SSL Check is true and Category Lookup (SNI) is Pinners	Allow	Bypass	-

Name
Bypass_Rule
Type the name of your custom policy.

Conditions
Category Lookup (All)
Financial Data and Services
Health and Medicine

Action Allow **SSL Forward Proxy Action** Bypass **Service Chain** ssloSC_MyServiceChain

Cancel OK

Name	Conditions	Action	SSL Forward Proxy Action	Service Chain
All Traffic	All	Allow	Intercept	ssloSC_MyServiceChain

5. バイパスルールが設定されていることを確認し、**Deploy** を押します。

SSL Orchestrator » Configuration
Security Policy Configuration **DEPLOYED**

Security Policy

Name
In the security policy Name field, type a name after the default prefix ssloP_.

ssloP_L3Explicit

Description

Policy Consumer
Outbound

Rules

Name	Conditions	Action	SSL Forward Proxy Action	Service Chain
Pinnars_Rule	SSL Check is true and Category Lookup (SNI) is Pinnars	Allow	Bypass	-
Bypass_Rule	Category Lookup (All) is Financial Data and Services, Health and Medicine	Allow	Bypass	ssloSC_MyServiceChain
All Traffic	All	Allow	Intercept	ssloSC_MyServiceChain

☐ Server Certificate Status Check

☐ Proxy Connect

Cancel **Deploy**

6. ポップアップが表示された場合、*Deploy* を押します。

SSL Orchestrator » Configuration
Security Policy Configuration **DEPLOYED**

Security

Name
In the security policy Name field

ssloP_L3Explicit

Description

Continue to deploy ?

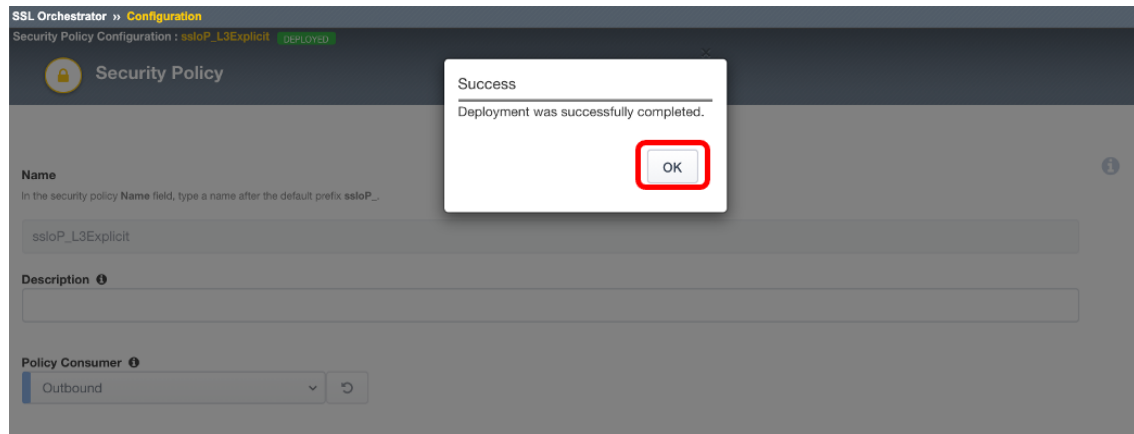
This configuration instance shares details with the following configuration details:
Editing this item will affect the referencing ones mentioned below.

- sslo_L3Explicit (Topology)

Do you still want to continue?

Deploy Cancel

7. Success ポップアップが表示されます。OK ボタンを押します。

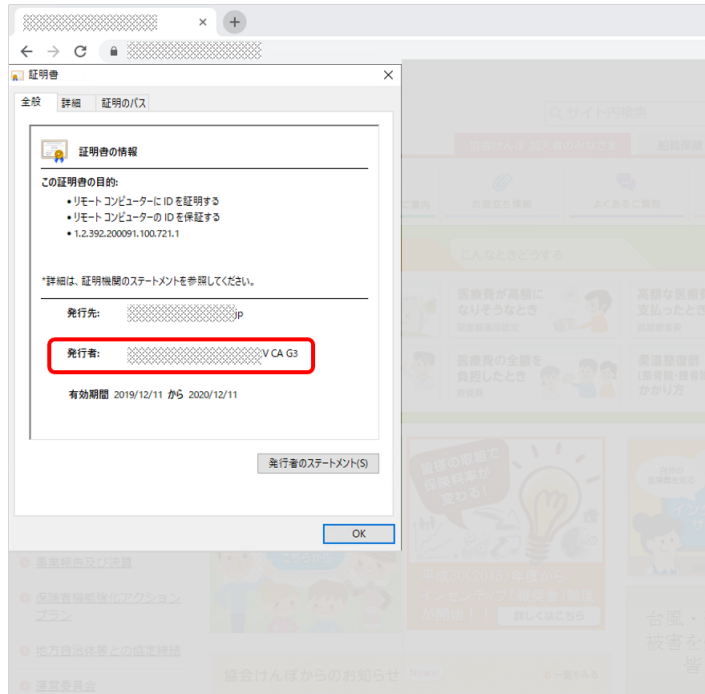


注釈:

- 送信元、宛先の IP サブネット、ポート番号、プロトコルタイプ、URL、IP ジオロケーションなどでも SSL 復号バイパスの設定が可能です。
 - セキュリティデバイスが ICAP サービス、HTTP サービスの場合、SSL 復号していないトラフィックをサービスチェーンに流せません。
-

2.1.10 クライアントからの接続テスト

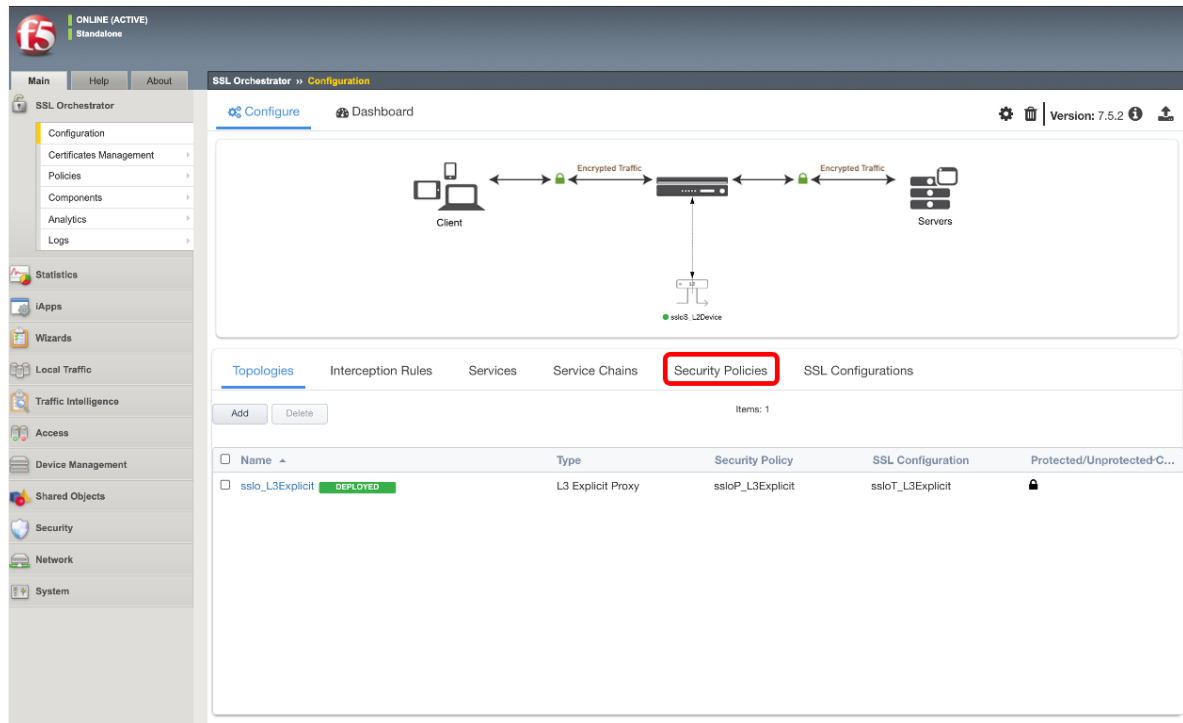
1. クライアントからバイパス設定したカテゴリのサイトに接続し、サーバ証明書が書換えられていないことを確認します。



2.1.11 SSL 復号バイパスルールの設定（クライアント IP サブネット）

SSLO では、SSL 復号をバイパスするためのルールを柔軟に設定可能です。ここでは、特定のクライアント IP サブネットからのアクセスは、SSL 復号をバイパスする設定を行います。

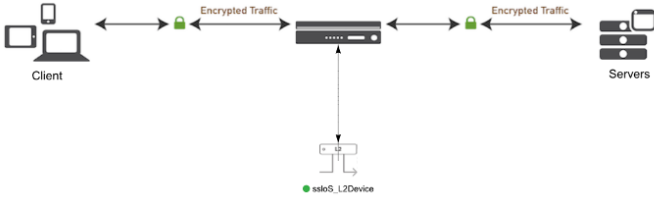
1. **SSL Orchestrator >> Configuration** にて、**Security Policies** を選択します。



2. 作成済みのポリシーを選択します。

SSL Orchestrator » Configuration

Configure Dashboard Version: 7.5.2



Topologies Interception Rules Services Service Chains **Security Policies** SSL Configurations

Add Delete Items: 1

<input type="checkbox"/>	Name	Topologies	Per Request Policies	Protected/Unprotected Configuration
<input type="checkbox"/>	ssloP_L3Explicit DEPLOYED	sslo_L3Explicit	ssloP_L3Explicit	

3. 前項で作成したバイパスルールを一旦削除します。

SSL Orchestrator » Configuration
Security Policy Configuration **DEPLOYED**

Security Policy

Name
In the security policy Name field, type a name after the default prefix ssloP_.

ssloP_L3Explicit

Description

Policy Consumer
Outbound

Rules Add

Name	Conditions	Action	SSL Forward Proxy Action	Service Chain
Pinners_Rule	SSL Check is true and Category Lookup (SNI) is Pinners	Allow	Bypass	-
Bypass_Rule	Category Lookup (All) is Financial Data and Services, Health and Medicine	Allow	Bypass	ssloSC_MyServiceChain
All Traffic	All	Allow	Intercept	ssloSC_MyServiceChain

4. OK ボタンを押します。

SSL Orchestrator » Configuration
Security Policy Configuration **DEPLOYED**

Security Policy

Name
In the security policy Name field, type a name after the default prefix ssloP_.

ssloP_L3Explicit

Description

Delete Rule

Do you want to delete rule?

Ok Cancel

5. Add を押します。

SSL Orchestrator » Configuration

Security Policy Configuration **DEPLOYED**

Security Policy

Name

In the security policy Name field, type a name after the default prefix ssloP_.

ssloP_L3Explicit

Description

Policy Consumer

Outbound

Rules Add

Name	Conditions	Action	SSL Forward Proxy Action	Service Chain
Pinners_Rule	SSL Check is true and Category Lookup (SNI) is Pinners	Allow	Bypass	-
All Traffic	All	Allow	Intercept	ssloSC_MyServiceChain

6. **Name** に任意の名前を設定し、**Conditions** にて **Client IP Subnet Match** を選択し、バイパスさせたいサブネットを設定し（F5 ハンズオンでは、10.1.10.0/24）、**SSL Forward Proxy Action** にて **Bypass** を選択し、SSL 復号していないトラフィックもセキュリティデバイスに転送したい場合は、**Service Chain** も選択し、**OK** を押します。

Rules

Name	Conditions	Action	SSL Forward Proxy Action	Service Chain
Pinners_Rule	SSL Check is true and Category Lookup (SNI) is Pinners	Allow	Bypass	-

Name

Bypass_Rule

Type the name of your custom policy.

Conditions

Client IP Subnet Match is 10.1.10.0/24

Action **SSL Forward Proxy Action** **Service Chain**

Allow Bypass ssloSC_MyServiceChain

Cancel OK

All Traffic	All	Allow	Intercept	ssloSC_MyServiceChain
-------------	-----	-------	-----------	-----------------------

7. バイパスルールが設定されていることを確認し、*Deploy* を押します。

SSL Orchestrator Configuration
Security Policy Configuration DEPLOYED

Security Policy

Name
In the security policy Name field, type a name after the default prefix ssloP_

ssloP_L3Explicit

Description

Policy Consumer
Outbound

Rules

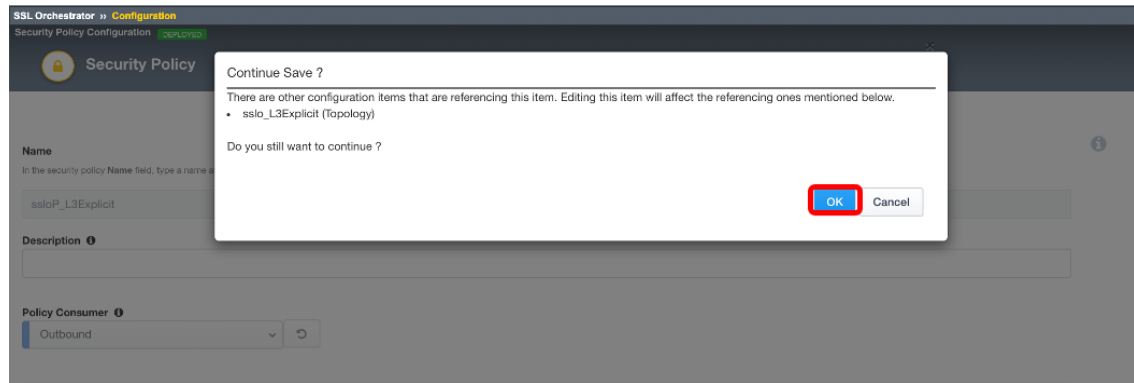
Name	Conditions	Action	SSL Forward Proxy Action	Service Chain
Pinners_Rule	SSL Check is true and Category Lookup (SNI) is Pinners	Allow	Bypass	-
Bypass_Rule	Client IP Subnet is 10.1.10.0/24	Allow	Bypass	ssloSC_MyServiceChain
All Traffic	All	Allow	Intercept	ssloSC_MyServiceChain

☐ Server Certificate Status Check

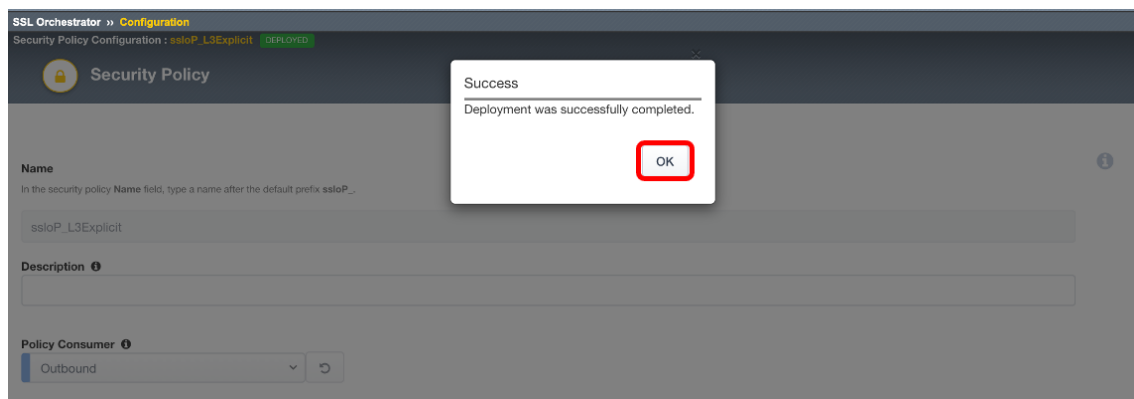
☐ Proxy Connect

Cancel **Deploy**

8. 編集の確認が表示されるので、*OK* ボタンを押します。



9. Success ポップアップが表示されます。OK ボタンを押します。



注釈:

- URL Filtering カテゴリ、宛先の IP サブネット、ポート番号、プロトコルタイプ、URL、IP ジオロケーションなどでも SSL 復号バイパスの設定が可能です。
- セキュリティデバイスが ICAP サービス、HTTP サービスの場合、SSL 復号していないトラフィックをサービスチェーンに流せません。

2.1.12 クライアントからの接続テスト

1. クライアントから任意の HTTPS サイトに接続し、サーバ証明書が書換えられていないことを確認します。

