
F5 SSLO セットアップガイド

i-FILTER 編

2021 年 08 月 16 日

目次:

第 1 章	はじめに	3
1.1	F5 SSLO (L3 Explicit Proxy) と i-FILTER ICAP 版の連携設定	3
1.2	F5 SSLO (L3 Explicit Proxy) と i-FILTER Proxy 版の連携設定	71

最終更新日: 2021 年 8 月 16 日

F5 SSL Orchestrator (SSLO) と WEB フィルタリング製品である i-FILTER との連携手順をご紹介します。(本ガイドは、一度 BIG-IP を設定したことのある方を対象とした内容となっております。)

第 1 章

はじめに

こちらのページでは、以下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あります。

- AskF5: <https://support.f5.com/csp/home>
- F5 Cloud Docs: <https://clouddocs.f5.com/>
- F5 DevCentral (コミュニティ) : <https://devcentral.f5.com/>

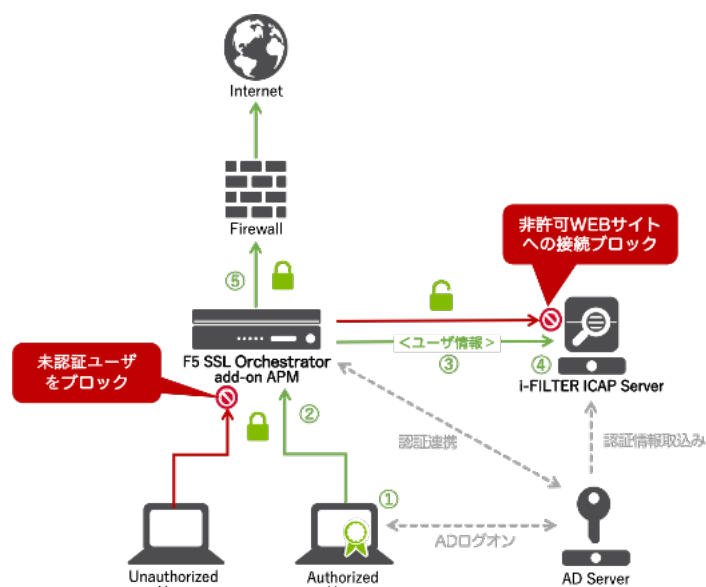
1.1 F5 SSLO (L3 Explicit Proxy) と i-FILTER ICAP 版の連携設定

本章では、SSLO の可視化ゾーンに i-FILTER ICAP 版を配置し、ICAP プロトコルで連携する構成について、ご紹介致します。

1.1.1 F5 SSLO と i-FILTER ICAP 版連携の流れ

F5 SSLO と i-FILTER ICAP 版の連携の流れは以下の通りです。

1. クライアントがパソコン (AD) にログオンします。
2. SSLO でユーザ認証を実施し (NTLM 認証、Kerberos 認証の場合は自動的に認証が実施されます)、SSL 通信を復号します。
3. WEB 接続先情報と SSLO で認証が成功したユーザ情報を i-FILTER に ICAP で送ります。
4. ユーザ情報を元に URL フィルタリングルールを適用し、接続が許可されていない WEB サイトの場合は、ブロック画面をクライアントに表示します。
5. 許可された通信に関しては、SSL 通信を再暗号化し、WEB サーバへ接続します。



1.1.2 本ガイドの利用バージョンと構成イメージ

本ガイドは、以下の製品バージョンを利用して、作成しております。

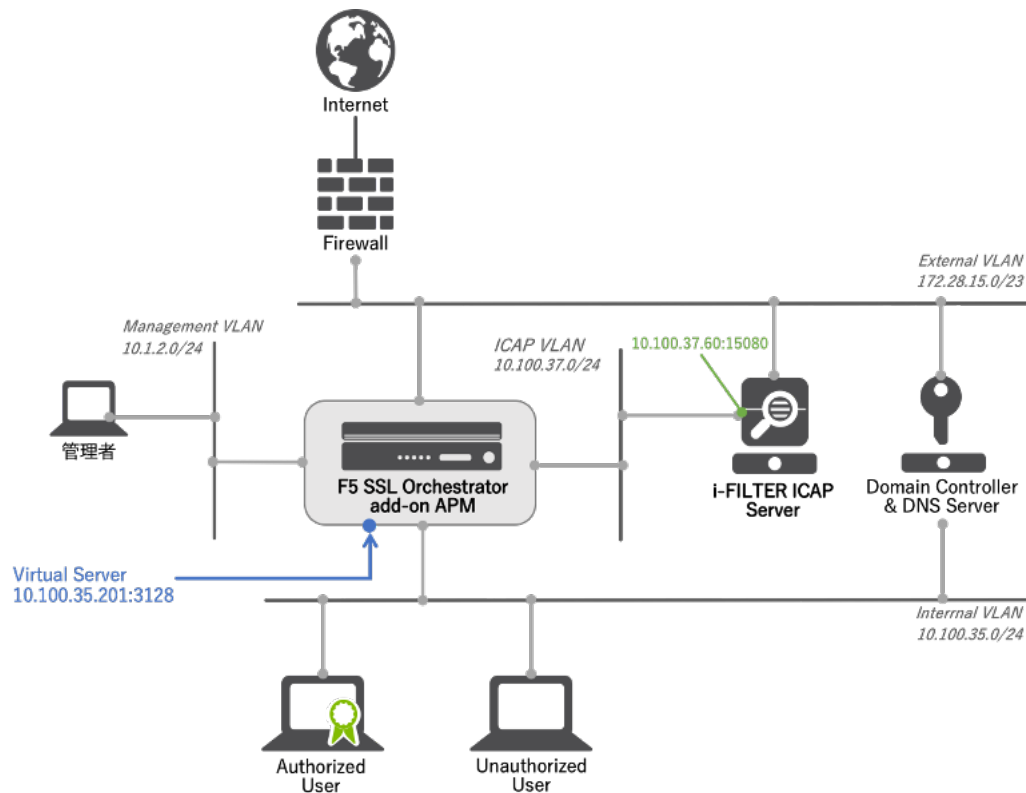
1. 利用バージョン

製品名	バージョン
F5 SSL Orchestrator	v15.1.2-0.0.9Final ~ 7.5.2
i-FILTER ICAP Server (Linux)	Ver.10.42R01-20200923 (CentOS v7.7.1908 ※) ※ デジタルアーツ様による製品サポート OS は Red Hat Enterprise Linux となります。

注釈:

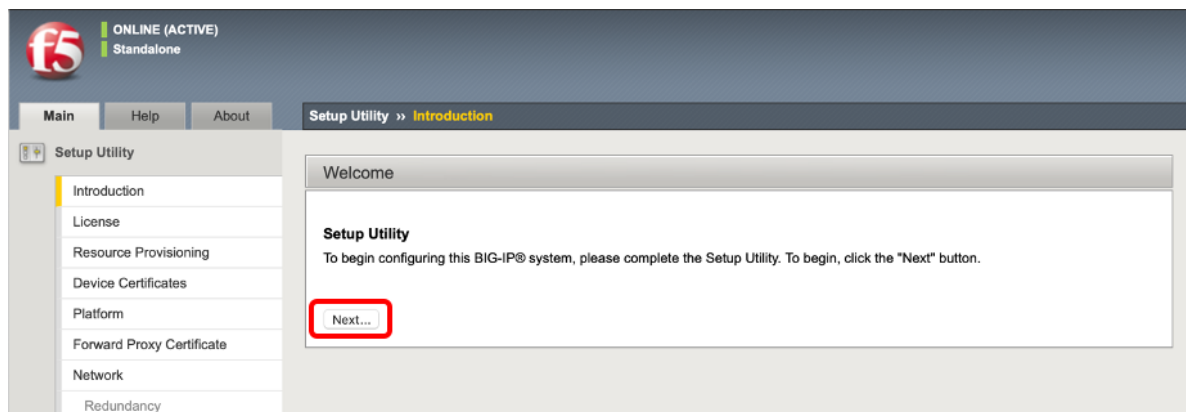
- **v15.1.2.1 以上** のバージョンをご利用下さい。(2021 年 3 月追記)
- (各 F5 代理店でサポート可能な範囲において、) 極力最新のバージョンを適用頂くことをおすすめ致します。最新のバージョンは AskF5 でご確認ください。
- Proxy 認証を行いたい場合、もしくは、i-FILTER のログに AD ユーザ名を出力したい場合は、APM のライセンスが必要となります。

2. 本ガイドにおける構成イメージ



1.1.3 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

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：LTM,AVR,iRulesLX,SSLO) & (認証：APM)）をプロビジョニングします。（ライセンスは SSLO と APM の 2 つを利用しています。）

Module	Provisioning	License Status	Required Disk (GB)	Required Memory (MB)
Management (MGMT)	Small	N/A	0	1264
Local Traffic (LTM)	☒ Nominal	Unlicensed	0	1856
Application Security (ASM)	☐ None	Unlicensed	20	1492
Fraud Protection Service (FPS)	☐ None	N/A	12	544
Global Traffic (DNS)	☐ None	Unlicensed	0	148
Link Controller (LC)	☐ None	Unlicensed	0	148
Access Policy (APM)	☒ Nominal	Licensed	12	494
Application Visibility and Reporting (AVR)	☒ Nominal	Licensed	16	576
Policy Enforcement (PEM)	☐ None	Unlicensed	16	1223
Advanced Firewall (AFM)	☐ None	Unlicensed	16	1058
Application Acceleration Manager (AAM)	☐ None	Unlicensed	32	2050
Secure Web Gateway (SWG)	☐ None	Unlicensed	24	4096
iRules Language Extensions (iRulesLX)	☒ Nominal	Licensed	0	748
URLDB Minimal (URLDB)	☐ None	Unlicensed	36	2048
SSL Orchestrator (SSLO)	☒ Nominal	Licensed	0	128
Carrier Grade NAT (CGNAT)	☐ 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

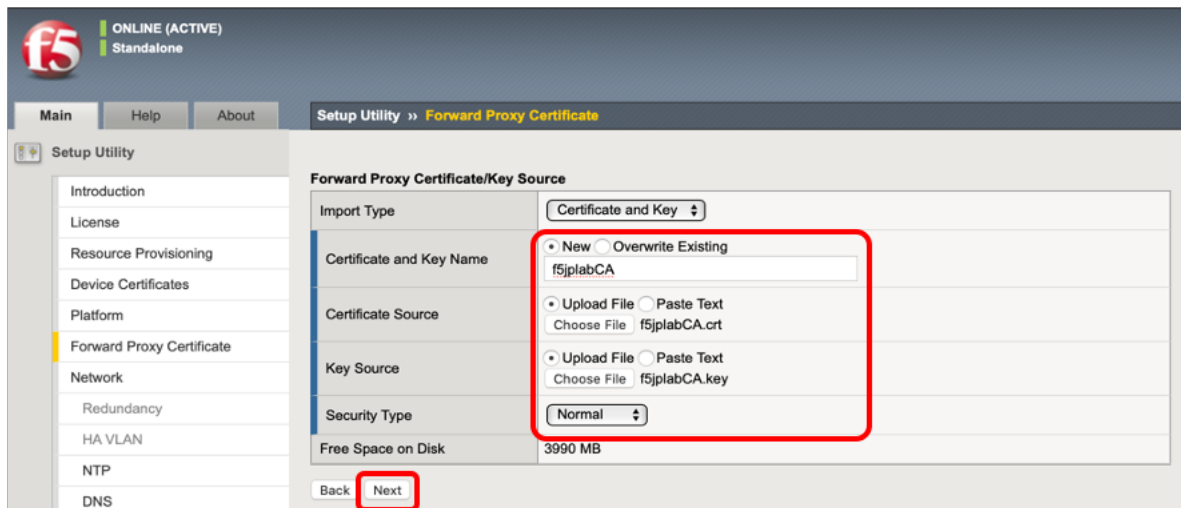
Root Account ☐ Disable login
Password: *****
Confirm: *****

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

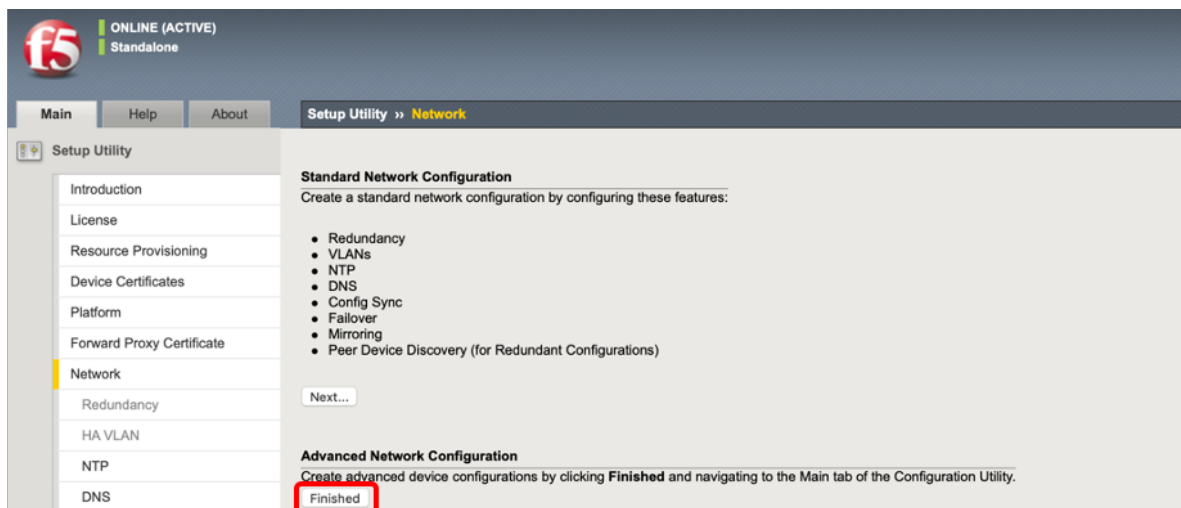
Back **Next...**

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。

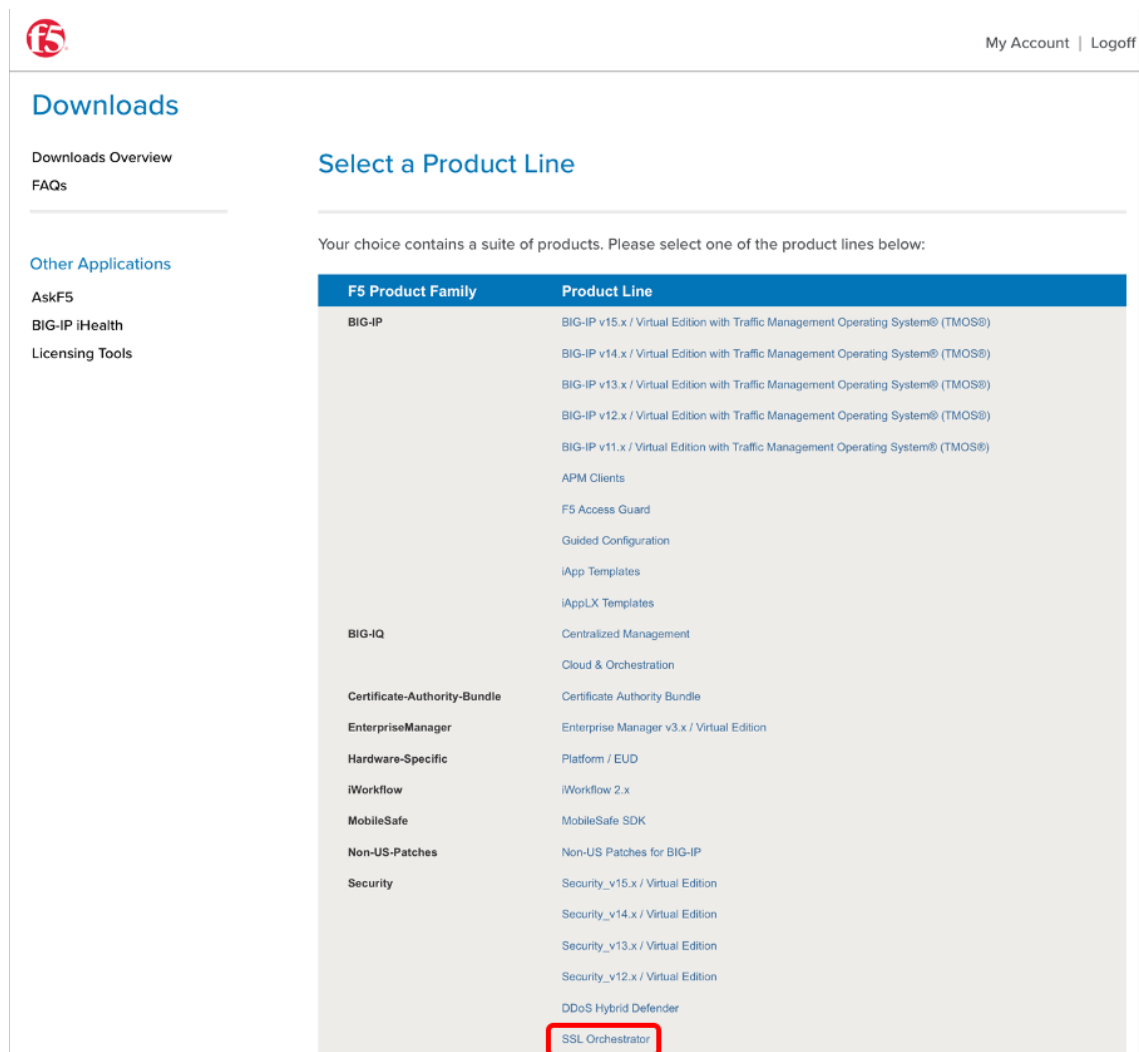


7. Finished ボタンを押します。



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

1. AskF5(<https://support.f5.com/>) より最新版の SSLO RPM をダウンロードします。(SSLO にプリインストールされている RPM のバージョンが最新の場合は、以下の操作は不要です。)



Downloads

Downloads Overview
FAQs

Other Applications

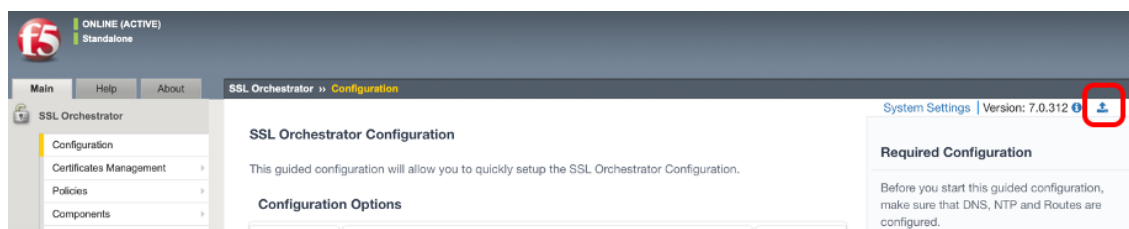
AskF5
BIG-IP iHealth
Licensing Tools

Select a Product Line

Your choice contains a suite of products. Please select one of the product lines below:

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。



ONLINE (ACTIVE)
Standalone

Main Help About

SSL Orchestrator >> Configuration

SSL Orchestrator Configuration

This guided configuration will allow you to quickly setup the SSL Orchestrator Configuration.

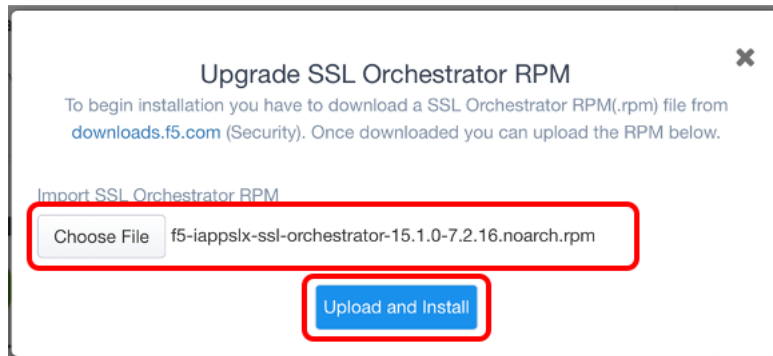
Configuration Options

System Settings | Version: 7.0.312

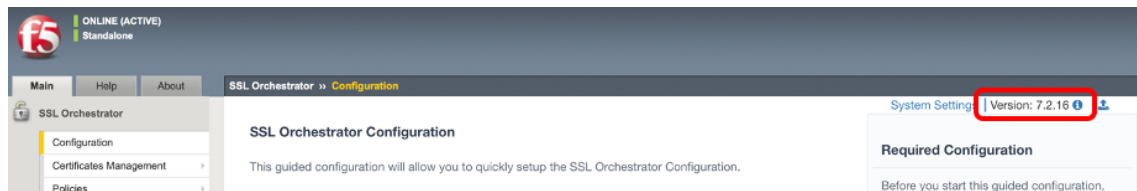
Required Configuration

Before you start this guided configuration, make sure that DNS, NTP and Routes are configured.

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。

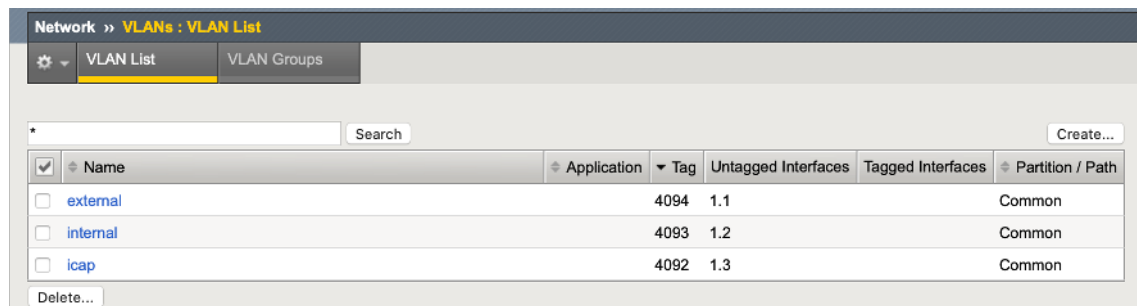


4. バージョンがアップグレードされていることを確認します。



1.1.5 Network の基本設定

1. VLAN の設定を行います。



2. Self IP の設定を行います。

☒	Name	Application	IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
☐	external-self		172.28.14.57	255.255.254.0	external	traffic-group-local-only	Common
☐	internal-self		10.100.35.57	255.255.255.0	internal	traffic-group-local-only	Common
☐	icap-self		10.100.37.57	255.255.255.0	icap	traffic-group-local-only	Common

3. デフォルトゲートウェイの設定を行います。

☒	Name	Application	Destination	Netmask	Route Domain	Resource Type	Resource	Partition / Path
☐	default-gw		Default IPv4		Partition Default Route Domain	Gateway	172.28.15.254	Common

1.1.6 DNS, NTP の設定

1. DNS の設定を行います。

Address: 10.100.35.156

DNS Lookup Server List

2. NTP の設定を行います。

The screenshot shows the 'System >> Configuration : Device : NTP' page. The 'Device' tab is selected. The 'Properties' section on the left is titled 'Time Server List'. On the right, there is an 'Address:' input field with an 'Add' button below it. Below the input field is a text area containing 'ntp.nict.jp'. At the bottom of the text area are 'Edit' and 'Delete' buttons. An 'Update' button is located at the bottom left of the main content area.

1.1.7 i-FILTER にて HTTP/HTTPS 判別するための設定（Local Traffic Policy の設定）

i-FILTER ICAP 版は、ICAP のリクエストヘッダの一部で HTTP サーバへの通信か HTTPS サーバへの通信かを判別しています。i-FILTER が HTTP/HTTPS 判別可能となるように Local Traffic Policy にてルールを作成します。同時に i-FILTER は ICAP レスポンスはチェックしないので、ICAP レスポンスチェックを無効にします。また、i-FILTER による URL Filtering チェック後に、リクエストヘッダを元の値に戻すための Local Traffic Policy ルールも作成します。こちらのルールでは実際に ICAP 通信は行わないので、ICAP 通信を無効にします。

1. **Local Traffic >> Policies >> Policies List** にて、*Create* ボタンを押します。

The screenshot shows the 'Local Traffic >> Policies : Policy List' page. The 'Policies List' tab is selected. On the left is a sidebar with navigation options: Main, Help, About, SSL Orchestrator, Statistics, iApps, Wizards, and Local Traffic. Under 'Local Traffic', 'Policies' is selected. The main area has a search bar and a 'Create' button (highlighted with a red box). Below are two sections: 'Draft Policies' and 'Published Policies'. Both sections have a table with columns: Name, Last Published, Description, and Partition / Path. Both sections currently show 'No records to display'.

2. 任意のポリシー名を入力し、*Create Policy* ボタンを押します。

Local Traffic >> Policies : Policy List >> New...

Policies List Strategy List Statistics

General Properties

Policy Name	ifilter_db_rules
Description	
Strategy	Execute first matching rule
Type	Traffic Policy

Cancel Create Policy

3. HTTPS 用のルールを作成します。Rules の *Create* ボタンを押します。

Rules

Create

✓ ID	Name	Description	Conditions	Actions
No records to display				

Delete

4. 任意の Rule 名を入力し、**Match all of the following conditions:** の + マークをクリックし、以下のように入力します。

Local Traffic » Policies : Policy List » /Common/ifilter_db_rules:New Rule...

Properties

General Properties

Policy Name: ifilter_db_rules

Name: **https_rule**

Description:

Match all of the following conditions:

TCP port is any of 443 at client accepted time.

Do the following when the traffic is matched:

Ignore

Options

☐ Skip this condition if it is missing from the request.

☐ Use case sensitive string comparison.

Apply to traffic on local side of external interface

Cancel Save Done

Match all of the following conditions:	必要有無
TCP port is any of 443 at client accepted time.	必須
Apply to traffic on local side of external interface	必須

5. 同様に、**Do the following when the traffic is matched:** の + マークをクリックし、以下のように入力し、**Save** ボタンを押します。（デバック用のログルールは任意で追加します。）

Do the following when the traffic is matched:

Insert HTTP Header named urihttps with value tcl:[HTTP::uri] at request time.

Replace HTTP URI full string with value tcl:https://[HTTP::host][HT at request time.

Disable response adapt at response time.

Log message tcl: HTTPs(443) URI was re at request time.

Options

Facility: local0

Priority: info

☐ Send log message to remote server:

Host:

Port: 0

Cancel Save Done

Do the following when the traffic is matched:	必要 有 無
Insert HTTP Header named urihttps with value tcl:[HTTP::uri] at request time.	必須
Replace HTTP URI full string with value tcl:https://[HTTP::host][HTTP::uri] at request time.	必須
Disable response adapt at response time.	必須
Log message tcl: HTTPS(443) URI was replaced to: [HTTP::uri] at request time.	任意
Facility: local0 Priority: info	任意

6. 同様に HTTP 用のルールを作成します。

Local Traffic » Policies : Policy List » /Common/ifilter_db_rules:http_rule

⚙️

Properties

General Properties

Policy Name	ifilter_db_rules
Name	http_rule
Description	

Match all of the following conditions:

TCP

port

is

any of

80

at

+

-

client accepted

time.

⚙️ Options

Do the following when the traffic is matched:

Insert

HTTP Header

named

urihttp

with value

tcl:[HTTP::uri]

at

request

time.

+

-

Replace

HTTP URI

full string

with value

tcl:http://[HTTP::host][HTT

at

request

time.

+

-

Disable

response adapt

at

response

time.

+

-

Log

message

tcl: HTTP(80) URI was repl

at

request

time.

⚙️ Options

+

-

Cancel

Save

Match all of the following conditions:	必要有 無
TCP port is any of 80 at client accepted time.	必須
Apply to traffic on local side of external interface	必須

Do the following when the traffic is matched:	必要 有無
Insert HTTP Header named urihttp with value tcl:[HTTP::uri]** at **request time.	必須
Replace HTTP URI full string with value tcl:http://[HTTP::host][HTTP::uri] at request time.	必須
Disable response adapt at response time.	必須
Log message tcl: HTTP(80) URI was replaced to: [HTTP::uri] at request time.	任意
Facility: local0 Priority: info	任意

7. 2つのルール作成後は、以下のようになります。*Save Draft* ボタンを押します。

Local Traffic » Policies : Policy List » ifilter_db_rules

Published Policy Draft Policy

General Properties

Policy Name	ifilter_db_rules
Partition / Path	Common/Drafts
Description	
Strategy	Execute first matching rule
Type	Traffic Policy

Cancel **Save Draft** Clone

Rules

Create

☒	ID	Name	Description	Conditions	Actions
☐	1	https_rule		TCP port is '443' at client accepted time.	1. Insert HTTP Header named 'urihttps' with value 'tcl:[HTTP::uri]' at request time. 2. Replace HTTP URI with value 'tcl:https://[HTTP::host][HTTP::uri]' at request time. 3. Disable response adapt at response time. 4. Log message 'tcl: HTTPS(443) URI was replaced to: [HTTP::uri]' at request time.
☐	2	http_rule		TCP port is '80' at client accepted time.	1. Insert HTTP Header named 'urihttp' with value 'tcl:[HTTP::uri]' at request time. 2. Replace HTTP URI with value 'tcl:http://[HTTP::host][HTTP::uri]' at request time. 3. Disable response adapt at response time. 4. Log message 'tcl: HTTP(80) URI was replaced to: [HTTP::uri]' at request time.

8. *Publish* ボタンを押すと、以下ようになります。

Local Traffic » Policies : Policy List

Policies List Strategy List Statistics

Create

Draft Policies

☒	Name	Last Published	Description	Partition / Path
No records to display				

Publish Delete

Published Policies

☒	Name	Description	Partition / Path
☐	ifilter_db_rules		Common

Delete

9. 上記手順と同様に、以下のようなリクエストヘッダをもとに戻す Local Traffic Policy ルールを作成します。

Local Traffic » Policies : Policy List » restore_header

Published Policy

Draft Policy

General Properties

Policy Name	restore_header
Partition / Path	Common/Drafts
Description	
Strategy	Execute first matching rule
Type	Traffic Policy

Cancel

Save Draft

Clone

Rules

Create

☒	ID	Name	Description	Conditions	Actions
☐	1	https_rule		TCP port is '443' at client accepted time.	1. Replace HTTP URI with value 'tcl:[HTTP::header values urihttps]' at request time. 2. Remove HTTP Header named 'urihttps' at request time. 3. Disable request adapt at request time. 4. Disable response adapt at response time.
☐	2	http_rule		TCP port is '80' at client accepted time.	1. Replace HTTP URI with value 'tcl:[HTTP::header values urihttp]' at request time. 2. Remove HTTP Header named 'urihttp' at request time. 3. Disable request adapt at request time. 4. Disable response adapt at response time.

Match all of the following conditions:	必要有無
TCP port is any of 443 at client accepted time.	必須
Apply to traffic on local side of external interface	必須

Do the following when the traffic is matched:	必要有無
Replace HTTP URI full string with value <code>cl:[HTTP::header values urihttps]</code> at request time.	必須
Remove HTTP Header named <code>urihttps</code> at request time.	必須
Disable request adapt at request time.	必須
Disable response adapt at response time.	必須

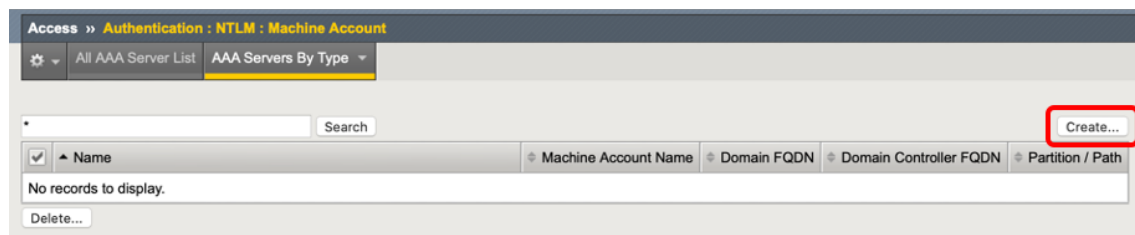
Match all of the following conditions:	必要有無
TCP port is any of 80 at client accepted time.	必須
Apply to traffic on local side of external interface	必須

Do the following when the traffic is matched:	必要有無
Replace HTTP URI full string with value cl:[HTTP::header values urihttp] at request time.	必須
Remove HTTP Header named urihttp at request time.	必須
Disable request adapt at request time.	必須
Disable response adapt at response time.	必須

1.1.8 NTLM 認証設定

APM で行う認証の設定を行います。ここでは、NTLM 認証の設定を行います。AD サーバ（ドメインコントローラ、DNS）の構築済みであることを前提としております。

1. **Access >> Authentication >> NTLM >> Machine Account** を選択し、*Create* ボタンを押します。



2. 任意の名前を設定し、**Machine Account Name** には **任意の SSLO 識別名** を入力し、**Domain FQDN**、

Admin ユーザ名 と パスワード を入力し、Join を押します。

Access » Authentication : NTLM : Machine Account » New Machine Account...

General Properties

Name: sslo_ntlm_ma

Configuration

Machine Account Name: F5

Domain FQDN: F5JPLAB.LOCAL

Domain Controller FQDN:

Admin User: Administrator

Admin Password: *****

Cancel Join

3. 以下のようになります。

Access » Authentication : NTLM : Machine Account

All AAA Server List AAA Servers By Type

* Search Create...

☒	Name	Machine Account Name	Domain FQDN	Domain Controller FQDN	Partition / Path
☐	sslo_ntlm_ma	F5	F5JPLAB.LOCAL		Common

Delete...

4. Access >> Authentication >> NTLM >> NTLM Auth Configuration を選択し、Create ボタンを押します。

Access » Authentication : NTLM : NTLM Auth Configuration

All AAA Server List AAA Servers By Type

* Search Create...

☒	Name	Machine Account Name	Domain Controller FQDN List	Partition / Path
No records to display.				

Delete...

5. 任意の名前を設定し、Machine Account Name は先程作成したものを選択します。Domain Controller FQDN List にはご利用のドメイン名 (FQDN 名) を指定し、Finished ボタンを押します。

Access >> Authentication : NTLM : NTLM Auth Configuration >> New NTLM Auth Configuration...

General Properties

Name: sslo_ntlm_auth

Configuration

Machine Account Name: sslo_ntlm_ma

Domain Controller FQDN List: winsvr2019.f5jplab.local

Buttons: Cancel, Finished

6. Access >> Profiles/Policies >> Access Profiles(Per-Session Policies) を選択し、Create ボタンを押します。

Access >> Profiles / Policies : Access Profiles (Per-Session Policies)

Access Profiles | Per-Request Policies | Policy Sync | Customization

Search

✓	Status	Access Profile Name	Application	Profile Type	Per-Session Policy	Export	Copy	Customization	Logs	Virtual Servers	Partition / Path
☐	✓	access	All	(none)	(none)	(none)	(none)				Common
☐	✓	ssloDefault_accessProfile	SSL Orchestrator			Export...	Copy...	Standard	default-sslo-log-setting		Common

Buttons: Delete..., Apply, Create..., Import...

7. 任意の名前を設定し、Policy Type に SWG-Explicit を選択し、Customization Type に Standard を選択し、User Identification Method にて、Credential を選択し、NTLM Auth Configuration に先程作成したものを選択し、Languages はご利用の言語を選択して、Finished ボタンを押します。

Access » Profiles / Policies : Access Profiles (Per-Session Policies) » New Profile...

General Properties

Name	sslo_ntlm_policy
Parent Profile	access
Profile Type	SWG-Explicit
Profile Scope	Profile
Customization Type	Standard

Settings

Custom ☐

Inactivity Timeout	900	seconds	☐
Access Policy Timeout	300	seconds	☐
Maximum Session Timeout	604800	seconds	☐
Minimum Authentication Failure Delay	2	seconds	☐
Maximum Authentication Failure Delay	5	seconds	☐
Max Concurrent Users	0		☐
Max Sessions Per User	0		☐
Max In Progress Sessions Per Client IP	128		☐
Restrict to Single Client IP	☐		☐
Use HTTP Status 503 for Error Pages	☐		☐

Configurations

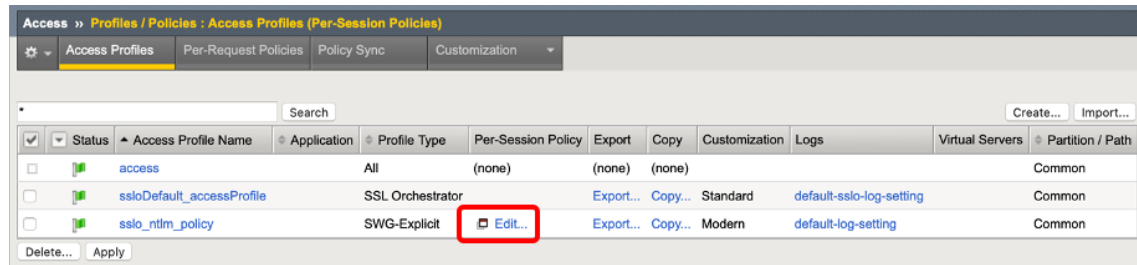
User Identification Method	Credentials
NTLM Auth Configuration	ntlm_sslo_auth

Language Settings

Additional Languages	Afar (aa)	Add
Languages	Accepted Languages Japanese (ja)	Factory BuiltIn Languages English (en) Chinese (Simplified) (zh-cn) Chinese (Traditional) (zh-tw) Korean (ko) Spanish (es) French (fr) German (de)
Default Language	Japanese (ja)	

Cancel Finished

8. 作成された Access Profile の一覧から先程作成したプロファイルを見つけ、Per-Session Policy 欄の *Edit* を押します。



9. ブラウザの別タブに VPE が表示されます。Start の右隣の + ボタンを押します。



10. Authentication タブの **NTLM Auth Result** を選択し、*Add Item*、*Save* を押します。

Begin typing to search

Logon Authentication Assignment Endpoint Security (Server-Side) General Purpose

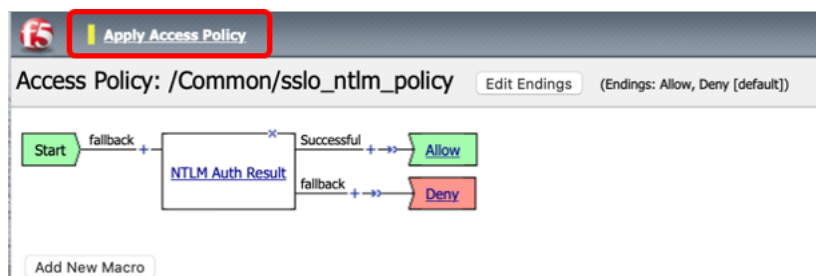
☐	AD Auth	Active Directory authentication of end user credentials
☐	AD Query	Active Directory query to pull user attributes for use with resource assignment or other functions, such as AD group mapping
☐	CRLDP Auth	Certificate Revocation List Distribution Point (CRLDP) client certificate authentication
☐	HTTP Auth	HTTP authentication of end user credentials
☐	Kerberos Auth	Kerberos authentication, typically following an HTTP 401 Response action
☐	LDAP Auth	LDAP authentication of end user credentials
☐	LDAP Query	LDAP query to pull user attributes for use with resource assignment or other functions, such as LDAP group mapping
☐	LocalDB Auth	Local Database Authentication
☒	NTLM Auth Result	NTLM authentication of end user credentials
☐	OAuth Scope	OAuth Scope
☐	OTP Generate	Generate One Time Passcode (OTP)
☐	RADIUS Acct	Send accounting messages to a RADIUS server when users log on and off
☐	RADIUS Auth	RADIUS authentication of end user credentials
☐	SAML Auth	SAML Auth using SAML Service Provider Interface
☐	Transparent Identity Import	Import Identity (user) information from IF-MAP server

Cancel Add Item Help

11. NTLM Auth Result の右の Successful につながるフローを **Deny** から **Allow** に変更します。



12. 左上の *Apply Access Policy* を押し、ブラウザの VPE タブを閉じます。



1.1.9 認証ヘッダ挿入用 iRule の作成

ここでは、ユーザ認証ヘッダ (X-Authenticated-User) と APM で認証されたユーザ名 (session.logon.last.username) を ICAP リクエストに挿入するための iRule を作成します。ICAP は HTTP をカプセルリングしますので、認証情報を挿入するためには以下の 2 つの iRule が必要となります。また、i-FILTER ICAP 版に認証ユーザ名を理解してもらうために、ユーザ名の手前に **ldap:///** を加え、**Base64 エンコーディング** をする必要があります。

1. **Local Traffic >> iRules** にて、**Create** ボタンを押します。**任意の名前** を入力して、**Definition** に以下サンプル iRule を入力し、**Finished** ボタンを押します。(以下の iRule はあくまでもサンプルとなります。同じ主旨の内容であれば下記と同じでなくても構いません。)

例1) HTTP リクエストヘッダに認証情報を挿入するための iRule サンプル

```
### Add this iRule to Virtual Server:ssloS_XXXX-t-4 ###

when HTTP_REQUEST {

    # Create the HDR list and insert the X-Server-IP value
    set hdr [list "X-Server-IP:[IP::local_addr]"]

    # Add the authenticated user information if it exists
    if { [ACCESS::session data get session.logon.last.username] ne "" } {
        # In case of NLTM/Basic Auth
        lappend hdr "X-Authenticated-User:[b64encode ldap:///[ACCESS::session_
        ↪data get session.logon.last.username]]"
    }

    # Add above info to the table temporarily and add an ICAP-X header
    set guid [expr {int(rand()*1e12)}]
    table set ${guid} ${hdr} 10 10
    HTTP::header replace ICAP-X ${guid}
}
```

例2) ICAP リクエストヘッダに認証情報を挿入するための iRule サンプル

```
### Add this iRule to ssloS-XXXX-req ###

when ICAP_REQUEST {

    if { [HTTP::header exists "ICAP-X"] } {

        # Get the header and the value from table
        set hdrs [table lookup [HTTP::header "ICAP-X"]]

        # Add it to ICAP header
        foreach x ${hdrs} {
            ICAP::header add [lindex [split ${x} ":"] 0] [lindex [split ${x}
            ↪":"] 1]
        }

        # Remove the temporary http header. But the data would show up in the_
        ↪ICAP header.
        HTTP::header remove "ICAP-X"
    }
}
```

2つ目の iRule において、ICAP-X ヘッダは HTTP ヘッダ上からは削除されますが、ICAP ヘッダに残

ります。このヘッダは無害ですが、気になる場合は、i-FILTER のヘッダコントロールにて削除して下さい。

また、接続テストをされる際には、変数情報をログ出力するなどして意図する値が入っているか確かめて頂くことをおすすめします。

例 1) 認証ユーザ名を確認するデバッグ

```
log local0. "Username: [ACCESS::session data get session.logon.last.username]"
```

例 2) エンコードされた内容を確認するデバッグ

```
log local0. "Encoded username: b64encode ldap:///[{ACCESS::session data get  
session.logon.last.username}]"
```

例 3) ヘッダー内容を確認するデバッグ

```
foreach attr "[HTTP::header names]" {  
    log local0. "$attr : [HTTP::header value $attr]"  
}
```

1.1.10 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。

SSL Orchestrator >> Configuration

System Settings | Version: 7.5.2

SSL Orchestrator Configuration

This guided configuration will allow you to quickly setup the SSL Orchestrator Configuration.

Configuration Options

L3 Outbound Transparent Proxy

L3 Outbound Transparent Proxy
An Outbound topology can be used to provide internal user access to external remote resources when the organization does not own the application resources and SSL keys.
1. The internal traffic takes a routed path into and out of the BIG-IP. The client is unaware of the SSL Orchestrator device while en route to the server.
2. The traffic is decrypted and is sent to security devices.
3. Then the traffic is re-encrypted and is routed out to the applications and Internet.

Configuring the following solution will guide you through creating the following objects:

- Topology**
Select the type of deployments you require and build on your configuration.
- SSL Configurations**
Configure your certificate chains for encrypting and decrypting packets.
- Services**
Define the security services to attach to SSL Orchestrator.
- Service Chaining**
Determine the flow of data through your network services.
- Security Policy**
Configure the traffic filtering and categorization to securely manage traffic.
- Interception Rules**
Create the rules for routing traffic.
- Egress Setting**
Manage SNAT Settings and configure Gateways.
- Log Settings**
Manage Log Settings.

Cancel **Next**

Required Configuration

Before you start this guided configuration, make sure that DNS, NTP and Routes are configured.

- ☒ DNS Configured
- ☒ NTP Configured
- ☒ Route Configured

Documentation

[Ask a question on F5 Support](#)

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

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

Topology Properties

Name
sslo. **L3ExplicitProxy**

Description
Provide a description for this deployment.

Protocol
TCP

IP Family
IPv4

SSL Orchestrator Topologies

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. 任意の名前を設定し、右上の *Show Advanced Setting* をクリックし、**Client-side SSL** にて、利用したい **TLS** のバージョンを選択します。

The screenshot shows the 'SSL Orchestrator Configuration' page for a profile named 'ssl0_L3ExplicitProxy'. The 'SSL Configuration' tab is selected in the top navigation bar. The 'Name' field contains 'ssl0_L3ExplicitProxy', which is highlighted with a red box. Below it, the 'Description' field is empty. The 'Client-side SSL' section is expanded, showing 'Processing Options'. A red box highlights the 'Enabled Options' list, which includes 'Filter', 'TLSv1', 'TLSv1.2', and 'TLSv1.3'. The 'Disabled Options' list includes 'SSLv3', 'TLS', and 'TLSv1.1'.

4. CA Certificate KeyChain にて、既にインポート済みの CA ファイルを選択して *Done* を押します。

The screenshot shows the 'CA Certificate Key Chain' dialog. The 'Certificate' and 'Key' fields both show the path '/Common/f5jplabCA', which is highlighted with a red box. The 'Chain' dropdown is set to '--Select--'. The 'Passphrase' field is empty. At the bottom, the 'Done' button is highlighted with a red box.

5. **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

Filter

TLSv1.1
TLSv1.2
TLSv1.3

Disabled Options

SSLv3
TLS
TLSv1

6. 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。

Cipher

/Common/f5-default

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

Trusted Certificate Authority ⓘ

/Common/ca-bundle.crt

Expire Certificate Response ⓘ

drop

Untrusted Certificate Authority ⓘ

drop

OCSP ⓘ

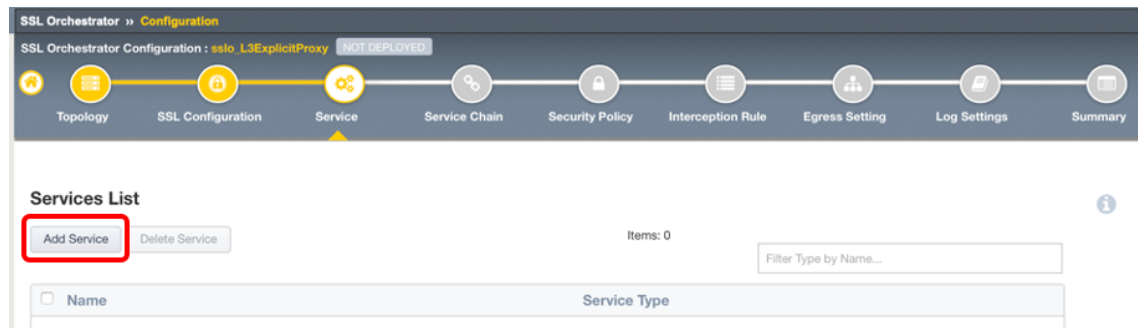
--Select--

CRL ⓘ

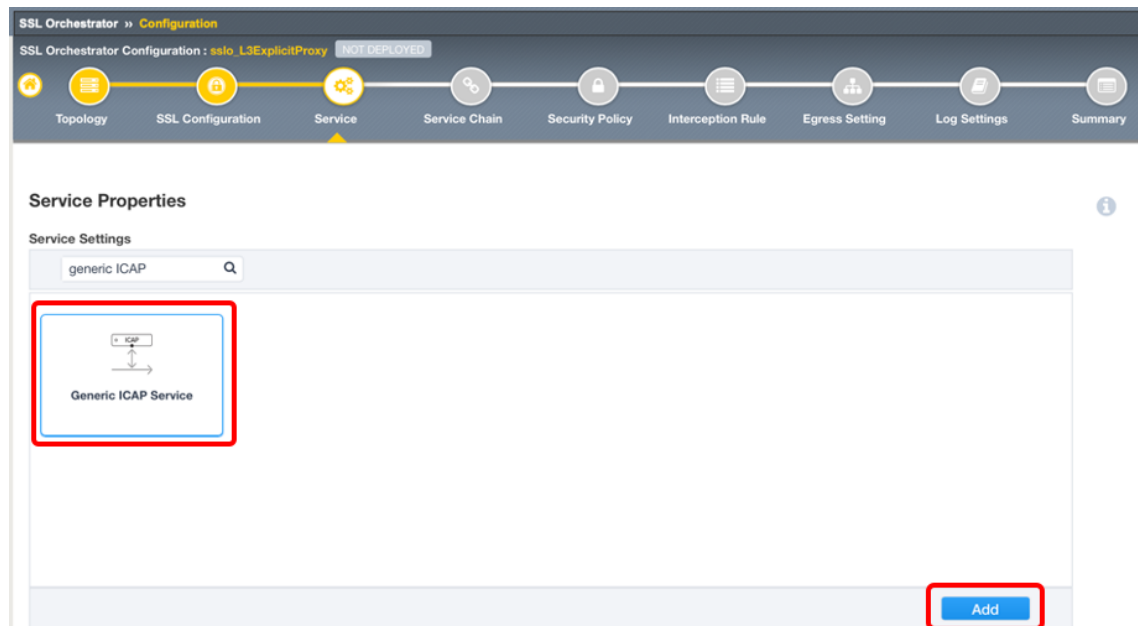
--Select--

Cancel Save Draft Back **Save & Next**

7. **Add Service** を押します。



8. **Generic ICAP Service** を選択し、**Add** ボタンを押します。



9. **任意の名前** を設定し、**ICAP Devices** に **i-FILTER の IP アドレス** と **ポート番号** を設定し、**Done** を押します。

SSL Orchestrator » Configuration

SSL Orchestrator Configuration : sslo_L3ExplicitProxy NOT DEPLOYED

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

Service Properties

Service Settings

Generic ICAP Service

Name
sslo: iFILTER

Description
Type: icap

IP Family
ipv4

ICAP Devices

IP Address
10.100.37.60

Port
15080

Cancel Done

No device configured

10. **Request Modification URI Path** に **/REQMOD** を入力し、**Preview Max Length** に **0** を入力し、**ICAP Policy** に既に作成済みの **Local Traffic Policy** を選択し、**Save** を押します。(i-FILTER ICAP 版は **ICAP Preview** に対応していないので、**0** を入力します。)

Request Modification URI Path ⓘ
/REQMOD

Response Modification URI Path ⓘ
/

Preview Max Length(bytes) ⓘ
0

Service Down Action ⓘ
Ignore

HTTP Version ⓘ
HTTP/1.0 & HTTP/1.1

ICAP Policy ⓘ
/Common/ifilter_db_rules

Cancel Save

11. Add Service を選択します。

SSL Orchestrator » Configuration
SSL Orchestrator Configuration : sslo_L3ExplicitProxy NOT DEPLOYED

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

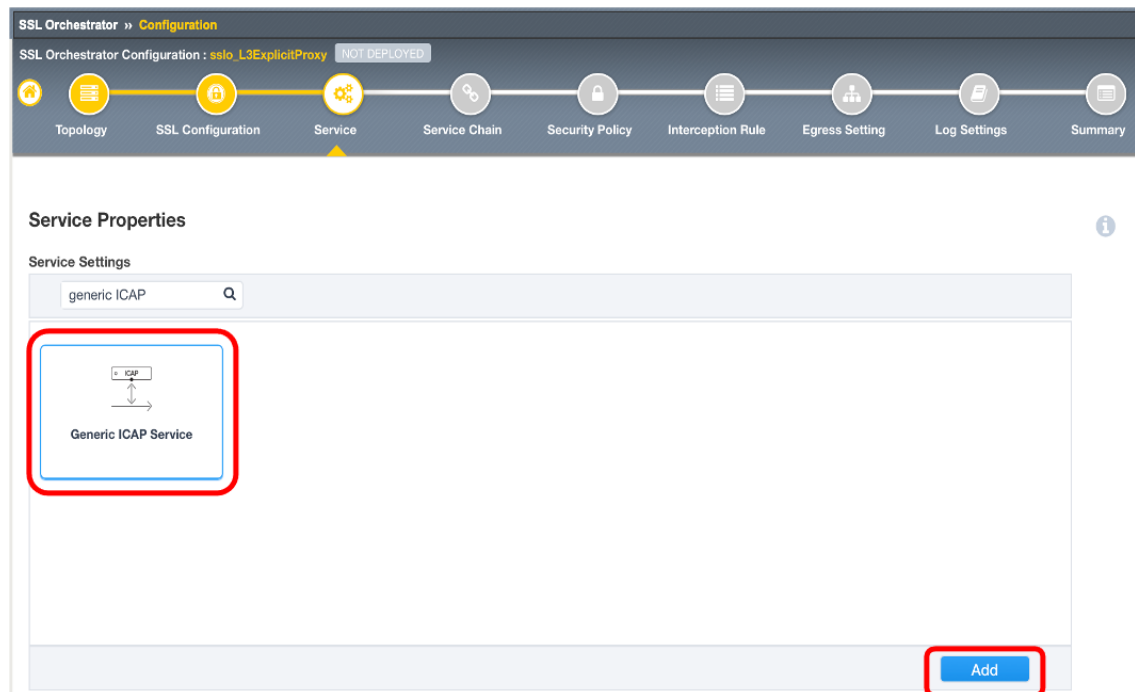
Services List ⓘ

Add Service Delete Service Items: 1 Filter Type by Name...

Name	Service Type
ssloS_iFILTER NOT DEPLOYED	ICAP

Cancel Save Draft Back Save & Next

12. **Generic ICAP Service** を選択し、**Add** ボタンを押します。



13. **任意の名前** を設定し、**ICAP Devices** に **任意の IP アドレス** と **任意のポート番号** を設定し、**Done** を押します。（こちらのサービスは実際には利用しませんので、設定する情報は何でも構いません。）

Service Properties

Service Settings


Generic ICAP Service

Name
ssloS_ restore_uri

In the ICAP service settings Name field, type a name after the default prefix ssloS_.

Description
Type: icap

Type a description for this service.

IP Family ⓘ
IPv4 only

ICAP Devices

IP Address ⓘ
1.1.1.1

Port
1344

Cancel Done

No device configured

14. **ICAP Policy** に既に作成済みのヘッダをもとに戻すための **Local Traffic Policy** を選択し、*Save* を押します。

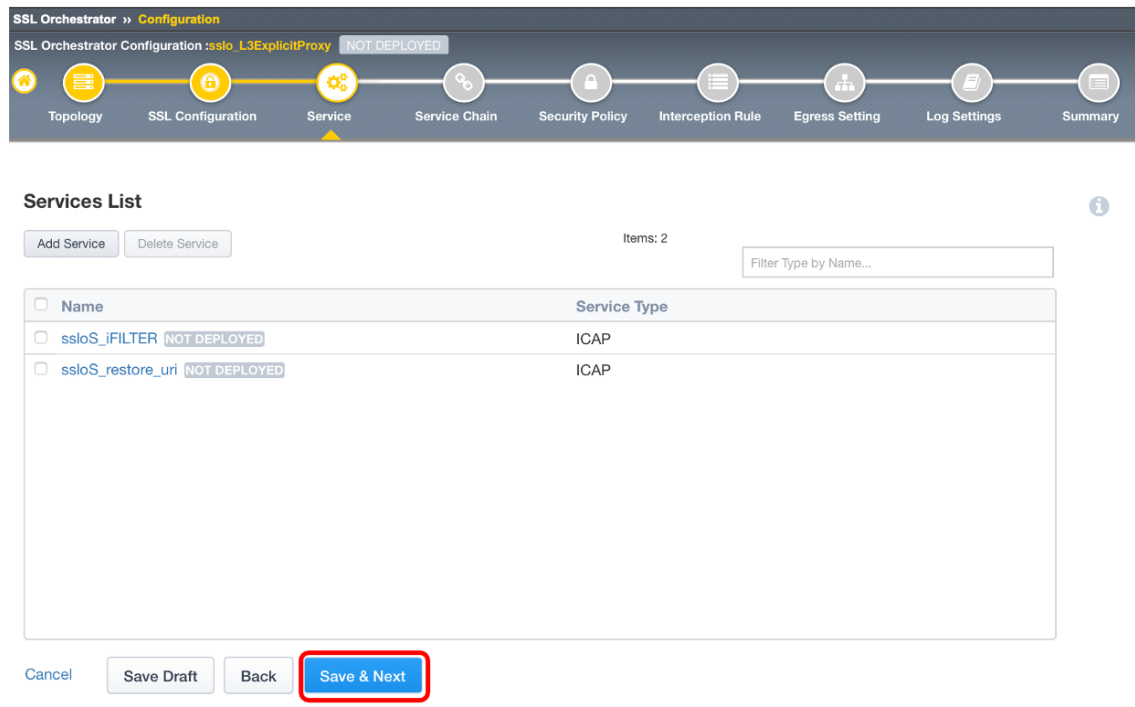
Service Down Action ⓘ
Ignore

HTTP Version ⓘ
HTTP/1.0 & HTTP/1.1

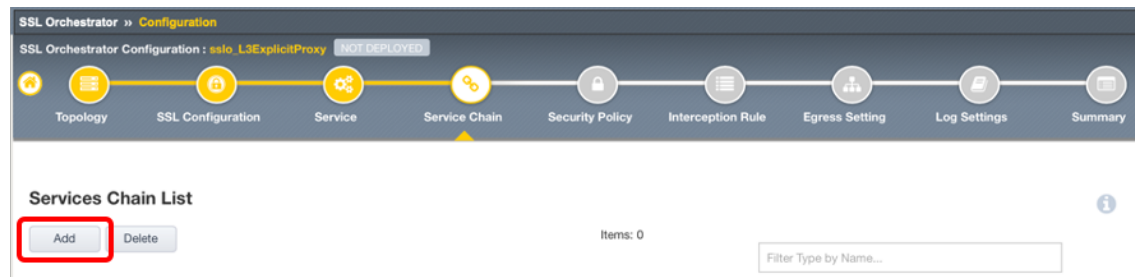
ICAP Policy ⓘ
/Common/restore_header

Cancel Save

15. *Save & Next* ボタンを押します。



16. **Service Chain List** で *Add* を押します。



17. **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。(i-FILTER のサービスが上にくるようにします。)

SSL Orchestrator » Configuration

SSL Orchestrator Configuration : sslo_L3ExplicitProxy 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

Filter

No available items

Selected Service Chain Order

ssloS_iFILTER

ssloS_restore_uri

Cancel **Save**

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

SSL Orchestrator » Configuration

SSL Orchestrator Configuration : sslo_L3ExplicitProxy NOT DEPLOYED

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

Services Chain List

Add Delete

Items: 1

Filter Type by Name...

Name	Description
☐ ssloSC_MyServiceChain NOT DEPLOYED	

Cancel Save Draft Back **Save & Next**

19. All Traffic の **ペンマーク** をクリックします。

SSL Orchestrator » Configuration

SSL Orchestrator Configuration : sslo_L3ExplicitProxy Not Deployed

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

Security Policy

Type **1**

☒ Create New ☐ Use Existing ☐ None

Name

ssloP_ L3ExplicitProxy

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

Description **1**

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	-

The edit icon (pencil) for the 'All Traffic' rule is highlighted with a red box.

20. 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
Pinners_Rule	SSL Check is true and Category Lookup (SNI) is Pinners	Allow	Bypass	-

Name

Default Rule

Type the name of your custom policy.

Action **1** Allow Intercept Service Chain **1**

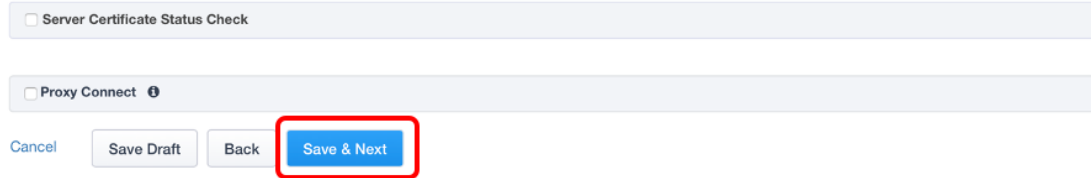
Cancel **OK**

Search

None

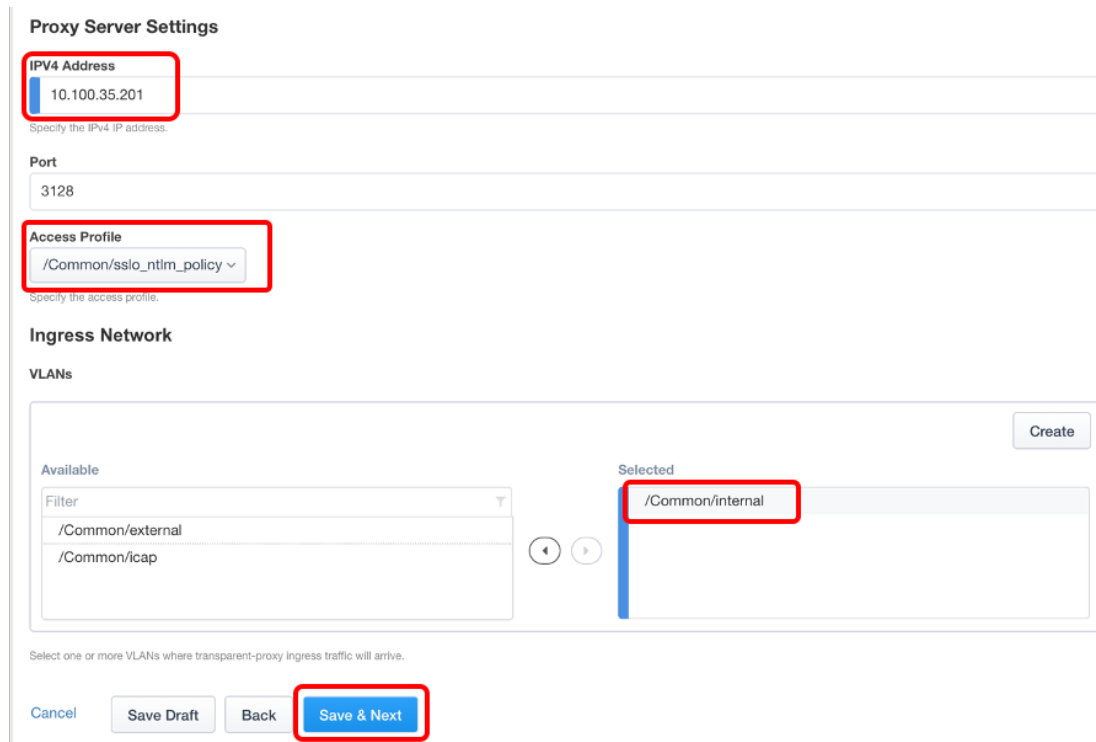
ssloSC_MyServiceChain

21. *Save & Next* ボタンを押します。



The screenshot shows a configuration page with two sections: "Server Certificate Status Check" and "Proxy Connect". Below these sections are four buttons: "Cancel", "Save Draft", "Back", and "Save & Next". The "Save & Next" button is highlighted with a red rectangular box.

22. **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 アドレスを入力し、既作成済みの **Access Profile** を選択し、**Ingress Network** として、クライアントからアクセス可能な **VLAN** を選択し、*Save & Next* ボタンを押します。



The screenshot shows the "Proxy Server Settings" configuration page. The following fields are highlighted with red boxes:

- IPv4 Address**: Contains the value "10.100.35.201".
- Access Profile**: A dropdown menu showing "/Common/sslo_ntlm_policy".
- Ingress Network**: A section titled "VLANs" containing two lists. The "Available" list on the left contains "/Common/external" and "/Common/icap". The "Selected" list on the right contains "/Common/internal".

At the bottom of the page, the "Save & Next" button is also highlighted with a red box.

23. 本テスト構成では、**Manage SNAT Settings** で **Auto Map**、**Gateways** で **Default Route** を選択し、*Save & Next* ボタンを押します。(設定は検証環境に合わせてください。)

SSL Orchestrator » Configuration

SSL Orchestrator Configuration : sslsso_L3ExplicitProxy 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**

24. **Save & Next** ボタンを押します。

SSL Orchestrator » Configuration

SSL Orchestrator Configuration : sslsso_L3ExplicitProxy NOT DEPLOYED

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

Log Settings

Applies to Access Profile ⓘ

/Common/sslsso_L3ExplicitProxy.app/sslsso_L3ExplicitProxy_accessProfile

Per-Request Policy ⓘ

Error

FTP ⓘ

Error

IMAP ⓘ

Error

POP3 ⓘ

Error

SMTPS ⓘ

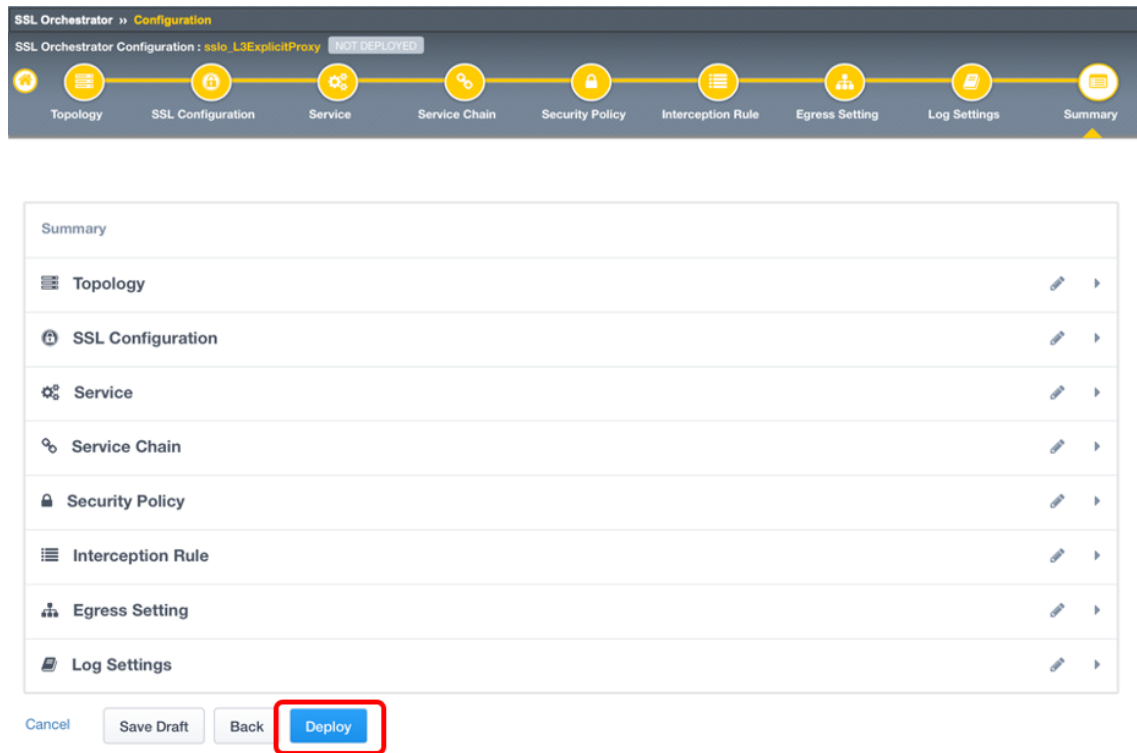
Error

SSL Orchestrator Generic ⓘ

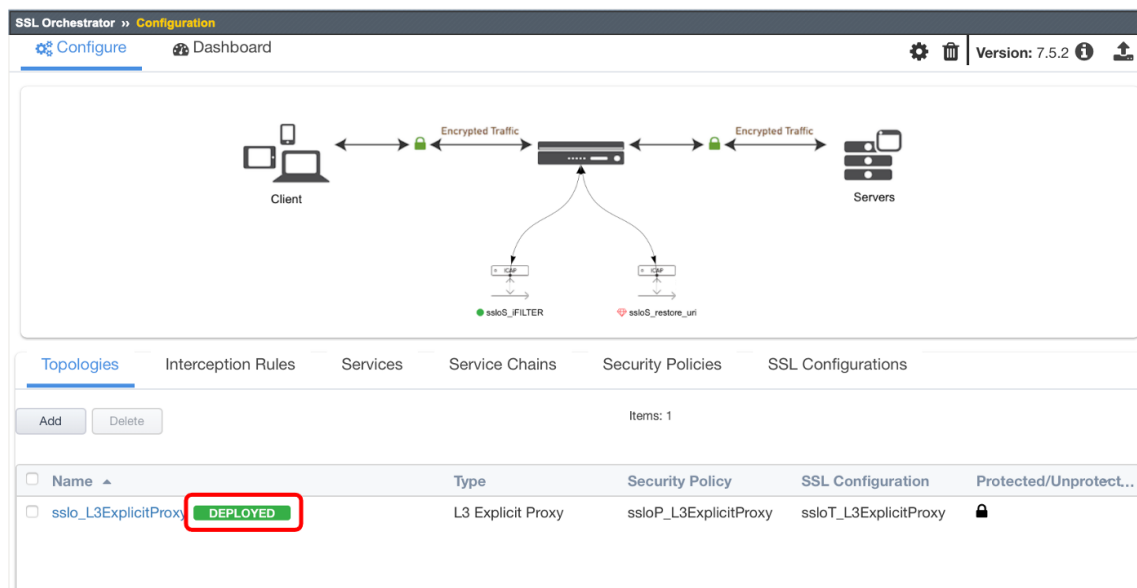
Error

Cancel Save Draft Back **Save & Next**

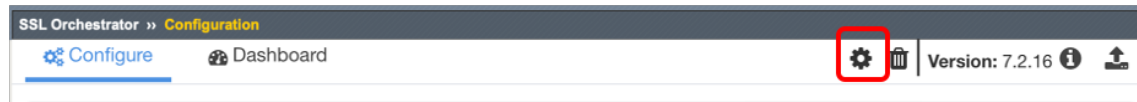
25. 必要に応じて、設定内容を見直し、*Deploy* ボタンを押します。



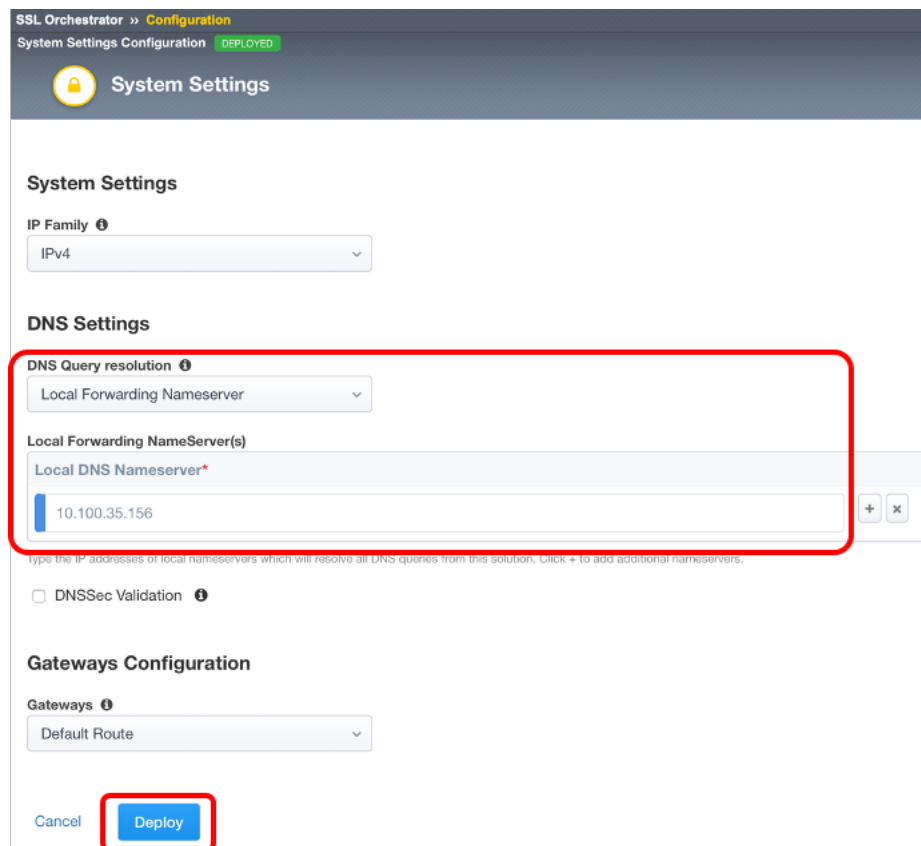
26. OK ボタンを押し、Deploy に成功すると以下のような緑色の **DEPLOYED** マークが表示されます。



27. 右上の **System Settings** アイコンを選択します。



28. SSLO が Explicit Proxy として利用する **DNS** を設定し、*Deploy* を押します。



29. i-FILTER と連携するサービスに関しては認証ヘッダを挿入するために、また、ヘッダをリストアするサービスに関してはモニタを停止するため、Protected の 鍵 マークを外します。

SSL Orchestrator » Configuration

Configure Dashboard Version: 7.5.2

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

Add Delete Items: 2

Name	Service Sta...	Pool Member Status	Service Type	Service Do...	Port Remap	Protected/
ssloS_iFILTER	DEPLOYED	Show All	ICAP	ignore	Not Applicable	
ssloS_restore_uri	DEPLOYED	Show All	ICAP	ignore	Not Applicable	

30. ヘッダをリストアするサービスに紐づく Pool のモニターの情報はずします。(設定を外す前は存在しないサーバに対して、モニターを投げているので、Availability が Offline となっているはずです。)

Local Traffic » Pools : Pool List » ssloS_restore_uri

Properties Members Statistics

General Properties

Name	ssloS_restore_uri
Application	ssloS_restore_uri
Partition / Path	Common/ssloS_restore_uri.app
Description	
Availability	☒ Unknown (Enabled) - The children pool member(s) either don't have service checking enabled, or servi

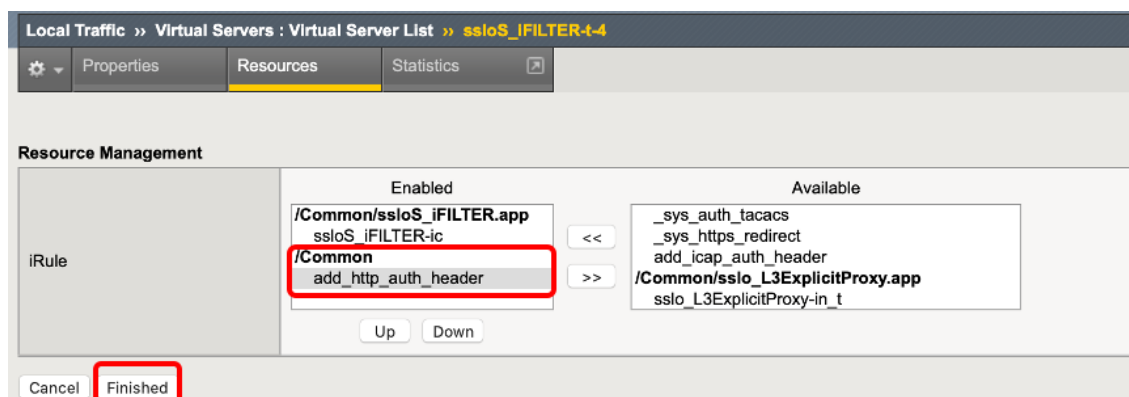
Configuration: Basic

Health Monitors

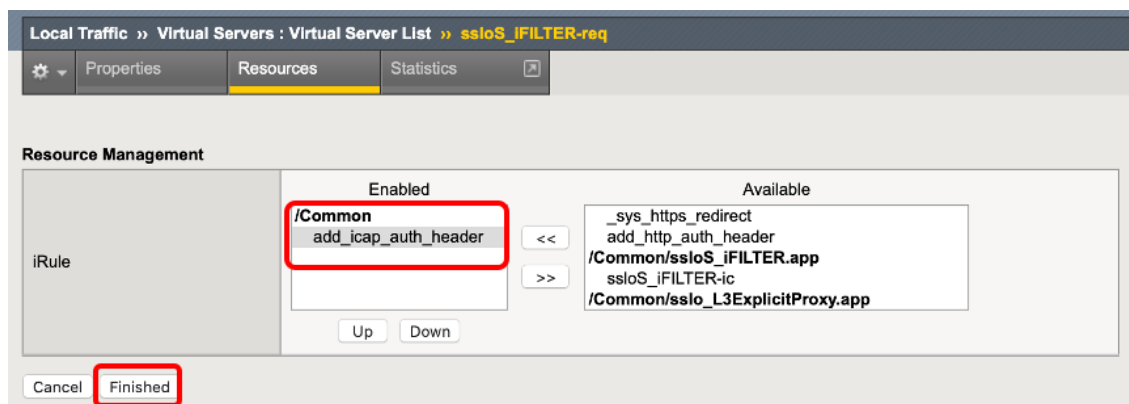
Active Available

Update Delete

31. 既に作成済みの **iRule** を追加します。**Local Traffic >> Virtual Servers>>**において、**ssloS_XXXX(任意)-t-4** という名称の Virtual Server を選択し、**Resources** タブを選択、HTTP リクエストヘッダに認証情報を挿入するための **iRule** を選択し、**Finished** を押します。



32. ICAP リクエストヘッダに加えるための **iRule** を追加します。**Local Traffic >> Virtual Servers** において、**ssloS_XXXX(任意)-req** という名称の Virtual Server を選択し、**Resources** タブを選択、ICAP リクエストヘッダに認証情報を挿入するための **iRule** を選択し、**Finished** を押します。



注釈:

- 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。

1.1.11 i-FILTER ICAP 版（Linux 版）の設定

i-FILTER のインストールは終了しているものとします。

ユーザ認証の設定

1. システム／ユーザ認証／基本設定 を選択します。
2. 基本設定 の ユーザ認証方式 において ICAP 認証 を選択します。

The screenshot shows the i-FILTER configuration interface. The top navigation bar includes 'i-FILTER', 'グループ', '共通', 'ルールセット', 'ログ', and 'システム'. The breadcrumb trail is 'システム / ユーザ認証 / 基本設定 *'. The 'ログインユーザー' is 'admin' with a 'ログアウト' button. A green '保存' (Save) button is in the top right. The '基本設定' (Basic Settings) section is expanded, showing 'ユーザー認証方式' (User Authentication Method) set to 'ICAP認証' (ICAP Authentication), '認証ダイアログ表示名' (Authentication Dialog Display Name) as 'inetnf.proxy', and 'LDAPv3 ページコントロール' (LDAPv3 Page Control) with '有効にする' (Enable) unchecked and 'ページサイズ' (Page Size) as 0.

3. ICAP 認証設定 の ICAP 認証ユーザ参照 において、有効にする をチェックします。

The screenshot shows the 'ICAP 認証設定' (ICAP Authentication Settings) section. The 'ICAP 認証ユーザ参照' (ICAP Authentication User Reference) checkbox is checked, and the text '有効にする' (Enable) is next to it. The 'Cache Time to Live' is set to 7200 秒 (seconds).

4. 右上の 保存 ボタンを押します。

The screenshot shows the i-FILTER configuration interface, similar to the previous one. The '保存' (Save) button in the top right corner is highlighted with a red box.

5. 次に、**システム／ユーザ認証／LDAP サーバ設定** を選択します。本ガイドでは認証ユーザ情報を AD サーバから取り込むため、以下のように設定し、**保存** ボタンを押します。

LDAPサーバ設定	
アドレス : ポート番号	172.28.14.56 : 389
サーバ状態	☒ 利用 ☐ 待機 ☐ 無効 振り分け比率 1
LDAPバージョン	3
BIND	BIND有効
BIND DN	cn=Administrator,cn=Users,dc=f5jplab,dc=local
BINDパスワード	☐ パスワードを更新する (※現在、パスワードが設定されています) 新パスワード 新パスワード(確認)
Search Base	dc=f5jplab,dc=local
Search Filter	(sAMAccountName=%1)
Search Group	(&[(objectclass=organizationalunit)(objectclass=groupofuniquenames)(objectclass=groupc
Search User	(&[(objectclass=person)(objectclass=account))
BINDタイムアウト	60 秒
Searchタイムアウト	60 秒

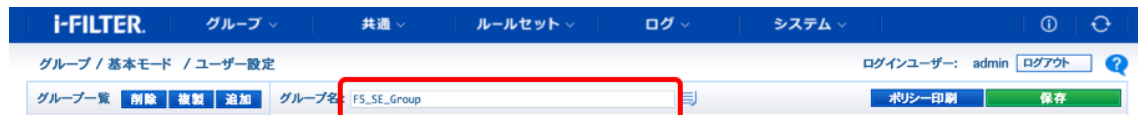
項目	設定例
アドレス:ポート番号	ご利用の AD 情報を登録
BIND	BIND 有効
BIND DN	ご利用の管理者 BIND DN 情報を登録 設定例 : cn=Administrator,cn=Users,dc=f5jplab,dc=local
BIND パスワード	ご利用のドメイン管理者のパスワードを登録
Search Base	ご利用のドメイン情報を登録 設定例 : dc=f5jplab,dc=local
Search Filter	(sAMAccountName=%1)

グループポリシーの作成、ユーザ情報の取り込み

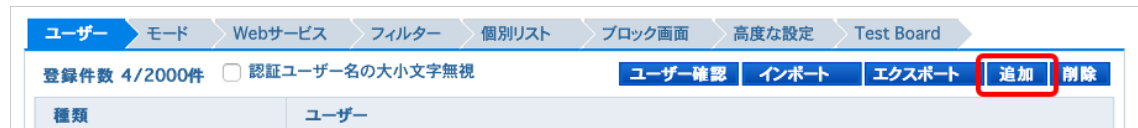
1. **グループ／基本モード／モード設定** において、**追加** ボタンを押します。



2. **グループ名** を分かりやすいグループ名に変更します。



3. **ユーザ** タブにおいて、**追加** ボタンをクリックします。



4. **認証ユーザ参照** を選択します。

ユーザー追加

編集モード: **認証ユーザー参照** ※ICAP認証ユーザー参照が有効です

利用する認証設定: デフォルト設定

検索: ☐ 条件なし ☐ ユーザー完全一致 ☐ 部分一致

サーバーから取得

キャンセル

5. 検索しやすい検索条件を設定し、AD から取り込みたい **ユーザ名** を追加します。

ユーザー追加

編集モード: **認証ユーザー参照** ※ICAP認証ユーザー参照が有効です

利用する認証設定: デフォルト設定

検索: f5 se ☐ 条件なし ☐ ユーザー完全一致 ☒ 部分一致

サーバーから取得

ユーザー検索結果 [3] 件

CN=f5 se001,OU=SeDepartment,DC=f5jplab,DC=local
 CN=f5 se002,OU=SeDepartment,DC=f5jplab,DC=local
 CN=f5 se003,OU=SeDepartment,DC=f5jplab,DC=local

追加

キャンセル

6. **Web サービス** タブを選択し、制御したいサービスを選択し、ユーザに利用不許可とする機能に対し、**ブロック** を選択します。（注：下記イメージはあくまでも一例です。）

グループ名: F5_SE_Group ポリシー印刷 保存

有効期間 開始日 2020/04/19 終了日 2020/05/31 clear: CTL+End

ユーザー モード **Webサービス** フィルター 個別リスト ブロック画面 高度な設定 Test Board

一括設定: リスク (未選択) アクション (未選択) プリセット 追加 削除

サービス名	有効	機能名	アクション	許可カテゴリ名	リスク
☐ Facebook	☒ ON	Facebook 閲覧	許可	SNS/動画配信/Web翻訳・URL変換	1
		Facebook ログイン	許可	SNS	2
		Facebook 投稿	ブロック	SNS/動画配信/アップローダー	2
		Facebook メッセージ送信	ブロック	SNS	2
		Facebook ファイルアップロード	ブロック	アップローダー/SNS/動画配信	3
		Facebook 連携アプリ認証 (OAuth認証)	許可	SNS	3
		Facebook アプリセンター	ブロック	総合ソフトウェアダウンロード/SNS/ゲーム	2
		Messenger messenger.com 閲覧	ブロック	チャット/インターネット電話	2
		Messenger messenger.com 投稿	ブロック	チャット/インターネット電話	3
		Messenger messenger.com アップロード	ブロック	チャット/インターネット電話	3
☐ YouTube (Google)	☒ ON	YouTube 閲覧	許可	動画配信/アップローダー/検索エンジン/Web翻訳・URL変換/音楽	1
		YouTube 一般動画閲覧	ブロック	動画配信/アップローダー	2
		文部科学省公式チャンネル 閲覧	許可	動画配信/アップローダー	2
		Tokyo 2020公式チャンネル 閲覧	許可	動画配信/アップローダー	2
		YouTube コメント投稿	ブロック	動画配信/アップローダー	3
		YouTube 動画アップロード	ブロック	動画配信/アップローダー	3

7. **個別リスト** タブを選択し、個別ブロックしたい URL/URI を追加し、右上の **保存** ボタンを押します。(注: 下記イメージはあくまでも検証目的で設定した内容です。)

グループ名: F5_SE_Group ポリシー印刷 保存

有効期間 開始日 2020/04/19 終了日 2020/05/31 clear: CTL+End

ユーザー モード Webサービス フィルター **個別リスト** ブロック画面 高度な設定 Test Board

個別リスト設定: ブラックリスト(優先カテゴリ) ↓

ブラックリスト(優先カテゴリ): 登録件数 3/5000件 インポート エクスポート

設定一覧	https://httpbin.org/get 【完全】 http://http.badssl.com/ 【完全】 https://rsa2048.badssl.com/ 【完全】
	削除
URL	追加 変更 タイプ: 部分一致 / アクション: ブロック メール通知: しない
コメント	
登録URLの有効設定	有効にする
有効期限	無期限 まで

ブロック画面のタイトル画像連携設定

1. システム／システムパラメーター／動作設定 において、仮想ホスト名設定 のコンテンツ転送 の値を、で設定した SSLO の Interception Rule の Destination Address の IP アドレスに変更します。

仮想ホスト名設定	
管理画面	inetnf.conf 127.0.0.1 / 15081
コンテンツ転送	10.100.35.201

2. i-FILTER v10.40R01 より、WEB 接続ブロック時にユーザに表示するブロック画面中のタイトル画像は、HTTPS 接続アク

3. ここでは、簡易的にブロック画面中にタイトル画像を表示せず、システム／デフォルト画面／ブロック画面において、タイトル画像を **表示しない** を選択し、**保存** ボタンを押します。必要に応じて、メッセージも変更します。

システム / デフォルト画面 / ブロック画面 ログインユーザー: admin ログアウト ?

インポート **プレビュー** **保存**

外部で作成したブロック画面を使用する

ブロック画面 ☐ ユーザーが作成したブロック画面を使用する
[インポートされていません。]

メッセージ設定

タイトル名

背景色

タイトル画像

メッセージ1

```
<font color=#ff0000 size=5 face=MS ゴシック><b>こちらのサイトは接続を許可されていません!</b></font>
<hr color=#ff0000 width=60% align=left size=3>
このページは「i-FILTER」によりブロックされました。
```

登録文字数 156/2000文字

追加メッセージ

☒ 「改ざんサイト」ブロック時に以下のメッセージを追加する
このURLから展開されるWebサイトで、一部改ざんされたWebページを検知しています。

登録文字数 43/2000文字

表示項目 ☒ URL ☒ ブロック理由 ☒ IPアドレス ☒ 認証ユーザー名

メッセージ2

F5 Networks Japan 検証ページ

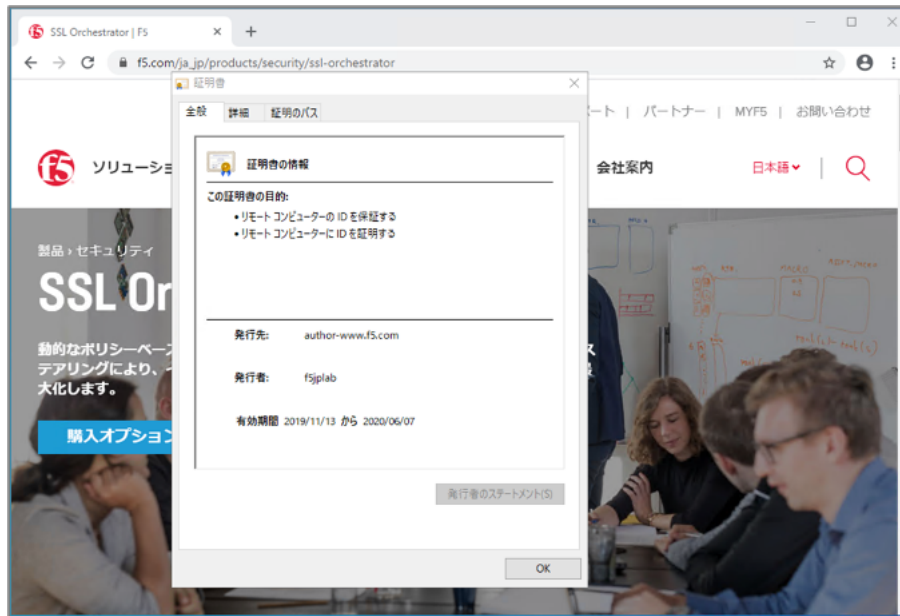
登録文字数 23/2000文字

1.1.12 クライアントからの接続テスト

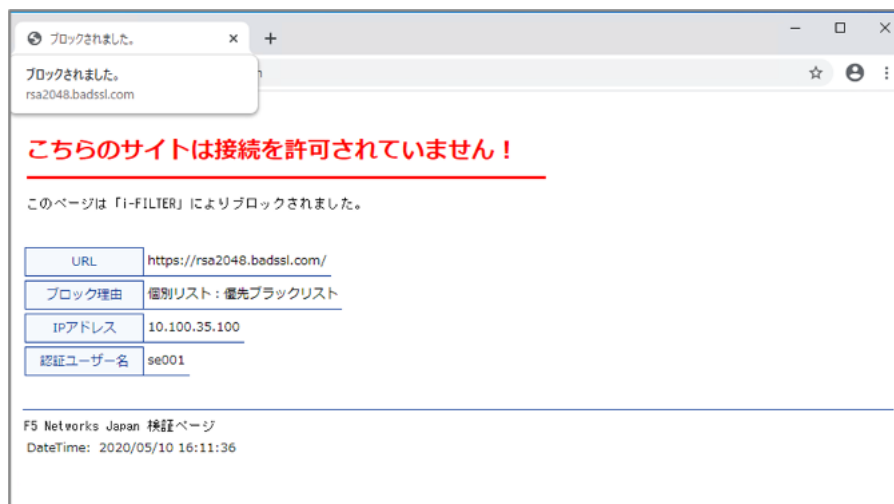
1. クライアントに SSLO の **CA 証明書** をインストールします。
2. コマンドラインで確認する場合は、以下を利用します。

```
curl -vk --proxy 10.100.35.201:3128 -proxy-ntlm -proxy-user 'se001:ilovef5!' --https://xxxx.xxx
```

3. ブラウザで確認する場合は、プロキシ設定に SSLO を加えてから WEB 接続を確認します。
4. WEB 通信が成功するか確認します。サーバ証明書が SSLO の CA 証明書で **書き換えられている** ことを確認します。



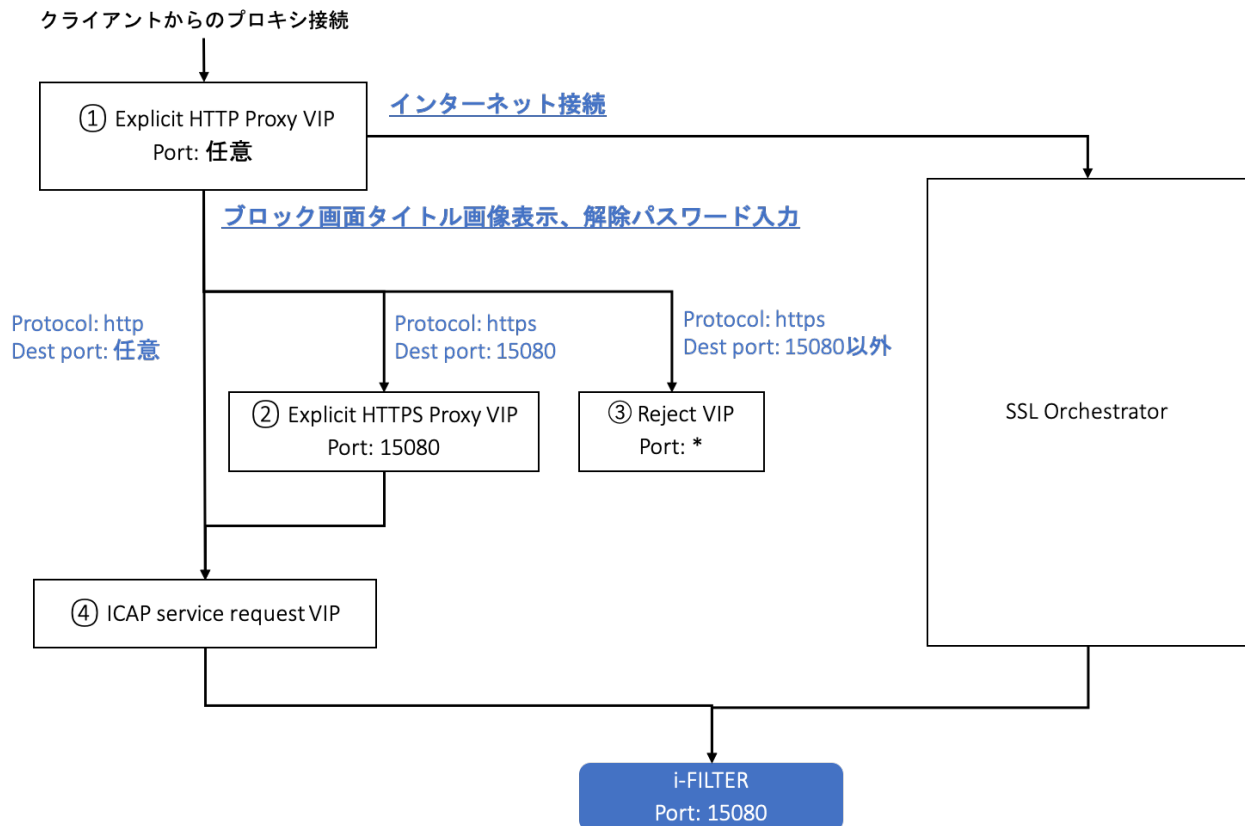
5. ブラックリストの宛先への通信が **ブロック** されることを確認します。



6. SSL 復号除外サイトの通信が成功するか確認します。サーバ証明書が SSLO の CA 証明書で **書き換えられていない** ことを確認します。

1.1.13 i-FILTER ブロック画面のタイトル画像の表示、パスワードブロック解除の設定

1.11.3. にて、SSLO 連携をするとブロック画面のタイトルが標準では表示されないと記載しましたが、以下の設定を追加することによって、表示させることが可能です。本設定を行うことにより、パスワード入力によるブロック解除も連携が可能となります。上記を実現するためには、下図の 4 つの Virtual Server が追加で必要となります。ここでは、下図の ①②③④ の順で作成していきます。



ICAP service request 用 Virtual Server の作成

1. まずは ICAP 用のプロファイルを以下のように作成します。 **Local Traffic >> Profiles >> Services >> ICAP** にて、**Create** ボタンを押します。 **任意の名前** を入力し、**URI** には以下のように入力し、**Finished** ボタンを押します。

icap://\${SERVER_IP}:\${SERVER_PORT}/REQMOD

The screenshot shows the 'New ICAP Profile...' configuration window. In the 'General Properties' section, the 'Name' field contains 'iFILTER-req' and the 'Parent Profile' is set to 'icap'. In the 'Settings' section, the 'URI' field contains 'icap://\${SERVER_IP}:\${SERVER_PO}'. The 'Finished' button at the bottom is highlighted with a red box.

2. 次に ICAP service request 用の Virtual Server を作成します。 **Local Traffic >> Virtual Servers** にて、**Create** ボタンを押します。 **任意の名前** を入力し、**Type** は **Internal** を選択します。

The screenshot shows the 'New Virtual Server...' configuration window. In the 'General Properties' section, the 'Name' field contains 'iFILTERicapReq' and the 'Type' is set to 'Internal'. The 'State' is set to 'Enabled'.

3. **Configuration** にて **Advanced** を選択し、**ICAP Profile** にて、作成済みの **ICAP プロファイル** を選択し

ます。

Configuration: **Advanced**

Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile (Client)	None
HTTP Profile (Server)	(Use Client Profile)
HTTP Proxy Connect Profile	None
SSL Profile (Server)	Selected Available / Common apm-default-serverssl crypto-client-default-serverssl f5aas-default-ssl pcoip-default-serverssl serverssl serverssl-insecure-compatible
Service Profile	None
SplitSession Client Profile	None
ICAP Profile	iFILTER-req
Request Adapt Profile	None

4. 最後に、**Default Pool** にて、SSLO Guided Configuration で作成済みの **Pool** を選択して、*Finished* ボタンを押します。

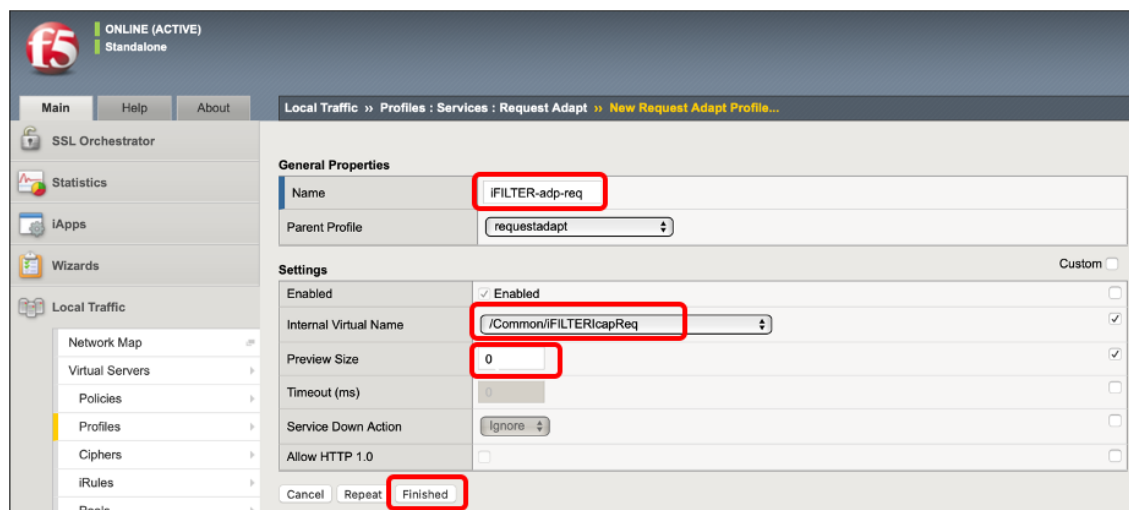
Resources

iRules	Enabled Available / Common _sys_APM_ExchangeSupport_OA_BasicAuth _sys_APM_ExchangeSupport_OA_NtlmAuth _sys_APM_ExchangeSupport_helper _sys_APM_ExchangeSupport_main
Default Pool	ssloS_iFILER
Default Persistence Profile	None
Fallback Persistence Profile	None

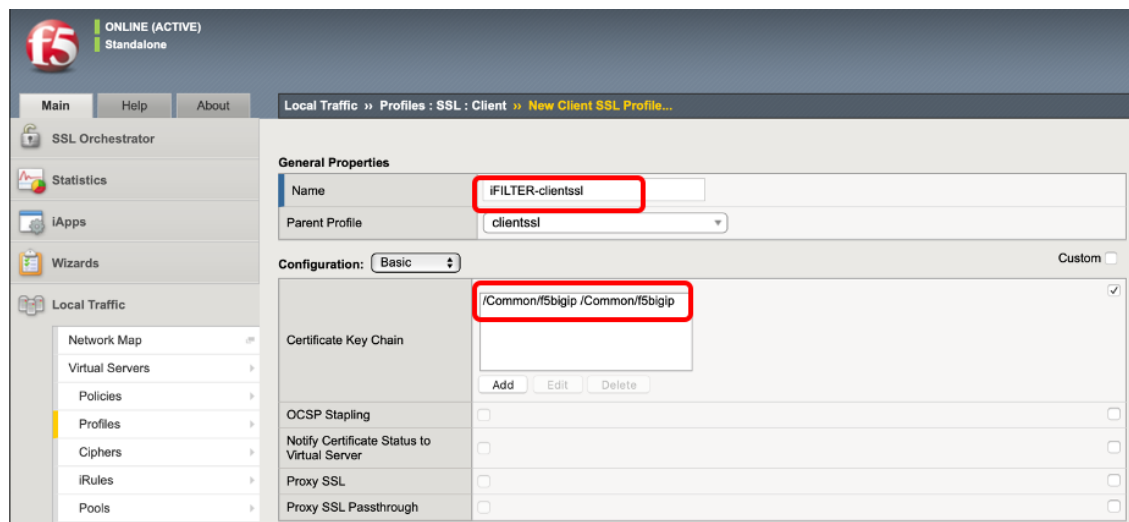
Cancel Repeat **Finished**

Explicit HTTPS Proxy 用 Virtual Server の作成

1. まず、ICAP 用の Virtual Server を呼び出すための Request Adapt プロファイルを作成します。**Local Traffic >> Profiles >> Services >> Request Adapt** にて、**Create** ボタンを押します。**任意の名前**を入力し、**Internal Virtual Name** にて、作成済みの **Virtual Sever** を選択し、**Preview Size** にて、**0**を入力し、**Finished** ボタンを押します。



2. 次に、SSL サイトにおけるブロック時に、ブロック画面内のタイトル画像に SSL 接続するための ClientSSL プロファイルを作成します。**Local Traffic >> Profiles >> SSL >> Client** にて、**Create** ボタンを押します。**任意の名前**を入力し、タイトル画像を SSL 経由で表示させるための **サーバ証明書** と **秘密鍵** を選択し、**Finished** ボタンを押します。(BIG-IP にて SSL オフロードを行うため、**System >> Certificate Management >> Traffic Certificate Management** にて、予め **サーバ証明書** と **秘密鍵** の登録が必要となります。)



3. 次に、Proxy 用の Tunnel を作成します。**Network >> Tunnel List** にて、*Create* ボタンを押します。**任意の名前**を入力し、**Profile** にて、**tcp-forward** を選択し、*Finished* ボタンを押します。

The screenshot shows the F5 i-Filter configuration interface. The left sidebar contains navigation options: Main, Help, About, SSL Orchestrator, Statistics, iApps, Wizards, Local Traffic, Traffic Intelligence, Access, and Device Management. The main area displays the 'Configuration' section for a new tunnel. The 'Name' field is 'L3ExplicitProxy-xp-tunnel', 'Description' is empty, 'Profile' is 'tcp-forward', 'MTU' is '0', 'Use PMTU' is 'Enabled', 'TOS' is 'Preserve', and 'Auto-Last Hop' is 'Default'. At the bottom, there are 'Cancel', 'Repeat', and 'Finished' buttons. Red boxes highlight the 'Name' field, the 'Profile' dropdown, and the 'Finished' button.

4. 次に、HTTPS トラフィックにおける URI 書き換え用の iRule を作成します。**Local Traffic >> iRules** にて、*Create* ボタンを押します。**任意の名前**を入力して、**Definition** に以下サンプル iRule を入力し、*Finished* ボタンを押します。(以下の iRule はあくまでもサンプルとなります。同じ主旨の内容であれば下記と同じでなくても構いません。)

例) URI 書き換え用の iRule

```
### Add this iRule to Explicit HTTPS Virtual Server ###
when HTTP_REQUEST {
    set OLDURI [HTTP::uri]
    HTTP::uri "https://[HTTP::host]$OLDURI"
}
```

5. 次に、SSL 用の Explicit HTTPS Virtual Server を作成します。**Local Traffic >> Virtual Servers** にて、*Create* ボタンを押します。**任意の名前**を入力し、**Destination Address/Mask** にて、**0.0.0.0/0**を入力、**Service Port** にて、**15080** と入力します。

The screenshot shows the F5 i-FILTER configuration interface. The top navigation bar includes 'Main', 'Help', and 'About'. The left sidebar shows the 'Local Traffic' menu with options like 'Network Map', 'Virtual Servers', 'Policies', 'Profiles', 'Ciphers', 'iRules', and 'Pools'. The main area displays the 'General Properties' for a Virtual Server named 'iFILTERProxy'. The properties are as follows:

Property	Value
Name	iFILTERProxy
Description	
Type	Standard
Source Address	Host Address List
Destination Address/Mask	0.0.0.0/0
Service Port	15080
Notify Status to Virtual Address	☒
State	Enabled

6. **Configuration** にて、**Advanced** を選択し、**HTTP Profile** にて、**http** を選択、**SSL Profile (Client)** にて、作成済みの **clientssl プロファイル** を選択します。

The screenshot shows the 'Configuration' tab of the F5 i-FILTER configuration interface. The 'Configuration' dropdown is set to 'Advanced'. The configuration parameters are as follows:

Parameter	Value
Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile (Client)	http
HTTP Profile (Server)	(Use Client Profile)
HTTP Proxy Connect Profile	None
FTP Profile	None
SOCKS Profile	None
Stream Profile	None
iRules LX Profile	None
XML Profile	None
MQTT	☐
SSL Profile (Client)	iFILTER-clientssl

The 'SSL Profile (Client)' section shows a list of available profiles. The 'Selected' list contains 'iFILTER-clientssl'. The 'Available' list contains the following profiles:

- /Common
- clientssl
- clientssl-insecure-compatible
- clientssl-quick
- clientssl-secure
- crypto-server-default-clientssl
- split-session-default-clientssl

7. **Request Adapt Profile** にて、作成済みの **プロファイル** を選択し、**VLAN and Tunnel Traffic** にて、**Enable on...** を選択し、**VLANs and Tunnels** にて作成済みの **Tunnel** を選択し、**Source Address Translation** にて **Auto Map** を選択し、**Address Translation** と **Port Translation** のチェックをはずします。

Request Adapt Profile	iFILTER-adp-req
Response Adapt Profile	None
Statistics Profile	None
VLAN and Tunnel Traffic	Enabled on...
VLANs and Tunnels	Selected /Common L3ExplicitProxy-xp-tunnel << >> Available /Common external http-tunnel icap internal
Source Address Translation	Auto Map
Bandwidth Controller	None
Traffic Class	Enabled << >> Available
Connection Limit	0
Eviction Policy	None
Eviction Protected	☐ Enabled
Connection Rate Limit	0
Connection Rate Limit Mode	Per Virtual Server
Address Translation	☐ Enabled
Port Translation	☐ Enabled

8. **iRules** にて、作成済みの **iRule** を選択し、**Finished** ボタンを押します。

Resources

iRules	Enabled	Available
	/Common iFILTER-https-rule	add_auth_http add_auth_icap /Common/ssloS_iFILER.app ssloS_iFILER-ic /Common/sslo_L3ExplicitProxy.app
Policies	Enabled	Available
		/Common ifilter_db_rules
Default Pool	None	
Default Persistence Profile	None	
Fallback Persistence Profile	None	

Cancel Repeat **Finished**

Explicit HTTP Proxy 用 Virtual Server の作成

1. まず、プロキシ用の Explicit Profile を作成します。**Local Traffic >> Profiles >> Services >> HTTP** にて、**Create** ボタンを押します。**Proxy Mode** にて、**Explicit** を選択します。

Local Traffic >> Profiles : Services : HTTP >> New HTTP Profile...

General Properties

Name	L3ExplicitProxy-xp
Proxy Mode	Explicit
Parent Profile	http-explicit

2. **DNS Resolver** にて、SSLO Guided Configuration で作成した **DNS Resolver** を選択し、**Tunnel Name** にて、作成済みの **Tunnel** を選択し、**Finished** ボタンを押します。

Explicit Proxy

DNS Resolver	ssloGS-net-resolver	☒
IPv6	☐	☐
Route Domain	0	☐
Tunnel Name	L3ExplicitProxy-xp-tunnel	☒

3. 次に、以下の2つの iRule を作成します。

- インターネット接続用の HTTP/HTTPS トラフィックと i-FILTER ブロックタイトル画面接続トラフィックを分ける iRule
- 上記後者のトラフィックにおいて、i-FILTER 向けに URI を書き換える iRule

Local Traffic >> iRules にて、*Create* ボタンを押します。**任意の名前**を入力して、**Definition** に以下サンプル **iRule** を入力し、*Finished* ボタンを押します。本 iRule では、トラフィックの内容をみて、ICAP プロファイルを紐付けるかの判断もしています。また、iRule 内のホスト名は、環境にあわせた FQDN/IP アドレスに変更して頂く必要があります。(以下の iRule はあくまでもサンプルとなります。同じ主旨の内容であれば下記と同じでなくても構いません。また、以下の2つの iRule は、1つのファイルにいただいても構いません。)

例) トラフィックを分ける用の iRule

```
### Add this iRule to Explicit Virtual Server ###
when HTTP_PROXY_REQUEST {
    set F5PROXY "bigip.f5jplab.local"
    if { [HTTP::host] contains $F5PROXY } {
        HTTP::proxy enable
        ADAPT::enable request false
    } else {
        HTTP::proxy disable
        virtual sslo_L3ExplicitProxy.app/sslo_L3ExplicitProxy-xp-4
        snat automap
    }
}
```

例) URI 書き換え用の iRule

```
### Add this iRule to Explicit Virtual Server ###
when HTTP_REQUEST {
    set F5PROXY "bigip.f5jplab.local"
    if { [HTTP::host] contains $F5PROXY } {
        set OLDURI [HTTP::uri]
        HTTP::uri "http://[HTTP::host]$OLDURI"
        ADAPT::enable request true
    } else {
        ADAPT::enable request false
    }
}
```

4. 次に Explicit HTTP Proxy 用の Virtual Server を作成します。**Local Traffic >> Virtual Servers** にて、*Create*

ボタンを押します。**任意の名前**を入力し、**Destination Address/Mask**にて、プロキシ接続用の **IP アドレス**を入力、**Service Port**にて、プロキシとして利用する **ポート番号**を入力します。

Local Traffic >> Virtual Servers : Virtual Server List >> New Virtual Server...

General Properties

Name	L3ExplicitProxy
Description	
Type	Standard
Source Address	Host Address List
Destination Address/Mask	Host Address List 10.100.35.211
Service Port	Port Port List 3128 Other:
Notify Status to Virtual Address	☒

5. **HTTP Profile(Client)**にて、作成済みの **HTTP Explicit Profile** を選択します。

Configuration: Advanced

Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile (Client)	L3ExplicitProxy-xp-http

6. **Request Adapt Profile**にて、作成済みのプロファイルを選択し、**Source Address Translation**にて、**Auto Map**を選択します。

Request Adapt Profile	iFILTER-adp-req
Response Adapt Profile	None
Statistics Profile	None
VLAN and Tunnel Traffic	All VLANs and Tunnels
Source Address Translation	Auto Map

7. **iRules** にて作成済みの 2 つの iRule を選択して、*Finished* ボタンを押します。



Reject 用 Virtual Server の作成

- 最後に、**15080 ポート以外はブロック** をする Virtual Server を作成します。（本 Virtual Server がなくても動作はします。） **任意の名前** を入力し、**Type** にて **Reject** を選択し、**Destination Address/Mask** にて、**0.0.0.0/0** と入力し、**Service Port** にて ***** と入力します。**VLAN and Tunnel Traffic** にて、**Enabled on...** を選択し、**VLANs and Tunnels** にて作成済みの Tunnel を選択し、*Finished* ボタンを押します。

Local Traffic » Virtual Servers : Virtual Server List » **New Virtual Server...**

General Properties

Name	RejectProxy
Description	
Type	Reject
Source Address	
Destination Address/Mask	0.0.0.0/0
Service Port	* All Ports
Notify Status to Virtual Address	☒
State	Enabled

Configuration: Advanced

Protocol	TCP
WebSocket Profile	None
IMAP Profile	None
SplitSession Client Profile	None
SplitSession Server Profile	None
Statistics Profile	None
VLAN and Tunnel Traffic	Enabled on...
VLANs and Tunnels	Selected / Common L3ExplicitProxy-xp-tunnel Available / Common external http-tunnel icap internal

i-FILTER 側の設定

1. システム／システムパラメーター／機能設定 にて、仮想ホスト転送モード を有効にし、コンテンツ転送用アドレス に BIG-IP の FQDN を入力し、ポート番号 に 15080 を入力します。(IP アドレスを入力しても動作はしますが、SSL 接続時にブラウザでプライバシー保護のエラーが表示されます。)

システム / システムパラメーター / 機能設定 *

ログインユーザー: admin ログアウト

保存

言語設定	
システム言語	日本語

ICAPサーバー設定	
スレド数	400 警告閾値 80 %
プロセス数 (マルチプロセス)	1
仮想ホスト転送モード	☒ 有効にする
コンテンツ転送用 アドレス:ポート番号	bigip.f5jplab.local : 15080

2. システム／システムパラメーター／動作設定にて、コンテンツ転送、ブロック解除のそれぞれに任意の値を設定します。(ブロック画面タイトル表示時、パスワードブロック解除時のURIの一部として利用されます。)

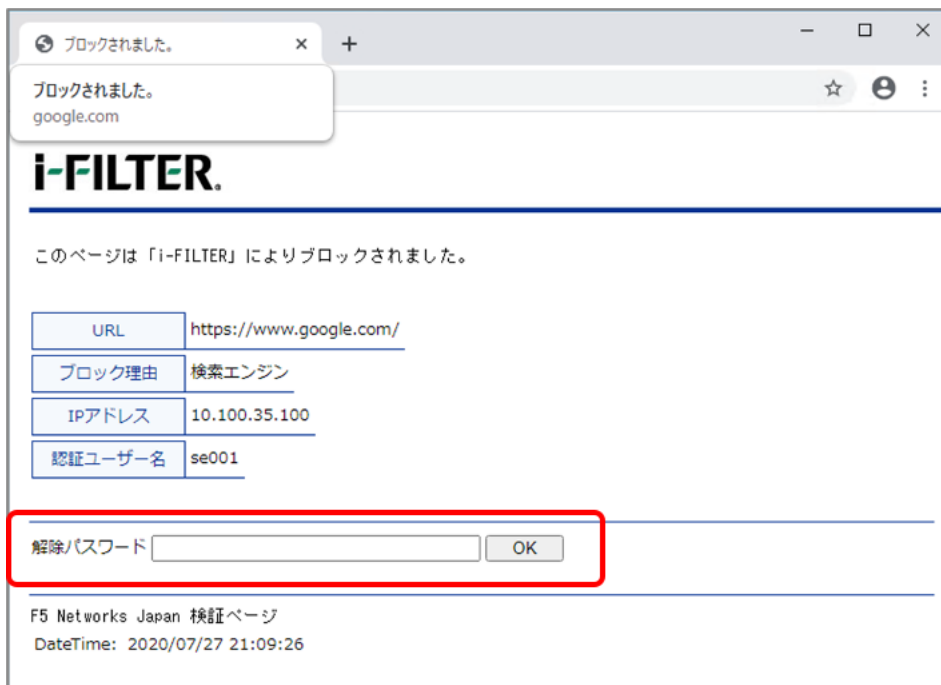
仮想ホスト名設定			
管理画面	inetnf.conf	127.0.0.1	/ 15081
コンテンツ転送	f5networks.cts		
ブロック解除	f5networks.msg		

クライアントからの接続テスト

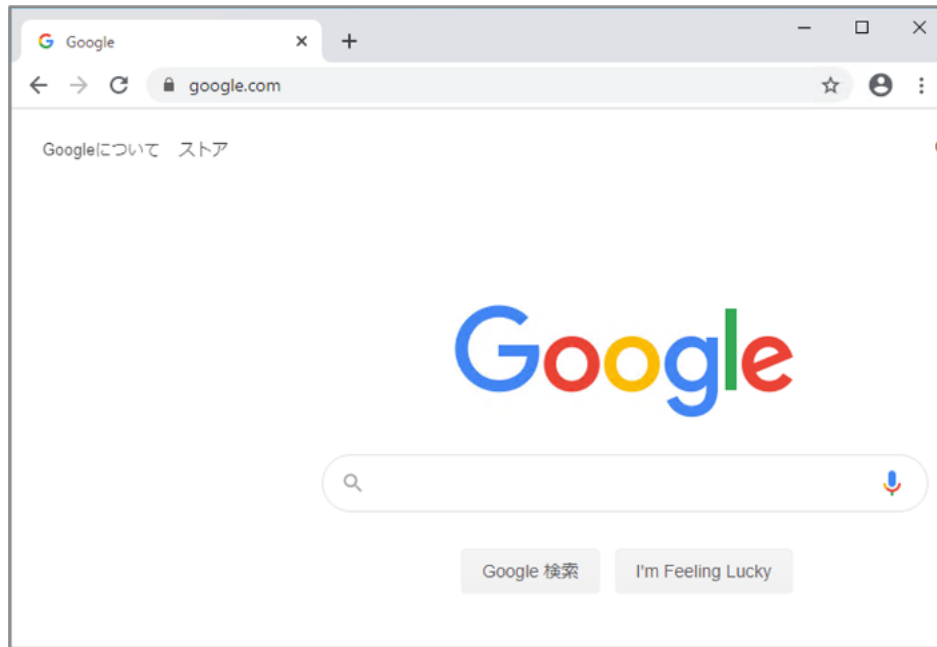
- ブラウザの **プロキシ設定** にて、作成済みの Explicit Proxy の IP アドレスに紐づく **FQDN** または、IP アドレスに変更します。
- ブラックリストの宛先への通信がブロックされ、タイトル画像が表示されることを確認します。



3. パスワードブロック解除が設定されている宛先へ接続し、パスワード入力画面が表示されることを確認します。



4. 解除パスワード入力後、無事 WEB 接続ができる事を確認します。



1.1.14 その他

各種ログ

1. テストの際には、以下の SSLO におけるログを参照して下さい。

- SSLO 全般ログや iRule で local0 で指定したログ /var/log/ltm
- APM（認証）のログ /var/log/apm
- SSL Guided Configuration (iAppLX/REST) に関わるログ /var/log/restnoded/restnoded.log
/var/log/restjava.0.log
- その他、SSLO に関するトラブルシューティングは以下の AskF5 記事をご参照下さい。
K26520133: Troubleshooting SSL Orchestrator(SSLO) <https://support.f5.com/csp/article/K26520133>

2. テストの際には、以下の i-FILTER におけるログを参照して下さい。

- アクセスログ /usr/local/ifilter10/logs/access.log0000

フィルター除外設定（必須ではありません）

1. 本テストでは、httpbin.org を接続先ホストとして利用させて頂いておりますが、現状デフォルトではブロックされるので、**システム／システムフィルター／推奨フィルター設定 – 除外設定**にて、テストで利用しているホスト名を **除外設定** に追加します。

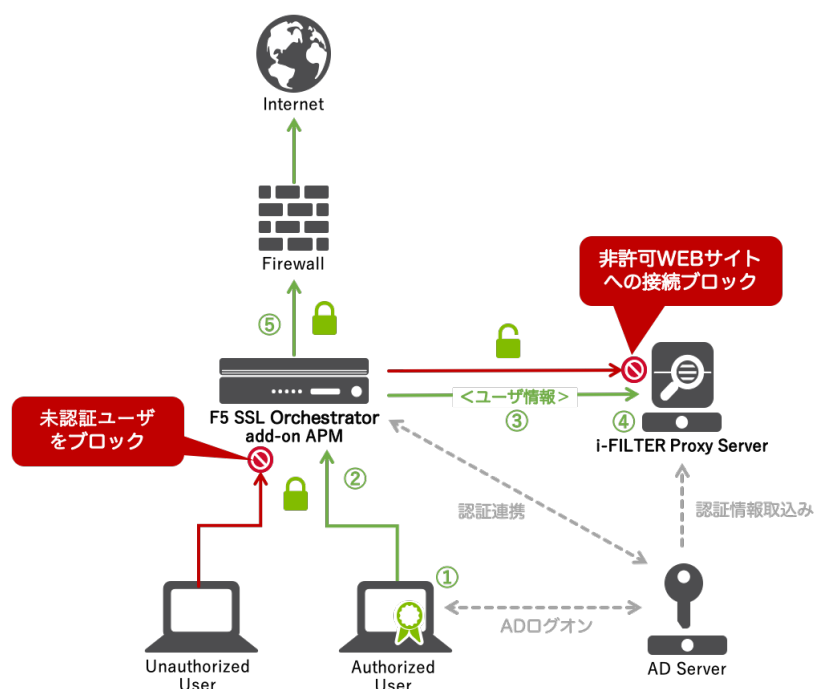
1.2 F5 SSLO (L3 Explicit Proxy) と i-FILTER Proxy 版の連携設定

本章では、SSLO の可視化ゾーンに i-FILTER Proxy 版を配置して連携する構成について、ご紹介致します。

1.2.1 F5 SSLO と i-FILTER PROXY 版連携の流れ

F5 SSLO と i-FILTER PROXY 版の連携の流れは以下の通りです。

1. クライアントがパソコン (AD) にログオンします。



2. SSLO でユーザ認証を実施し (NTLM 認証、Kerberos 認証の場合は自動的に認証が実施されます)、SSL 通信を復号します。
3. WEB 接続の情報と SSLO で認証が成功したユーザ情報を i-FILTER に HTTP で送ります。
4. ユーザ情報を元に URL フィルタリングルールを適用し、接続が許可されていない WEB サイトの場合は、ブロック画面をクライアントに表示します。
5. 許可された通信に関しては、SSL 通信を再暗号化し、WEB サーバへ接続します。

1.2.2 本ガイドの利用バージョンと構成イメージ

本ガイドは、以下の製品バージョンを利用して、作成しております。

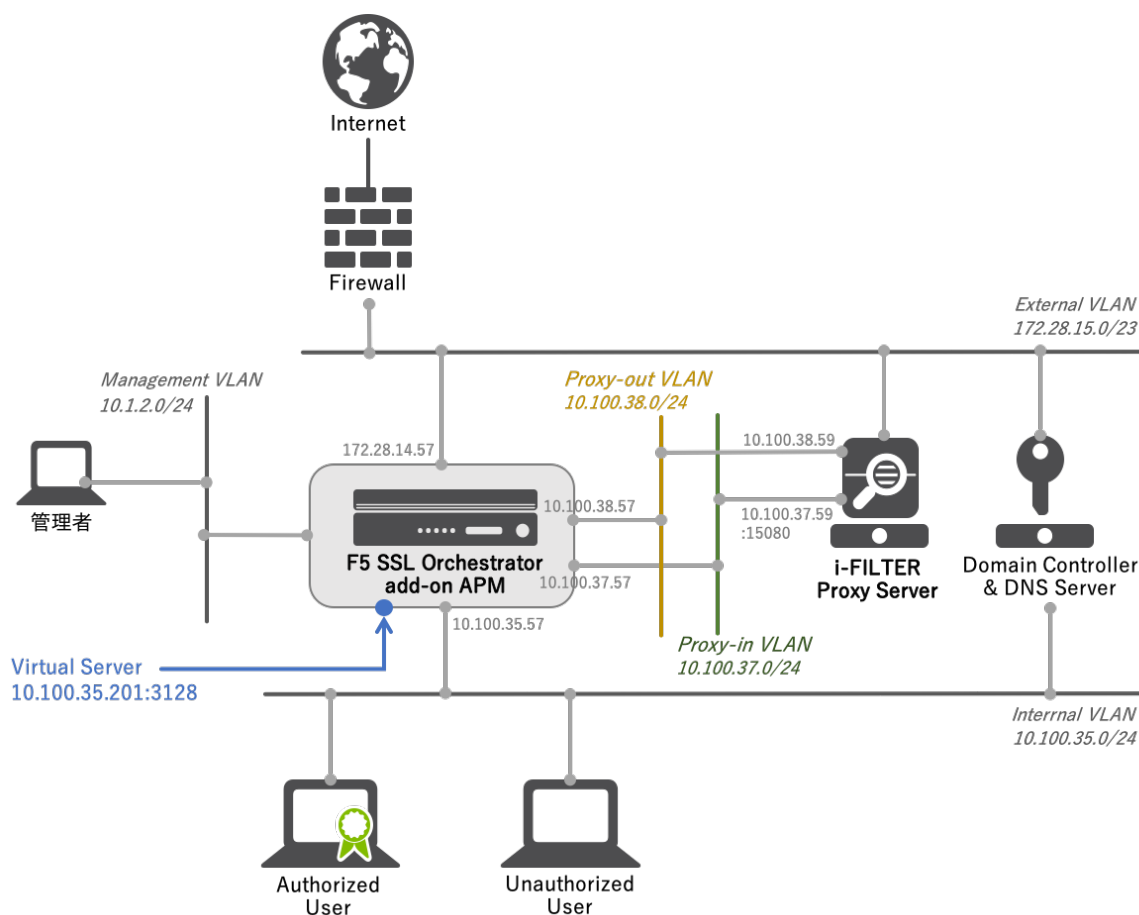
1. 利用バージョン

製品名	バージョン
F5 SSL Orchestrator	v15.1.0.5-0.0.8 ~ 7.4.9
i-FILTER Proxy Server (Linux)	Ver.10.41R01-20200807 (CentOS v7.7.1908 ※) ※ デジタルアーツ様による製品サポート OS は Red Hat Enterprise Linux となります。

注釈:

- (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、i-FILTER のログにユーザ名を出力したい場合は、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



1.2.3 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

1- 1.3 と同じです。

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

1- 1. 4 と同じです。

1.2.5 Network の基本設定

1. VLAN の設定を行います。

Network » VLANs : VLAN List

VLAN List | VLAN Groups

* Search Create...

☒	Name	Application	Tag	Untagged Interfaces	Tagged Interfaces	Partition / Path
☐	external		4094	1.1		Common
☐	internal		4093	1.2		Common

Delete...

2. Self IP の設定を行います。

Network » Self IPs

Self IP List

* Search Create...

☒	Name	Application	IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
☐	external-self		172.28.14.57	255.255.254.0	external	traffic-group-local-only	Common
☐	internal-self		10.100.35.57	255.255.255.0	internal	traffic-group-local-only	Common

Delete...

3. デフォルトゲートウェイの設定を行います。

Network » Routes

Route List

Add...

☒	Name	Application	Destination	Netmask	Route Domain	Resource Type	Resource	Partition / Path
☐	default-gw		Default IPv4		Partition Default Route Domain	Gateway	172.28.15.254	Common

Delete...

1.2.6 DNS, NTP の設定

1- 1.6 と同じです。

1.2.7 i-FILTER にて HTTP/HTTPS 判別するための iRule の作成

i-FILTER PROXY 版は、HTTP のリクエストヘッダで HTTP サーバへの通信か HTTPS サーバへの通信かを判別しています。i-FILTER が HTTP/HTTPS 判別可能となるための iRule を作成します。**X-Forwarded-Proto** というヘッダーに利用プロトコル (http or https) を加えて、HTTP リクエストに挿入します。ここではあわせて、クライアントの IP アドレスも **X-Forwarded-For** に挿入しています。

1. **Local Traffic >> iRules** にて、**Create** ボタンを押します。**任意の名前** を入力して、**Definition** に以下サンプル iRule を入力し、**Finished** ボタンを押します。(以下の iRule はあくまでもサンプルとなります。同じ主旨の内容であれば下記と同じでなくても構いません。)

例) HTTP リクエストに i-FILTER 連携のヘッダを挿入するための iRule サンプル

```
### Add this iRule to Virtual Server:ssloS_XXXX-t-4 ###

when HTTP_REQUEST {

    if { [TCP::local_port] == 80 } {
        # For HTTP protocol
        HTTP::header replace "X-Forwarded-Proto" "http"

    } elseif { [TCP::local_port] == 443 } {
        # For HTTPS protocol
        HTTP::header replace "X-Forwarded-Proto" "https"
    }

    sharedvar ctx
    # For Client IP address
    lappend ctx(headers) "X-Forwarded-For" [IP::client_addr]

    if { [expr { [llength $ctx(headers)] % 2 }] == 0 } {
        foreach {h_name h_value} $ctx(headers) {
            HTTP::header replace ${h_name} ${h_value}
        }
    }
}
```

接続テストをされる際には、変数情報をログ出力するなどして意図する値が入っているか確かめて頂くことをおすすめします。

例1) ヘッダー内容を確認するデバッグ

```
foreach attr "[HTTP::header names]" {
    log local0. "$attr : [HTTP::header value $attr]"
}
```

1.2.8 NTLM 認証設定

1- 1.8 と同じです。

1.2.9 認証ヘッダ挿入用 iRule の作成

ここでは、ユーザ認証ヘッダ (Proxy-Authorization) と APM で認証されたユーザ名 (session.logon.last.username) を HTTP リクエストに挿入するための iRule を作成します。i-FILTER PROXY 版連携では、**Proxy-Authorization** というヘッダー名に、ユーザ名を Base64 エンコーディングした Basic 認証の形式で挿入します。

1. **Local Traffic >> iRules** にて、2- 2.7 で作成済みの iRule にユーザ名用のヘッダーを挿入するための箇所を追記します。(以下の iRule はあくまでもサンプルとなります。同じ主旨の内容であれば下記と同じでなくても構いません。)

例) HTTP リクエストに i-FILTER 連携のヘッダを挿入するための iRule サンプル

```
### Add this iRule to Virtual Server:ssloS_XXXX-t-4 ###

when HTTP_REQUEST {

    if { [TCP::local_port] == 80 } {
        # For HTTP protocol
        HTTP::header replace "X-Forwarded-Proto" "http"

    } elseif { [TCP::local_port] == 443 } {
        # For HTTPS protocol
        HTTP::header replace "X-Forwarded-Proto" "https"
    }

    sharedvar ctx
    # For Client IP address
    lappend ctx(headers) "X-Forwarded-For" [IP::client_addr]

    # For Username
    if { [ACCESS::session data get session.logon.last.username] ne "" } {
        set PROXYAUTH "Basic [b64encode [ACCESS::session data get session.
        ↪logon.last.username]:]"
    }
}
```

(次のページに続く)

(前のページからの続き)

```

    } else {
        set PROXYAUTH ""
    }
    lappend ctx(headers) "Proxy-Authorization" $PROXYAUTH

    if { [expr { [llength $ctx(headers)] % 2 }] == 0 } {
        foreach {h_name h_value} $ctx(headers) {
            HTTP::header replace ${h_name} ${h_value}
        }
    }
}

```

接続テストをされる際には、変数情報をログ出力するなどして意図する値が入っているか確かめて頂くことをおすすめします。

例1) 認証ユーザ名を確認するデバッグ

```
log local0. "Username: [ACCESS::session data get session.logon.last.username]"
```

例2) エンコードされた内容を確認するデバッグ

```
log local0. "Encoded username: b64encode [ACCESS::session data get session.logon.last.username]"
```

例3) ヘッダー内容を確認するデバッグ

```
foreach attr "[HTTP::header names]" {
    log local0. "$attr : [HTTP::header value $attr]"
}

```

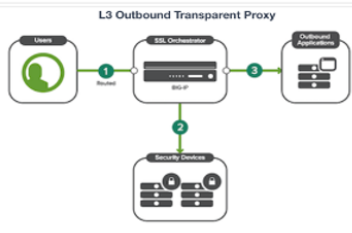
1.2.10 SSLO Guided Configuration による SSLO の設定

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。

SSL Orchestrator Configuration

This guided configuration will allow you to quickly setup the SSL Orchestrator Configuration.

Configuration Options



L3 Outbound Transparent Proxy
An Outbound topology can be used to provide internal user access to external remote resources when the organization does not own the application resources and SSL keys.
1. The internal traffic takes a routed path into and out of the BIG-IP. The client is unaware of the SSL Orchestrator device while en route to the server.
2. The traffic is decrypted and is sent to security devices.
3. Then the traffic is re-encrypted and is routed out to the applications and Internet.

Configuring the following solution will guide you through creating the following objects:

- Topology**
Select the type of deployments you require and build on your configuration.
- SSL Configurations**
Configure your certificate chains for encrypting and decrypting packets.
- Services**
Define the security services to attach to SSL Orchestrator.
- Service Chaining**
Determine the flow of data through your network services.
- Security Policy**
Configure the traffic filtering and categorization to securely manage traffic.
- Interception Rules**
Create the rules for routing traffic.
- Egress Setting**
Manage SNAT Settings and configure Gateways.
- Log Settings**
Manage Log Settings.

Cancel **Next**

System Settings | Version: 7.4.9

Required Configuration
Before you start this guided configuration, make sure that DNS, NTP and Routes are configured.

- ☒ DNS Configured
- ☒ NTP Configured
- ☒ Route Configured

Documentation
[Ask a question on F5 Support](#)

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. L3ExplicitProxy

Description
In the topology Name field, type a name after the default prefix sslo.
Provide a description for this deployment.

Protocol
TCP

IP Family
IPv4

SSL Orchestrator Topologies

L2 Outbound L3 Outbound L3 Explicit Proxy L2 Inbound L3 Inbound Existing Application

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

Cancel Save Draft Save & Next

3. 任意の名前を設定し、右上の *Show Advanced Setting* をクリックし、**Client-side SSL** にて、利用したい **TLS** のバージョンを選択します。

SSL Orchestrator » Configuration

SSL Orchestrator Configuration : sso, L3ExplicitProxy NOT DEPLOYED

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

SSL Configurations

Hide Advanced Setting

SSL Profile ⓘ

☒ Create New ☐ Use Existing

Name

ssoT_ L3ExplicitProxy

In the SSL configurations Name field, type a name after the default prefix ssoT_.

Description

Provide a description for the SSL configuration.

Client-side SSL

Processing Options ⓘ

Enabled Options

Filter

SSLv3

TLS

TLSv1

TLSv1.1

Disabled Options

4. CA Certificate KeyChain にて、既にインポート済みの CA ファイルを選択して *Done* を押します。

CA Certificate Key Chain ⓘ

CA Certificate Key Chains

Certificate

/Common/f5jplabCA

Key

/Common/f5jplabCA

Chain

--Select--

Passphrase

Cancel Done

5. **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

Filter

- SSLv3
- TLS
- TLSv1
- TLSv1.1

Disabled Options

6. 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。

Cipher

/Common/f5-default

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

Trusted Certificate Authority ⓘ

/Common/ca-bundle.crt

Expire Certificate Response ⓘ

drop

Untrusted Certificate Authority ⓘ

drop

OCSP ⓘ

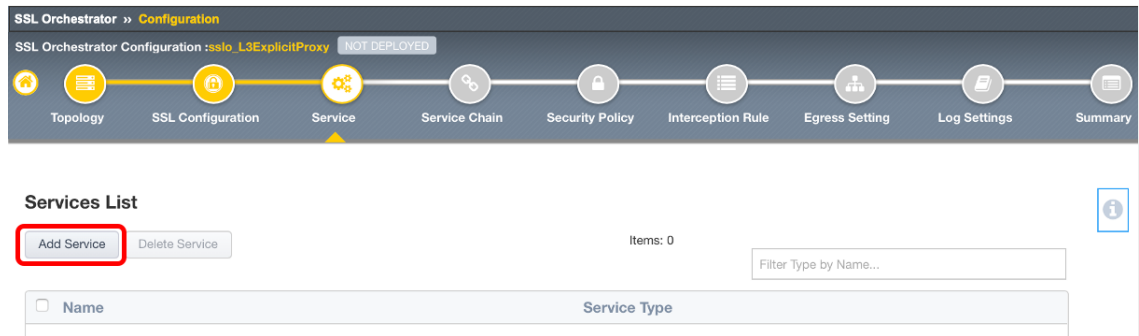
--Select--

CRL ⓘ

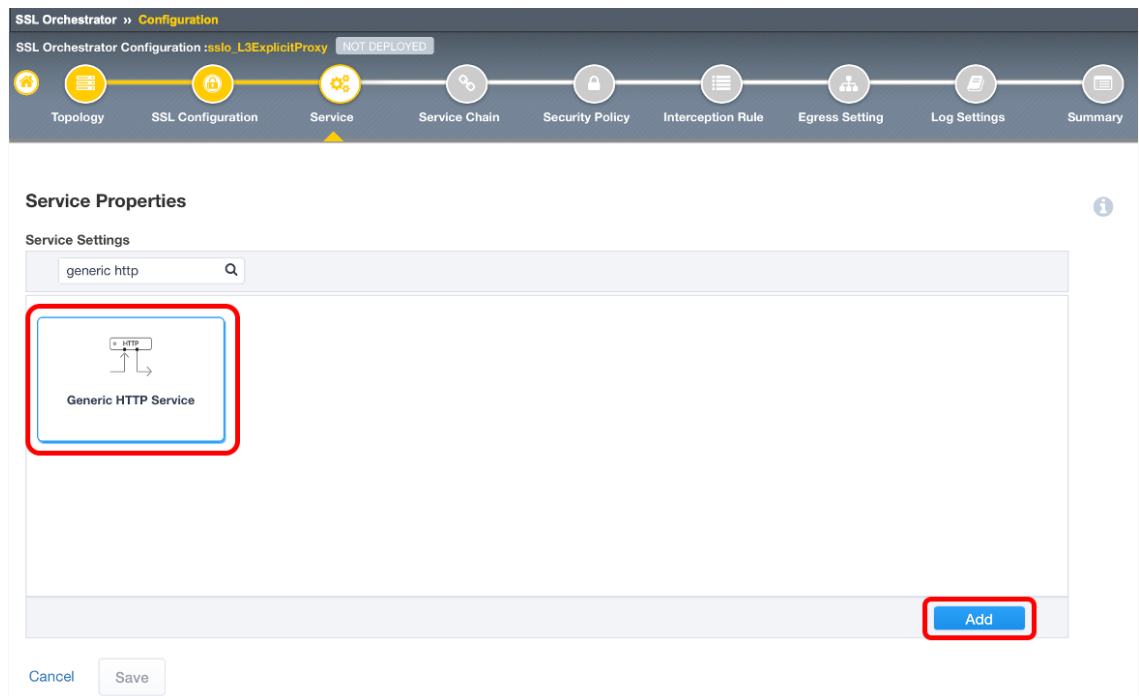
--Select--

Cancel Save Draft Back **Save & Next**

7. **Add Service** を押します。



8. **Generic HTTP Service** を選択し、**Add** ボタンを押します。



9. **任意の名前** を設定します。

The screenshot shows the 'SSL Orchestrator » Configuration' page. At the top, a progress bar indicates the current step is 'Service' (highlighted with a yellow circle and gear icon), with other steps like 'Topology', 'SSL Configuration', 'Service Chain', 'Security Policy', 'Interception Rule', 'Egress Setting', 'Log Settings', and 'Summary' shown as greyed-out icons. Below the progress bar, the 'Service Properties' section is active. It includes a 'Service Settings' box with a 'Generic HTTP Service' icon. Below this, the 'Name' field contains 'sslo_iFILTERProxy' (the 'iFILTERProxy' part is highlighted with a red box). A small note below the name field states: 'In the HTTP service settings Name field, type a name after the default prefix ssloS_'. The 'Description' field contains 'Type: http-proxy'. Below the description, the 'IP Family' dropdown is set to 'ipv4'.

SSL Orchestrator » Configuration

SSL Orchestrator Configuration : sslo_L3ExplicitProxy NOT DEPLOYED

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

Service Properties

Service Settings

Generic HTTP Service

Name

sslo_iFILTERProxy

In the HTTP service settings Name field, type a name after the default prefix ssloS_.

Description

Type: http-proxy

Type a description for this service.

IP Family

ipv4

10. **Service Definition** にて、**Auto Manage Addresses** のチェックをはずし、SSLO から i-FILTER Proxy へ HTTP トラフィックを転送する VLAN, Self IP の情報を入力します。（ここでは、検証環境の都合で Auto Manage Addresses は利用していません。）

Service Definition

☐ Auto Manage Addresses ⓘ

⚠ We recommend that you do not disable auto manage. Any traffic passed outside SSL managed control might face security vulnerabilities.

Proxy Type

Explicit ▼

Specify whether you want the system to operate in transparent proxy mode or explicit proxy mode.

To Service Configuration ⓘ

☐ Use Existing ☒ Create New

Name

ssl0N_ Proxy_in

In the From Network Self IP Name field, type a name for the self IP.

VLAN

☐ Use Existing ☒ Create New

Interface

1.3 ▼

Select the associated BIG-IP system interface.

Tag

Network Settings

Self IP

10.100.37.57

Specifies the self IP address definition address. This can be either an IPv4 or an IPv6 address.

Netmask ⓘ

255.255.255.0

Route Domain ⓘ

☒ Use Route Domain 0 ☐ Create New

注釈:

- SSL 可視化ゾーン（ここでは i-FILTER Proxy 版）では、HTTP トラフィックは暗号化されておりませんので、第三者からのアクセスを避ける必要があります。そこで、SSLO では、Auto Manage Addresses（RFC2544 に定められているインターナル利用アドレス）をセキュリティ機器に利用頂くことを推奨しております。

11. i-FILTER Proxy のインライン側の **IP アドレス** と **ポート番号** を入力し、*Done* を押します。

Service Down Action ⓘ
Ignore ▼

Security Devices ⓘ

HTTP Proxy Devices

IP Address ⓘ
10.100.37.59

Port
15080

Cancel Done

No HTTP Proxy Devices Added

Device Monitor ⓘ
/Common/gateway_icmp ▼

12. i-FILTER Proxy から SSLO へ HTTP トラフィックを転送する VLAN, Self IP の情報を入力します。

From Service Configuration ⓘ

☐ Use Existing ☒ Create New

Name

ssl0N_ Proxy_out

In the To Network Self IP Name field, type a name for the self IP.

VLAN

☐ Use Existing ☒ Create New

Interface

1.4

Select the associated BIG-IP system interface.

Tag

Network Settings

Self IP

10.100.38.57

Specifies the self IP address definition address. This can be either an IPv4 or an IPv6 address.

Netmask ⓘ

255.255.255.0

Route Domain ⓘ

☒ Use Route Domain 0 ☐ Create New

13. 検証環境では **Auto Map** を設定し、作成済みの iRule を右に移動させ、*Save* を押します。

Manage SNAT Settings ⓘ

Auto Map ▾

☐ Authentication Offload ⓘ

Resources

iRules ⓘ

Available		Selected
Filter ▾	◀ ▶ ↑ ↓	/Common/Insert_iFILTERheader
No available items		

Cancel Save

14. Service が追加されるとこのような画面になります。Save & Next を押します。

SSL Orchestrator >> Configuration

SSL Orchestrator Configuration : sslo_L3ExplicitProxy NOT DEPLOYED

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

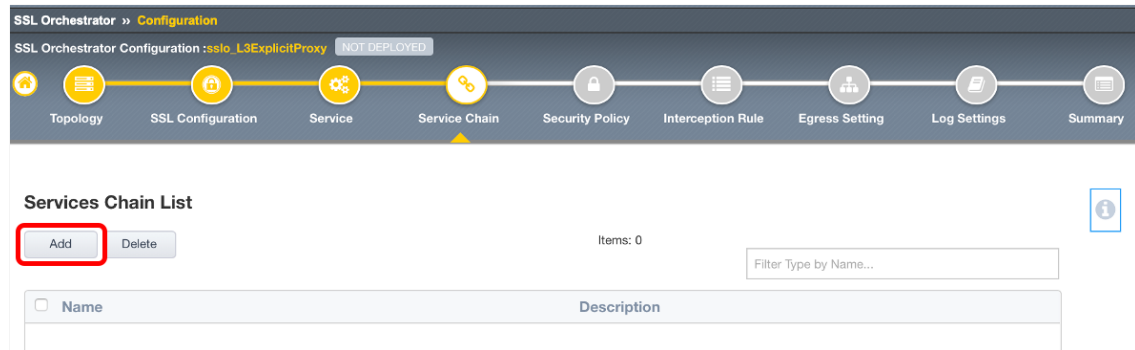
Services List ⓘ

Add Service Delete Service Items: 1 Filter Type by Name...

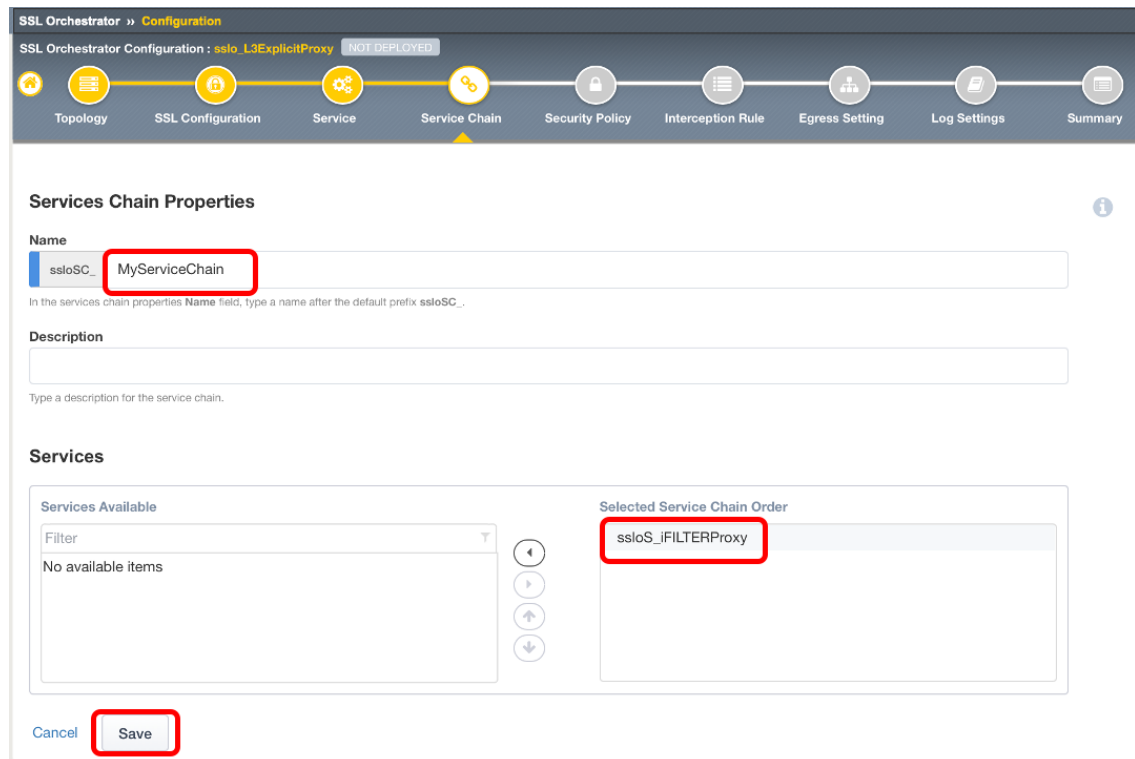
Name	Service Type
☐ ssloS_iFILTERProxy NOT DEPLOYED	HTTP

Cancel Save Draft Back Save & Next

15. **Add** をクリックし、サービスチェーンを作成します。



16. **任意の名前** を設定し、作成済みの Service を右に移動させ、**Save** ボタンを押します。



17. サービスチェーンが作成されると、このような画面になります。 *Save & Next* ボタンを押します。

SSL Orchestrator » Configuration

SSL Orchestrator Configuration :sslo_L3ExplicitProxy NOT DEPLOYED

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

Services Chain List

Add Delete Items: 1 Filter Type by Name...

Name	Description
ssloSC_MyServiceChain NOT DEPLOYED	

Cancel Save Draft Back **Save & Next**

18. All Traffic の **ペンマーク** をクリックします。

SSL Orchestrator » Configuration

SSL Orchestrator Configuration :sslo_L3ExplicitProxy 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_L3ExplicitProxy

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

Description

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	-

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

The screenshot shows the 'Rules' configuration page. A table lists rules, with 'Pinners_Rule' selected. Below the table, the 'Service Chain' dropdown is open, showing 'None' and 'ssloSC_MyServiceChain'. The 'OK' button is highlighted with a red box.

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

Below the table, the 'Service Chain' dropdown is open, showing 'None' and 'ssloSC_MyServiceChain'. The 'OK' button is highlighted with a red box.

20. All Traffic に Service Chain が追加されると以下のような画面になります。

The screenshot shows the 'Rules' configuration page after adding a new rule. The table now includes 'All Traffic' with 'All' as the condition, 'Allow' as the action, and 'ssloSC_MyServiceChain' as the Service Chain. The 'ssloSC_MyServiceChain' dropdown is highlighted with a red box.

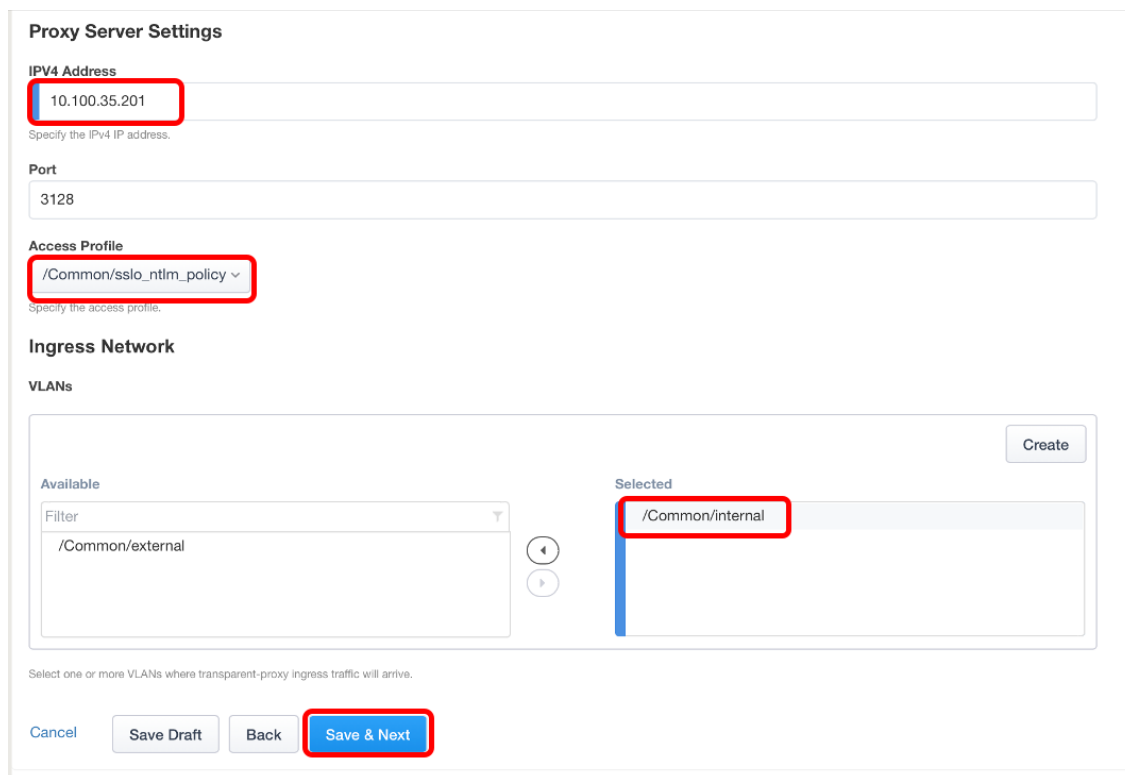
Name	Conditions	Action	SSL Forward Proxy Action	Service Chain
Pinners_Rule	SSL Check is true and Category Lookup (SNI) is Pinners	Allow	Bypass	-
All Traffic	All	Allow	Intercept	ssloSC_MyServiceChain

21. **Save & Next** ボタンを押します。

The screenshot shows the bottom of the configuration page with the 'Save & Next' button highlighted with a red box.

Buttons: Cancel, Save Draft, Back, **Save & Next**

22. 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 アドレスを入力し、既に作成済みの Access Profile を選択し（プロキシ認証しない場合は不要）、Ingress Network として、クライアントからアクセス可能な VLAN を選択し、**Save & Next** ボタンを押します。



The image shows the 'Proxy Server Settings' configuration form. The 'IPv4 Address' field contains '10.100.35.201'. The 'Port' field contains '3128'. The 'Access Profile' dropdown is set to '/Common/ssl0_ntlm_policy'. Under 'Ingress Network', the 'Available' list contains '/Common/external' and the 'Selected' list contains '/Common/internal'. At the bottom, the 'Save & Next' button is highlighted.

Proxy Server Settings

IPv4 Address
10.100.35.201
Specify the IPv4 IP address.

Port
3128

Access Profile
/Common/ssl0_ntlm_policy
Specify the access profile.

Ingress Network

VLANs

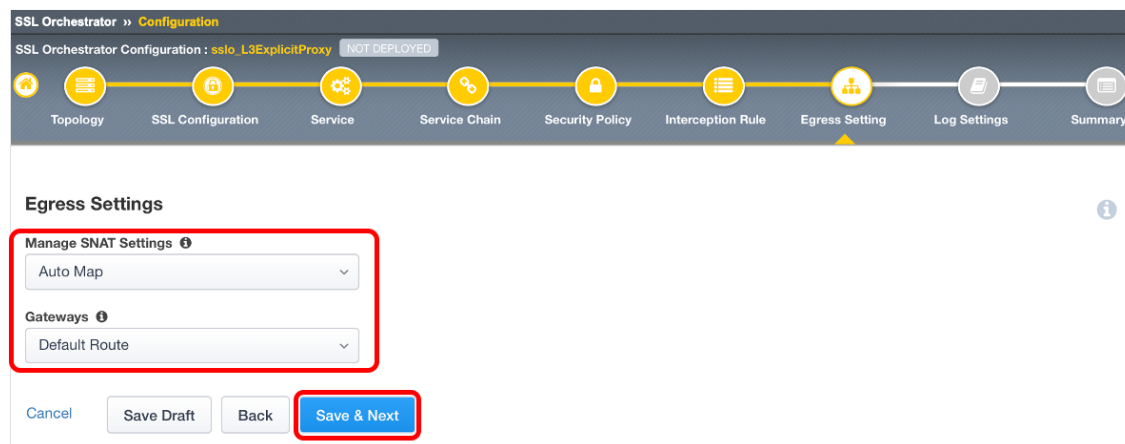
Available
Filter
/Common/external

Selected
/Common/internal

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

Cancel Save Draft Back **Save & Next**

23. 本テスト構成では、Manage SNAT Settings で Auto Map、Gateways で Default Route を選択し、**Save & Next** ボタンを押します。（設定は検証環境に合わせてください。）



The image shows the 'Egress Settings' configuration form. The 'Manage SNAT Settings' dropdown is set to 'Auto Map' and the 'Gateways' dropdown is set to 'Default Route'. At the bottom, the 'Save & Next' button is highlighted.

SSL Orchestrator » Configuration

SSL Orchestrator Configuration : ssl0_L3ExplicitProxy NOT DEPLOYED

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

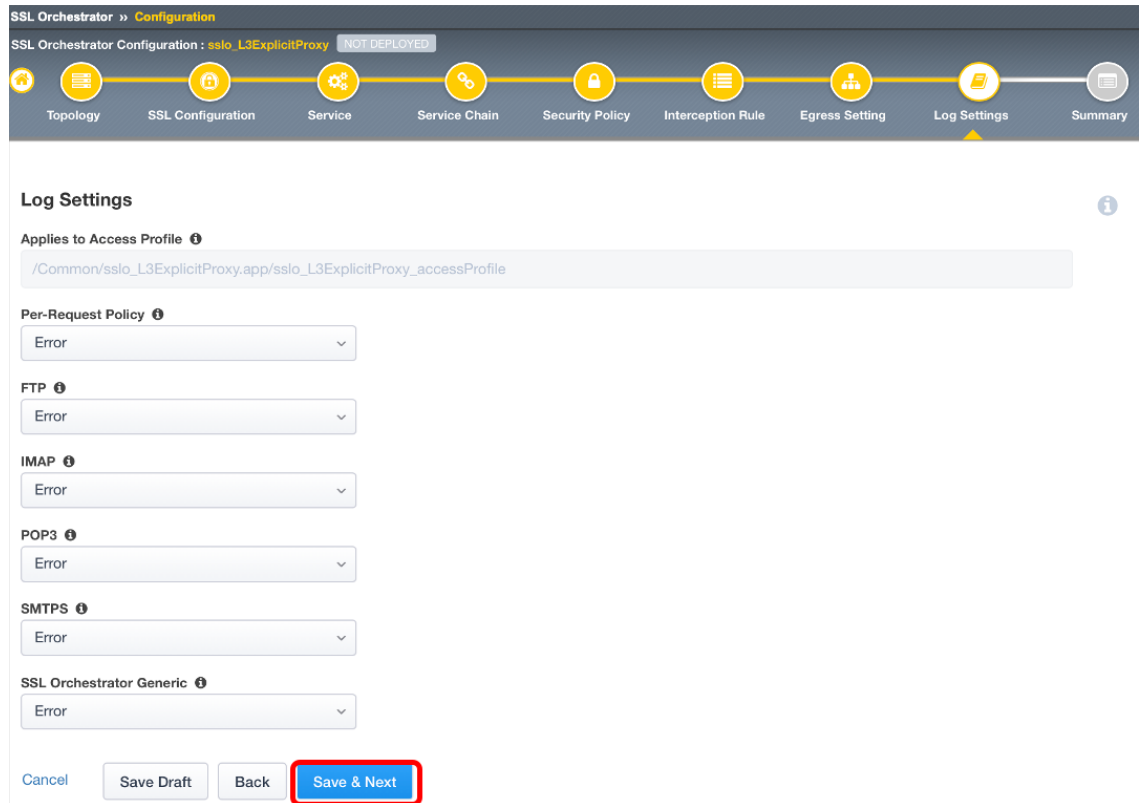
Egress Settings

Manage SNAT Settings
Auto Map

Gateways
Default Route

Cancel Save Draft Back **Save & Next**

24. *Save & Next* ボタンを押します。



SSL Orchestrator » Configuration

SSL Orchestrator Configuration : ssl_L3ExplicitProxy NOT DEPLOYED

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

Log Settings

Applies to Access Profile ⓘ

/Common/ssl_L3ExplicitProxy.app/ssl_L3ExplicitProxy_accessProfile

Per-Request Policy ⓘ

Error

FTP ⓘ

Error

IMAP ⓘ

Error

POP3 ⓘ

Error

SMTPS ⓘ

Error

SSL Orchestrator Generic ⓘ

Error

Cancel Save Draft Back **Save & Next**

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

SSL Orchestrator » Configuration

SSL Orchestrator Configuration : ssls_L3ExplicitProxy NOT DEPLOYED

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

Summary

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

Cancel Save Draft Back **Deploy**

26. OK ボタンを押し、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。

SSL Orchestrator » Configuration

Configure Dashboard Version: 7.4.9

Client Encrypted Traffic Servers

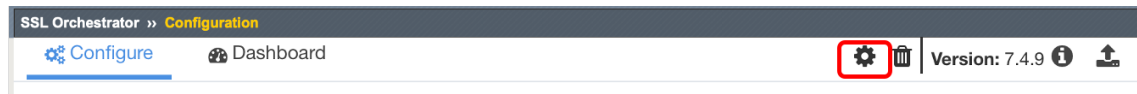
sslo_iFILTERProxy

Topologies Interception Rules Services Service Chains Security Policies SSL Configurations

Add Delete Items: 1

Name	Type	Security Policy	SSL Configuration	Protected/Unprotected
ssls_L3ExplicitProxy DEPLOYED	L3 Explicit Proxy	sslsP_L3ExplicitProxy	sslsT_L3ExplicitProxy	Protected

27. 右上の **System Settings** アイコンを選択します。



28. SSLO が Explicit Proxy として利用する **DNS** を設定し、*Deploy* を押します。

System Settings

IP Family ⓘ
IPv4

DNS Settings

DNS Query resolution ⓘ
Local Forwarding Nameserver

Local Forwarding NameServer(s)
Local DNS Nameserver*

10.100.35.156

☐ DNSSec Validation ⓘ

Gateways Configuration

Gateways ⓘ
Default Route

Cancel Deploy

注釈:

- 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。

1.2.11 i-FILTER Proxy 版 (Linux 版) の設定

i-FILTER のインストールは終了しているものとします。

注釈:

- SSL 可視化ゾーン（ここでは i-FILTER Proxy 版）では、HTTP トラフィックは暗号化されておりませんので、第三者からのアクセスを避ける必要があります。そこで、SSLO では、Auto Manage Addresses（RFC2544 に定められているインターナル用アドレス、198.19.x.y/19）をセキュリティ機器に利用頂くことを推奨しております。
- 上記推奨設定を採用できる場合、i-FILTER 用のサーバ構築時にこのアドレス帯を割り当てて下さい。

SSLO 連携の設定

1. conf/ifilter.conf に以下のパラメータを追加します。

```
proxy_header_rewrite_protocol_enable = on
```

ユーザ認証の設定

1. システム／ユーザ認証／基本設定 を選択します。
2. 基本設定 の ユーザ認証方式 において SNOOP 認証 を選択します。

The screenshot shows the i-FILTER web management interface. At the top, there's a navigation bar with tabs like 'グループ', '共通', 'ルールセット', 'ログ', 'システム', and 'オプション'. Below this, the breadcrumb path is 'システム / ユーザー認証 / 基本設定 *'. The main content area is titled '基本設定' and contains a table of settings. The 'ユーザー認証方式' (User Authentication Method) is set to 'SNOOP認証' (SNOOP authentication), which is highlighted with a red rectangle. Other settings include '認証ダイアログ表示名' (Authentication Dialog Display Name) set to 'inetnf.proxy', 'Keep-Alive時の動作' (Keep-Alive Action) with a checked box for 'Keep-Alive中は再認証しない' (Do not re-authenticate during Keep-Alive), 'LDAPv3ページコントロール' (LDAPv3 Page Control) with a checked box for '有効にする' (Enable), and '認証失敗時ユーザー名出力' (Authentication Failure User Name Output) with a checked box for '有効にする' (Enable). A '保存' (Save) button is visible at the top right of the settings area.

3. ICAP 認証設定 の SNOOP 認証ユーザ参照 において、**有効にする** をチェックします。

SNOOP認証設定	
SNOOP認証ユーザ参照	☒ 有効にする
Cache Time to Live	7200 秒

4. 右上の **保存** ボタンを押します。

i-FILTER	
グループ ▾ 共通 ▾ ルールセット ▾ ログ ▾ システム ▾ オプション ▾ ⓘ ↺	
システム / ユーザ認証 / 基本設定 *	
ログインユーザー: admin ログアウト ?	
保存	

5. 次に、**システム／ユーザ認証／LDAP サーバ設定** を選択します。本ガイドでは認証ユーザ情報を AD サーバから取り込むため、以下のように設定し、**保存** ボタンを押します。

LDAPサーバー設定	
アドレス : ポート番号	172.28.14.56 : 389
サーバー状態	☒ 利用 ☐ 待機 ☐ 無効 振り分け比率 1
LDAPバージョン	3
BIND	BIND有効
BIND DN	cn=Administrator,cn=Users,dc=f5jplab,dc=local
BINDパスワード	☐ パスワードを更新する (※現在、パスワードが設定されています) 新パスワード 新パスワード(確認)
Search Base	dc=f5jplab,dc=local
Search Filter	(sAMAccountName=%1)
Search Group	(!(objectclass=organizationalunit)(objectclass=groupofuniqueNames)(objectclass=groupc
Search User	(!(objectclass=person)(objectclass=account))
BINDタイムアウト	60 秒 Searchタイムアウト 60 秒

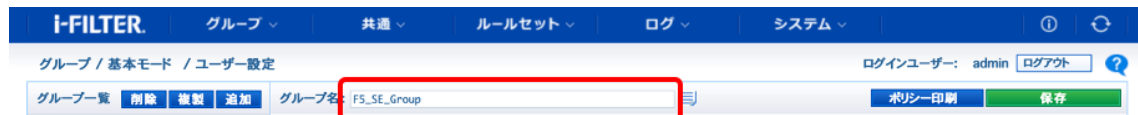
項目	設定例
アドレス:ポート番号	ご利用の AD 情報を登録
BIND	BIND 有効
BIND DN	ご利用の管理者 BIND DN 情報を登録 設定例 : cn=Administrator,cn=Users,dc=f5jplab,dc=local
BIND パスワード	ご利用のドメイン管理者のパスワードを登録
Search Base	ご利用のドメイン情報を登録 設定例 : dc=f5jplab,dc=local
Search Filter	(sAMAccountName=%1)

グループポリシーの作成、ユーザ情報の取り込み

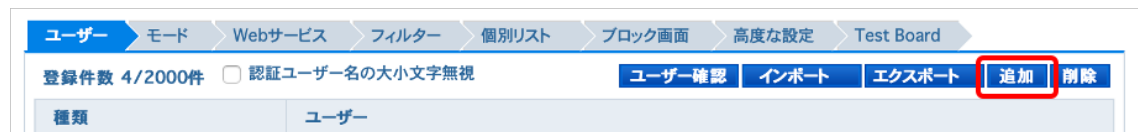
1. グループ／基本モード／モード設定 において、追加 ボタンを押します。



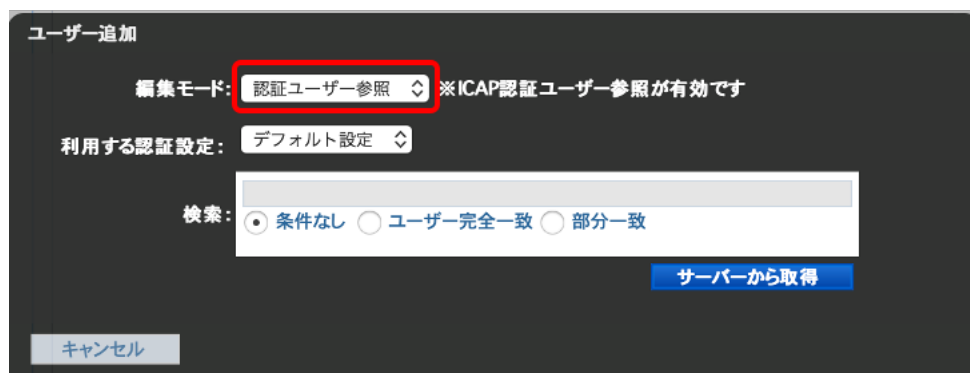
2. **グループ名** を分かりやすいグループ名に変更します。



3. **ユーザ** タブにおいて、**追加** ボタンをクリックします。



4. **認証ユーザ参照** を選択します。



5. 検索しやすい検索条件を設定し、AD から取り込みたい **ユーザ名** を追加します。

The screenshot shows the 'ユーザー追加' (Add User) dialog box. At the top, it says '編集モード: 認証ユーザー参照' and '※ICAP認証ユーザー参照が有効です'. Below that, '利用する認証設定: デフォルト設定'. The search input field contains 'f5 se'. The search criteria are set to '部分一致' (Partial Match). A button 'サーバーから取得' (Get from Server) is visible. Below the search field, it says 'ユーザー検索結果 [3] 件' (User search results [3] items). The results list shows three entries: 'CN=f5 se001,OU=SeDepartment,DC=f5jplab,DC=local', 'CN=f5 se002,OU=SeDepartment,DC=f5jplab,DC=local', and 'CN=f5 se003,OU=SeDepartment,DC=f5jplab,DC=local'. At the bottom right is a blue '追加' (Add) button, and at the bottom left is a grey 'キャンセル' (Cancel) button.

6. **Web サービス** タブを選択し、制御したいサービスを選択し、ユーザに利用不許可とする機能に対し、**ブロック** を選択します。(注：下記イメージはあくまでも一例です。)

グループ名: F5_SE_Group ポリシー印刷 保存

有効期間 開始日 2020/04/19 終了日 2020/05/31 clear: CTL+End

ユーザー モード **Webサービス** フィルター 個別リスト ブロック画面 高度な設定 Test Board

一括設定: リスク (未選択) アクション (未選択) プリセット 追加 削除

サービス名	有効	機能名	アクション	許可カテゴリ名	リスク
☐ Facebook	☒	Facebook 閲覧	許可	SNS/動画配信/Web翻訳・URL変換	1
		Facebook ログイン	許可	SNS	2
		Facebook 投稿	ブロック	SNS/動画配信/アップローダー	2
		Facebook メッセージ送信	ブロック	SNS	2
		Facebook ファイルアップロード	ブロック	アップローダー/SNS/動画配信	3
		Facebook 連携アプリ認証 (OAuth認証)	許可	SNS	3
		Facebook アプリセンター	ブロック	総合ソフトウェアダウンロード/SNS/ゲーム	2
		Messenger messenger.com 閲覧	ブロック	チャット/インターネット電話	2
		Messenger messenger.com 投稿	ブロック	チャット/インターネット電話	3
		Messenger messenger.com アップロード	ブロック	チャット/インターネット電話	3
Messenger messenger.com ビデオ電話	ブロック	チャット/インターネット電話	3		
☐ YouTube (Google)	☒	YouTube 閲覧	許可	動画配信/アップローダー/検索エンジン/Web翻訳・URL変換/音楽	1
		YouTube 一般動画閲覧	ブロック	動画配信/アップローダー	2
		文部科学省公式チャンネル 閲覧	許可	動画配信/アップローダー	2
		Tokyo 2020公式チャンネル 閲覧	許可	動画配信/アップローダー	2
		YouTube コメント投稿	ブロック	動画配信/アップローダー	3
		YouTube 動画アップロード	ブロック	動画配信/アップローダー	3

7. **個別リスト** タブを選択し、個別ブロックしたい URL/URI を追加し、右上の **保存** ボタンを押します。(注：下記イメージはあくまでも検証目的で設定した内容です。)

グループ名: F5_SE_Group ポリシー印刷 保存

有効期間 開始日 2020/04/19 終了日 2020/05/31 clear: CTL+End

ユーザー モード Webサービス フィルター 個別リスト ブロック画面 高度な設定 Test Board

個別リスト設定: ブラックリスト(優先カテゴリ) ▾

ブラックリスト(優先カテゴリ): 登録件数 3/5000件 インポート エクスポート

設定一覧	https://httpbin.org/get 【完全】 http://http.badssl.com/ 【完全】 https://rsa2048.badssl.com/ 【完全】 削除
URL	追加 変更 タイプ: 部分一致 ▾ / アクション: ブロック ▾ メール通知: しない ▾
コメント	
登録URLの有効設定	有効にする ▾
有効期限	無期限 ▾ まで

ヘッダーコントローラの設定

1. iRule で挿入した X-Forwarded-For (クライアント IP アドレス) を i-FILTER ログに出力するための設定を行います。
2. **／システム／ヘッダーコントローラ** を選択します。
3. 以下のように、設定します。

i-FILTER.

グループ

共通

ルールセット

ログ

システム

オプション

①

🔄

システム / ヘッダーコントローラー

ログインユーザー: admin

ログアウト

?

行の追加

行の削除

保存

登録件数 3/256件

	タイプ	対象	動作/値	条件	有効期限
1	リクエストヘッダー監視	Accept-Encoding			なし
2	リクエストヘッダー操作	Accept-Encoding	変更	*Accept-Encoding制御用ACL	なし
3	通信設定をヘッダーの値で変更	X-Forwarded-For	クライアントIP		なし

ブロック画面のタイトル画像連携設定

1. システム／システムパラメーター／動作設定 において、**仮想ホスト名設定** の **コンテンツ転送** の値を、で設定した SSLO の Interception Rule の Destination Address の IP アドレスに変更します。

仮想ホスト名設定			
管理画面	inetnf.conf	127.0.0.1	15081
コンテンツ転送	10.100.35.201		

2. HTTPS 接続の場合、SSLO を通すとブロック画面のタイトル画像が表示されません。回避方法例は 1.13 で説明します。
3. ここでは、簡易的にブロック画面中にタイトル画像を表示せず、**システム／デフォルト画面／ブロック画面** において、タイトル画像を **表示しない** を選択し、**保存** ボタンを押します。必要に応じて、メッセージも変更します。

システム / デフォルト画面 / ブロック画面

ログインユーザー: admin ログアウト

インポート プレビュー 保存

外部で作成したブロック画面を使用する

ブロック画面 ☐ ユーザーが作成したブロック画面を使用する
[インポートされていません。]

メッセージ設定

タイトル名

背景色

タイトル画像

メッセージ1

`<font color=#ff0000 size=5 face=MS ゴシック><b>こちらのサイトは接続を許可されていません！</b></font><br color=#ff0000 width=60% align=left size=3>このページはi-FILTER.JIによりブロックされました。`

登録文字数 156/2000文字

追加メッセージ

☒ 「改ざんサイト」ブロック時に以下のメッセージを追加する
このURLから展開されるWebサイトで、一部改ざんされたWebページを検知しています。

登録文字数 43/2000文字

表示項目 ☒ URL ☒ ブロック理由 ☒ IPアドレス ☒ 認証ユーザー名

メッセージ2

F5 Networks Japan 検証ページ

登録文字数 23/2000文字

注釈:

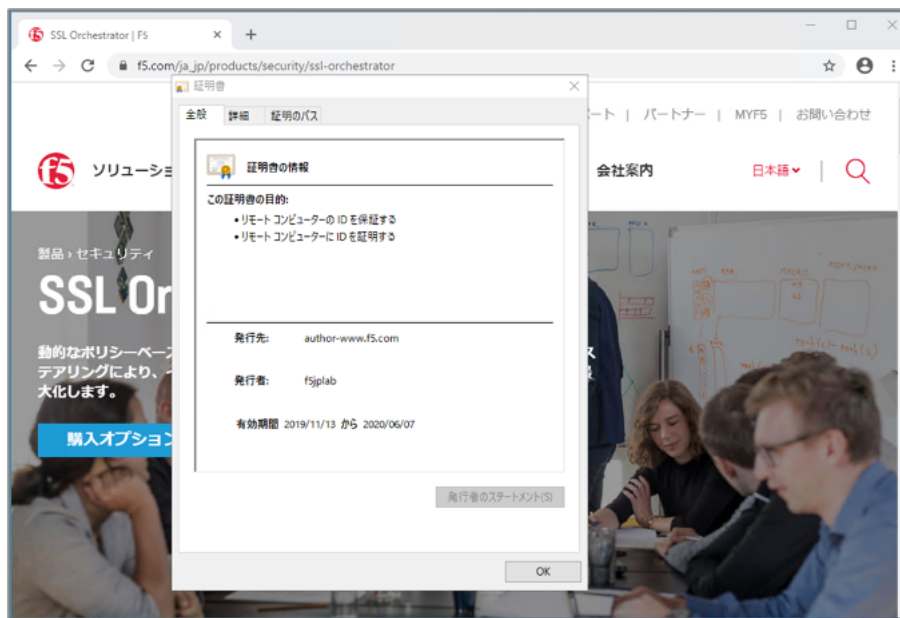
- 必要に応じて、Connection: keep-alive を有効にしてください。
- i-FILTER 製品の詳細に関しては、メーカーにお問い合わせください。

1.2.12 クライアントからの接続テスト

1. クライアントに SSLO の **CA 証明書** をインストールします。
2. コマンドラインで確認する場合は、以下を利用します。

```
curl -vk --proxy 10.100.35.201:3128 -proxy-ntlm -proxy-user 'se001:ilovef5!' -https://xxxx.xxx
```

3. ブラウザで確認する場合は、プロキシ設定に SSLO を加えてから WEB 接続を確認します。
4. WEB 通信が成功するか確認します。サーバ証明書が SSLO の CA 証明書で **書き換えられている** ことを確認します。



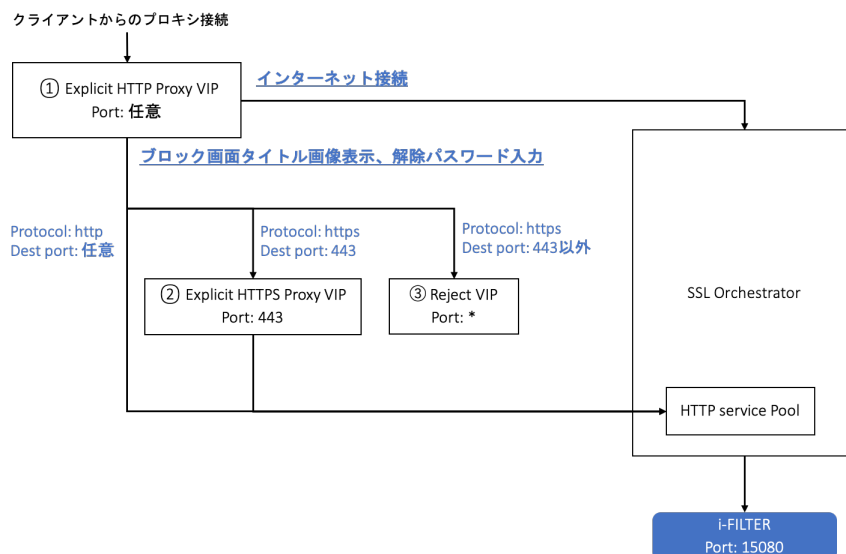
5. ブラックリストの宛先への通信が **ブロック** されることを確認します。



6. SSL 復号除外サイトの通信が成功するか確認します。サーバ証明書が SSLO の CA 証明書で **書き換えられていない** ことを確認します。

1.2.13 i-FILTER ブロック画面のタイトル画像の表示、パスワードブロック解除の設定

2.11.3 にて、SSLO 連携をするとブロック画面のタイトルが標準では表示されないと記載しましたが、以下の設定を追加することによって、表示させることが可能です。本設定を行うことにより、パスワード入力によるブロック解除も連携が可能となります。上記を実現するためには、下図の 3 つの Virtual Server が追加で必要となります。ここでは、下図の ①②③ の順で作成していきます。



Explicit HTTP Proxy 用 Virtual Server の作成

1. Proxy 用の Tunnel を作成します。**Network >> Tunnel List**にて、**Create** ボタンを押します。任意の名前 Åを入力し、**Profile** Åにて、tcp-forward Åを選択し、**Finished** ボタンを押します。

The screenshot shows the F5 SSLO configuration interface. The top navigation bar includes 'Main', 'Help', and 'About'. The left sidebar contains various management tools like 'SSL Orchestrator', 'Statistics', 'iApps', 'Wizards', 'Local Traffic', 'Traffic Intelligence', 'Access', and 'Device Management'. The main content area is titled 'Network >> Tunnels : Tunnel List >> New Tunnel...'. The 'Configuration' section contains the following fields:

Name	L3ExplicitProxy-xp-tunnel
Description	
Profile	tcp-forward
MTU	0
Use PMTU	☒ Enabled
TOS	Preserve
Auto-Last Hop	Default

At the bottom of the configuration section, there are three buttons: 'Cancel', 'Repeat', and 'Finished'. The 'Finished' button is highlighted with a red box.

2. プロキシ用の Explicit Profile を作成します。**Local Traffic >> Profiles >> Services >> HTTP** Åにて、**Create** Åボタンを押します。任意の名前を設定し、**Proxy Mode** Åにて、**Explicit** Åを選択します。

The screenshot shows the F5 SSLO configuration interface. The top navigation bar includes 'Local Traffic >> Profiles : Services : HTTP >> New HTTP Profile...'. The main content area is titled 'General Properties' and contains the following fields:

Name	L3ExplicitProxy-xp
Proxy Mode	Explicit
Parent Profile	http-explicit

3. **DNS Resolver** Åにて、SSLO Guided Configuration で作成した Å**DNS Resolver** Åを選択し、**Tunnel Name** Åにて、作成済みの Å**Tunnel** Åを選択し、**Finished** ボタンを押します。

Explicit Proxy			
DNS Resolver	+	ssloGS-net-resolver	☒
IPv6		☐	☐
Route Domain		0	☐
Tunnel Name		L3ExplicitProxy-xp-tunnel	☒

4. 次に、以下の2つの iRule を作成します。

- インターネット接続用の HTTP/HTTPS トラフィックと i-FILTER ブロックタイトル画面接続トラフィックを分ける iRule
- 上記後者のトラフィックにおいて、i-FILTER 向けにヘッダーを追加する iRule

1 つ目の iRule では、ホスト名でインターネット接続トラフィックと判断した場合、SSLO の Explicit 用の Virtual Server に転送します。2 つ目の iRule では、ホスト名で i-FILTER 宛の通信と判断した場合、ヘッダーを追記して、i-FILTER 用の Pool に転送します。各 iRule 内のホスト名は、環境にあわせた FQDN/IP アドレスに変更して頂く必要があります。

Local Traffic >> iRules にて、**Create** ボタンを押します。**任意の名前** を入力して、**Definition** に以下サンプル iRule を入力し、**Finished** ボタンを押します。(以下の iRule はあくまでもサンプルとなります。同じ主旨の内容であれば下記と同じでなくても構いません。また、以下の2つの iRule は、1 つのファイルにしていいただいても構いません。)

例) トラフィックを分ける用の iRule

```
### Add this iRule to Explicit HTTP Proxy Virtual Server ###
when HTTP_PROXY_REQUEST {
    set F5PROXY "bigip.f5jplab.local" # For block jpg #
    set F5PROXY2 "10.100.35.221" # For password bypass #
    if { [HTTP::host] contains $F5PROXY || [HTTP::host] contains $F5PROXY2 }
    →{
        HTTP::proxy enable
    } else {
        HTTP::proxy disable
        virtual sslo_L3ExplicitProxy.app/sslo_L3ExplicitProxy-xp-4
        snat automap
    }
}
```

例) ヘッダー追加用の iRule

```

### Add this iRule to Explicit HTTP Proxy Virtual Server ###
when HTTP_REQUEST {
    set F5PROXY "bigip.f5jplab.local" # For block jpg #
    set F5PROXY2 "10.100.35.221"      # For password bypass #
    if { [HTTP::host] contains $F5PROXY || [HTTP::host] contains $F5PROXY2 } {
        if { [HTTP::method] ne "CONNECT" } {
            HTTP::header replace "X-Forwarded-Proto" "http"
            pool ssloS_iFILTERProxy.app/ssloS_iFILTERProxy
        }
    }
}

```

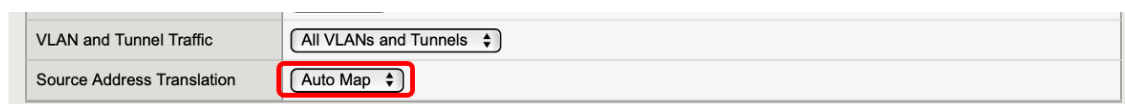
5. Explicit Proxy 用の Virtual Server を作成します。**Local Traffic >> Virtual Servers**にて、**Create** ボタンを押します。**任意の名前** を入力し、**Destination Address/Mask**にて、プロキシ接続用の **IP アドレス** を入力、**Service Port**にて、プロキシとして利用する **ポート番号** を入力します。

General Properties	
Name	L3ExplicitProxy
Description	
Type	Standard
Source Address	Host Address List
Destination Address/Mask	Host Address List 10.100.35.221
Service Port	Port Port List 3128 Other:
Notify Status to Virtual Address	☒
State	Enabled

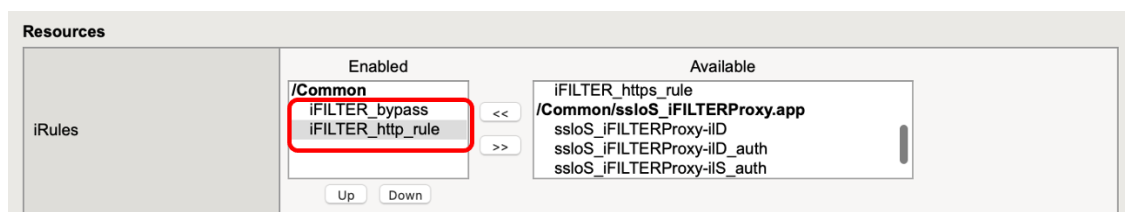
6. **HTTP Profile(Client)**にて、作成済みの **HTTP Explicit Profile** を選択します。

Configuration: Advanced	
Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile (Client)	L3ExplicitProxy-xp-http

7. Source Address Translation にて、Auto Map を選択します。



8. iRules にて作成済みの 2 つの iRule を選択して、Finished ボタンを押します。



Explicit HTTPS Proxy 用 Virtual Server の作成

1. HTTPS トラフィックにおける i-FILTER 向けヘッダ追加用の iRule を作成します。この iRule では、ヘッダーを追記して、i-FILTER 用の Pool に転送します。 **Local Traffic >> iRules** にて、 **Create** ボタンを押します。 **任意の名前** を入力して、 **Definition** に以下サンプル **iRule** を入力し、 **Finished** ボタンを押します。（以下の iRule はあくまでもサンプルとなります。同じ主旨の内容であれば下記と同じでなくても構いません。）

例) ヘッダー追加用の iRule

```
### Add this iRule to Explicit HTTPS Proxy Virtual Server ###
when HTTP_REQUEST {
    HTTP::header replace "X-Forwarded-Proto" "https"
    pool ssloS_iFILTERProxy.app/ssloS_iFILTERProxy
}
```

2. ブロック画面内のタイトル画像に SSL 接続するために BIG-IP にて SSL オフロードを行うため、 **サーバ証明書** と **秘密鍵** の登録します。 **System >> Certificate Management >> Traffic Certificate Management** にて、 **利用するサーバ証明書** と **秘密鍵** の登録します。下記が登録したサーバ証明書のイメージです。ここでは、SAN に FQDN と IP アドレスを登録しています。

System » Certificate Management : Traffic Certificate Management : SSL Certificate List » bigip

General Properties

Name	bigip
Partition / Path	Common
Certificate Subject(s)	bigip.f5jplab.local

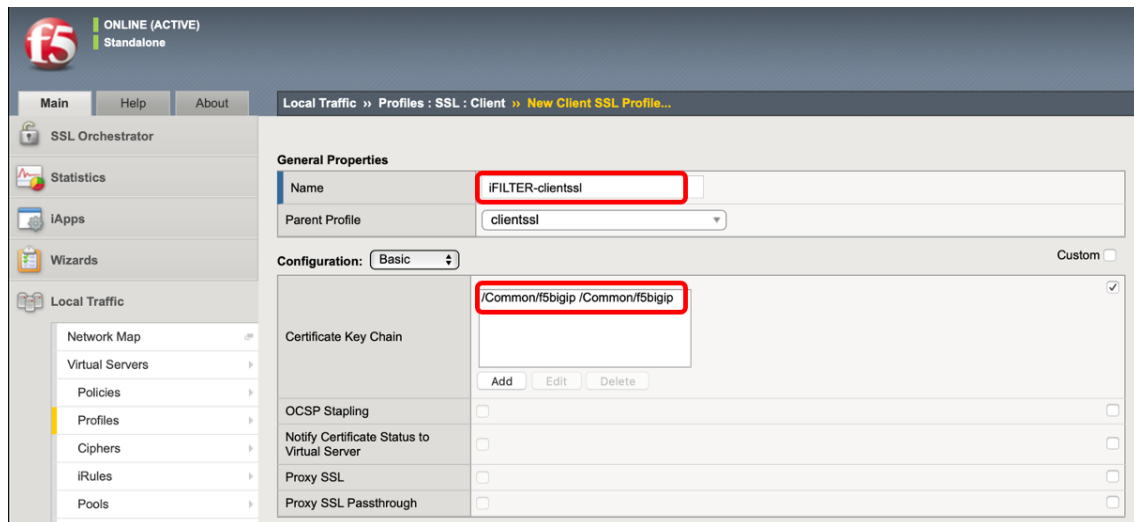
Certificate Properties

Public Key Type	RSA
Public Key Size	2048 bits
Expires	Oct 08 2021 19:14:22 JST
Version	1
Serial Number	7
Fingerprint	84:82:83:84:85:86:87:88:89:8A:8B:8C:8D:8E:8F:90:91:92:93:94:95:96:97:98:99:9A:9B:9C:9D:9E:9F
Subject	Common Name: bigip.f5jplab.local Organization: Division: Locality: State Or Province: Country: JP
Issuer	Common Name: f5jplab Organizational Unit: f5jplab Division: se Locality: minato-ku State Or Province: tokyo Country: jp
Email	
Subject Alternative Name	DNS:bigip.f5jplab.local, DNS:10.100.35.221

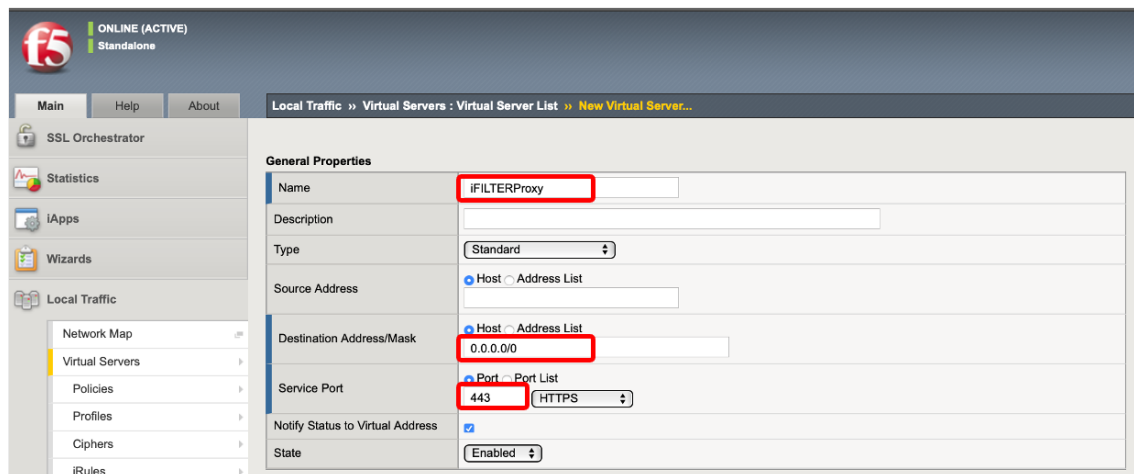
Monitoring Properties

Monitoring Type	☐ OCSP
Issuer Certificate	None
OCSP	+ None
Status	☐

3. 次に、SSL サイトにおけるブロック時に、ブロック画面内のタイトル画像に SSL 接続するための ClientSSL プロファイルを作成します。**Local Traffic >> Profiles >> SSL >> Client** にて、**Create** ボタンを押します。**任意の名前** を入力し、先程登録した **サーバ証明書** と **秘密鍵** を選択し、**Finished** ボタンを押します。



4. HTTPS 用の Explicit Proxy Virtual Server を作成します。Local Traffic >> Virtual Servers にて、Create ボタンを押します。任意の名前を入力し、Destination Address/Mask にて、0.0.0.0/0 を入力、Service Port にて、443 と入力します。



5. Configuration にて、Advanced を選択し、HTTP Profile にて、http を選択、SSL Profile (Client) にて、作成済みの iFILTER-clientssl プロファイルを選択します。

Configuration: **Advanced**

Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile (Client)	http
HTTP Profile (Server)	(Use Client Profile)
HTTP Proxy Connect Profile	None
FTP Profile	None
PPTP Profile	None
SOCKS Profile	None
Stream Profile	None
iRules LX Profile	None
XML Profile	None
MQTT	☐
SSL Profile (Client)	Selected iFILTER-clientssl Available /Common clientssl clientssl-insecure-compatible clientssl-quick clientssl-secure crypto-server-default-clientssl split-session-default-clientssl

6. **VLAN and Tunnel Traffic** にて、**Enabled on...** を選択し、**VLANs and Tunnels** にて作成済みの **Tunnel** を選択します。

VLAN and Tunnel Traffic	Enabled on...
VLANs and Tunnels	Selected /Common L3ExplicitProxy-xp-tunnel Available /Common DB-tunnel external http-tunnel internal
Source Address Translation	Auto Map
Bandwidth Controller	None
Traffic Class	Enabled Available
Connection Limit	0
Eviction Policy	None
Eviction Protected	☐ Enabled
Connection Rate Limit	0
Connection Rate Limit Mode	Per Virtual Server
Address Translation	☒ Enabled
Port Translation	☒ Enabled

7. iRules にて、作成済みの iRule を選択し、*Finished* ボタンを押します

Reject 用 Virtual Server の作成

- 最後に、443 ポート以外はブロックをする Virtual Server を作成します。（本 Virtual Server がなくても動作はします。）任意の名前を入力し、**Type** にて **Reject** を選択し、**Destination Address/Mask** にて、**0.0.0.0/0** と入力し、**Service Port** にて * と入力します。**VLAN and Tunnel Traffic** にて、**Enabled on...** を選択し、**VLANs and Tunnels** にて作成済みの **Tunnel** を選択し、*Finished* ボタンを押します。

Local Traffic » Virtual Servers : Virtual Server List » New Virtual Server...

General Properties

Name	RejectProxy
Description	
Type	Reject
Source Address	
Destination Address/Mask	0.0.0.0/0
Service Port	* * All Ports
Notify Status to Virtual Address	☒
State	Enabled

Configuration: Advanced

Protocol	TCP
WebSocket Profile	None
IMAP Profile	None
SplitSession Client Profile	None
SplitSession Server Profile	None
Statistics Profile	None
VLAN and Tunnel Traffic	Enabled on...
VLANs and Tunnels	Selected / Common L3ExplicitProxy-xp-tunnel << >> Available / Common external http-tunnel icap internal

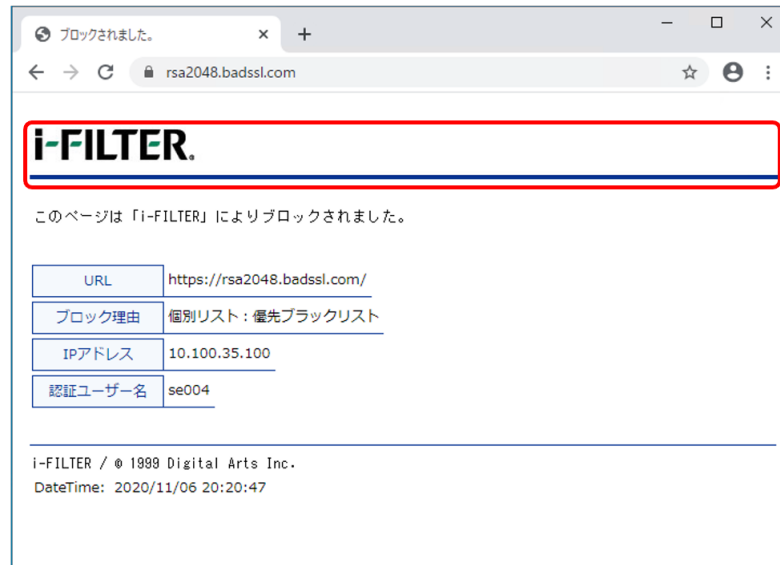
i-FILTER 側の設定

1. システム／システムパラメーター／動作設定 にて、コンテンツ転送、ブロック解除 のそれぞれにサーバ証明書に登録した DNS 名を設定します。（ブロック画面タイトル表示時、パスワードブロック解除時の URI の一部として利用されます。）

仮想ホスト名設定			
管理画面	inetnf.conf	127.0.0.1	/ 15081
コンテンツ転送	bigip.f5jplab.local		
ブロック解除	10.100.35.221		

クライアントからの接続テスト

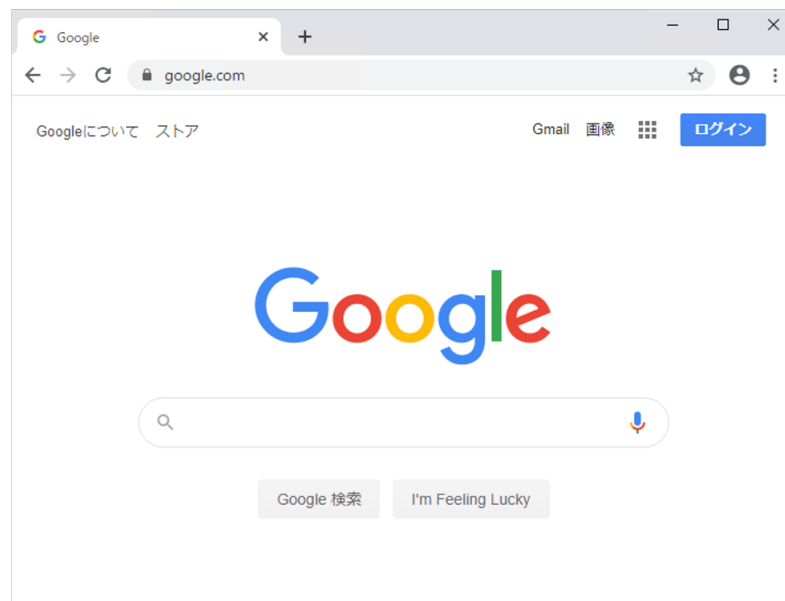
1. ブラウザの proxy 設定 にて、作成済みの Explicit Proxy の IP アドレスに紐づく FQDN または、**IP アドレス** に変更します。
2. ブラックリストの宛先への通信がブロックされ、タイトル画像が表示されることを確認します。



3. パスワードブロック解除が設定されている URL へ接続し、パスワード入力画面が表示されることを確認します。



4. 解除パスワード入力後、無事 WEB 接続ができる事を確認します。



1.2.14 その他

各種ログ

1. テストの際には、以下の SSLO におけるログを参照して下さい。

- SSLO 全般ログや iRule で local0 で指定したログ `/var/log/ltm`
- APM（認証）のログ `/var/log/apm`
- SSL Guided Configuration (iAppLX/REST) に関わるログ `/var/log/restnoded/restnoded.log`
`/var/log/restjava.0.log`
- その他、SSLO に関するトラブルシューティングは以下の AskF5 記事をご参照下さい。
K26520133: Troubleshooting SSL Orchestrator(SSLO) <https://support.f5.com/csp/article/K26520133>

2. テストの際には、以下の i-FILTER におけるログを参照して下さい。

- アクセスログ `/usr/local/ifilter10/logs/access.log0000`

フィルター除外設定（必須ではありません）

- 本テストでは、`httpbin.org` を接続先ホストとして利用させて頂いておりますが、現状デフォルトではブロックされるので、システム／システムフィルター／推奨フィルター設定－除外設定にて、テストで利用しているホスト名を除外設定に追加します。

除外設定	
除外ホスト	☒ 有効にする (登録件数 1/2000件) ホスト名 httpbin.org
	☐ 完全一致 ☒ 部分一致 ☐ 正規表現 ☐ 大文字小文字を無視する
	☐ 有効にする (登録件数 0/2000件) ホストIP

i-FILTER 通信について

1. i-FILTER の DB アップデートやシステムアップデートに必要な通信に関しては、i-FILTER 用サーバにて管理用 VLAN を通して、アップデートできるように設定して下さい。