BIG-IP Forward Proxy セットアップガイド Documentation

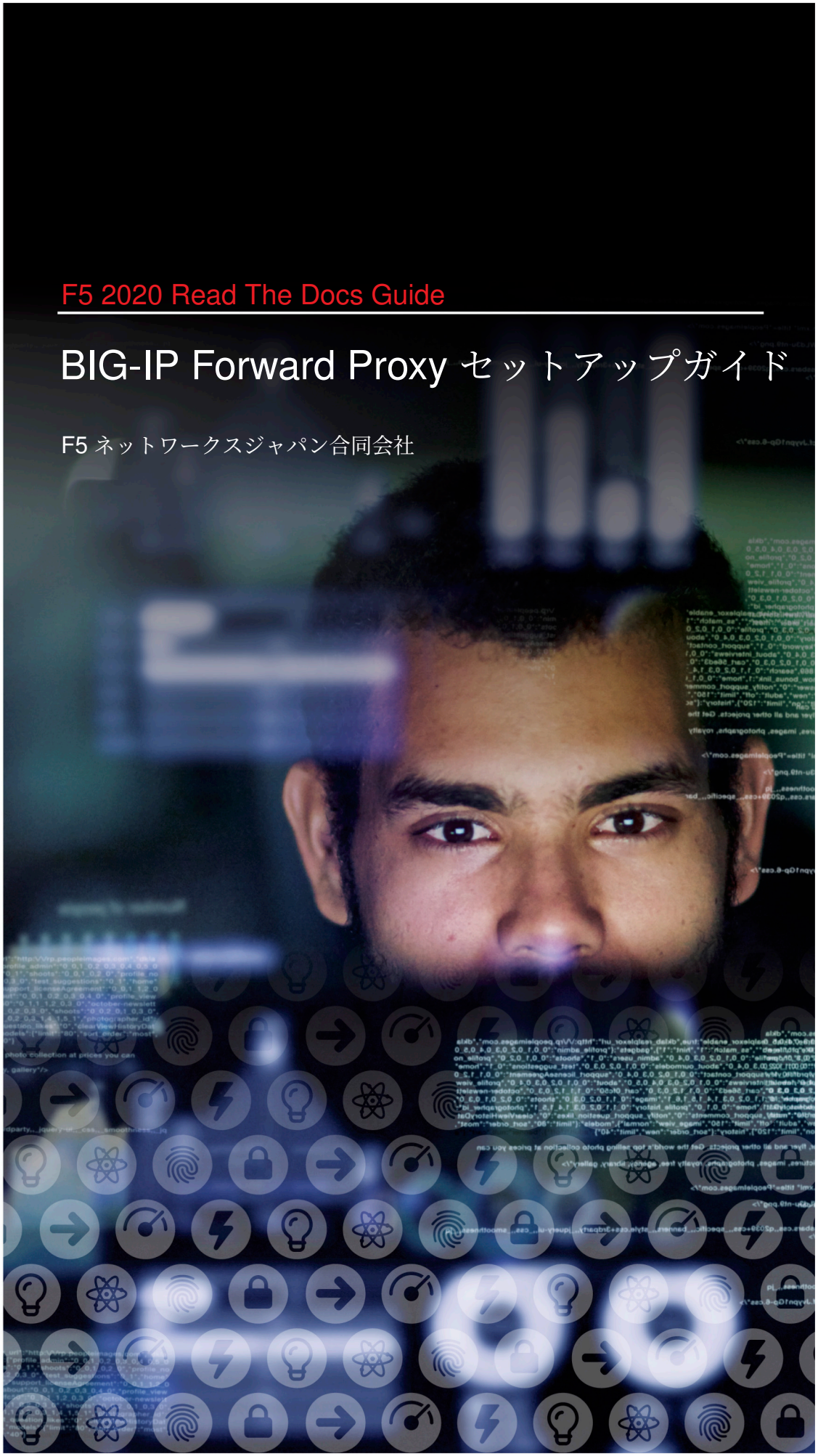
F5 ネットワークスジャパン合同会社

2020 年 08 月 03 日

F5 2020 Read The Docs Guide

BIG-IP Forward Proxy セットアップガイド

F5 ネットワークスジャパン合同会社



目次:

第 1 章 BIG-IP Forward Proxy における基礎知識 5
1.1 関連するオブジェクト . . . 5
1.2 HTTP プロファイルの種類 . . . 6
1.3 HTTP-Tunnel . . . 6
1.4 Explicit Forward Proxy トポロジー . . . 6
1.5 Transparent Forward Proxy トポロジー . . . 7

第 2 章 HTTPS Explicit Forward Proxy の基本設定 9
2.1 サンプル構成 . . . 9
2.2 DNS リゾルバの設定 . . . 10
2.3 TLS をサポートする HTTP Tunnel の設定 . . . 10
2.4 HTTP プロファイル設定 . . . 10
2.5 Explicit Proxy 用 Virtual Server 設定 . . . 13
2.6 トンネル用 Virtual Server 設定 . . . 13
2.7 アクセス確認 . . . 14

第 3 章 SSL Forward Proxy の基本設定 17
3.1 CA 証明書の設定例 . . . 17
3.2 SSL プロファイル設定 . . . 19
3.3 トンネル用 Virtual Server 設定 . . . 20
3.4 アクセス確認 . . . 21

1 BIG-IP Forward Proxy における基礎知識

本章では、BIG-IP を Forward Proxy として構成する際に前提となる基礎知識について、紹介します。

1.1 関連するオブジェクト

本節では、BIG-IP を Forward Proxy で利用する上で必要となる、オブジェクトの概要について紹介します。詳細は、下図をご参照ください。

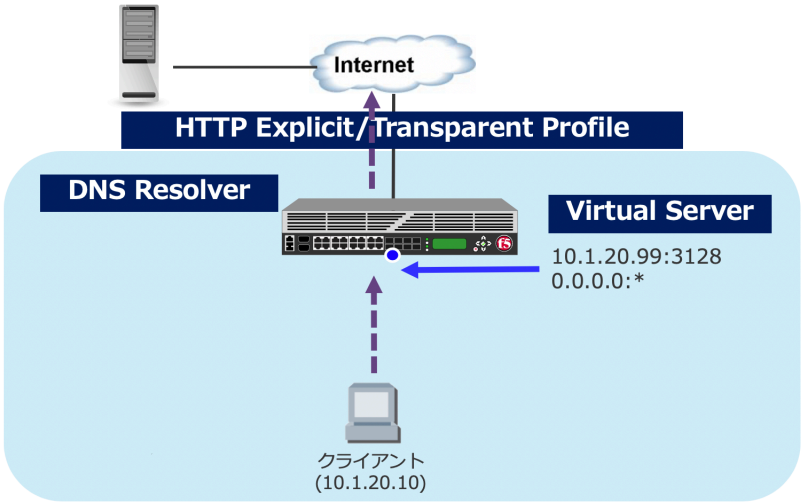


図 1　BIG-IP で Forward Proxy を構成する際のオブジェクト

- **HTTP Explicit Profile**

  BIG-IP をクライアントから見た明示 (Explicit) プロキシとして設定する場合に利用するプロファイルです。

- **HTTP Transparent Profile**

  BIG-IP をクライアントから見た透過 (Transparent) プロキシとして設定する場合に利用するプロファイル

です。

- **DNS Resolver**

  Forward Proxy として動作する BIG-IP がクエリを行う、DNS サーバのアドレスを指定します。DNS サーバのレスポンスは、BIG-IP 内にキャッシュされます。

- **Virtual Server**

  BIG-IP で、サービスを受け付けるリスナーとして動作します。Virtual Server で指定した IP アドレスおよびポート番号を、クライアント端末の Web ブラウザ等に設定します。

1.2 HTTP プロファイルの種類

プロキシモードを指定する HTTP プロファイルは、下表の通りです。

プロキシモード	説明
Reverse (デフォルト)	リバースプロキシとして利用
Explicit	明示プロキシとして利用
Transparent	透過プロキシとして利用

アウトバウンド (=内部からインターネットへのアクセス) 通信処理を行う際には、Explicit もしくは Transparent を指定した HTTP プロファイルを割り当てます。

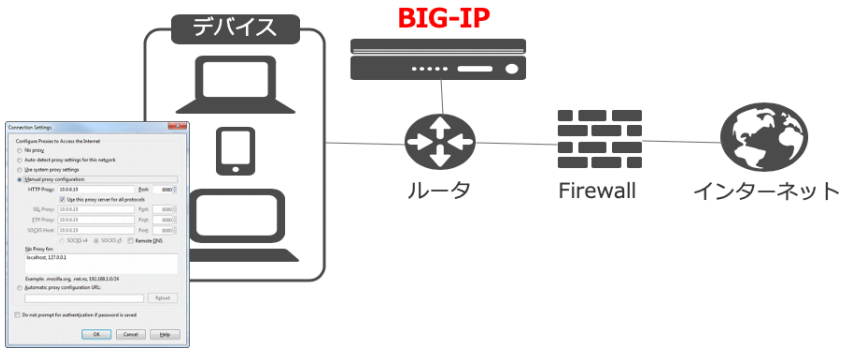
1.3 HTTP-Tunnel

プロキシサーバを経由した HTTPS 通信では、http の CONNECT メソッドが使われます。クライアントから CONNECT メソッドを受け取ると、HTTPS プロキシ (=BIG-IP) は対象ホストに TCP 3-way ハンドシェイクによる接続を行います。HTTPS プロキシはソケット接続を代行して送受信データを処理するのみで、流れるデータの内容には一切関与はしません。(IP ヘッダと TCP ヘッダのみ変更します。)

上記の処理を、BIG-IP では ” HTTP-Tunnel ” と明記しています。

1.4 Explicit Forward Proxy トポロジー

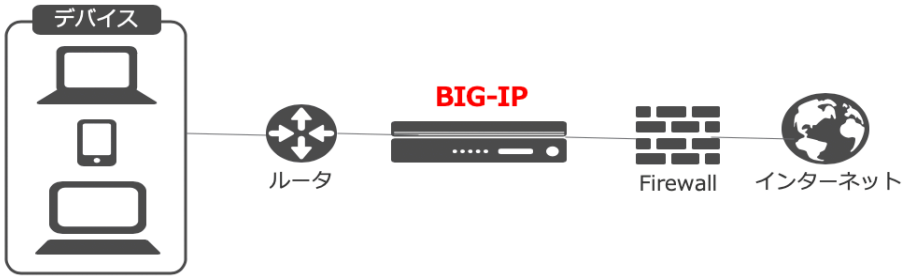
BIG-IP を明示 (Explicit) プロキシとして使用するの場合のトポロジーは、下図の通りです。



- BIG-IP を明示 (Explicit) プロキシとして構成する場合は、クライアント端末の Web ブラウザ等でリクエストをプロキシサーバ宛に送信するように設定します。PAC (Proxy Auto Config) ファイルや WPAD (Web Proxy Auto Discovery Protocol) を使用することで、ブラウザ側の設定を自動化することも可能です。
- 既存ネットワーク構成の変更は最小限で済むトポロジーです。

1.5 Transparent Forward Proxy トポロジー

BIG-IP を透過 (Transparent) プロキシとして使用するの場合のトポロジーは、下図の通りです。



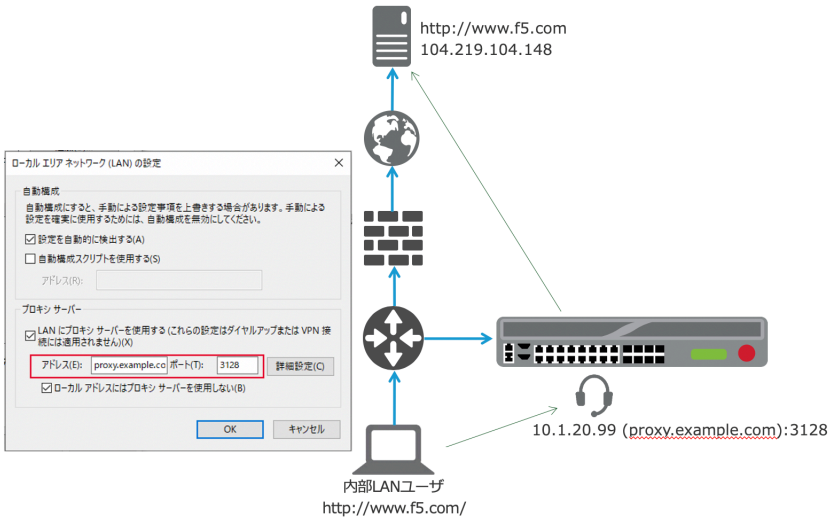
- BIG-IP を透過 (Transparent) プロキシとして構成する場合は、BIG-IP をルータや FireWall 等の間に"挟み込む"形で導入することで、クライアントからのリクエストが自動的にプロキシサーバに送信されます。この構成の場合、クライアントはプロキシの存在を意識しないため、Web ブラウザ等の設定は不要です。
- リクエストがプロキシサーバに送られるようにするために、既存ネットワーク構成の変更が必要となる場合があります。

2 HTTPS Explicit Forward Proxy の基本設定

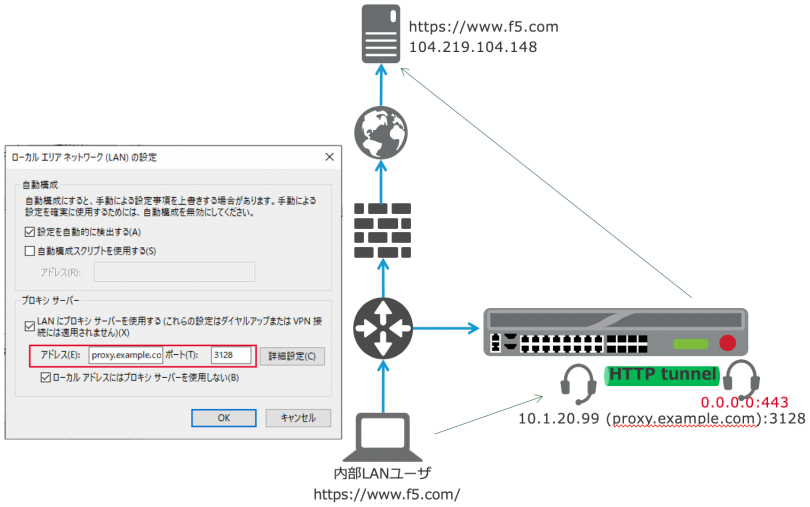
本章では、BIG-IP を HTTPS 用の Explicit プロキシとして構成する手順について、紹介します。

2.1 サンプル構成

本章で紹介する構成は、以下の通りです。



- クライアントソフトウェア (ブラウザ) では、リクエストを直接プロキシサーバ (=BIG-IP) に転送するように設定します。
- BIG-IP において、プロキシサーバとして動作する Virtual Server を設定します。また、BIG-IP (プロキシサーバ) はホストの名前解決に DNS リゾルバを使用します。 (例: www.f5.com → 104.219.104.148)



- HTTPS Forward Proxy の場合は、HTTP における設定に加えて、前述の HTTP トンネル用の Virtual Server の設定が必要となります。

2.2 DNS リゾルバの設定

BIG-IP の Configuration Utility で、DNS リゾルバを設定します。

Network >> DNS Resolver を選択して、DNS リゾルバを作成します。下図の例では"dns_resolover"という名前の DNS リゾルバを作成しています。

作成した DNS リゾルバにおいて、**Forward Zone** を選択します。

Forward Zone の名前を". (ドット)"と指定して、BIG-IP がクライアントとして名前解決を行う DNS サーバのアドレスを入力します。

2.3 TLS をサポートする HTTP Tunnel の設定

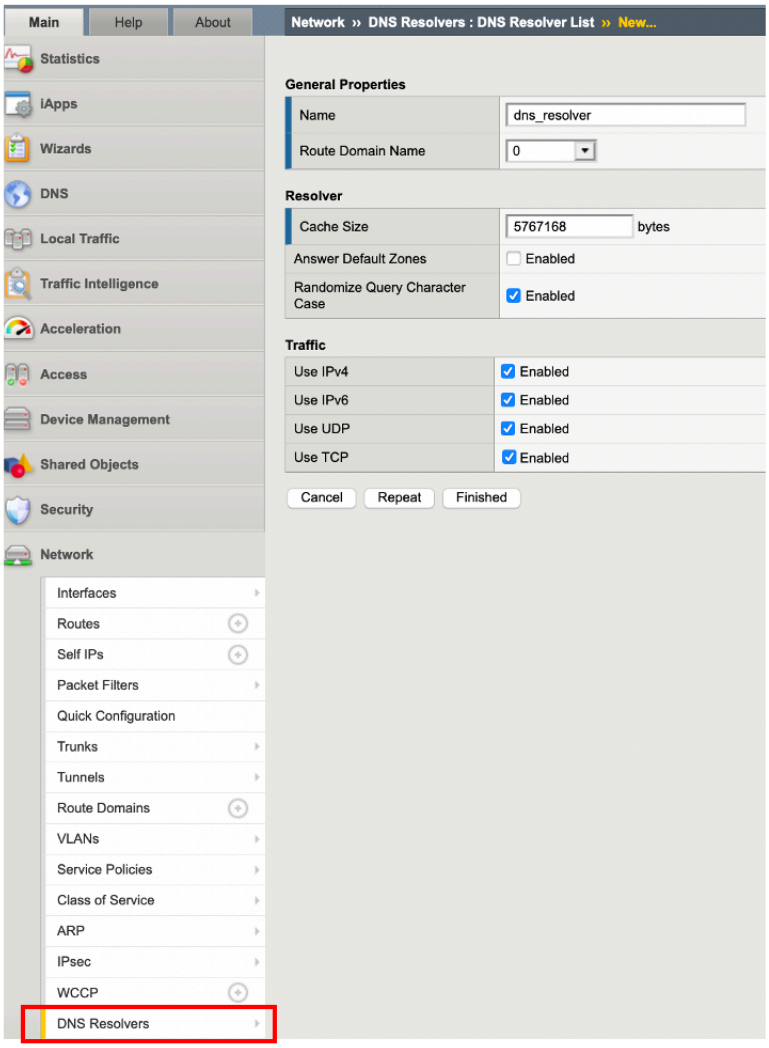
TLS (SSL) をサポートする HTTP Tunnel を設定します。

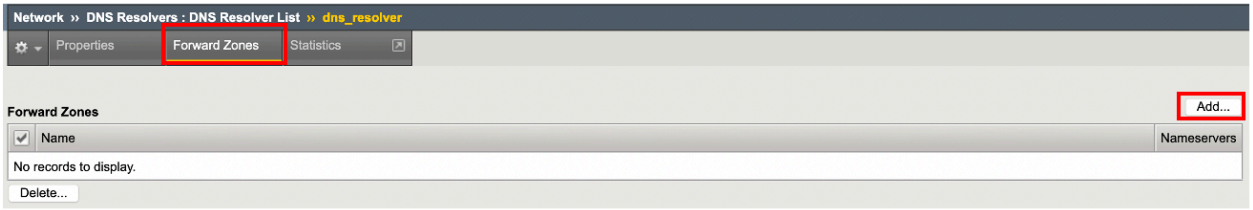
Network >> Tunnels を選択して、HTTP Tunnel を作成します。ここでは Forward Proxy として構成するため、Profile として **tcp-forward** を指定します。

2.4 HTTP プロファイル設定

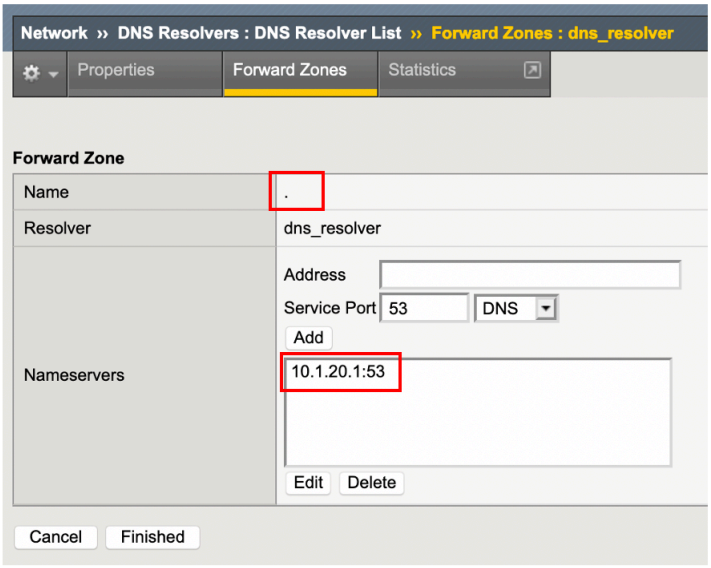
Explicit Forward Proxy を構成する HTTP プロファイルを設定します。

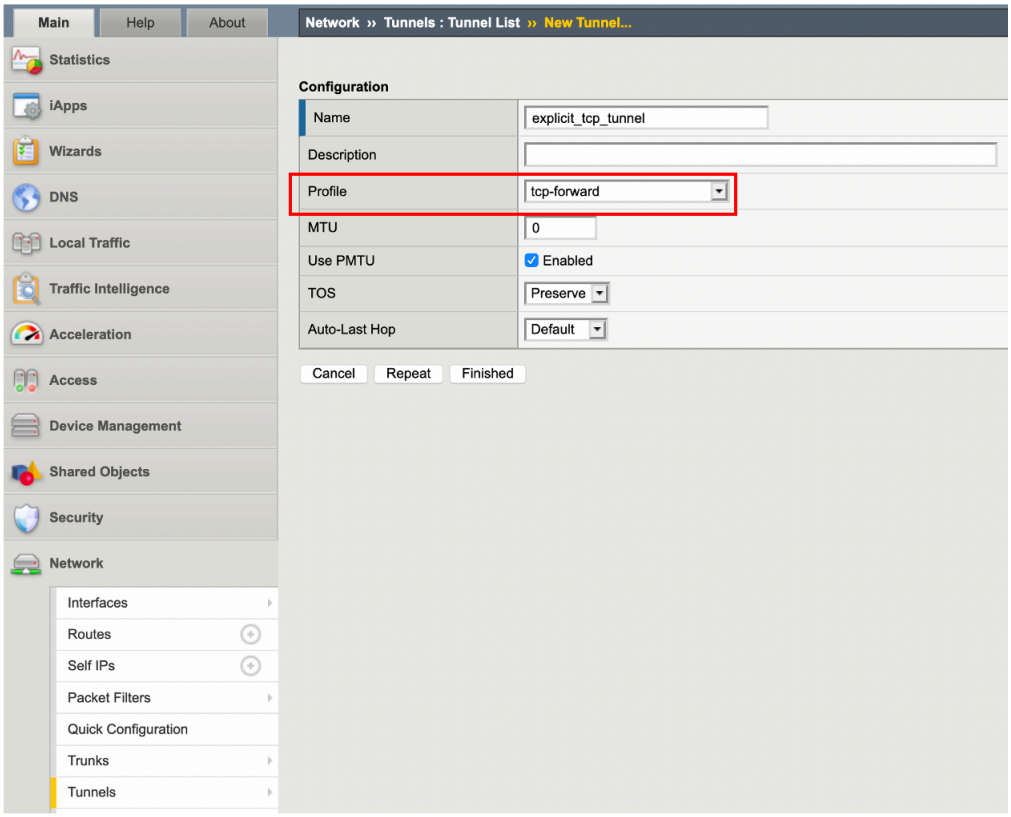
Local Traffic >> Profiles >> Services を選択して、HTTP プロファイルを作成します。

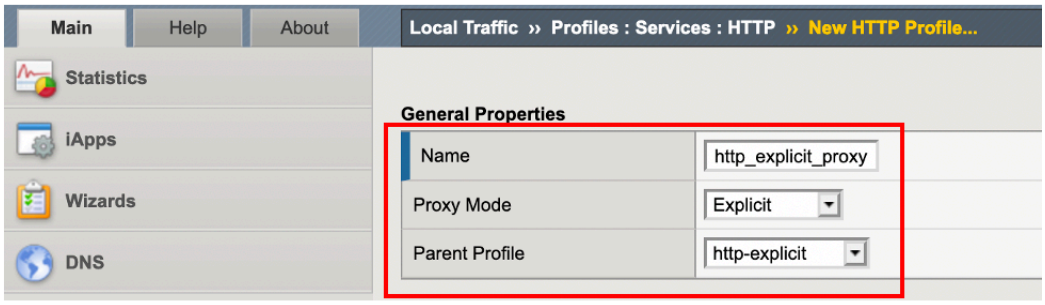




- **General Properties** のセクションで以下の設定を行います。
  - Proxy Mode: "Explicit"を選択
  - Parent Profile: "http-explicit"を選択
  - **Explicit Proxy** のセクションで以下の設定を行います。
    - DNS Resolver: "DNS リゾルバの設定"の項で作成したものを選択します。
    - Tunnel Names: "TLS をサポートする TCP トンネルの設定"の項で作成したものを選択します。


Network » DNS Resolvers : DNS Resolver List » Forward Zones : dns_resolver
Properties
Forward Zones
Statistics
Forward Zone
Name
.
Resolver
dns_resolver
Address
Service Port
53
DNS
Add
Nameservers
10.1.20.1:53
Edit
Delete
Cancel
Finished


Main
Help
About
Network » Tunnels : Tunnel List » New Tunnel...
Statistics
iApps
Wizards
DNS
Local Traffic
Traffic Intelligence
Acceleration
Access
Device Management
Shared Objects
Security
Network
Interfaces
Routes
Self IPs
Packet Filters
Quick Configuration
Trunks
Tunnels
Configuration
Name
explicit_tcp_tunnel
Description
Profile
tcp-forward
MTU
0
Use PMTU
Enabled
TOS
Preserve
Auto-Last Hop
Default
Cancel
Repeat
Finished



2.5 Explicit Proxy 用 Virtual Server 設定

Explicit Forward Proxy を構成する Virtual Server を設定します。この Virtual Server は、クライアントから見たプロキシサーバとして動作します。

Local Traffic >> Virtual Server を選択して新規に Virtual Server を構成し、以下の設定を行います。

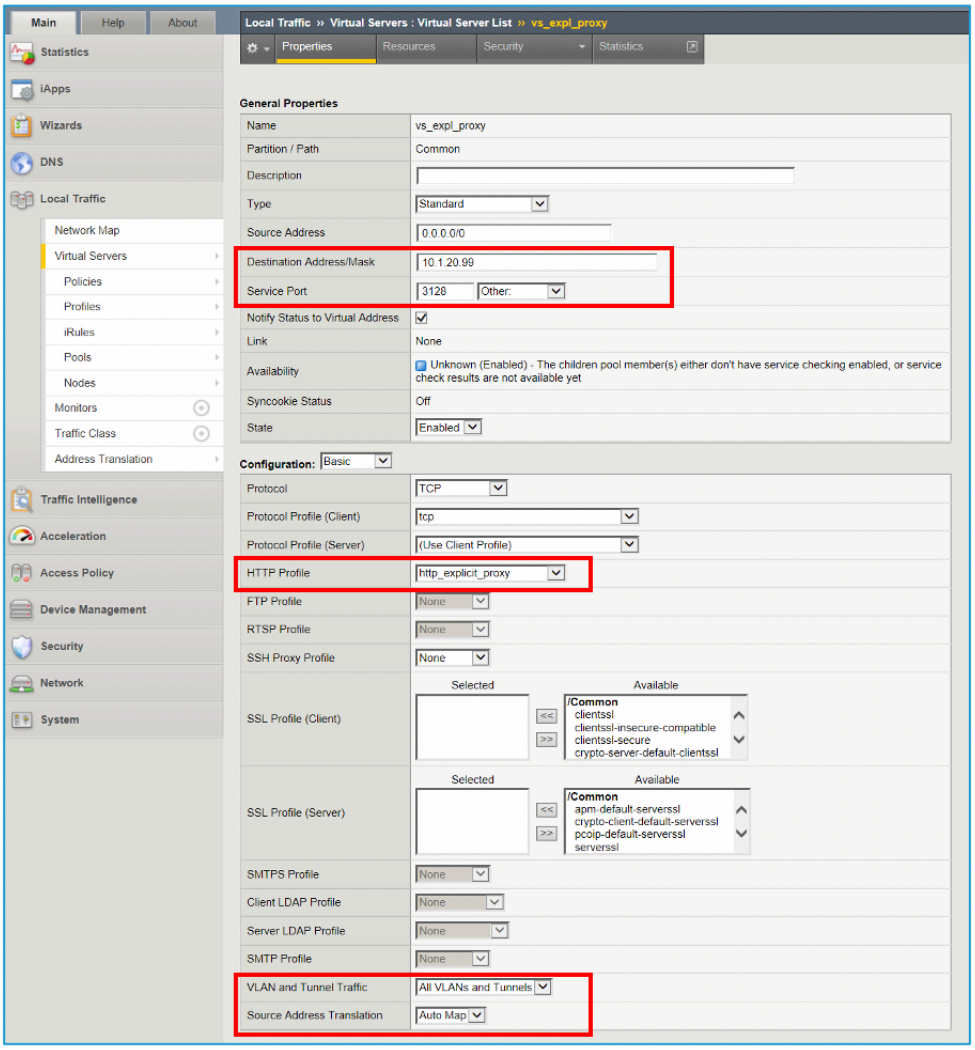
- Destination Address/Mask: クライアントのブラウザで指定する IP アドレス、およびサブネットマスク
- Service Port: クライアントのブラウザで指定するポート番号
- HTTP Profile: "HTTP Profile 設定"の項で作成したものを指定
- VLAN and Tunnel Traffic: 必要な VLAN とトンネルを指定
- Source Address Translation: "Automap"もしくは"SNAT"を指定
- Address Translation: **有効** (チェックを入れる)
- Port Translation: **有効** (チェックを入れる)

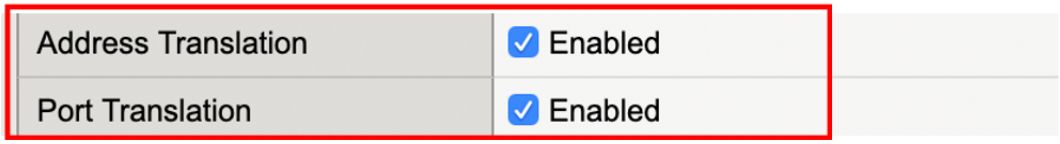
2.6 トンネル用 Virtual Server 設定

HTTPS 通信においてトンネルを構成する Virtual Server を設定します。

Local Traffic >> Virtual Server を選択して新規に Virtual Server を構成し、以下の設定を行います。

- Destination Address/Mask: "0.0.0.0/0"を指定
- Service Port: 通常は"443" (HTTPS) を指定
- Source Address Translation: "Automap"もしくは"SNAT"を指定

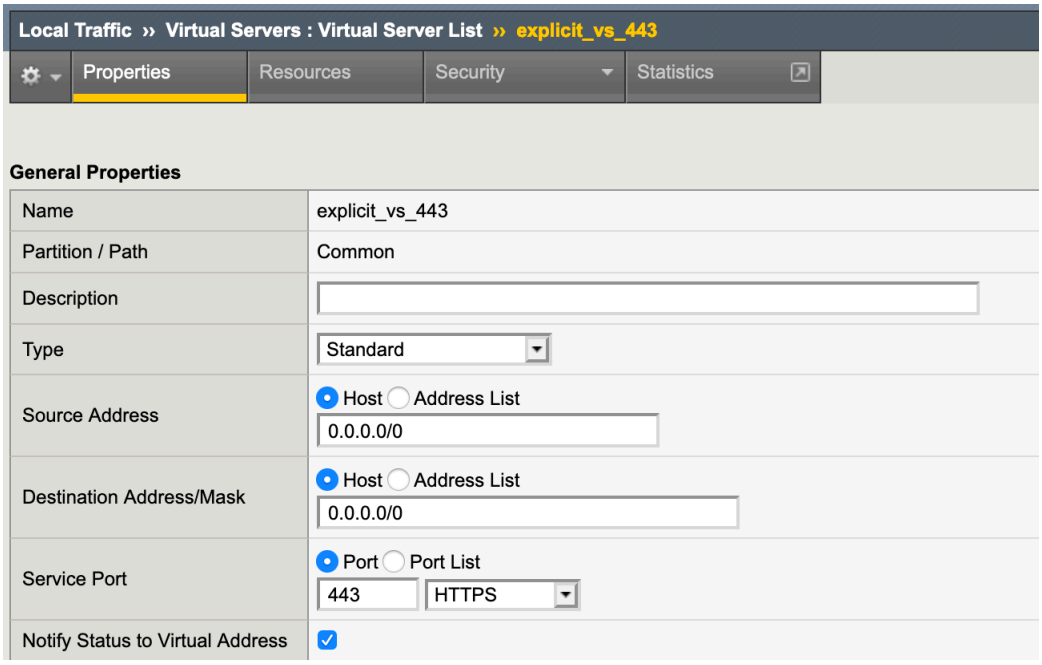


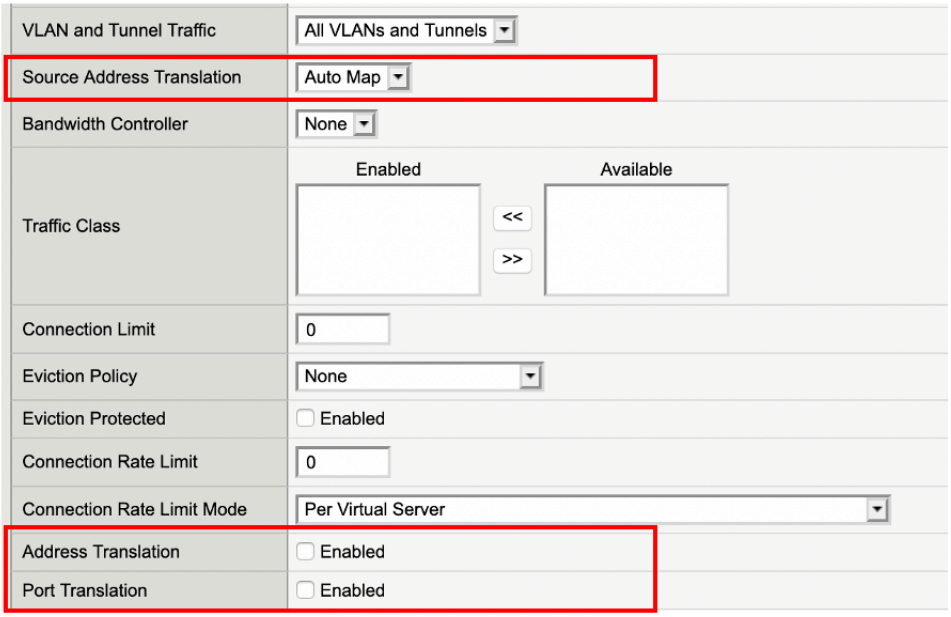


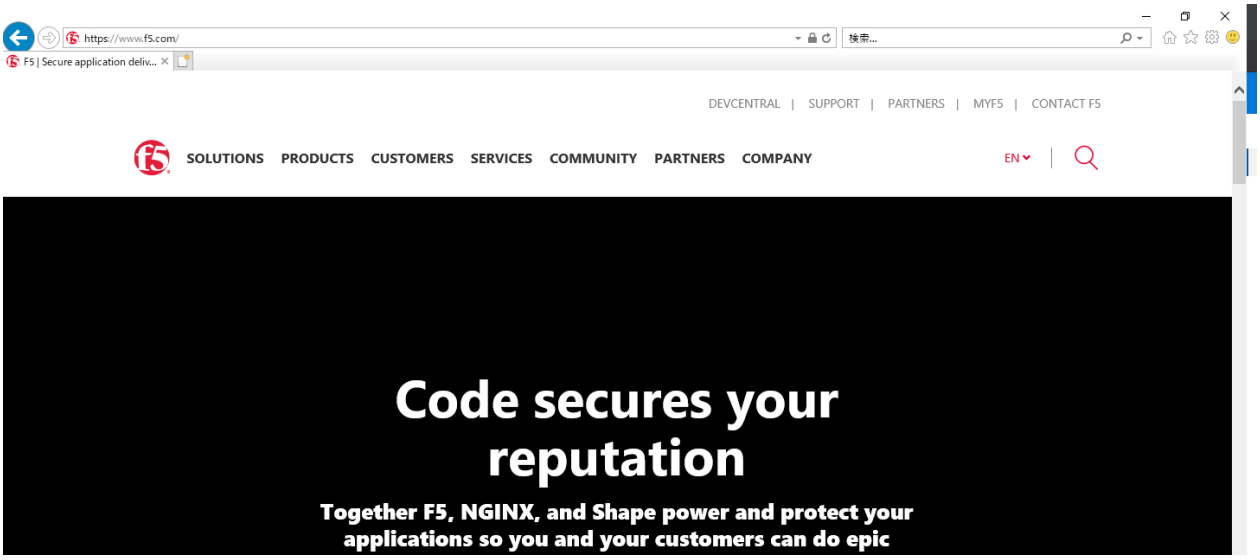
- Address Translation: **無効** (チェックを外す)
- Port Translation: **無効** (チェックを外す)

2.7 アクセス確認

クライアント PC の Web ブラウザから正常にアクセスできることを確認します。この例では https://www.f5.com にアクセスします。


Local Traffic ›› Virtual Servers : Virtual Server List ›› explicit_vs_443
Properties
Resources
Security
Statistics
General Properties
Name
explicit_vs_443
Partition / Path
Common
Description
Type
Standard
Source Address
Host
Address List
0.0.0.0/0
Destination Address/Mask
Host
Address List
0.0.0.0/0
Service Port
Port
Port List
443
HTTPS
Notify Status to Virtual Address


VLAN and Tunnel Traffic
All VLANs and Tunnels
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


https://www.f5.com/
検索...
F5 | Secure application deliv...
DEVCENTRAL | SUPPORT | PARTNERS | MYF5 | CONTACT F5
SOLUTIONS PRODUCTS CUSTOMERS SERVICES COMMUNITY PARTNERS COMPANY
EN
Code secures your reputation
Together F5, NGINX, and Shape power and protect your applications so you and your customers can do epic

3 SSL Forward Proxy の基本設定

本章では、BIG-IP を SSL Forward プロキシとして構成する手順について、紹介します。SSL Forward プロキシを構成することで、BIG-IP で SSL 通信を可視化することができます。

以下の設定については、前章の手順を参照してください。

- サンプル構成
- DNS リゾルバの設定
- TLS トンネルをサポートする HTTP Tunnel の設定
- HTTP プロファイル設定
- Explicit Proxy 用 Virtual Server 設定

本章では上記の設定に加えて、以下の内容を紹介します。

3.1 CA 証明書の設定例

SSL Forward Proxy を構成する場合は、BIG-IP に CA 証明書と秘密鍵をインストールします。ここでは、BIG－IP 上で CLI で設定する手順を紹介します。

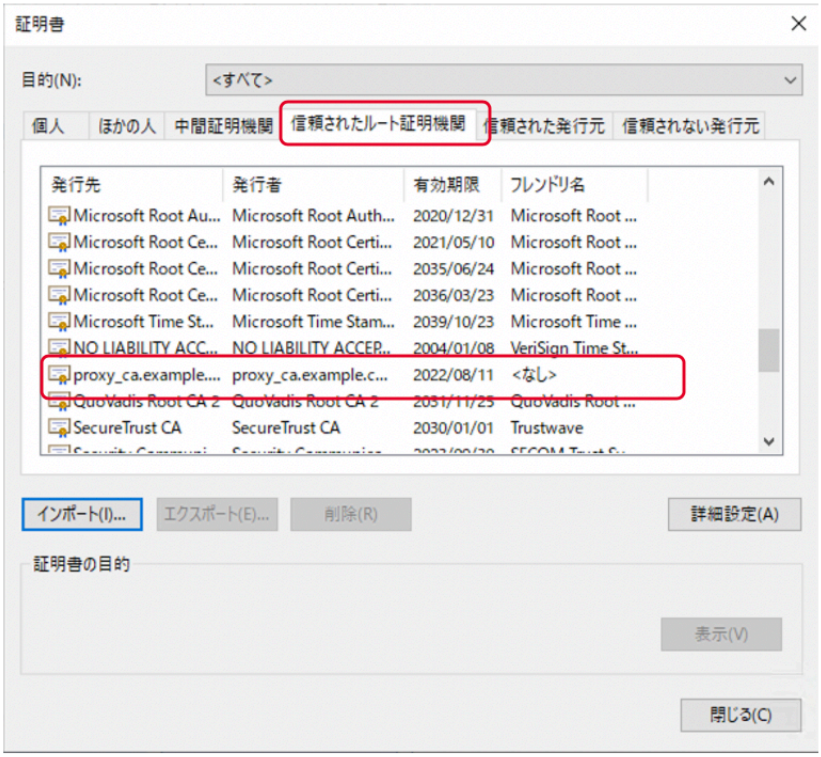
```
# openssl に必要なファイルとディレクトリの作成
mkdir /config/ca
cd /config/ca
mkdir /config/ca/newcerts
mkdir /config/ca/private
mkdir /config/ca/crl
touch /config/ca/index.txt
echo 01 > /config/ca/serial
```

(次のページに続く)

(前のページからの続き)

```
# openssl 設定ファイルをコピー
cp /etc/pki/tls/openssl.cnf /config/ca

# openssl.cnf ファイルの設定
vi /config/ca/openssl.cnf
unique_subject  = no
dir             = /config/ca

# BIG-IP が SSL 可視化を行うために使用する、CA 証明書とキーを生成
# 注: Common Name として "proxy_ca.example.com" を指定
openssl req -x509 -nodes -days 3650 -newkey rsa:2048 -out proxy_ca.pem -outform PEM -
↪keyout proxy_ca.key

# CA 証明書を確認
openssl x509 -in proxy_ca.pem -noout -text

# BIG-IP のファイルストアにインポート
tmsh install sys crypto cert proxy_ca.crt from-local-file /config/ca/proxy_ca.pem
tmsh install sys crypto key proxy_ca.key from-local-file /config/ca/proxy_ca.key
```

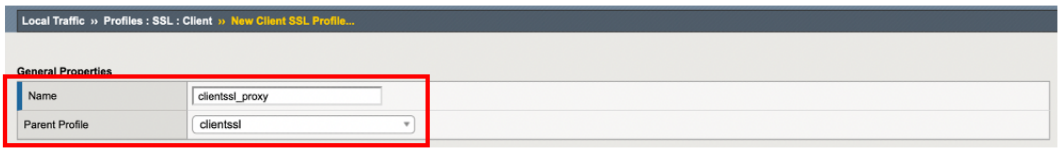
ブラウザでのアクセス時にセキュリティ警告が表示されるのを防ぐため、上記で生成した CA 証明書をクライアント端末にインポートします。例えば Windows の場合、「信頼されたルート証明機関」に BIG-IP が再署名に使用する証明書を追加します。



3.2 SSL プロファイル設定

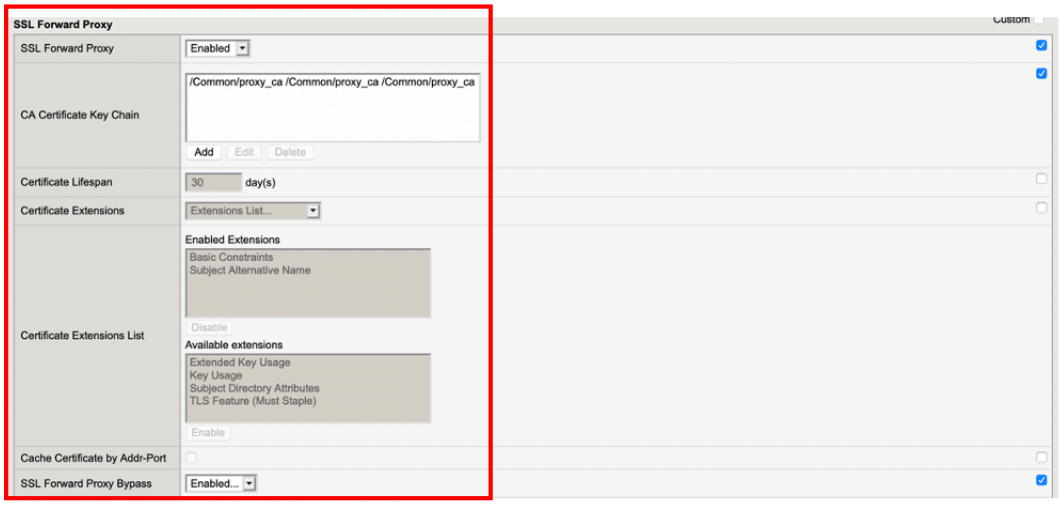
Explicit Forward Proxy を構成するクライアントおよびサーバ SSL プロファイルを設定します。

- **クライアント SSL プロファイル**
  - **Local Traffic >> Profiles >> SSL >> Client** を選択して、クライアント SSL プロファイルを作成します (この例では"clientssl_proxy")。親プロファイル (Parent Profile) として、clientssl を指定します。

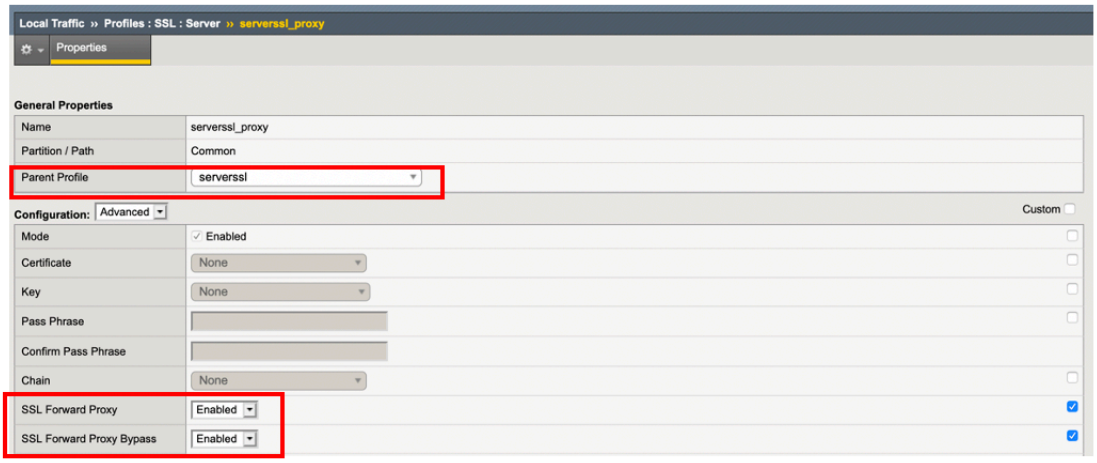


- **SSL Forward Proxy** のセクションで以下の設定を行います。

  - SSL Forward Proxy: **有効** (Enabled)
  - CA Certificate Key Chain: "CA 証明書の設定例"の項で作成した CA 証明書およびキーを指定
  - SSL Forward Proxy Bypass: **有効** (Enabled)



- **サーバ SSL プロファイル**
  - **Local Traffic >> Profiles >> SSL >> Server** を選択して、サーバ SSL プロファイルを作成します (この例では"serverssl_proxy")。親プロファイル (Parent Profile) として、serverssl を指定します。合わせて、以下の設定を行います。
    - SSL Forward Proxy: **有効** (Enabled)
    - SSL Forward Proxy Bypass: **有効** (Enabled)
  - **Server Authentication** のセクションで以下の設定を行います。



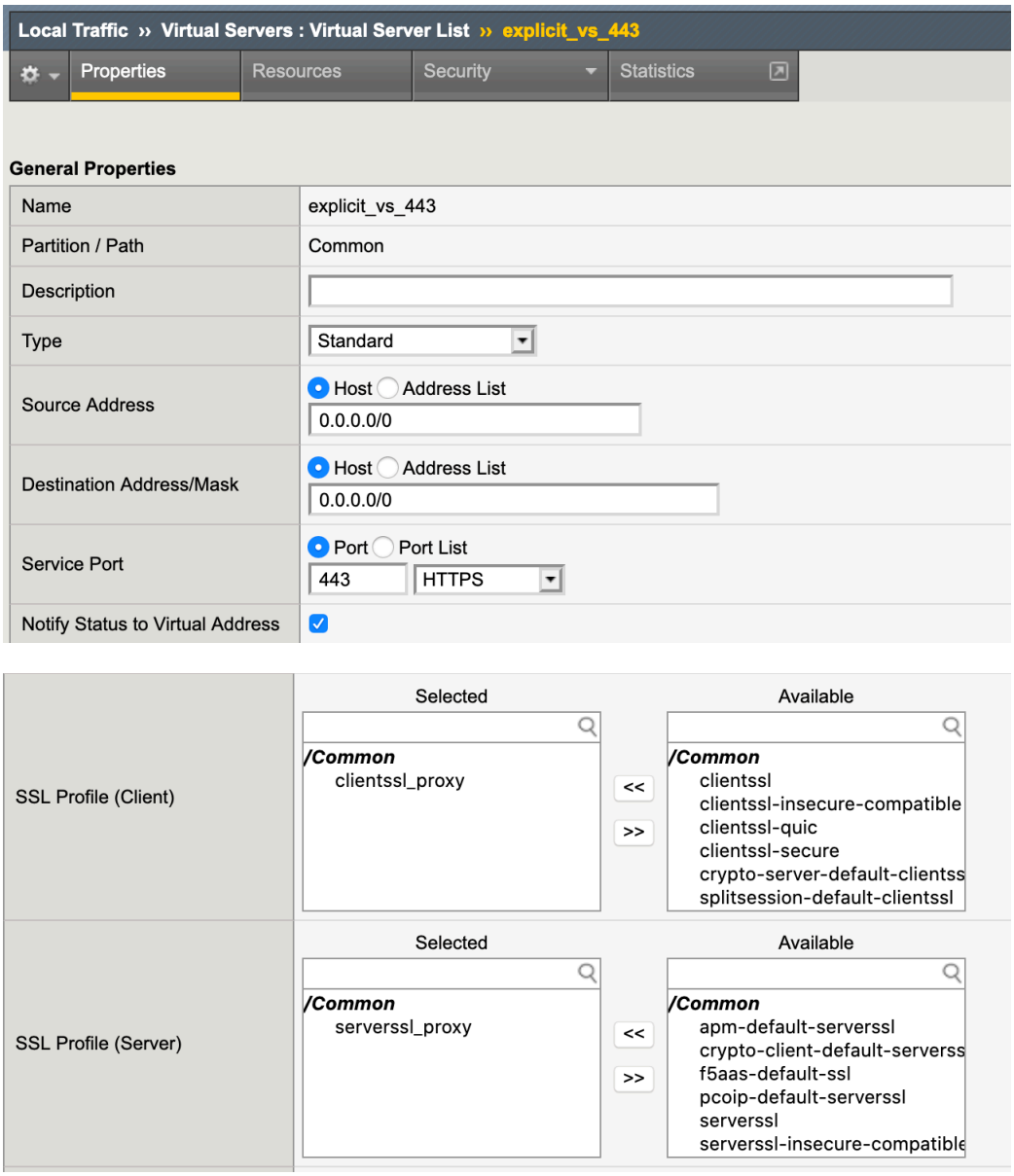
* Server Certificate: "require..."を選択
* Trusted Bundled Authority: "ca-bundle.crt"を選択

3.3 トンネル用 Virtual Server 設定

HTTPS 通信においてトンネルを構成する Virtual Server を設定します。

Local Traffic >> Virtual Server を選択して新規に Virtual Server を構成し、以下の設定を行います。

- Destination Address/Mask: "0.0.0.0/0"を指定
- Service Port: 通常は"443" (HTTPS) を指定
- SSL Profile (Client): "SSL プロファイル設定"の項で作成した Client SSL Profile を指定
- SSL Profile (Server): "SSL プロファイル設定"の項で作成した Server SSL Profile を指定
- Source Address Translation: "Automap"もしくは"SNAT"を指定
- Address Translation: **無効** (チェックを外す)
- Port Translation: **無効** (チェックを外す)



3.4 アクセス確認

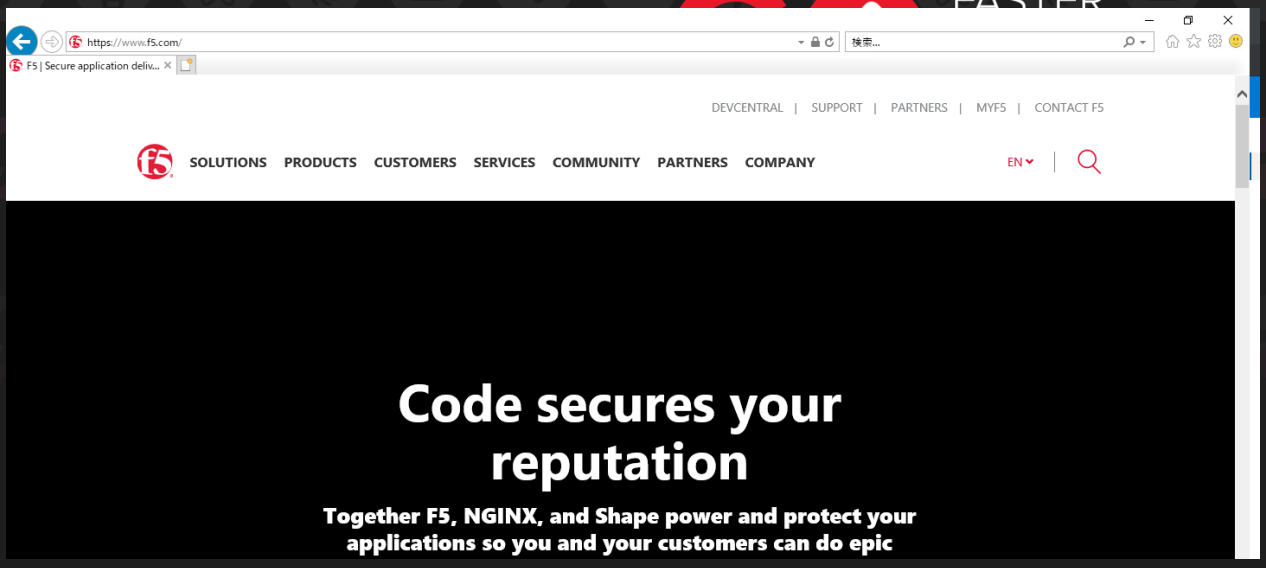
クライアント PC の Web ブラウザから正常にアクセスできることを確認します。この例では https://www.f5.com にアクセスします。

また、証明書の詳細を確認します。

"CA 証明書の設定例"の項で作成した証明書が利用されていることがわかります。

VLAN and Tunnel Traffic	All VLANs and Tunnels
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

FASTER



F5 Networks, Inc. | f5.com

US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com
©2017 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. These training materials and documentation are F5 Confidential Information and are subject to the F5 Networks Reseller Agreement. You may not share these training materials and documentation with any third party without the express written permission of F5.

証明書
全般
詳細
証明のパス
証明のパス(P)
proxy_ca.example.com
author-www.f5.com
証明書の表示(V)
証明書の状態(S):
この証明書は問題ありません。
OK