Getting Started with BIG-IP APM SWG
Follow-Along Lab Guide

INTRODUCTION

The following lab instructions are meant to be used alongside the BIG-IP APM SWG Web-Based Training. Although there is currently no formal lab associated with the WBT, it is hoped that you—the viewer—have access to a BIG-IP with APM and SWG licenses and that you would follow along on your BIG-IP. The WBT has been designed so you can follow along without these instructions, but the author is hoping these instructions will make it easier and will encourage you to take a hands-on approach to the WBT.

LESSON 3 LAB, PART 1: CERTIFICATE CONFIGURATION

In this section of the lab we're going to create a self-signed Certification Authority cert that we will then use to sign our host cert.

Step 1: We're going to shorten the BASH and TMSH prompts, so the command lines will be easier to read

```
PS1="bash1# "

tmsh
edit cli preference all-properties
```

Change the prompt value to the keyword none, like this: **`prompt none`**

Step 2: Create a temporary workspace

```
mkdir /tmp/cert

cd /tmp/cert
```

Step 3: Create a random number and use that number to create a key for the CA cert

```
openssl rand -out random1 2048

openssl genrsa -rand random1 -out ca-f5trn-com.key 2048
```

Step 4: Create a CA cert

The following command will prompt you for a number of values. You can either provide values or leave them blank. You must enter a value of **ca.f5trn.com** for **Common Name**

```
openssl req -x509 -new -key ca-f5trn-com.key -out ca-f5trn-com.crt -days 365
```

Step 5: Install the CA key and cert on BIG-IP

```
tmsh install sys crypto key  ca-f5trn-com.key from-local-file ca-f5trn-com.key

tmsh install sys crypto cert ca-f5trn-com.crt from-local-file ca-f5trn-com.crt
```

Step 6: Create a CA cert and import it into the Windows client

You will be prompted for an export password. Make it blank by pressing return at the prompt and the verification prompt.

```
openssl pkcs12 -export -in ca-f5trn-com.crt -inkey ca-f5trn-com.key
-out ca-f5trn-com.p12 -name "f5trn CA"
```

A CA cert is only useful if a browser trusts the CA. Copy the cert to the Windows client. Double click the cert to import it into Windows. When prompted, place the cert in the **Trusted Root Certification Authorities** certificate store

Step 7: Create a random number and use that to create a key for the logon cert

```
openssl rand -out random2 2048

openssl genrsa -rand random2 -out logon-f5trn-com.key 2048
```

Step 8: Create a request for the logon cert

The following command will prompt you for a number of values. You can either provide values or leave them blank. You must enter a value of **logon.f5trn.com** for **Common Name** and leave the “extra” attributes blank, including the challenge password, by pressing return at the prompt

```
openssl req -new -out logon-f5trn-com.req -key logon-f5trn-com.key
```

Step 9: Sign the logon cert request with the f5trn CA cert

```
openssl x509 -req -in logon-f5trn-com.req -out logon-f5trn-com.crt
-CAkey ca-f5trn-com.key -CA ca-f5trn-com.crt -days 365
-CAcreateserial -CAserial serial
```

Step 10: Install the key and cert on BIG-IP

```
tmsh install sys crypto key  logon-f5trn-com.key
from-local-file logon-f5trn-com.key

tmsh install sys crypto cert logon-f5trn-com.crt
from-local-file logon-f5trn-com.crt
```

LESSON 3 LAB, PART 2: CLIENT SSL PROFILE CONFIGURATION

In this section of the lab we're going to create both a client and a server SSL profile to be used with the virtual servers that will be created lated.

Step 1: Create a client-facing SSL profile using the CA cert with SSL forward proxy bypass enabled
Navigate to **Local Traffic ›› Profiles ›› SSL ›› Client**

Name	**transp-prx-client.ssl**
SSL Forward Proxy (Mode)	**Advanced**
SSL Forward Proxy	**Enabled**
CA Certificate	**ca-f5trn-com.crt**
CA Key	**ca-f5trn-com.key**
SSL Forward Proxy Bypass	**Enabled...**

Step 2: Create server-facing SSL profiles with forward proxy bypass enabled
Navigate to **Local Traffic ›› Profiles ›› SSL ›› Server**

Name	**transp-prx-server.ssl**
SSL Forward Proxy	**Enabled...**
SSL Forward Proxy Bypass	**Enabled...**

Step 3: Create a client-facing SSL profile for the captive logon page
Navigate to **Local Traffic ›› Profiles ›› SSL ›› Client**

Name	**transp-prx-logon-client.ssl**
Certificate	**logon-f5trn-com.crt**
Key	**logon-f5trn-com.key**

LESSON 3 LAB, PART 3: NETWORK CONFIGURATION

In this section of the lab we're going to add static host entries, configure DNS and default routes to both the BIG-IP and the Windows client

Step 1: Add the **logon.f5trn.com** static hostname to BIG-IP
Navigate to **System ›› Configuration ›› Devices ›› Hosts**

IP Address	**172.16.1.101**
Hostname	**logon.f5trn.com**

Step 2: Add a DNS server to BIG-IP
Navigate to **System ›› Configuration ›› Devices ›› DNS**

DNS Lookup Server Address	**172.16.1.254**

Step 3: Add a default route to BIG-IP
Navigate to **Network ›› Routes**

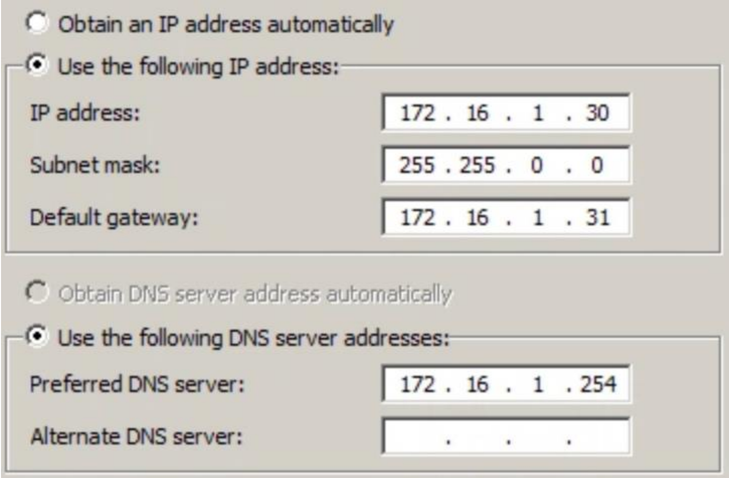
Name	**default.rt**
Destination / Netmask	**0.0.0.0 / 0.0.0.0**
Gateway IP Address	**10.10.1.254**

Step 4: Add the **logon.f5trn.com** static hostname to the Windows client

Logged in as **Administrator**, use **Notepad** to edit **C:\Windows\System32\drivers\etc\hosts**
Add the following line:

```
172.16.1.101        logon.f5trn.com
```

Step 5: Add the following default route and DNS server to the Windows client



○ Obtain an IP address automatically
● Use the following IP address:
IP address: 172 . 16 . 1 . 30
Subnet mask: 255 . 255 . 0 . 0
Default gateway: 172 . 16 . 1 . 31

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 172 . 16 . 1 . 254
Alternate DNS server: . . .

LESSON 4 LAB: HTTP AND HTTPS FORWARDING VIRTUAL SERVER CONFIGURATION

In this lab we're going create two forwarding virtual servers for our transparent proxy

Step 1: Create a forwarding virtual server for port 80
Navigate to **Local Traffic ›› Virtual Servers**

Name	**transp-prx-fw-80.vs**
Destination Network	**0.0.0.0/0**
Destination Port	**80**
Configuration (Mode)	**Advanced**
HTTP Profile	**http**
Source Address Translation	**Auto Map**
Address Translation	**Disabled**

Step 2: Create a forwarding virtual server for port 443
Navigate to **Local Traffic ›› Virtual Servers**

Name	**transp-prx-fw-443.vs**
Destination Network	**0.0.0.0/0**
Destination Port	**443**
Configuration (Mode)	**Advanced**
HTTP Profile	**http**
SSL Profile (Client)	**transp-prx-client.ssl**
SSL Profile (Server)	**transp-prx-server.ssl**
Source Address Translation	**Auto Map**
Address Translation	**Disabled**

Step 3: Test

LESSON 5 LAB, PART 1: USER DATABASE AND USER CONFIGURATION

In this section of the lab we're going to create a local user database instance and create a local user in that database.

Step 1: Create a local user database instance
Navigate to **Access Policy ›› Local User DB ›› Manage Instances**

Name	**user.db**

Step 2: Create a local user
Navigate to **Access Policy ›› Local User DB ›› Manage Users**

User Name	**student1**
Password	**student1**
Instance	**/Common/user.db**

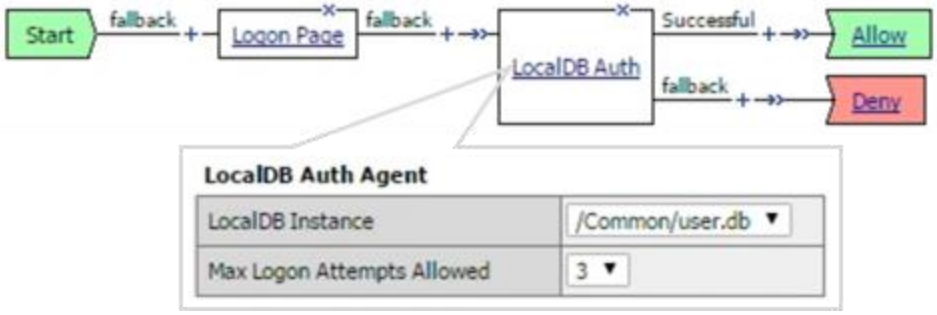
LESSON 5 LAB, PART 2: ACCESS POLICY CONFIGURATION

In this section of the lab we're going to create an access profile and then edit the associated access policy to provide captive portal functionality

Step 1: Create an access profile
Navigate to **Access Policy ›› Access Profile**

Name	**transp-prx.ap**
Profile Type	**SWG-Transparent**
Captive Portals	**Enabled**
Primary Authentication URI	**https://logon.f5trn.com**
Accepted Language	**English (en)**

Step 2: Edit the access policy to look like the following



LocalDB Auth Agent

LocalDB Instance	/Common/user.db ▼
Max Logon Attempts Allowed	3 ▼

LESSON 5 LAB, PART 3: CAPTIVE PORTAL VIRTUAL SERVER CONFIGURATION

In this section of the lab we're going to create a captive portal virtual server

Step 1: Create a virtual server
Navigate to **Local Traffic ›› Virtual Servers**

Name	**transp-prx-logon.vs**
Destination Network	**172.16.1.101**
Destination Port	**443**
HTTP Profile	**http**
SSL Profile (Client)	**transp-prx-logon-client.ssl**
Access Policy	**transp-prx.ap**

Step 2: Modify virtual server **transp-prx-fw-80.vs**
Navigate to **Local Traffic ›› Virtual Servers**

Access Policy	**transp-prx.ap**

Step 3: Modify virtual server **transp-prx-fw-443.vs**
Navigate to **Local Traffic ›› Virtual Servers**

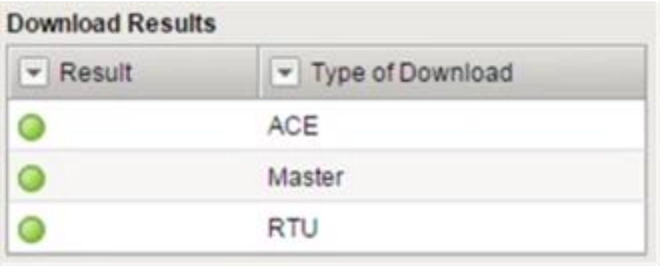
Access Policy	**transp-prx.ap**

Step 4: Test

LESSON 6 LAB, PART 1: WEBSENSE IPI DATABASE CONFIGURATION AND CONFIRMATION

In this section of the lab we're going to download the WebSense database and test to confirm it has loaded correctly

Step 1: Download the database
Navigate to **Access Policy ›› Secure Web Gateway ›› Database Settings ›› Database Download**



Download Results

Result	Type of Download
●	ACE
●	Master
●	RTU

Once the database download has completed, you should see the above download results

Step 2: Test several URLs
Navigate to **Access Policy ›› Secure Web Gateway ›› Database Settings ›› URL Category Lookup**
Try several URLs and determine if they are categorized correctly

LESSON 6 LAB, PART 2: URL FILTER CONFIGURATION

In this section of the lab we're going to create and edit a URL filter that will block traffic that does not match our fictitious corporate Internet Acceptable Use Policy.

Step 1: Create a URL Filter
Navigate to **Access Policy ›› Secure Web Gateway ›› URL Filters**

Name	**block-non-acceptable.urlf**

Step 2: Note the filtering actions already assigned to **Adult Material, Drugs, Extended Protection,** etc. For most categories, either Allowed or Blocked, you can drill into sub-categories by click the **plus sign** next to the category

Step 3: Select the **checkbox** next to the **Bandwidth** category

Step 4: Scroll to the bottom of the list and click **Block**

Step 5: Now click the **plus sign** next to the **Bandwidth** category

Step 6: Select the **checkbox** next to the **Educational Video** sub category

Step 7: Scroll to the bottom of the list and click **Allow**

Step 8: Review the categories and sub-categories of your newly created **URL Filter**

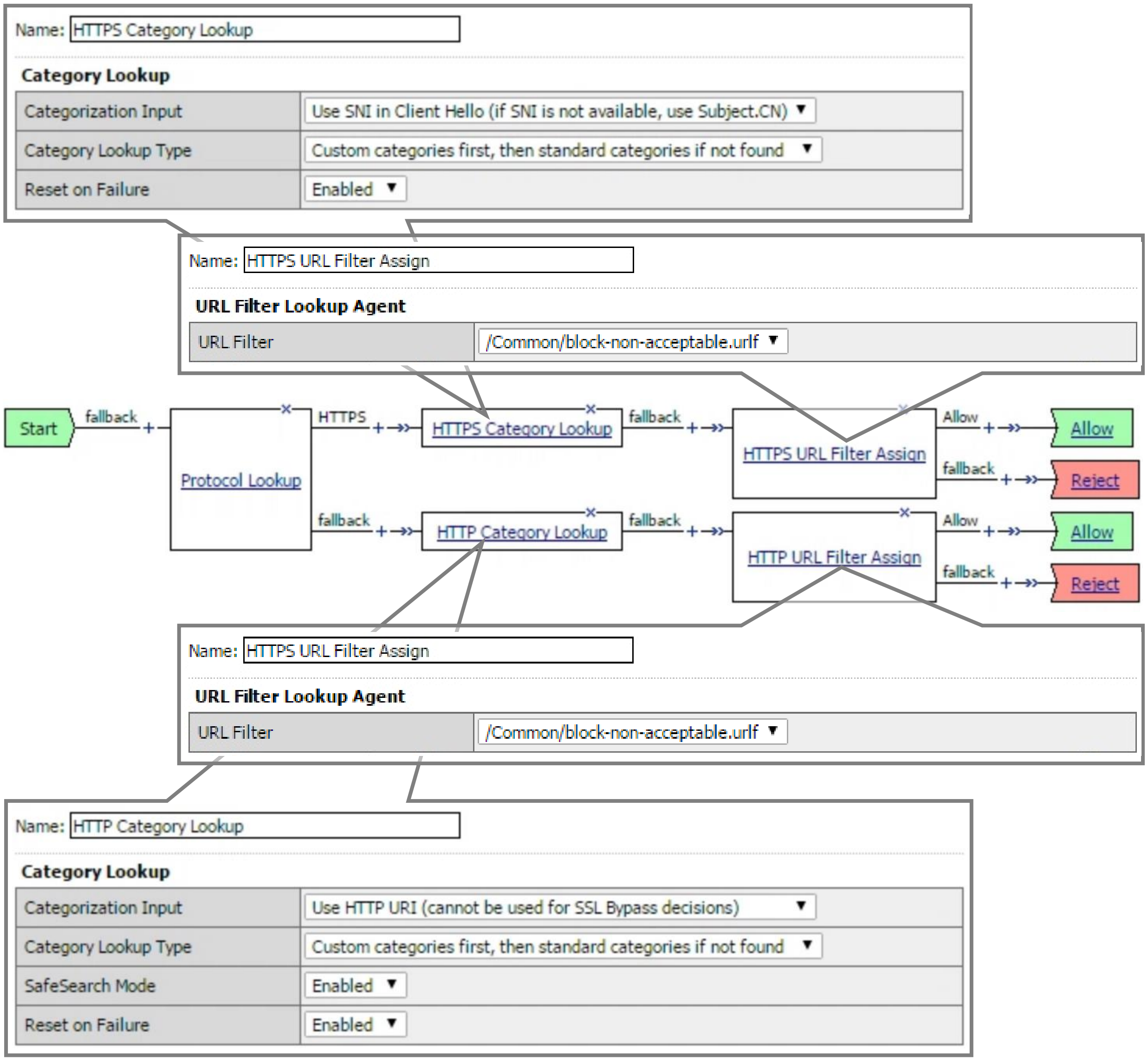
LESSON 6 LAB, PART 3: PER-REQUEST POLICY CONFIGURATION

In this section of the lab we're going to create and edit a per-request policy that will inspect each request and determine if it should be allowed or rejected

Step 1: Create a per-request policy
Navigate to **Access Policy ›› Per-Request Policy**

Name	`transp-prx.prp`

Step 2: Edit the per-request policy to look like the following
Note the HTTPS and HTTP Category Lookup agents were originally name **Category Look**
Note the HTTPS and HTTP URL Filter Assign agents were originally named **URL Filter Assign**
Note if you are using version 12.1, delete the "Confirm" branches from the **URL Filter Assign** agents



Name: HTTPS Category Lookup

Category Lookup

Categorization Input	Use SNI in Client Hello (if SNI is not available, use Subject.CN) ▼
Category Lookup Type	Custom categories first, then standard categories if not found ▼
Reset on Failure	Enabled ▼

Name: HTTPS URL Filter Assign

URL Filter Lookup Agent

URL Filter	/Common/block-non-acceptable.urlf ▼

Name: HTTPS URL Filter Assign

URL Filter Lookup Agent

URL Filter	/Common/block-non-acceptable.urlf ▼

Name: HTTP Category Lookup

Category Lookup

Categorization Input	Use HTTP URI (cannot be used for SSL Bypass decisions) ▼
Category Lookup Type	Custom categories first, then standard categories if not found ▼
SafeSearch Mode	Enabled ▼
Reset on Failure	Enabled ▼

LESSON 6 LAB, PART 4: VIRTUAL SERVER CONFIGURATION

In this section of the lab we're going to modify the forwarding virtual servers to use the per-request policy

Step 1: Modify virtual server **transp-prx-fw-80.vs**
Navigate to **Local Traffic ›› Virtual Server**

Per-Request Policy	**transp-prx.prp**

Step 2: Modify virtual server **transp-prx-fw-443.vs**
Navigate to **Local Traffic ›› Virtual Servers**

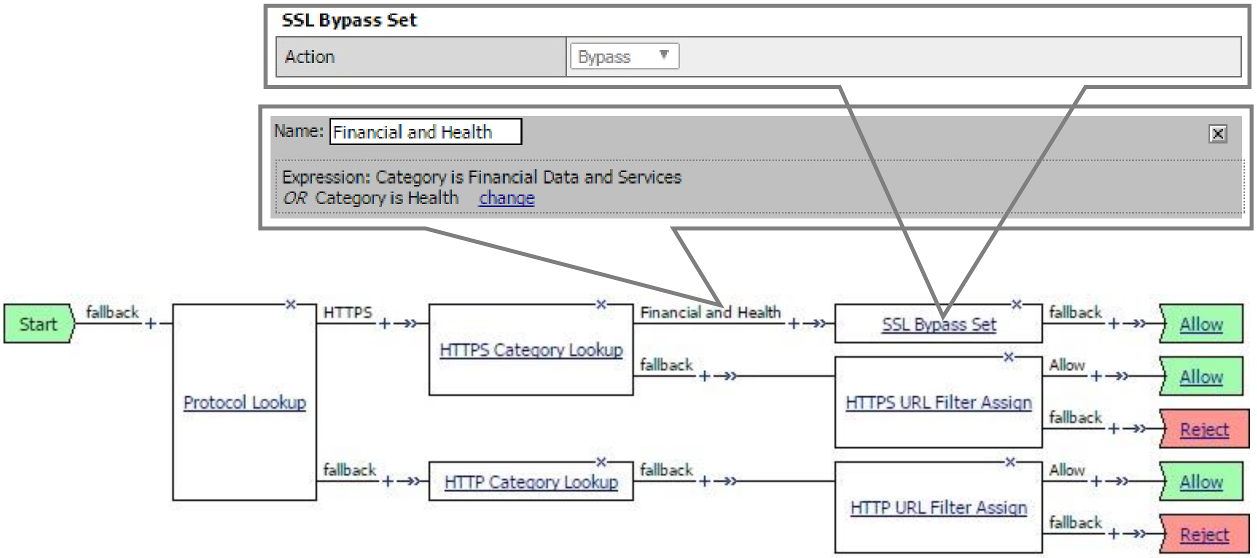
Per-Request Policy	**transp-prx.prp**

Step 3: Test

LESSON 7 LAB: SSL BYPASS CONFIGURATION

In this lab we're going to modify the per-request policy to include an SSL bypass for URLs that are categorized as banking or health

Step 1: Modify the existing per-request policy to look like the following



SSL Bypass Set

Action	Bypass

Name: Financial and Health

Expression: Category is Financial Data and Services
OR Category is Health change

Step 2: Test