Technical white paper

HP Access Control – Load Balancer Security in HP AC 16.7 and newer

Table of Contents

Overview

In an ongoing effort to increase security, HP Access Control (HP AC) version 16.7 and newer will no longer support a passthrough Network Load Balancer (NLB) configuration. HP AC now ensures that the IP address of the requestor matches the IP address in the request. For jobs that go through an NLB, a header is inserted so that the IP address of the original requesting client is preserved.

The order in which HP AC will resolve a requesting client's IP address is as follows:

1. HP AC will first look for an arbitrary HTTP Header named CLIENT-IP.

2. If Client-IP is not present, then the first IP address in the HTTP Header X-Forwarded-For.

3. If XFF is not present, then it will use the REMOTE_ADDR (which will be IP address the packet came from)

For this reason, HP AC Load balancer configurations will require, at a minimum, Client-IP or X-Forward-For configurations for the HTTPS virtual servers.

Additionally, because the packets are encrypted, the load balancer will need to decrypt the data, insert the appropriate header information, then re-encrypt it as it passes it on to the HP AC nodes. Therefore, the certificate used for HP AC, both the private and Public key certificate, needs to be imported into the load balancer and assigned to the HTTPS virtual server.

Below is an example of what the HTTP header would appear with Client -IP and or X-Forward-For enabled.

Note: The sections below are intended to provide information on where to apply the settings discussed above for both the F5 and NetScaler. Any changes made to production environments should be done by the customer with the approval of the appropriate IT administrators.

Citrix NetScaler

Certificate

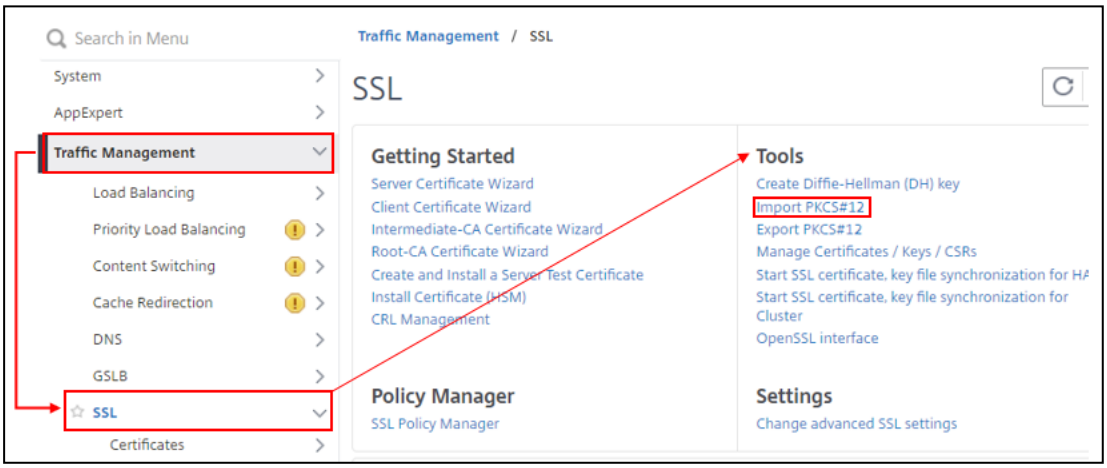
To allow the load balancer to decrypt and re-encrypt traffic, the certificate used by HP AC must be applied to the SSL Service Group.

First import the HP AC certificate (root CA) into the Citrix NetScaler

Note: this document assumes administrators already have the .PFX containing the public and private key along with the associated password.

1. Navigate to **Traffic Management > SSL > Tools**

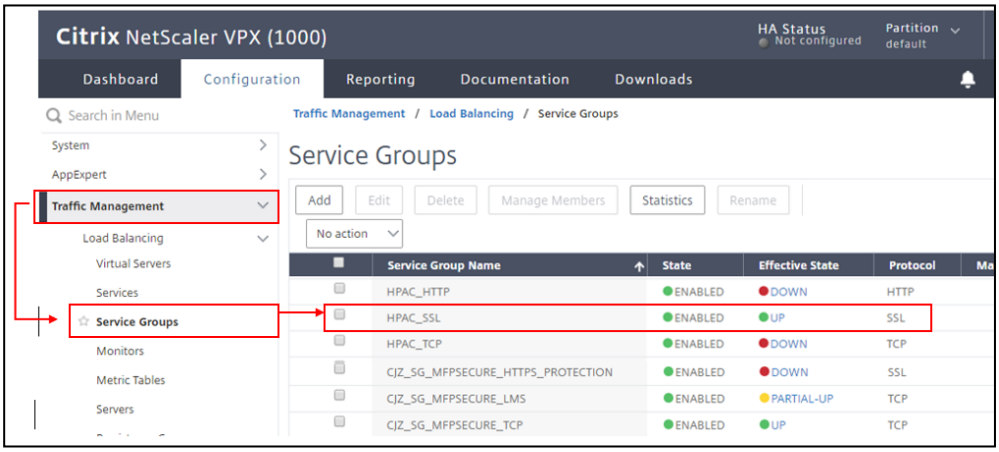
2. Select **Import PKCS#12** from the **Tools** menu



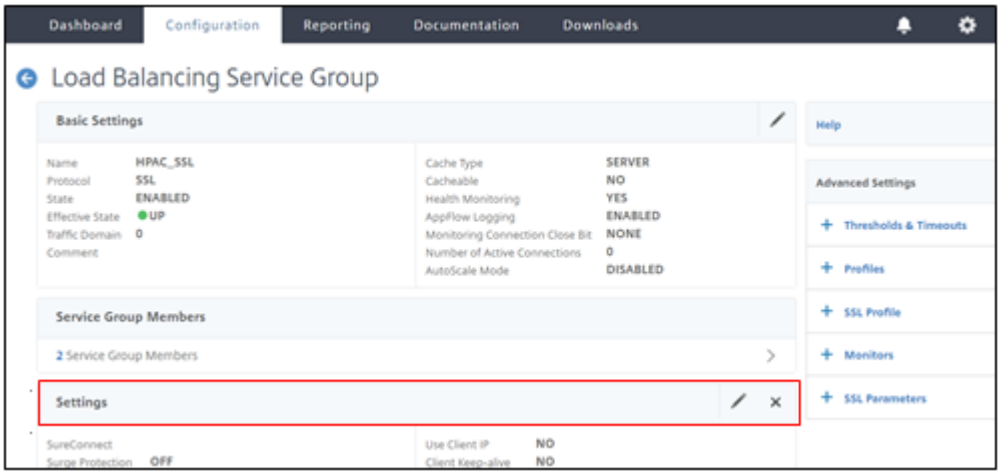
Citrix NetScaler Service Groups

For the NetScaler, the Client-IP setting is made in the Service Group settings page

1. Navigate to Traffic Management – Service Groups



2. Edit **Settings**



3. Select the Client-IP Check box and add “Client-IP” in the Header section

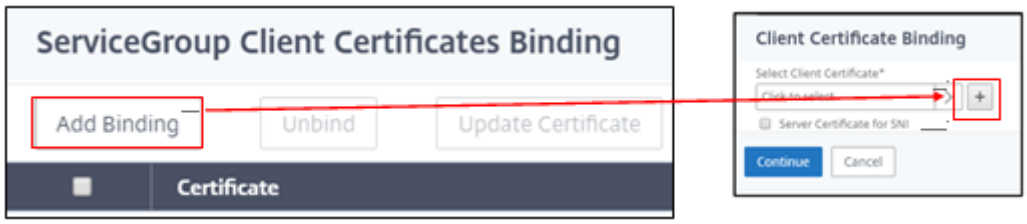
   To use the X-Forward Setting, use “X-Forwarded-For” in the header section

From the steps above, you will be in the SSL Service Group.

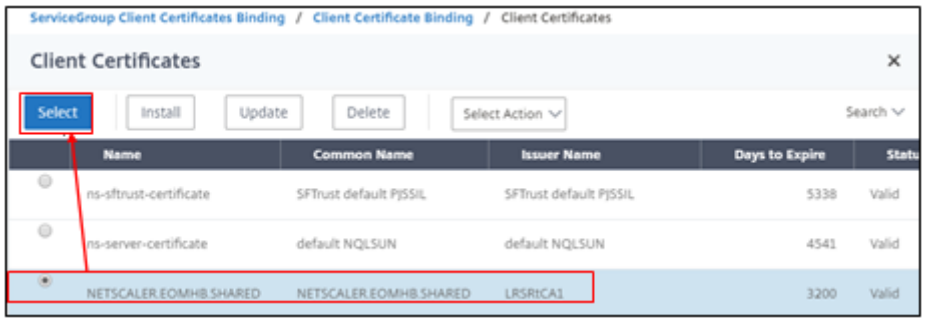
4. On the Basic Settings Page, Select the Plus sign next to Certificates on the Right-hand tool bar

5. Select the arrow to the right of Client Certificate

6. A pop up will appear for Client Certificate binding- Select Add Binding then select the arrow on the following pop-up



7. The Client Certificate list appears- Locate and select the correct certificate, then press the Select button in the upper left

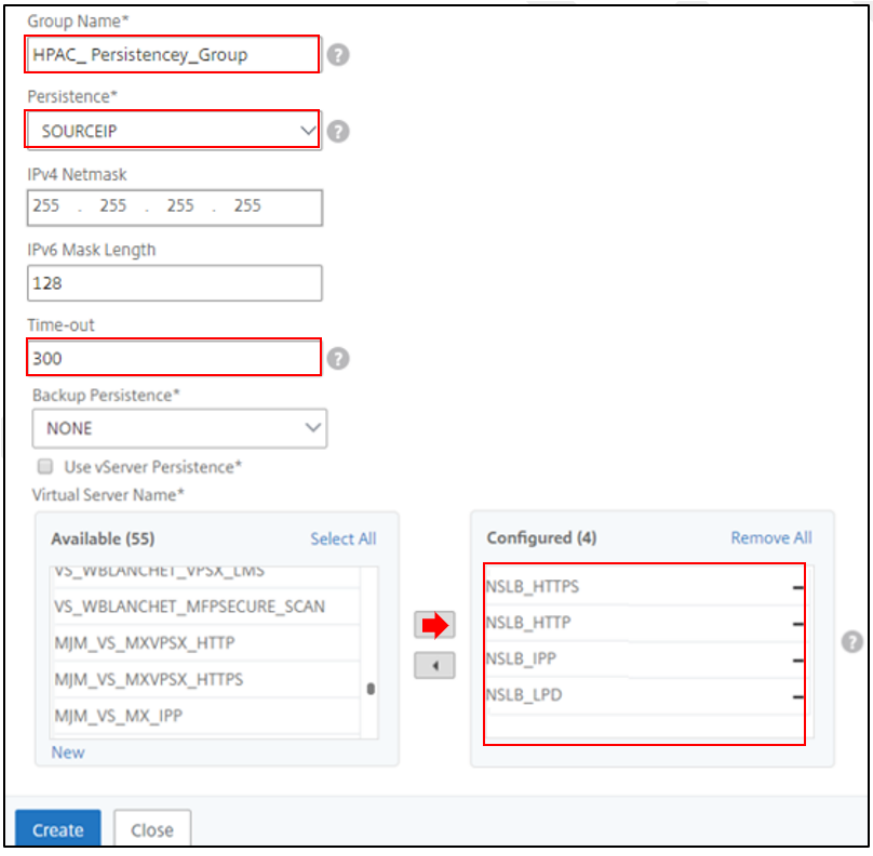


Session Persistence

Best practice in HP AC is ensuring the load balancer virtual server's session persistence is set with a value high enough to prevent conflicts with end user during an HP AC associated interaction.

For NetScaler, the settings are completed with Persistency Groups

1. Navigate to Traffic Management-Persistency Groups
2. Select **Add**
3. Provide a name for the group
4. In Persistence select **SOURCEIP**
5. Set the Time-Out to a minimum of **300 (seconds)**
6. In the Virtual Servers box, add all of the HP AC virtual servers
7. Select Create in the bottom left



F5 Load Balancers

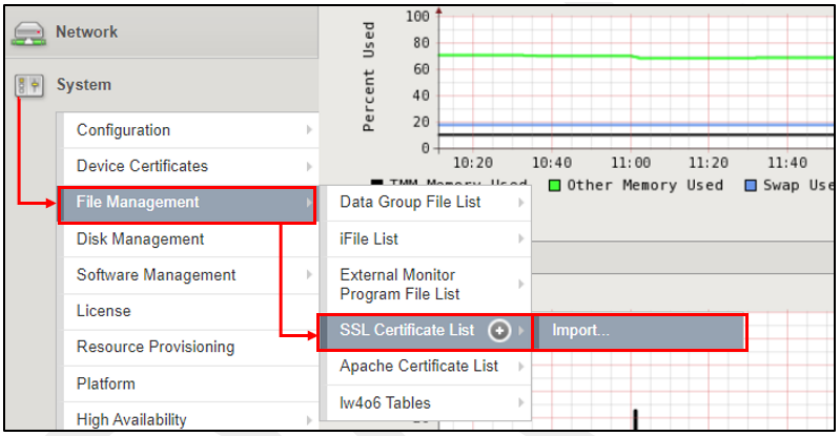
For the F5 configuration the HTTP profile is how the Client_IP or X-Forwarded-For settings are applied. The SSL profile (s) is where the certificate(s) used by HP AC are applied. These profiles are then applied to the virtual servers created for HP AC.

In this version of F5 (BIG-IP 12.1.2 Build 0.0.249), the Profile section is located under Local Traffic from the left-hand main menu section.

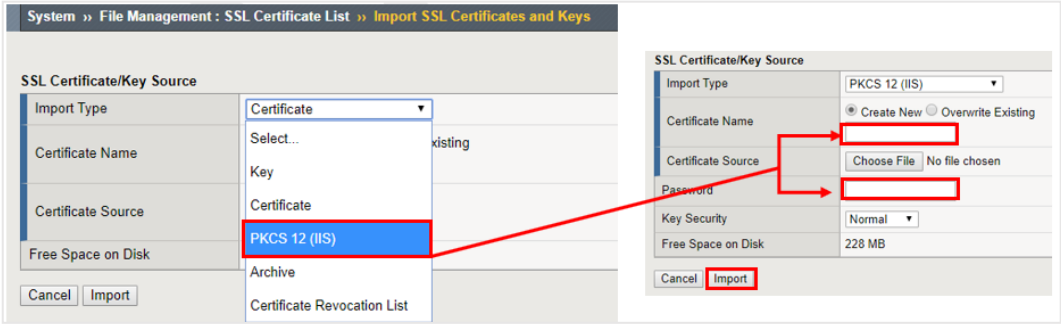
Importing the HP AC Certificate to the F5

Add the Certificate used by HP AC. Normally this will be the root CA if using a signed certificate. If using a self-signed certificate created by HP AC, the certificate PFX file will be in the root of HP AC with the NLB virtual hostname as the friendly name.

1. Navigate to **System – File Management – SSL Certificate List – Import**



2. From the drop-down list, select the **PKCS 12** option.
3. In the following pop-up, create a **Certificate name** and add the **Password** then click **Import**

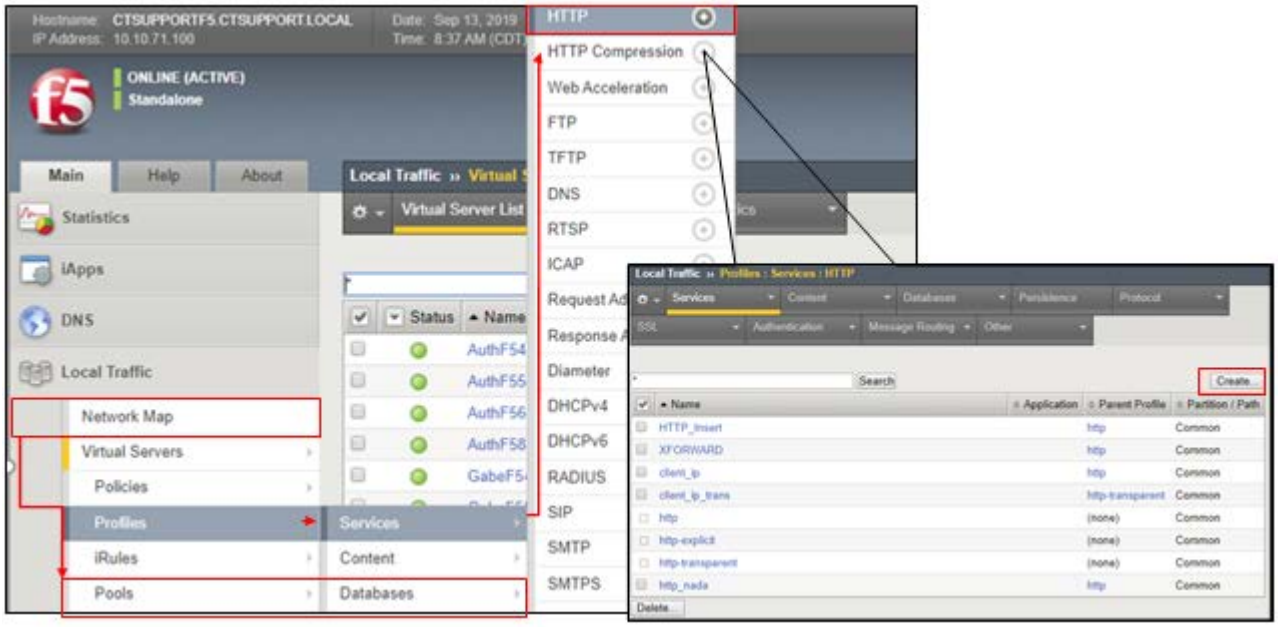


Once successful and the certificate appears in the SSL Certificate list, create the HTTP profile.

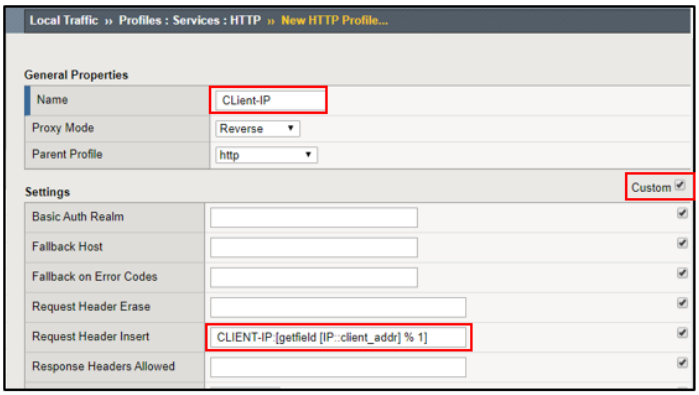
F5- Client-IP HTTP Profile

The first profile will be the HTTP profile for Client-IP

1. Expand Local Traffic-Profiles-Services-HTTP
2. In the HTTP window, select Create from the right

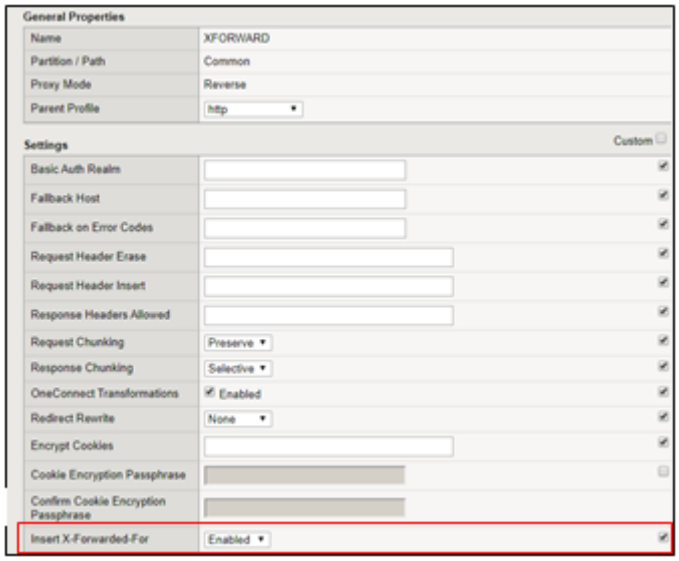


3. Provide a name for the profile and under **Settings**, check the **Custom** box from the left.
4. In the **Request Header Insert** field add the following syntax- *CLIENT-IP:[getfield [IP::client_addr] % 1]*
5. The remainder of the settings can be left as default- Select **Update** at the bottom of the page.



F5- X-Forwarded-For HTTP Client Profile

Alternatively, the X-Forwarded-For profile can be used. Follow the same steps above but instead of using Request Header Insert field, enable the Insert X-Forwarded-For option further down in the settings section

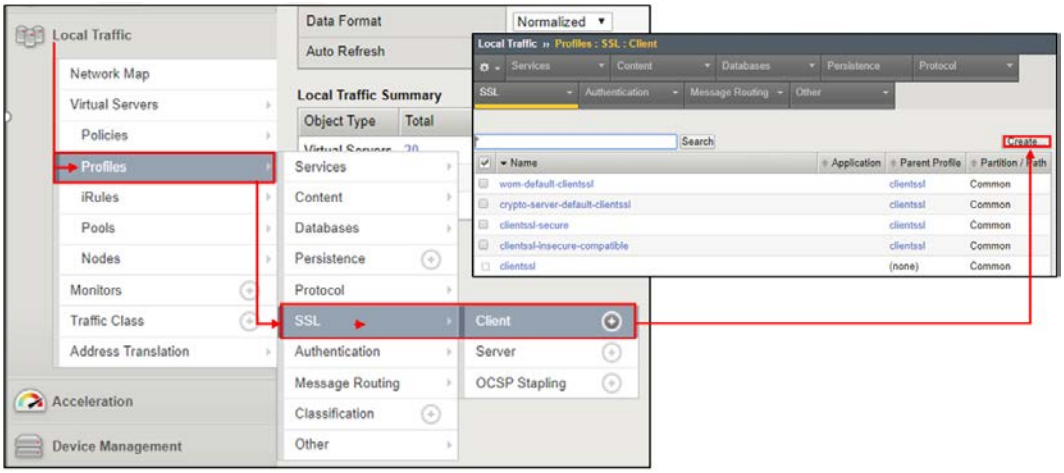


F5 - SSL Client and Server Certificate Profiles

As discussed at the beginning of this white paper, the HP AC certificates need to be applied to allow the load balancer to open the encrypted packets, insert header information, and re-encrypt before forwarding on to the HP AC Pull Print nodes.

1. Navigate to Local Server-Profiles-SSL-Client

2. Click Create on the right of the new SSL Client window



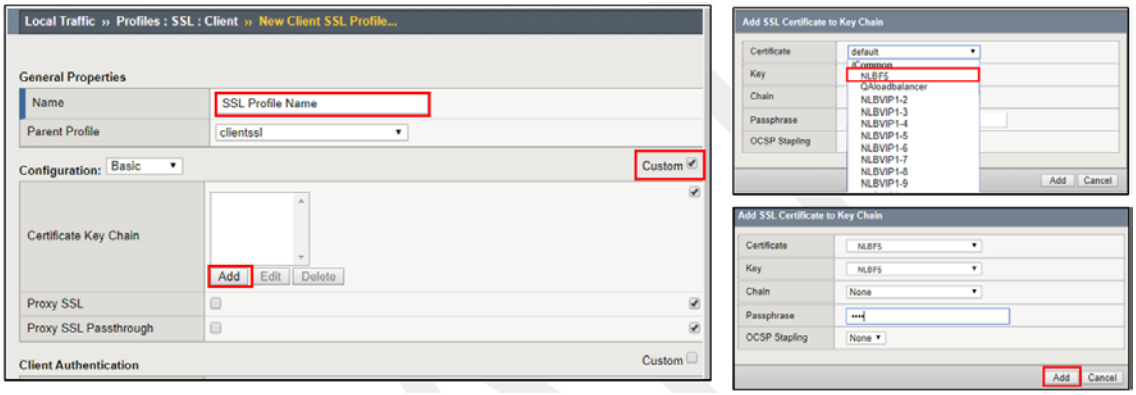
3. Create a Profile name then check the **Custom** box on the left

4. The Certificate key Chain configuration becomes available, click **Add**

5. Select the appropriate certificate from the drop-down. Provide the passphrase if required.

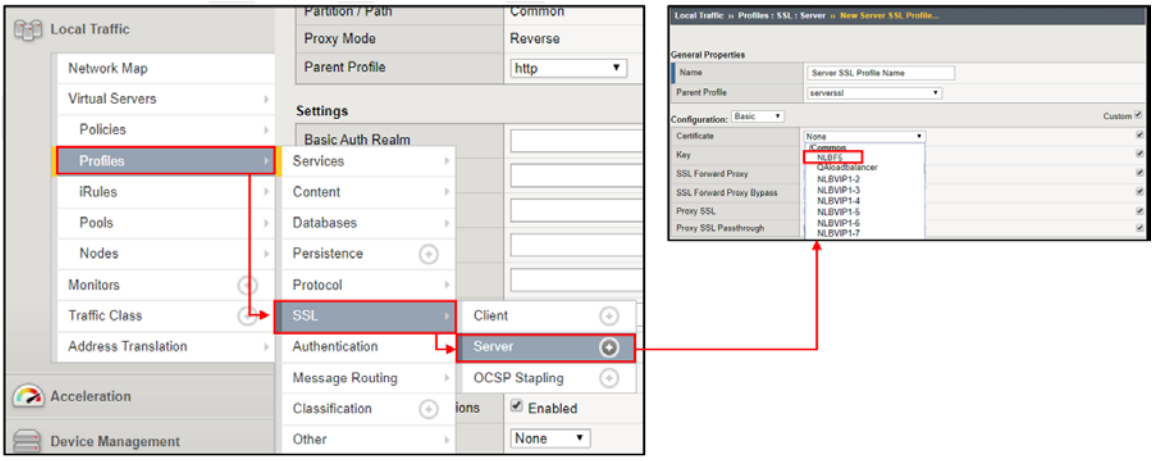
6. Click **Add** when complete

   Note: If a PFX file was originally imported into the F5 then the certificate name may appear the same. Otherwise you may have a Key (Root CA) with a different name than the certificate.



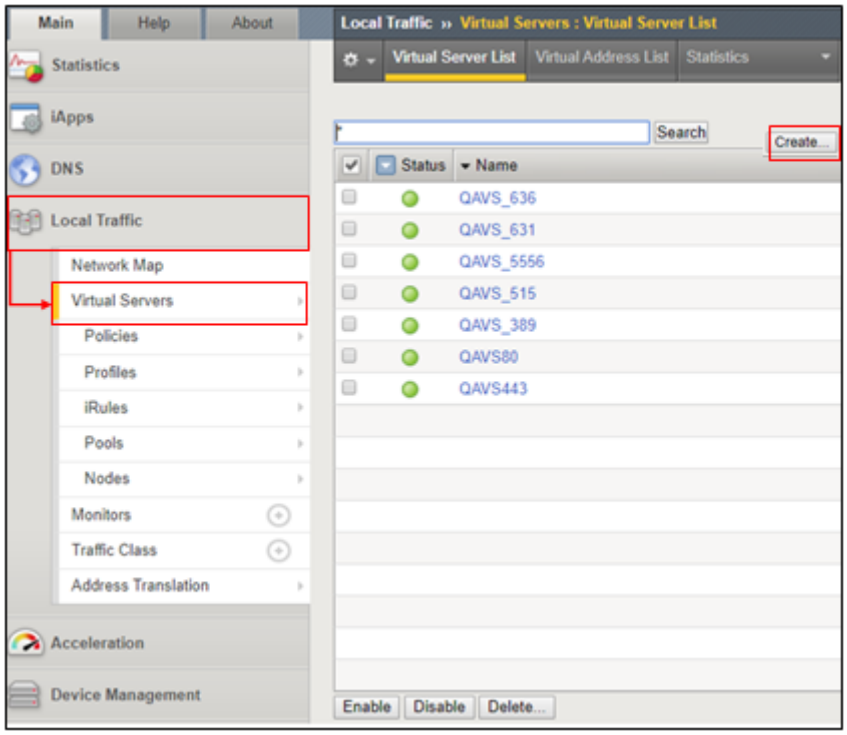
7. Follow step 2 above but select **Server** this time instead of **Client**

8. Complete the remaining steps 3-6 to add the certificates to the SSL Server Profile.



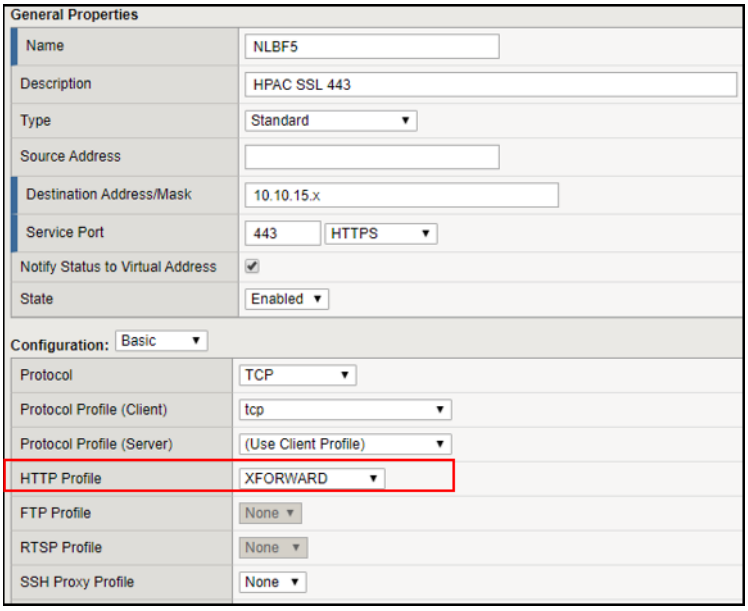
Now that the profiles have been created, they can be assigned to the SSL virtual server

1. Select Local Traffic-Virtual Servers and Edit or Create the SSL Virtual Server



2. If the virtual server currently exists, navigate to the configuration section.

3. Locate the HTTP Profile and select either the Client-IP or X-Forward profile created earlier in this white paper.



4. Next, navigate further down to the Server and Client SSL Profile and move the proper certificate profiles to the selected box

5. Select **Update** at the bottom of the page.

Session Persistence

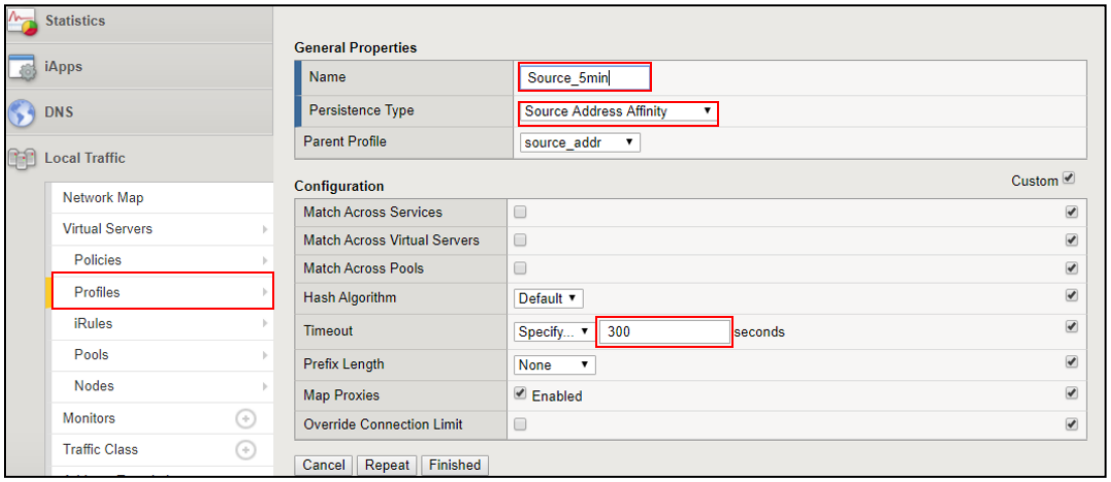
Best practice in HP AC is ensuring the load balancer virtual server's session persistence is set with a value high enough to prevent conflicts with end user during an HP AC associated interaction.

To create the Persistence Profile, Navigate to Local Traffic- Profiles- Persistence

1. Select **Create** on the right
2. Persistence Type - **Source Address Affinity**
3. Select **Custom** to enable the configuration options
4. Set the Timeout value to minimum of 300 (5 minutes)

   NOTE: Administrators may choose a different value however, best practice is a minimum of 5 minutes

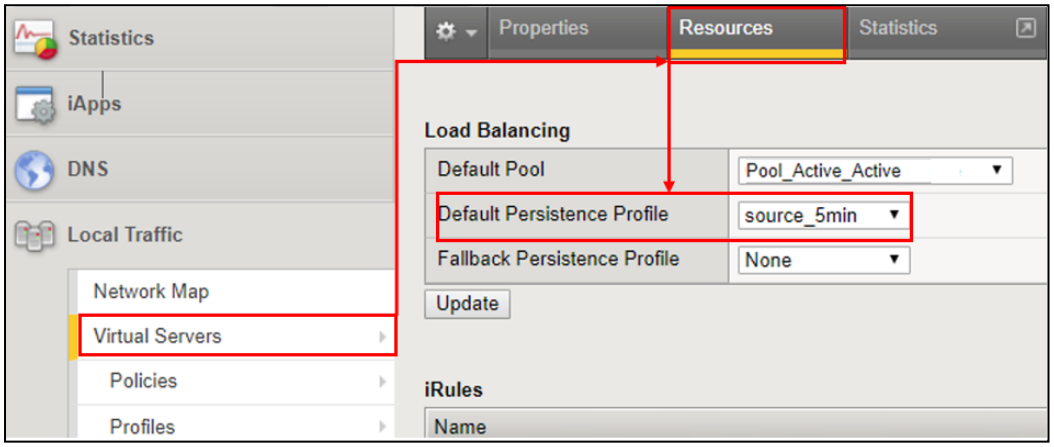
   NOTE: "Source_5min" is used here as an example only.



For F5, the Persistence profile is applied in each virtual server

1. Navigate to Local Traffic-Virtual Servers
2. Select the first HP AC virtual server
3. Select **Resources** tab at the top
4. Set the **Default Persistence Profile**

   NOTE: "source_5min" is used here as an example only.



hp.com/go/support

Current HP driver, support, and security alerts
delivered directly to your desktop

Created September 2019