

Configuration guide for an F5 LTM v16 for Load Balancing
USS Gateway Proxies.

Contents

Step 1. Preparing everything.	2
Step 2. Configuring the Primary Proxy.	3
Step 3. Configuring the Secondary Proxy	7
Step 4. Configuring your F5 LTM	11



Please note, this document is intended as a rough guide for preparing an F5 LTM for Load Balancing Censornet USS Gateway proxies. Please contact your F5 provider for assistance with the best practices or troubleshooting this setup.

Instructions on installing the Censornet Cloud USS proxies are outside of the scope of this document. The instructions can be found here:

<https://help.clouduss.com/gateway/uss-gateway-installation>



Step 1. Preparing everything.

In order for load balancing of the USS proxies to work, you have to ensure that both are using the same SSL configuration and duplicate the authentication configuration between them. This guide will assume you are load balancing only two proxies. However, you can add more if you wish.

You will need:

- Two USS proxy servers.
- Three static IP addresses.
- An SSL certificate generated on one of the proxies.
- Kerberos keys generated on one of the proxies.

For our example, we will be using the following IP addresses:

- Primary: 10.10.10.5
- Secondary: 10.10.10.6
- Load Balancer: 10.10.10.10

We will also be using the following hostnames:

- gateway1.domain.local
- gateway2.domain.local
- filter.domain.local

Ultimately we will end up with a configuration of:

- gateway1.domain.local on 10.10.10.5
- gateway2.domain.local on 10.10.10.6
- filter.domain.local on 10.10.10.10

However please note that during the configuration we will have to configure the proxies with the details for filter.domain.local and then change it afterwards. This is due to Kerberos using the hostname as part of it's hashing algorithm.



Step 2. Configuring the Primary Proxy.

This first proxy will be our primary proxy and used to generate the Kerberos keys and the SSL certificate.

Build the proxy as per the installation instructions linked above, but with the hostname and IP address that will become our load balancer hostname and IP address. So give it the hostname filter.domain.local and the IP address 10.10.10.10.

First, configure the IP address:

Configuration

Interface: ens160

Friendly name:

IP address (IPv4):

Netmask:

Then configure the hostname (please note, this is the SHORT hostname you need to use here):

Network Settings

Default Gateway:

Primary DNS:

Secondary DNS:

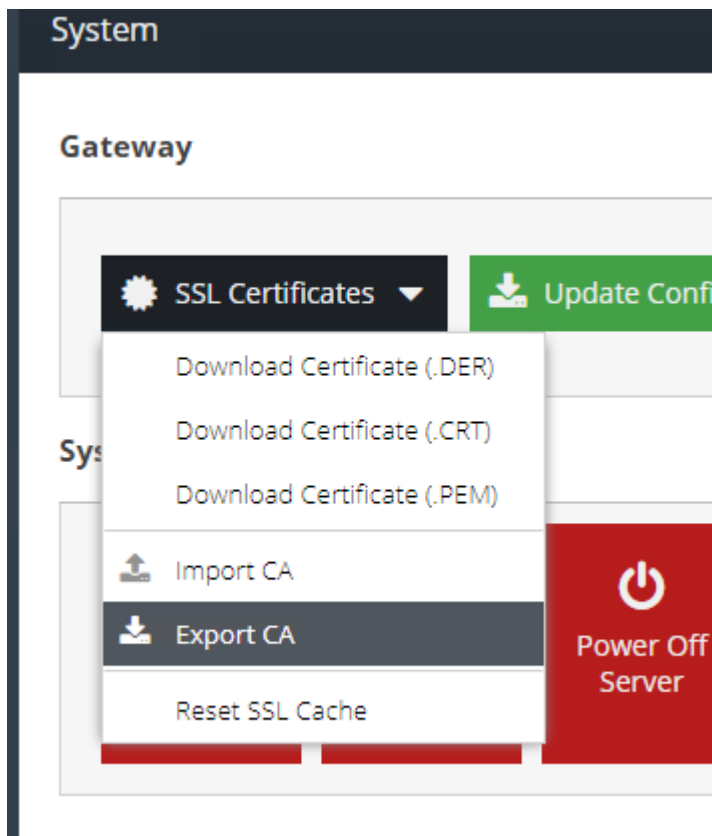
Hostname:

Agent name (leave blank to default to hostname):



Reboot the proxy to ensure that these settings take effect. This is very important, as we will be generating the Kerberos keys using this hostname.

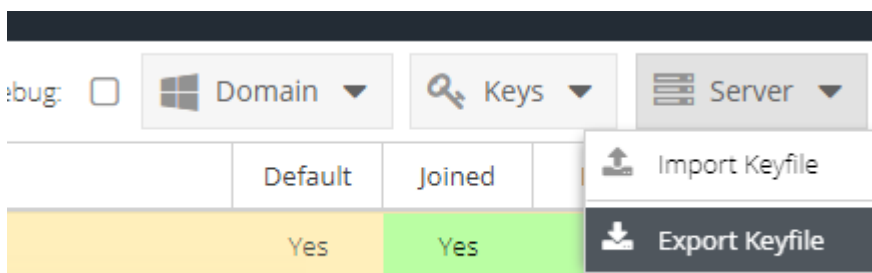
Next, export the SSL CA Certificate:



Save this somewhere safe as you may need to use this again if any of the proxies fail for any reason in the future.

Now configure the authentication as per the instructions here:
<https://help.clouduss.com/configure/authentication-identification>

Once this is complete, export the Kerberos keys:





Again, please save this somewhere safe as you may need to reuse this at a later date.



Now, you need to configure this proxy with its final hostname and IP address – in the case of our example gateway1.domain.local and 10.10.10.5:

Configuration

 Save  Manage ▼


Interface: ens160

Friendly name:

IP address (IPv4):

Netmask:

Network Settings

 Save

Default Gateway:

Primary DNS:

Secondary DNS:

Hostname:


Agent name (leave blank to default to hostname):



Reboot the proxy again for this configuration to take effect.

Finally, configure the load balancer VIP setting. This is very important, and if you miss this step, it will not work:

Advanced

 Save

- Early Access:** Enable proxy version (includes web socket support)
- Reduce noise from background Web requests to increase performance and report visibility
- Reuse the same key when using temporary/ephemeral Diffie-Hellman key exchanges

Loadbalancer VIP:



Step 3. Configuring the Secondary Proxy.

Initially, the configuration here is identical to the primary proxy. You need to build it and configure it with the hostname and IP address that will ultimately become the load balancers.

So give it the hostname `filter.domain.local` and the IP address `10.10.10.10`.

First, configure the IP address:

Configuration

Interface: `ens160`

Friendly name:

IP address (IPv4):

Netmask:

Then configure the hostname (please note, this is the SHORT hostname you need to use here):

Network Settings

Default Gateway:

Primary DNS:

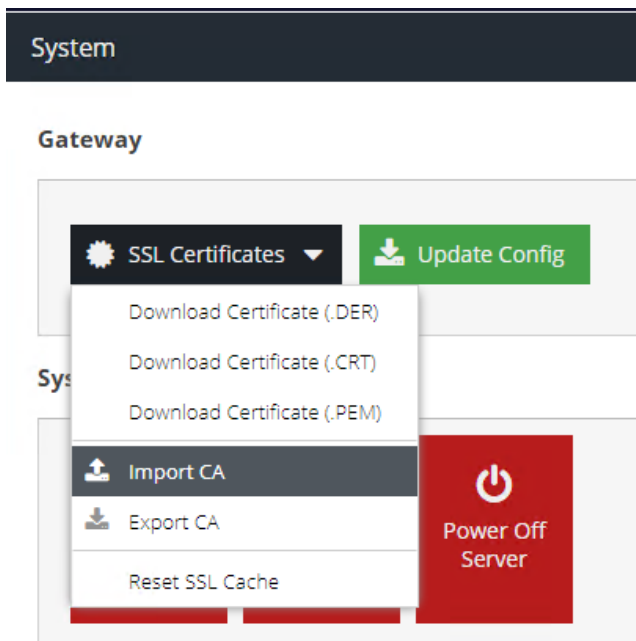
Secondary DNS:

Hostname:

Agent name (leave blank to default to hostname):



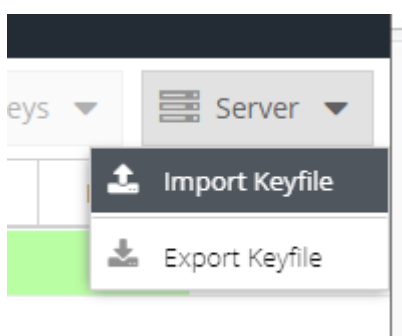
Next, you need to import the SSL CA certificate you exported earlier:



When this is done, you will again need to follow the instructions on joining the proxy to your active directory domain: <https://help.clouduss.com/configure/authentication-identification>

NB: It is very important that you DO NOT create the keys here, just create the domain configuration and join the proxy to it.


Once this is done, please import the keys you exported from the first proxy:






Next, you need to reconfigure the proxy to its final hostname and IP address. In this example, gateway1.domain.local and 10.10.10.6

Configuration

 Save

 Manage ▼

Interface: ens160

Friendly name:

Main


IP address (IPv4):

10.10.10.6

Netmask:

255.255.0.0

Network Settings

 Save

Default Gateway:

10.10.10.254

Primary DNS:

10.10.10.253

Secondary DNS:

Hostname:

gateway2


Agent name (leave blank to default to hostname):



Reboot the proxy for this to take effect.

Once it's back upon its new IP address, connect to it and configure the load balancer VIP setting with the IP address for the load balancer:

Advanced

 Save

- Early Access:** Enable proxy version (includes web socket support)
- Reduce noise from background Web requests to increase performance and report visibility
- Reuse the same key when using temporary/ephemeral Diffie-Hellman key exchanges

Loadbalancer VIP:

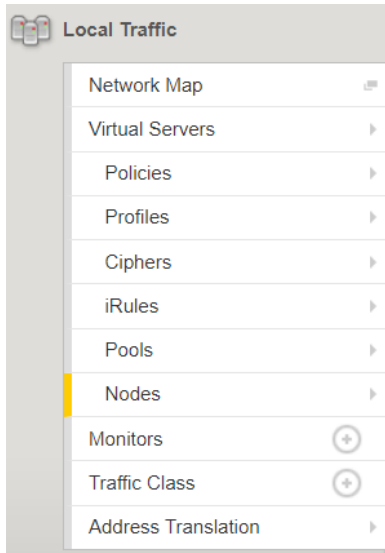


Step 4. Configuring your F5 LTM.

NOTE: You may need to consult your F5 partner or F5 documentation/support to assist with best practices for this setup and how to configure this for your environment, as Censornet cannot provide direct support for third-party software. This guide offers a configuration that will work for load balancing Censornet USS Gateways assumes that your F5 LTM environment is already set up ready for these steps.



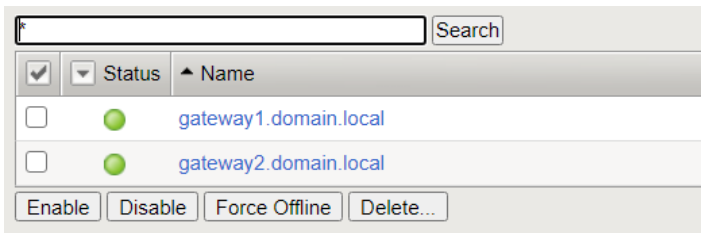
First, add the Censornet USS Gateways as Nodes on the F5 LTM. Navigate to LTM, Nodes



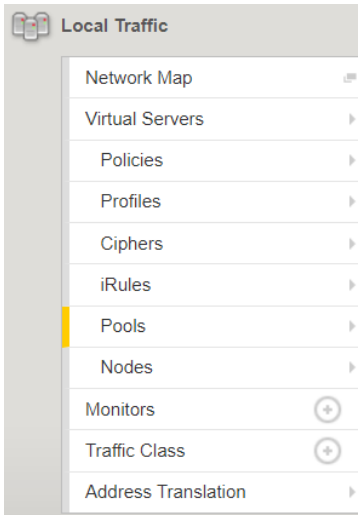
This will show the "Node List" page, now click the [Create...](#) in the far right-hand corner of the page, add both of the Censornet USS Gateway as shown below, select your required Health Monitor of choice. Click Finish to add the configuration.

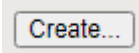
General Properties					
Name	gateway1.domain.local				
Description					
Address	<input checked="" type="radio"/> Address <input type="radio"/> FQDN 10.10.10.5				
Configuration					
Health Monitors	Node Specific				
Select Monitors	<table border="1"><thead><tr><th>Active</th><th>Available</th></tr></thead><tbody><tr><td>/Common gateway_icmp</td><td>/Common Port_8080 https_443 icmp real_server</td></tr></tbody></table>	Active	Available	/Common gateway_icmp	/Common Port_8080 https_443 icmp real_server
Active	Available				
/Common gateway_icmp	/Common Port_8080 https_443 icmp real_server				
Availability Requirement	All Health Monitor(s)				
Ratio	1				
Connection Limit	0				
Connection Rate Limit	0				
<input type="button" value="Cancel"/> <input type="button" value="Repeat"/> <input type="button" value="Finished"/>					

Both Gateways added.



Next, create a Pool on the F5 LTM. Navigate to LTM, Pools



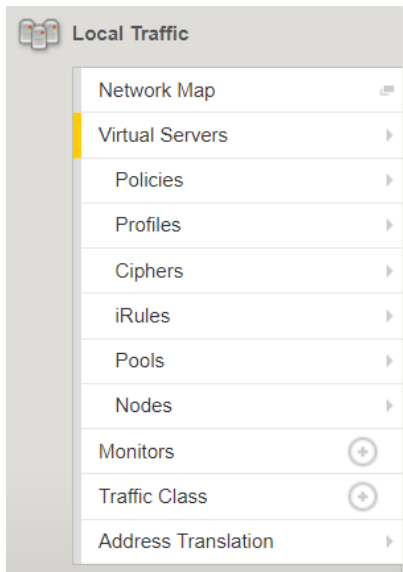
This will show the "Pool List" page, now click the  in the far right-hand corner of the page. Add a name for the pool, select your required Health Monitor of choice, add both of the Censornet USS Gateway to the pool and use 8080 as the service port as shown below. Click Finish to add the configuration.



Name	Censornet_Pool															
Description																
Health Monitors	<table border="1"><thead><tr><th>Active</th><th>Available</th></tr></thead><tbody><tr><td>/Common Port_8080</td><td>/Common gateway_icmp http http2 http2_head_f5</td></tr></tbody></table>	Active	Available	/Common Port_8080	/Common gateway_icmp http http2 http2_head_f5											
Active	Available															
/Common Port_8080	/Common gateway_icmp http http2 http2_head_f5															
Resources																
Load Balancing Method	Round Robin															
Priority Group Activation	Disabled															
New Members	<p><input type="radio"/> New Node <input type="radio"/> New FQDN Node <input checked="" type="radio"/> Node List</p> <p>Address: Gateway2.domain.local (10.10.10.6)</p> <p>Service Port: 8080 Select...</p> <p>Add</p> <table border="1"><thead><tr><th>Node Name</th><th>Address/FQDN</th><th>Service Port</th><th>Auto Populate</th><th>Priority</th></tr></thead><tbody><tr><td>Gateway1.domain.local</td><td>10.10.10.5</td><td>8080</td><td></td><td>0</td></tr><tr><td>Gateway2.domain.local</td><td>10.10.10.6</td><td>8080</td><td></td><td>0</td></tr></tbody></table> <p>Edit Delete</p>	Node Name	Address/FQDN	Service Port	Auto Populate	Priority	Gateway1.domain.local	10.10.10.5	8080		0	Gateway2.domain.local	10.10.10.6	8080		0
Node Name	Address/FQDN	Service Port	Auto Populate	Priority												
Gateway1.domain.local	10.10.10.5	8080		0												
Gateway2.domain.local	10.10.10.6	8080		0												
Cancel Repeat Finished																



Next, create a Virtual Server on the F5 LTM. Navigate to LTM, Virtual Servers



This will show the "Virtual Server List" page, now click the [Create...](#) in the far right-hand corner of the page. Under the General Properties section select Performance (Layer 4) add the IP Address 10.10.10.10 and add Port 8080 for the service port.

General Properties	
Name	<input type="text" value="filter.domain.local"/>
Description	<input type="text"/>
Type	Performance (Layer 4) ▾
Source Address	<input checked="" type="radio"/> Host <input type="radio"/> Address List <input type="text"/>
Destination Address/Mask	<input checked="" type="radio"/> Host <input type="radio"/> Address List <input type="text" value="10.10.10.10"/>
Service Port	<input checked="" type="radio"/> Port <input type="radio"/> Port List <input type="text" value="8080"/> Other: ▾
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
State	Enabled ▾



Under Configuration, Source Address Translation select Auto Map

Configuration: Basic ▾	
Protocol	TCP ▾
Protocol Profile (Client)	fastL4 ▾
HTTP Profile (Client)	None ▾
HTTP Profile (Server)	(Use Client Profile) ▾
HTTP Proxy Connect Profile	None ▾
VLAN and Tunnel Traffic	All VLANs and Tunnels ▾
Source Address Translation	Auto Map ▾

Under Resources, Default Pool, select the Censornet_Pool, Default Persistence Profile select source_addr. Click Finish to add the configuration.

Resources	
iRules	Enabled [Empty List] Up Down
Default Pool	+ Censornet_Pool ▾
Default Persistence Profile	source_addr ▾
Fallback Persistence Profile	None ▾
Cancel Repeat Finished	

The F5 LTM is now configured to load balance request to a pool of Censornet USS Gateways.