Introduction

This paper details the setup of F5 BIG IP 11.3 with Horizon Workspace 1.0 to load balance gateway-VAs for internal and external access.

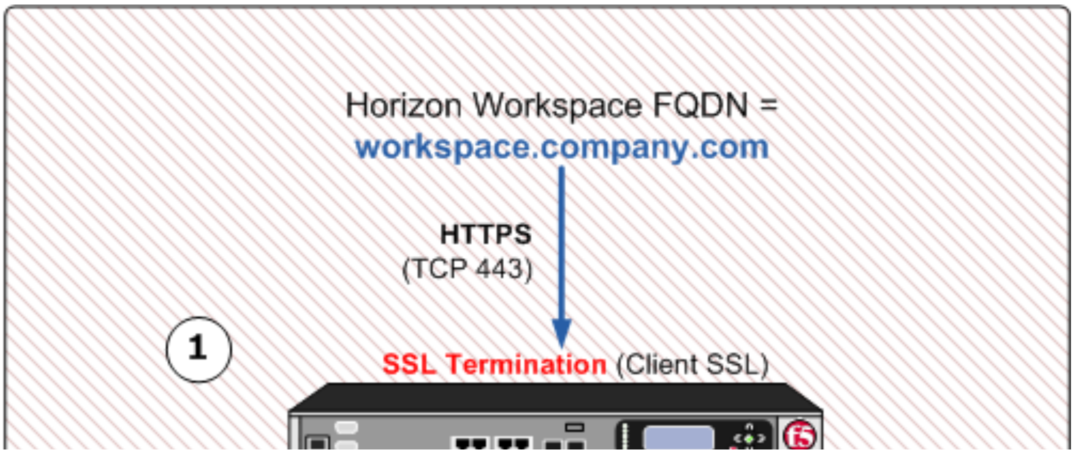
Objective

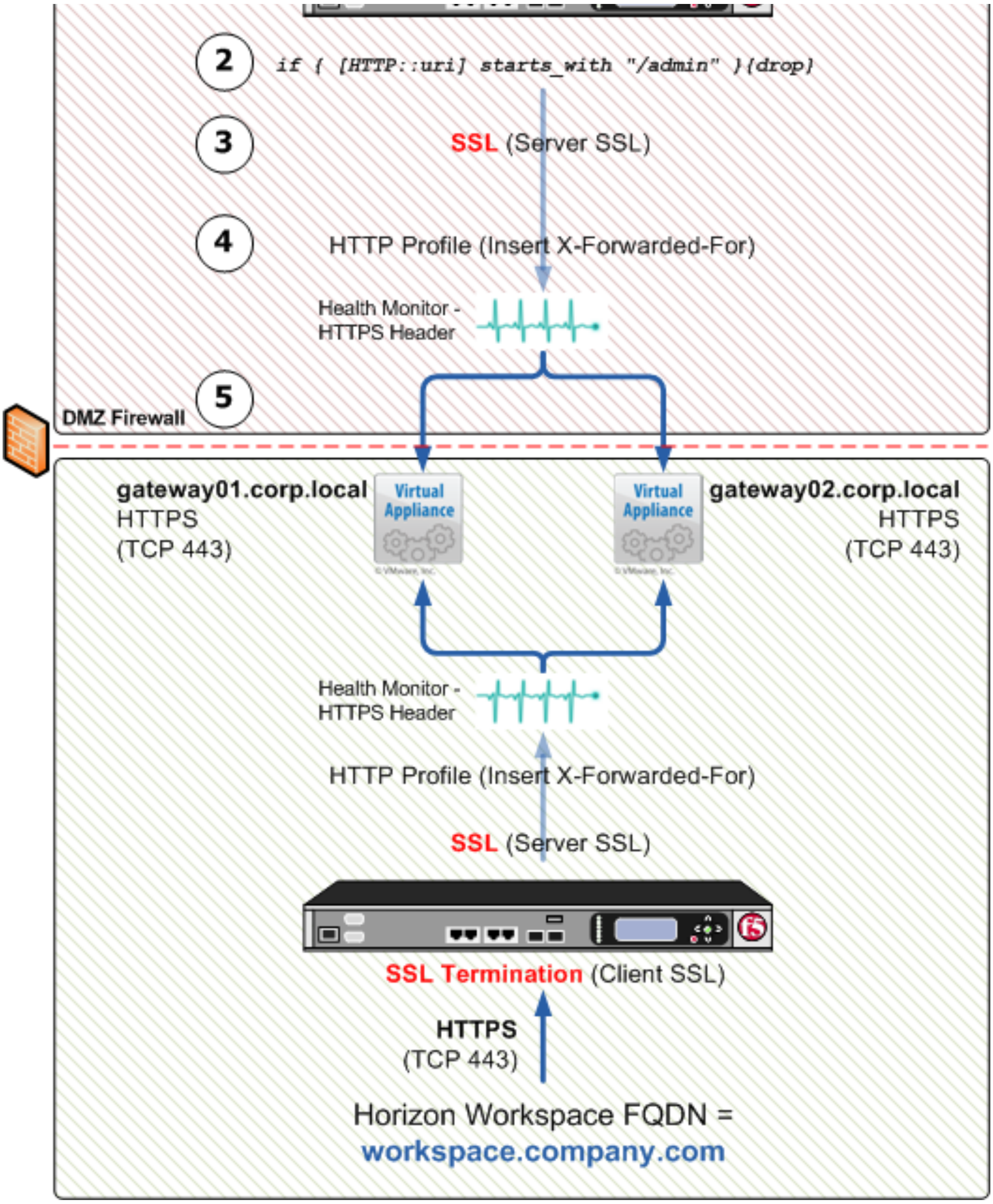
When setting up Horizon Workspace 1.0 for production usage a typical requirement is to have service level reduncancy for the different virtual appliances that makes up Horizon Workspace. This setup requires load balancers in front of the Gateway Virtual Appliance(s).
If the Horizon Workspace will be used externally a Load Balancer also needs to be placed in the DMZ. **It is not supported to place Gateway VA(s) the DMZ.**

Solution

F5 offers load balancing solutions that covers the criterias above which means they can cover the load balancing requirements for multiple gateway-VAs and external access to Horizon Workspace by placing F5 in the DMZ and routing those requests to the internal gateway-VAs. Below a brief solutions overview with a description of the flow.

1. A user goes to the Horizon Workspace URL - Which points to the F5 LTM VIP - SSL (HTTPS 433) traffic terminates at the F5 LTM.
2. If accessing the Horizon Workspace URL externally an iRule denies access to the admin part of Horizon Workspace (**Optional**)
3. F5 LTM continues to use SSL (HTTPS 443) against Horizon Workspace gateway-va(s)
4. X-Forwarded-For header is inserted with the requesting clients IP address
5. The users request is taken to an available gateway-va. This validation is based on a successful HTTPS header response.




2
if { [HTTP::uri] starts_with "/admin" }{drop}
3
SSL (Server SSL)
4
HTTP Profile (Insert X-Forwarded-For)
Health Monitor - HTTPS Header
5
DMZ Firewall
gateway01.corp.local HTTPS (TCP 443)
Virtual Appliance
Virtual Appliance
gateway02.corp.local HTTPS (TCP 443)
Health Monitor - HTTPS Header
HTTP Profile (Insert X-Forwarded-For)
SSL (Server SSL)
SSL Termination (Client SSL)
HTTPS (TCP 443)
Horizon Workspace FQDN =
workspace.company.com

NOTE: In the above diagram 2 F5 LTM appliances are pictured but they can be the same physical/virtual appliance with 2 logical configurations. In such a setup the VIP for providing external access would typically be defined on the 'Public' VLAN and the VIP for internal access to would be defined on the 'Private' VLAN.

The F5 deployment scenario does not matter in the case of using it for providing external access to Horizon Workspace meaning that both "In-Line" and "One-Arm" deployments would work equilly well.

This document discusses the following:

1. Configuration of F5 BIG IP 11.0 and Horizon Workspace 1.0 to support:
   - Load balancing gateway-VAs
2. Using proper CA signed certificates (not self-signed supplied with Horizon Workspace)

This tech-note assumes a requirement for using CA signed certificates and not the self-signed certificates by Horizon Workspace.

The Horizon Workspace FQDN (Namespace) cannot be changed post installation. The name initially specified during deployment has to be used. If this needs changing the Horizon Workspace vApp needs to be re-deployed.
If providing external access to Horizon Workspace the FQDN needs to be the same both internally and externally. Eg. workspace.company.com

NOTE: This tech-note does not cover installation or deployment of any F5 BIG IP products. For F5 BIG IP deployment and configuration options please refer to the BIG-IP LTM / VE 11.3.0 Documentation

Pre-reqs

- All pre-reqs to meet a successfull Horizon Workspace deployment (Installing Horizon Workspace 1.0)
- F5 BIG IP 11.3 setup to integrate with your existing environment
- Certificates to be used with the Horizon Workspace deployment
- Admin access to F5 BIG IP 11.3 used for the deployment
- DNS A and PTR records pointing to the Horizon Workspace FQDN URL - The VIP configured on the F5 LTM

Import certificates on F5 BIG IP

This guides assumes the usage of a proper CA signed certificate that matches the FQDN of the Horizon Workspace URL eg. workspace.company.com including the full certificate chain (root, subordinate, issuing etc.) imported on the F5 BIG IP 11.3 as well.
Just as would be required for Horizon Workspace the following is needed:

- Certificate to match Horizon Workspace URL / FQDN
  - Including Private Key
- Root, and/or any issuing/subordinate certificate to build full trust chain

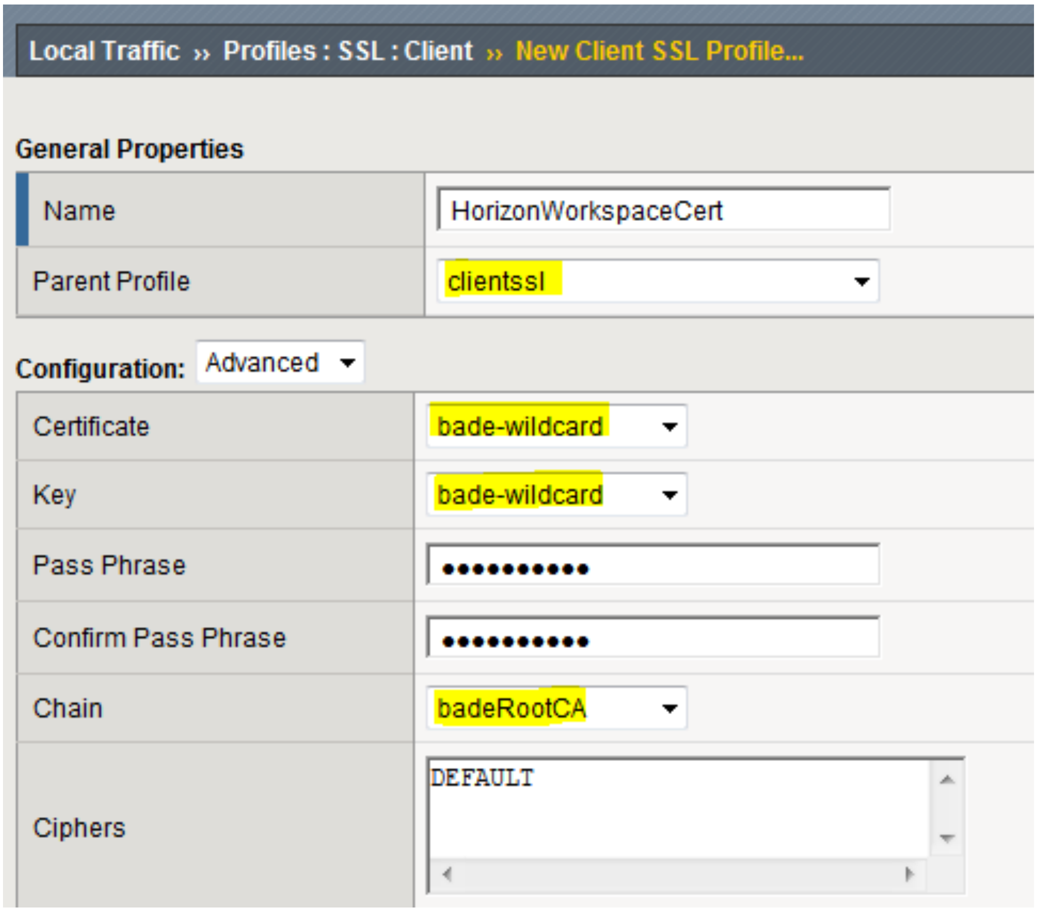
Go to System ›› File Management : SSL Certificate List ›› Import SSL Certificates and Keys and click "Import"

Here you have the options for importing your certificate, private key and certificate chain. Everything can be imported as PKCS12 if such a keystore is available containing all required certificates and private keys. If this is not available import the required certificates, keys and CA certificates individually.

Create Client SSL profile

Go to Local Traffic ›› Profiles : SSL : Client and click "Create".
Chose "Advanced" and click "Custom" to enable making changes.

Type a name thats going to be associated with the Client SSL profile and chose the Certificate, Private Key and Chain



Local Traffic ›› Profiles : SSL : Client ›› New Client SSL Profile...

General Properties

Name	HorizonWorkspaceCert
Parent Profile	clientssl

Configuration: Advanced

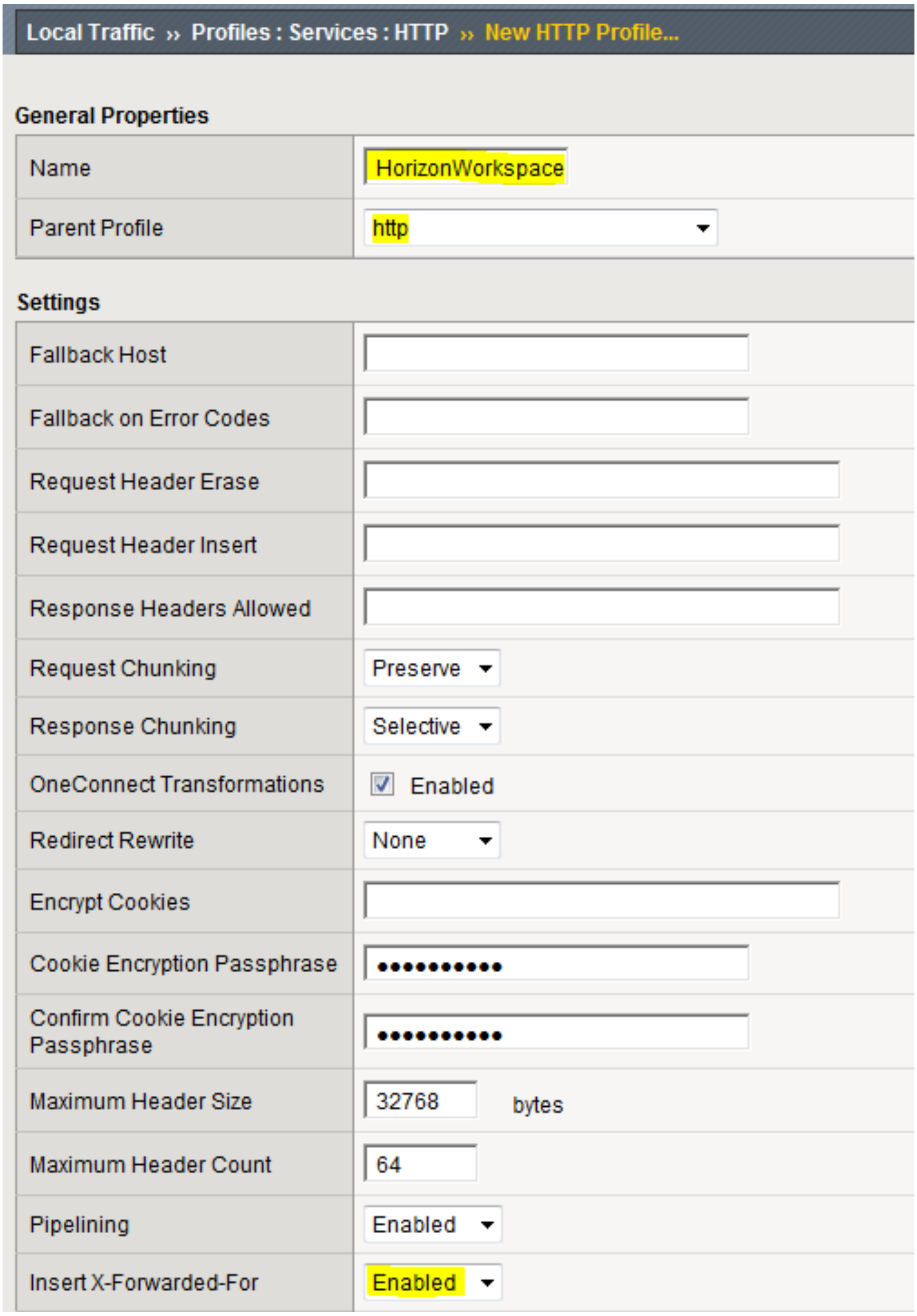
Certificate	bade-wildcard
Key	bade-wildcard
Pass Phrase	●●●●●●●●●●●
Confirm Pass Phrase	●●●●●●●●●●●
Chain	badeRootCA
Ciphers	DEFAULT

Scroll to the bottom and click "Finished"

Create HTTP Profile

Go to Local Traffic ›› Profiles : Services : HTTP and click "Create"
Click "Custom" to enable making changes.

Type a name that is going to be associated with this HTTP Profile and make sure Parent Profile is set to http as well as enabling "Insert X-Forwarded-For"



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

General Properties

Name	HorizonWorkspace
Parent Profile	http

Settings

Fallback Host	
Fallback on Error Codes	
Request Header Erase	
Request Header Insert	
Response Headers Allowed	
Request Chunking	Preserve
Response Chunking	Selective
OneConnect Transformations	☑ Enabled
Redirect Rewrite	None
Encrypt Cookies	
Cookie Encryption Passphrase	••••••••••
Confirm Cookie Encryption Passphrase	••••••••••
Maximum Header Size	32768 bytes
Maximum Header Count	64
Pipelining	Enabled
Insert X-Forwarded-For	Enabled

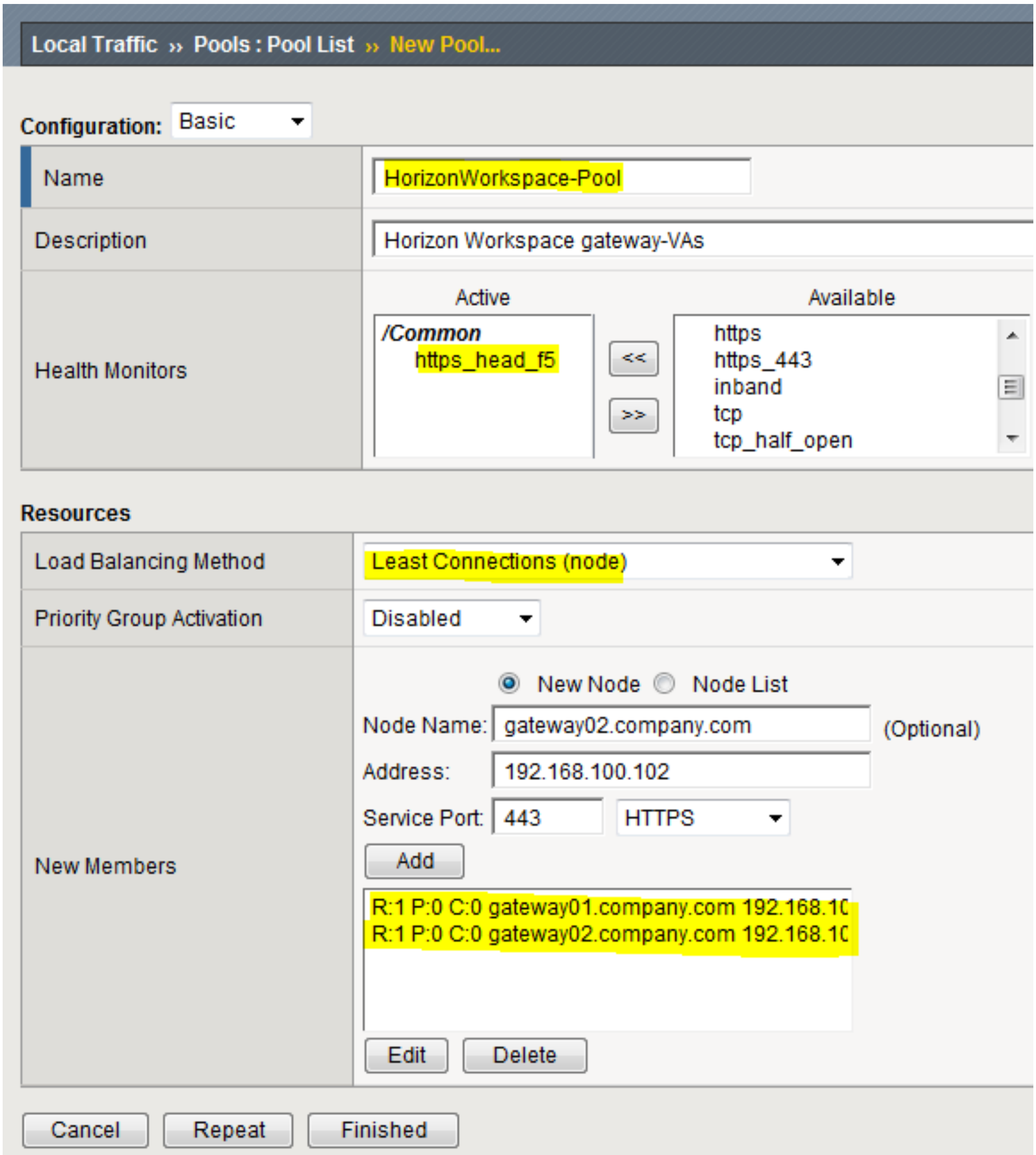
Scroll to the bottom and click "Finished"

Create Pool

Go to Local Traffic ›› Pools : Pool List and click "Create"

Type a name thats going to be associated with this pool and chose *https_head_f5* as health monitor and "Least Connections (node)" as load balanching method.

Then add the gateway-VA(s) with the node name, IP and Service Port (HTTPS) of the gateway-VA(s)



Local Traffic ›› Pools : Pool List ›› New Pool...

Configuration: Basic

Name	HorizonWorkspace-Pool
Description	Horizon Workspace gateway-VAs
Health Monitors	Active: /Common https_head_f5 Available: https, https_443, inband, tcp, tcp_half_open

Resources

Load Balancing Method	Least Connections (node)
Priority Group Activation	Disabled
New Members	● New Node ○ Node List Node Name: gateway02.company.com (Optional) Address: 192.168.100.102 Service Port: 443 HTTPS

R:1 P:0 C:0 gateway01.company.com 192.168.10
R:1 P:0 C:0 gateway02.company.com 192.168.10

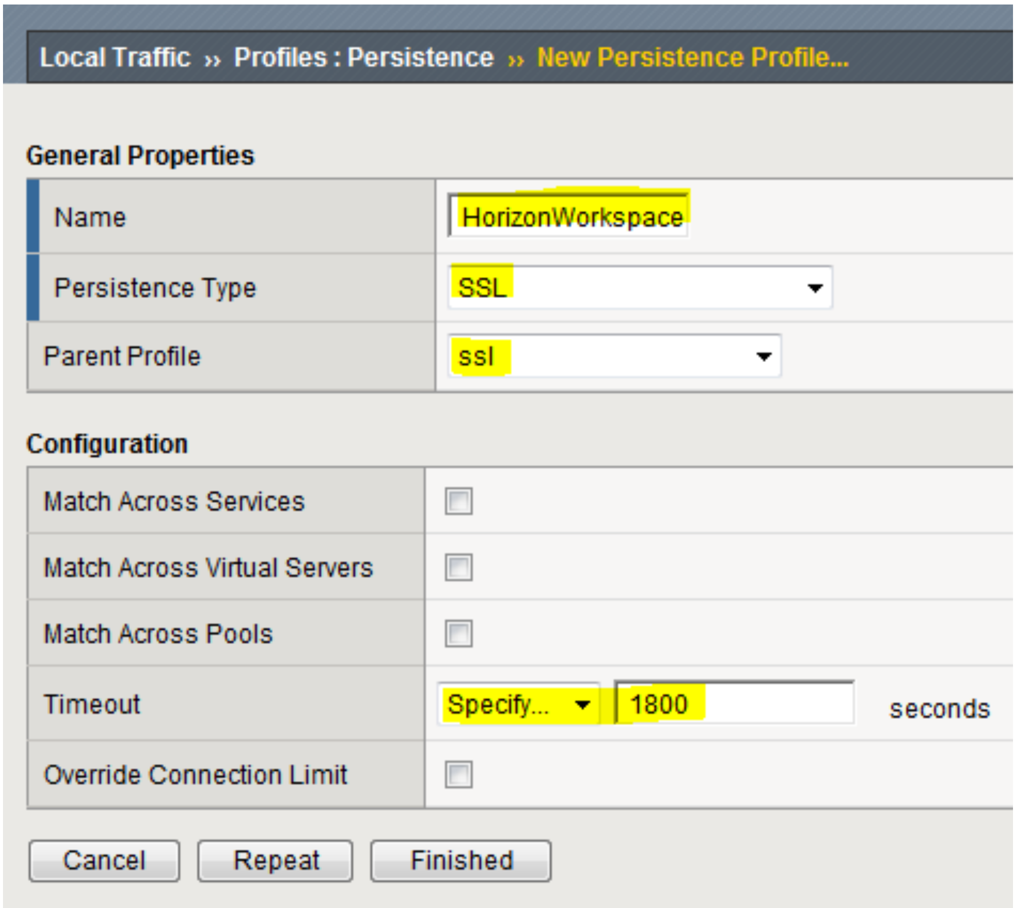
Scroll to the bottom and click "Finished"

Create Persistence Profile

Go to Local Traffic ›› Profiles : Persistence and click "Create"

Chose SSL as "Persistence Type" and "ssl" as Parent Profile.

Under "Timeout" specify 1800 seconds (30 min). This will keep user sessions tied to the same gateway-VA for up to 30 min to avoid timeout errors like: “502 error: The service is currently unavailable."



Local Traffic ›› Profiles : Persistence ›› New Persistence Profile...

General Properties

Name	HorizonWorkspace
Persistence Type	SSL
Parent Profile	ssl

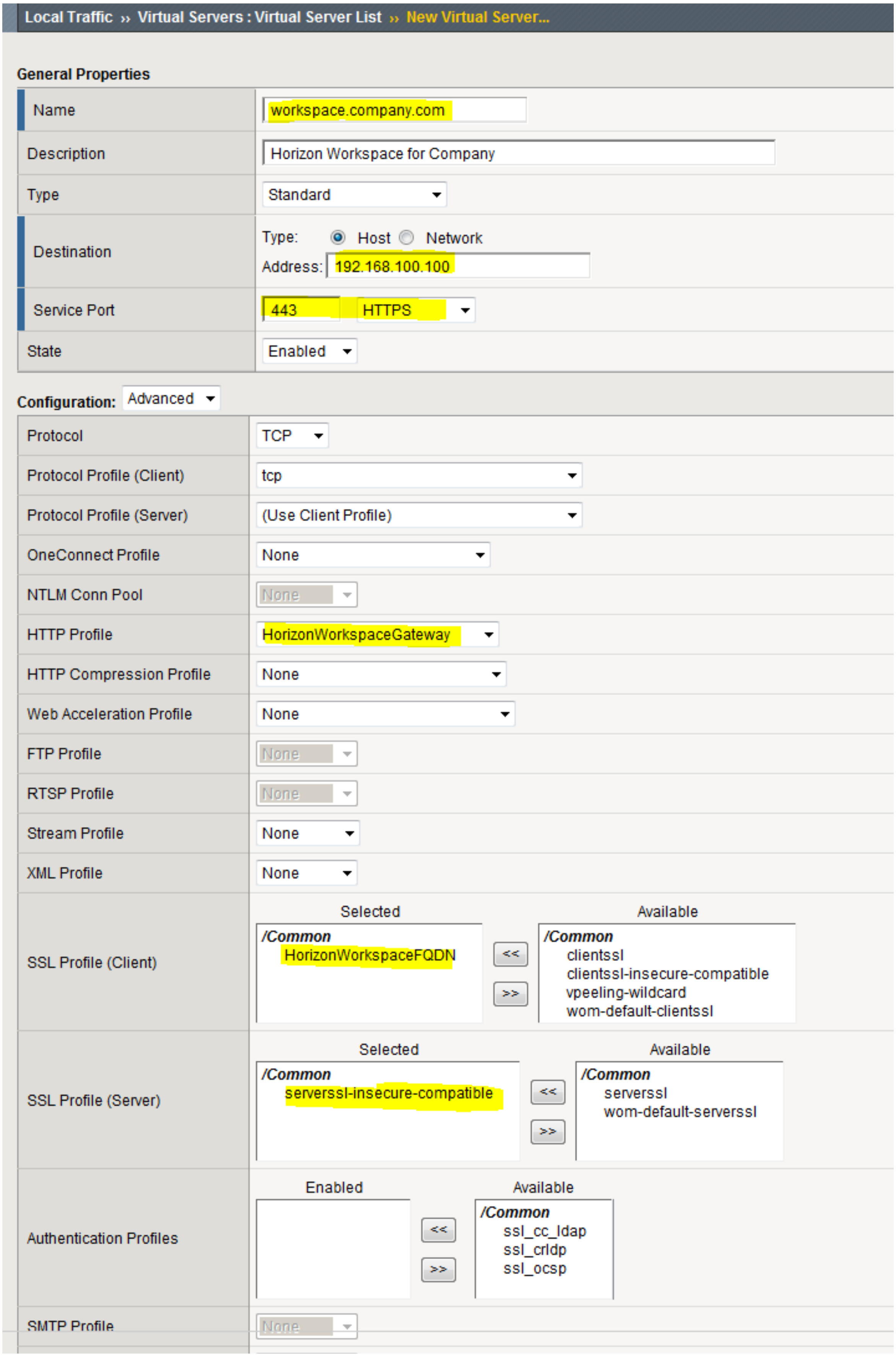
Configuration

Match Across Services	□
Match Across Virtual Servers	□
Match Across Pools	□
Timeout	Specify... 1800 seconds
Override Connection Limit	□

Scroll to the bottom and click "Finished"

Create Virtual Server

Go to Local Traffic ›› Virtual Servers : Virtual Server List and click "Create".
Chose "Advanced" under Configuration and configure with the different settings as created above. Make sure yo use the correct Client SSL Profile, HTTP profile, Pool and Persistence Profile.



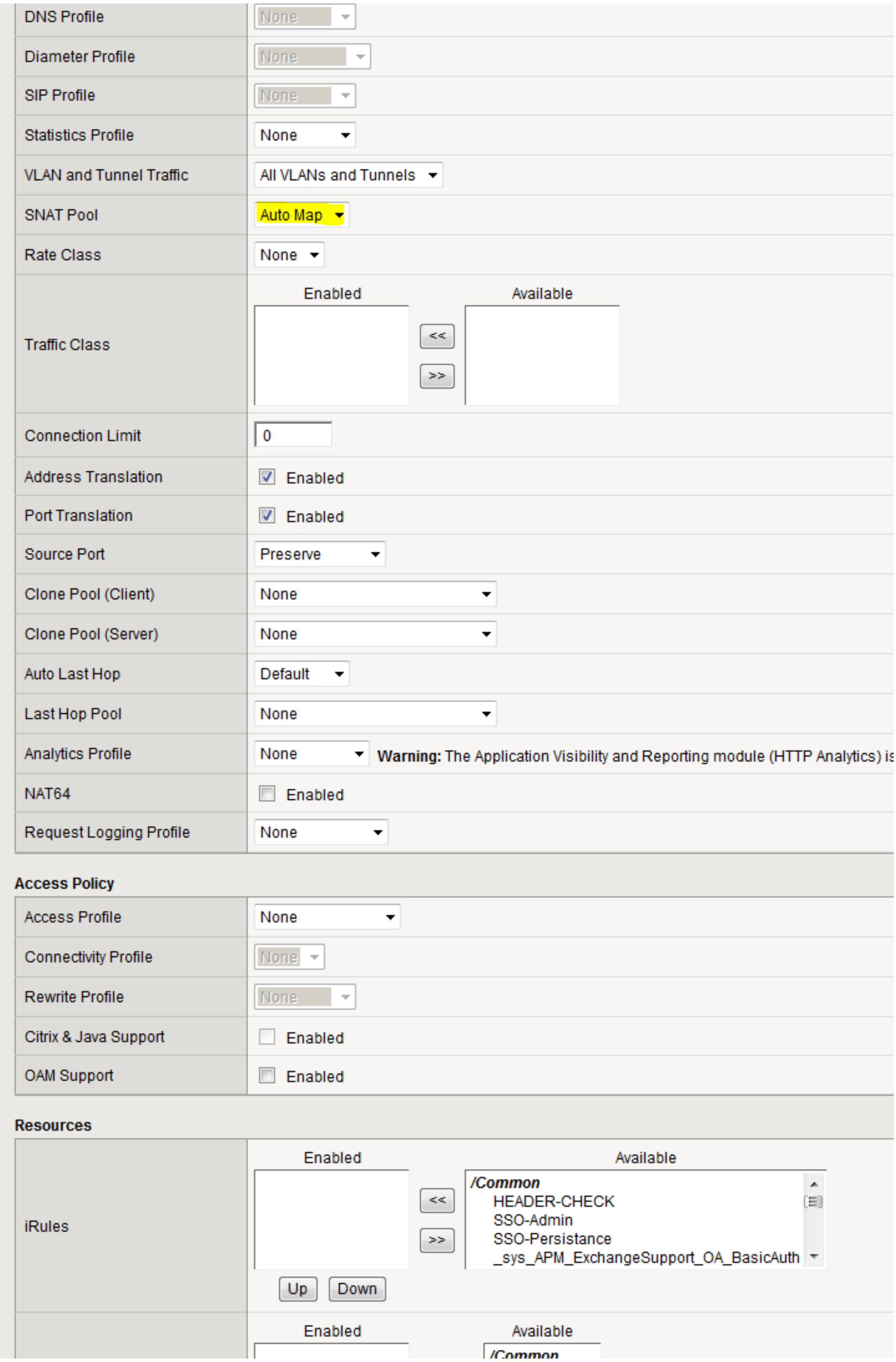
Local Traffic » Virtual Servers : Virtual Server List » New Virtual Server...

General Properties

Name	workspace.company.com
Description	Horizon Workspace for Company
Type	Standard
Destination	Type: ● Host ○ Network Address: 192.168.100.100
Service Port	443 HTTPS
State	Enabled

Configuration: Advanced

Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
OneConnect Profile	None
NTLM Conn Pool	None
HTTP Profile	HorizonWorkspaceGateway
HTTP Compression Profile	None
Web Acceleration Profile	None
FTP Profile	None
RTSP Profile	None
Stream Profile	None
XML Profile	None
SSL Profile (Client)	Selected: /Common HorizonWorkspaceFQDN Available: /Common clientssl clientssl-insecure-compatible vpeeling-wildcard wom-default-clientssl
SSL Profile (Server)	Selected: /Common serverssl-insecure-compatible Available: /Common serverssl wom-default-serverssl
Authentication Profiles	Enabled: Available: /Common ssl_cc_ldap ssl_crldp ssl_ocsp
SMTP Profile	None



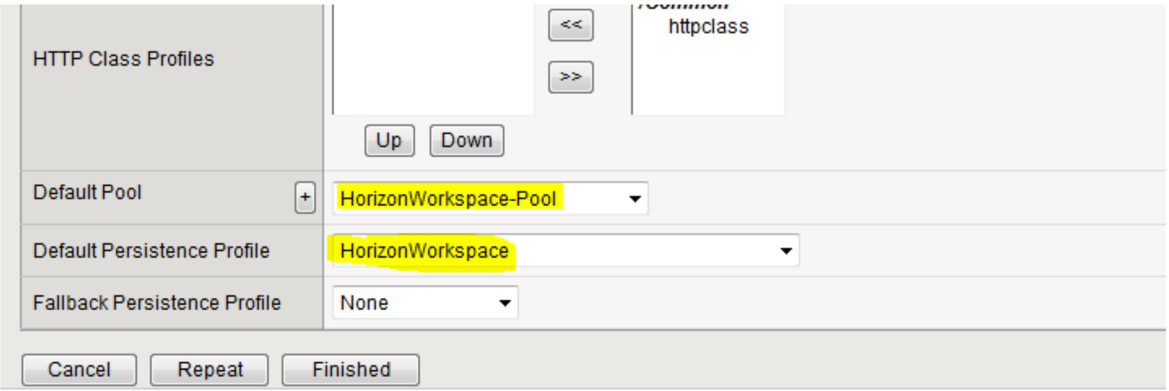
DNS Profile	None
Diameter Profile	None
SIP Profile	None
Statistics Profile	None
VLAN and Tunnel Traffic	All VLANs and Tunnels
SNAT Pool	Auto Map
Rate Class	None
Traffic Class	Enabled << >> Available
Connection Limit	0
Address Translation	☑ Enabled
Port Translation	☑ Enabled
Source Port	Preserve
Clone Pool (Client)	None
Clone Pool (Server)	None
Auto Last Hop	Default
Last Hop Pool	None
Analytics Profile	None **Warning:** The Application Visibility and Reporting module (HTTP Analytics) is
NAT64	□ Enabled
Request Logging Profile	None

Access Policy

Access Profile	None
Connectivity Profile	None
Rewrite Profile	None
Citrix & Java Support	□ Enabled
OAM Support	□ Enabled

Resources

iRules	Enabled << >> Up Down Available */Common* HEADER-CHECK SSO-Admin SSO-Persistance _sys_APM_ExchangeSupport_OA_BasicAuth
	Enabled Available */Common*



HTTP Class Profiles: httpclass

Default Pool: HorizonWorkspace-Pool

Default Persistence Profile: HorizonWorkspace

Fallback Persistence Profile: None

Scroll to the bottom and click "Finished"

Validate that the Horizon Workspace FQDN is accessible.

Configure nginx components on gateway-VA(s)

This change is required to allow the F5 BIG IP to request web-services behind the gateway-VA(s) as its now the F5 BIG IP making the requests.
X-Forwarded-For in the HTTP profile created earlier ensures that the connecting Client IP is being presented to the gateway-VA(s).

NOTE: This change needs to be done on all gateway-VA(s) thats sits behind the F5 BIG IP Load balancer.

SSH into gateway-VA with the sshuser and then su to root.

Edit the following file using vi or any other preferred editor:

/opt/vmware/nginx/conf/nginx.conf

Locate the section that reads like the below:

```
real_ip_header    X-Forwarded-For;
  real_ip_recursive off;
  include gen/real_ip.conf;
```

Below the *include gen/real_up.conf* add a line called *set_real_ip_from <F5-ip-addres>;*

An example is provided below:

```
real_ip_header    X-Forwarded-For;
  real_ip_recursive off;
  include gen/real_ip.conf;
  set_real_ip_from 192.168.100.100;
```

Commit the changes (is ufing VI type *:wq!*) and restart the nginx service:

```
service nginx restart
```

TROUBLESHOOTING - Finding the F5 BIG IP address

If setting the *set_real_ip_from* in the above steps does not work its possible that the wrong IP for the F5 BIG IP was entered as the *set_real_ip_from*.
If that is the case it is possible to disable the IP checks completely. This allows for accessing the Audit report where the real IP that the F5 BIG IP uses as forwarder address.

NOTE: The F5 BIG IP LTM will typically identify itself with the IP configured on the 'Private' interface.

Edit the following file using vi or any other preferred editor:

/opt/vmware/nginx/conf/location-443.conf

Search for /AUDIT (If using vi just enter /AUDIT and press enter)

Comment out the following lines so they look like the below:

```
#allow 127.0.0.1;
#include gen/all.allow;
#deny all;
```

Commit the changes (is ufing VI type *:wq!*) and restart the nginx service:

```
service nginx restart
```

Now when accessing the Audit Report in Horizon Workpace the IP address used by F5 BIG IP will show up in the logs.

For more information on these configuration changes go to the Installing Horizon Workspace 1.0 guide on page 56.

Validate login and AUDIT

Login to the Horizon Workspace URL as an admin and verify that you can successfully access the Audit Report

Click on one of the "LOGIN" event types and verify that the correct client IP shows up in the logs. There will be 2 entries for every login; One with information on which gateway-VA was used and the other containing client IP information. An example is provided below:

```
{
  "baseType" : "Action",
  "objectType" : "LOGIN",
  "values" : {
    "success" : "true"
  },
  "actorId" : 7,
  "actorUserName" : "administrator",
  "clientId" : null,
  "deviceId" : null,
  "sourceIp" : "192.168.0.12",
  "objectId" : null,
  "timestamp" : 1366270172165,
  "uuid" : "64fc70ec-417e-4e2a-9fb0-2f11025db9c9",
  "organizationId" : 1
}
```

Miscellaneous configuration options

This section details optional configuration options that can be performed to tighten security, provide additional features etc.

Redirecting HTTP to HTTPS for the Horizon Workspace URL

The default option for a Horizon Workspace gateway-va is to forward HTTP (80) to HTTPS (443) to avoid an error if https:// was not explicitly specified by the user accessing the Horizon Workspace service.
It is possible to achieve the same HTTP > HTTPS forward with F5 BIG IP by creating a new Virtual Server with the same VIP as used for HTTPS and then associating it with the same Pool as used by the VIP serving HTTPS.
To get the HTTPS redirect associate the *_sys_https_redirect* iRule with the newly created Virtual Server. This will forward HTTP > HTTPS so a user will automatically get transfered to the HTTPS VIP for proper Horizon Workspace access.

Deny access to the Horizon Workspace admin interface using iRule

It is possible to deny access to the admin interface of Horizon Workspace when exposing the service externally. This allows for a more secure implementation where the admin interface cannot be accessed from the VIP providing the external access.
This is achieved by using an iRule on the externally facing Virtual Server that drops any request for the admin URL.

Enter the following into a new iRule and afterwards associate it with the Virtual Server being used for providing external access to Horizon Workspace.

```
when HTTP_REQUEST {
        switch -glob [string tolower [HTTP::uri]] {
              "/admin*" {
        # Block Access to Admin URL From External
        log local0. "Access Blocked For URI- [HTTP::uri]"
        HTTP::respond 403 content {<html>Page Not Found</html>}
        return
        }
        default {
        # Do Nothing
        }
    }
}
```

External resources / links

- VMware Horizon Workspace Documentation
- F5 BIG-IP LTM / VE 11.3.0 Documentation

Changelog

Version 0.1

- Initial version including overview and general configuration procedure for load balancing gateway-VA(s).

Version 0.2

- Added troubleshooting info for nginx configuration

- Changed the overview diagram and added information on not to deploy gateway-VA(s) in DMZ as this is not a supported configuration.
- Updated the solutions section with F5 deployment scenarios description
- Added configuration steps for HTTP > HTTPS redirection
- Added configuration steps to block admin access to external users with an iRule