Technical Article

Big-IP and ADFS Part 1 – “Load balancing the ADFS Farm”

February 24, 2012 by Greg Coward 255

article active directory adfs apm availability coward exchange federation firewall government hardware infrastructure load balancer ltm microsoft network partner security us

Just like the early settlers who migrated en masse across the country by wagon train along the Oregon Trail, enterprises are migrating up into the cloud. Well okay, maybe not exactly like the early settlers. But, although there may not be a mass migration to the cloud, it is true that more and more enterprises are moving to cloud-based services like Office 365.

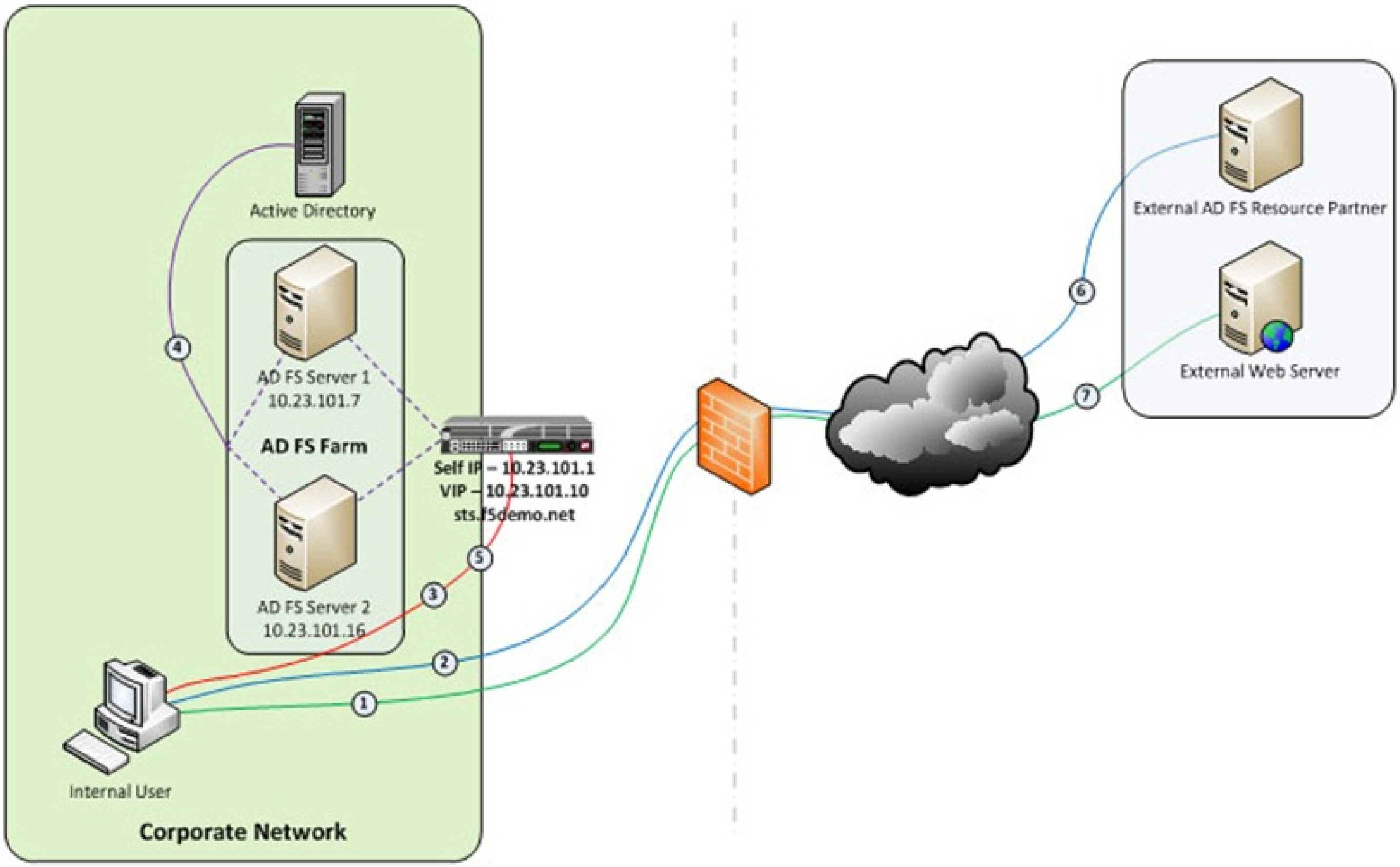
So how do you provide seamless, or at least relatively seamless, access to resources outside of the enterprise? Well, one answer is federation and if you are a Microsoft shop then the current solution is ADFS, (Active Directory Federation Services). The ADFS server role is a security token service that extends the single sign-on, (SSO) experience for directory-authenticated clients to resources outside of the organization’s boundaries. As cloud-based application access and federation in general becomes more prevalent, the role of ADFS has become equally important. Below, is a typical deployment scenario of the ADFS Server farm and the ADFS Proxy server farm, (recommended for external access to the internally hosted ADFS farm).

Warning…. If the ADFS server farm is unavailable then access to federated resources will be limited if not completely inaccessible. To ensure high-availability, performance, and scalability the F5 Big-IP with LTM, (Local Traffic Manager), can be deployed to load balance the ADFS and ADFS Proxy server farms. Yes! When it comes to a load balancing and application delivery, F5’s Big-IP is an excellent choice. Just had to get that out there.

So let’s get technical! Part one of this blog series addresses deploying and configuring the Big-IP’s LTM module for load balancing the ADFS Server farm and Proxy server farm. In part two I’m going to show how we can greatly simplify and improve this deployment by utilizing Big-IP’s APM, (Access Policy Manager) so stay tuned.

Load Balancing the Internal ADFS Server Farm

Assumptions and Product Deployment Documentation - This deployment scenario assumes an ADFS server farm has been installed and configured per the deployment guide including appropriate trust relationships with relevant claims providers and relying parties. In addition, the reader is assumed to have general administrative knowledge of the BIG-IP LTM module. If you want more information or guidance please check out F5’s support site, ASKF5. The following diagram shows a typical, (albeit simplified) process flow of the Big-IP load balanced ADFS farm.



1. Client attempts to access the ADFS-enabled external resource;
2. Client is redirected to the resource's applicable federation service;
3. Client is redirected to its organization's internal federation service, (assuming the resource's federation service is configured as trusted partner);
4. The ADFS server authenticates the client to active directory;
5. The ADFS server provides the client with an authorization cookie containing the signed security token and set of claims for the resource partner;
6. The client connects to the resource partner federation service where the token and claims are verified. If appropriate, the resource partner provides the client with a new security token; and
7. The client presents the new authorization cookie with included security token to the resource for access.

VIRTUAL SERVER AND MEMBER POOL – A virtual server, (aka VIP) is configured to listen on port 443, (https). In the event that the Big-IP will be used for SSL bridging, (decryption and re-encryption), the public facing SSL certificate and associated private key must be installed on the BIG-IP and associated client SSL profile created. However, as will be discussed later SSL bridging is not the preferred method for this type of deployment. Rather, SSL tunneling, (pass-thru) will be utilized.

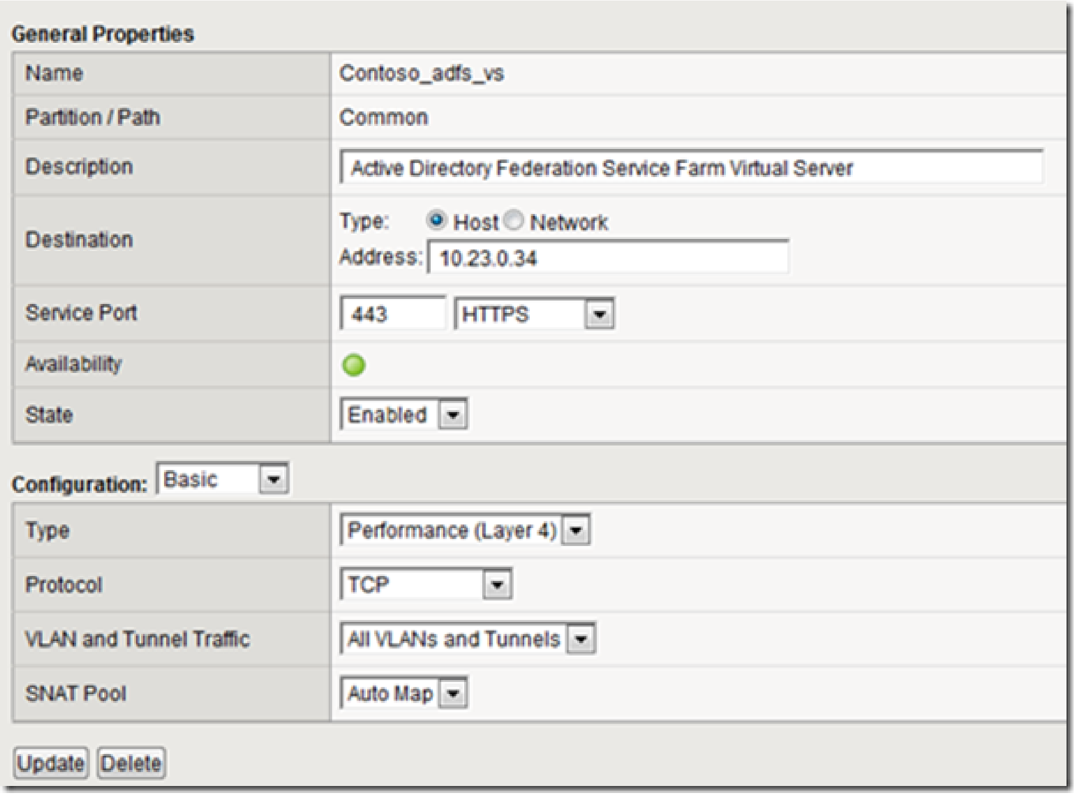
ADFS requires Transport Layer Security and Secure Sockets Layer (TLS/SSL). Therefore pool members are configured to listen on port 443, (https).

LOAD BALANCING METHOD – The 'Least Connections (member)' method is utilized.

POOL MONITOR – To ensure the AD FS service is responding as well as the web site itself, a customized monitor can be used. The monitor ensures the AD FS federation service is responding. Additionally, the monitor utilizes increased interval and timeout settings. The custom https monitor requires domain credentials to validate the service status. A standard https monitor can be utilized as an alternative.

PERSISTENCE – In this AD FS scenario, clients establish a single TCP connection with the AD FS server to request and receive a security token. Therefore, specifying a persistence profile is not necessary.

SSL TUNNELING, (preferred method) – When SSL tunneling is utilized, encrypted traffic flows from the client directly to the endpoint farm member. Additionally, SSL profiles are not used nor are SSL certificates required to be installed on the Big-IP. In this instance Big-IP profiles requiring packet analysis and/or modification, (ex. compression, web acceleration) will not be relevant. To further boost the performance, a Fast L4 virtual server will be used.



General Properties

Name	Contoso_adfs_vs
Partition / Path	Common
Description	Active Directory Federation Service Farm Virtual Server
Destination	Type: ● Host ○ Network Address: 10.23.0.34
Service Port	443 HTTPS
Availability	●
State	Enabled

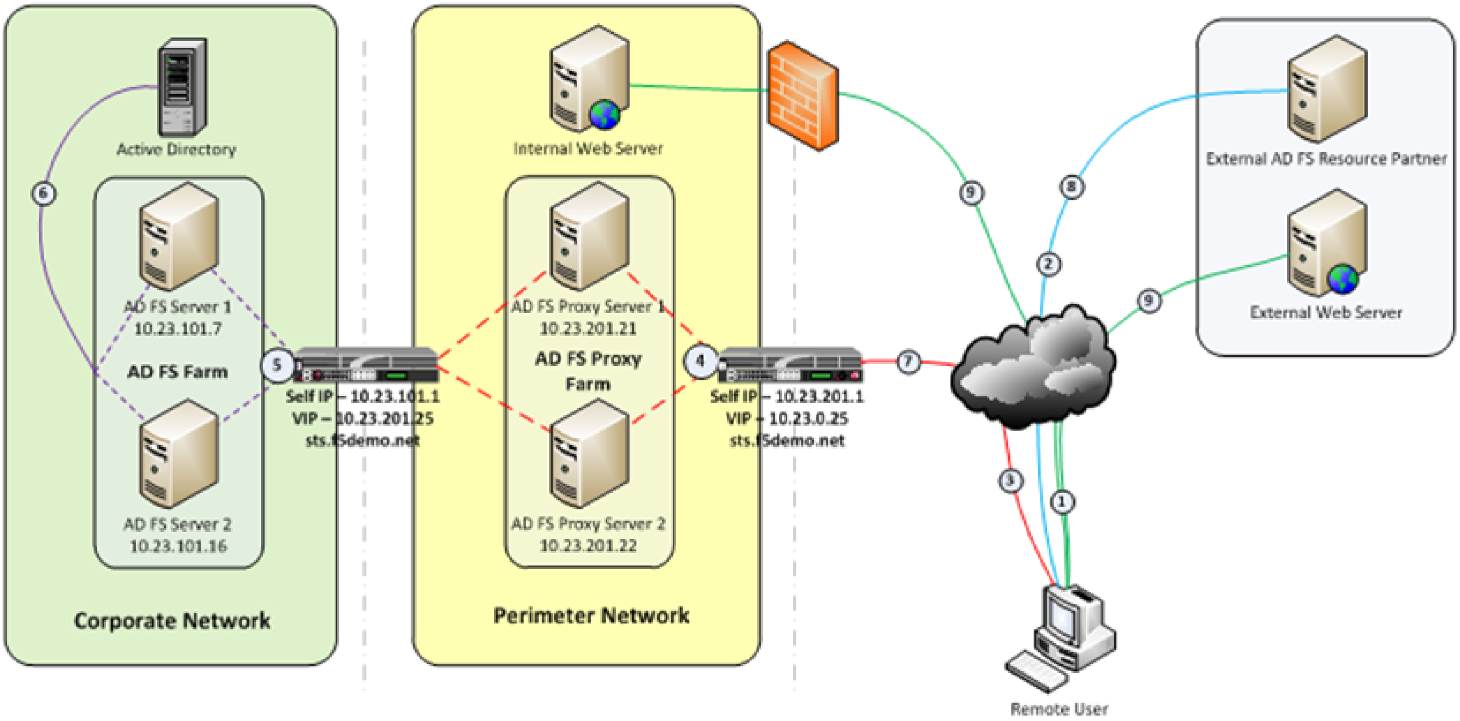
Configuration: Basic

Type	Performance (Layer 4)
Protocol	TCP
VLAN and Tunnel Traffic	All VLANs and Tunnels
SNAT Pool	Auto Map

Load Balancing the ADFS Proxy Server Farm

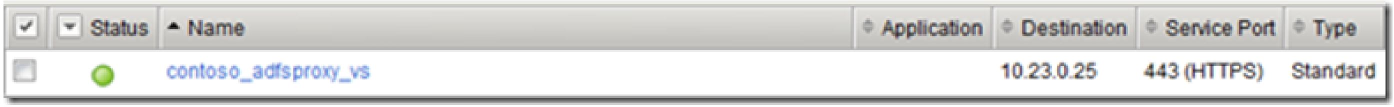
Assumptions and Product Deployment Documentation - This deployment scenario assumes an ADFS Proxy server farm has been installed and configured per the deployment guide including appropriate trust relationships with relevant claims providers and relying parties. In addition, the reader is assumed to have general administrative knowledge of the BIG-IP LTM module. If you want more information or guidance please check out F5's support site, ASKF5.

In the previous section we configure load balancing for an internal AD FS Server farm. That scenario works well for providing federated SSO access to internal users. However, it does not address the need of the external end-user who is trying to access federated resources. This is where the AD FS proxy server comes into play. The AD FS proxy server provides external end-user SSO access to both internal federation-enabled resources as well as partner resources like Microsoft Office 365.



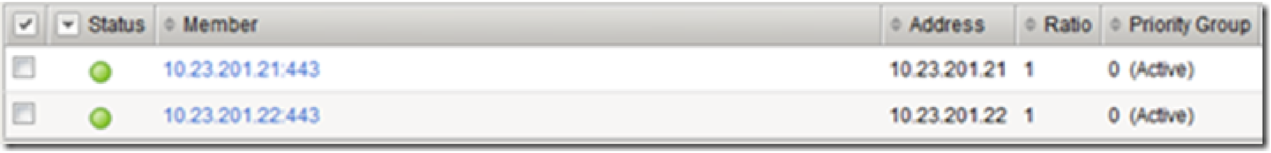
1. Client attempts to access the AD FS-enabled internal or external resource;
2. Client is redirected to the resource’s applicable federation service;
3. Client is redirected to its organization’s internal federation service, (assuming the resource’s federation service is configured as trusted partner);
4. The AD FS proxy server presents the client with a customizable sign-on page;
5. The AD FS proxy presents the end-user credentials to the AD FS server for authentication;
6. The AD FS server authenticates the client to active directory;
7. The AD FS server provides the client, (via the AD FS proxy server) with an authorization cookie containing the signed security token and set of claims for the resource partner;
8. The client connects to the resource partner federation service where the token and claims are verified. If appropriate, the resource partner provides the client with a new security token; and
9. The client presents the new authorization cookie with included security token to the resource for access.

VIRTUAL SERVER AND MEMBER POOL – A virtual server is configured to listen on port 443, (https). In the event that the Big-IP will be used for SSL bridging, (decryption and re-encryption), the public facing SSL certificate and associated private key must be installed on the BIG-IP and associated client SSL profile created.



☑	Status	Name	Application	Destination	Service Port	Type
□	●	contoso_adfsproxy_vs		10.23.0.25	443 (HTTPS)	Standard

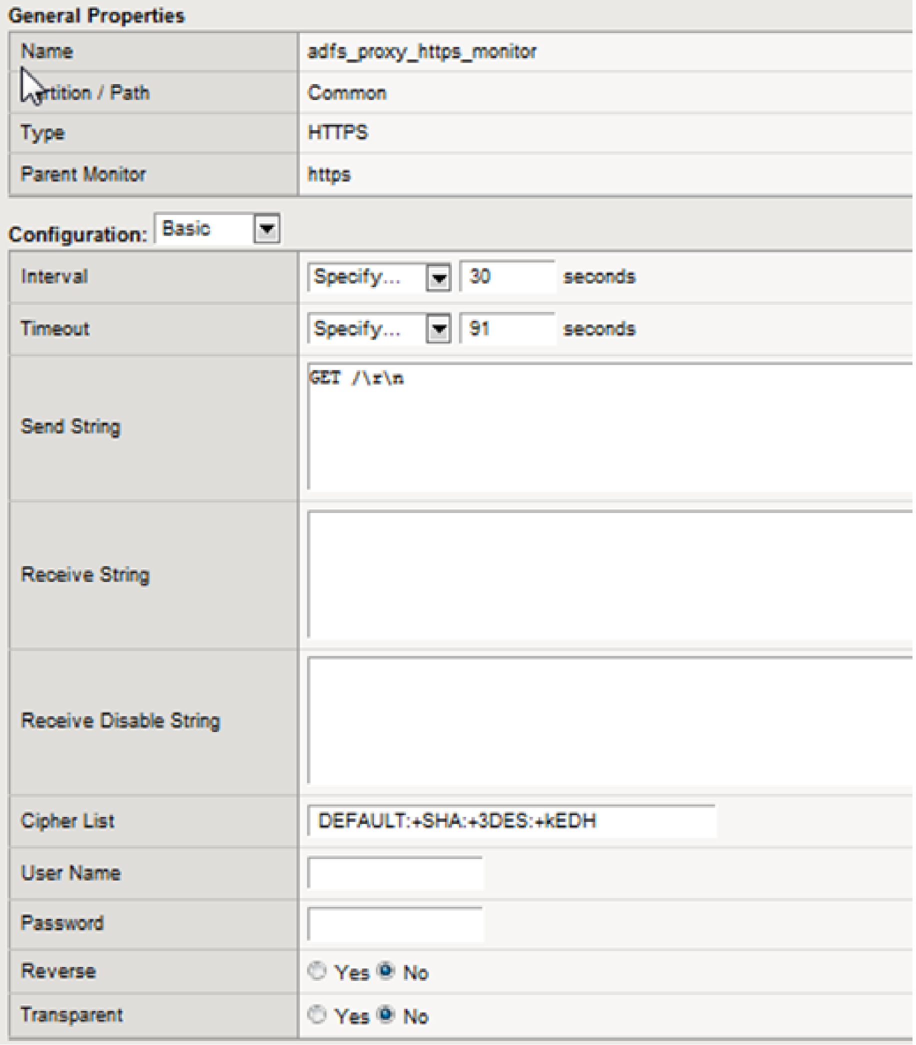
ADFS requires Transport Layer Security and Secure Sockets Layer (TLS/SSL). Therefore pool members are configured to listen on port 443, (https).



☑	Status	Member	Address	Ratio	Priority Group
□	●	10.23.201.21:443	10.23.201.21	1	0 (Active)
□	●	10.23.201.22:443	10.23.201.22	1	0 (Active)

LOAD BALANCING METHOD – *The ‘Least Connections (member)’ method is utilized.*

POOL MONITOR – *To ensure the web servers are responding, a customized ‘HTTPS’ monitor is associated with the AD FS proxy pool. The monitor utilizes increased interval and timeout settings.*



General Properties

Name	adfs_proxy_https_monitor
Partition / Path	Common
Type	HTTPS
Parent Monitor	https

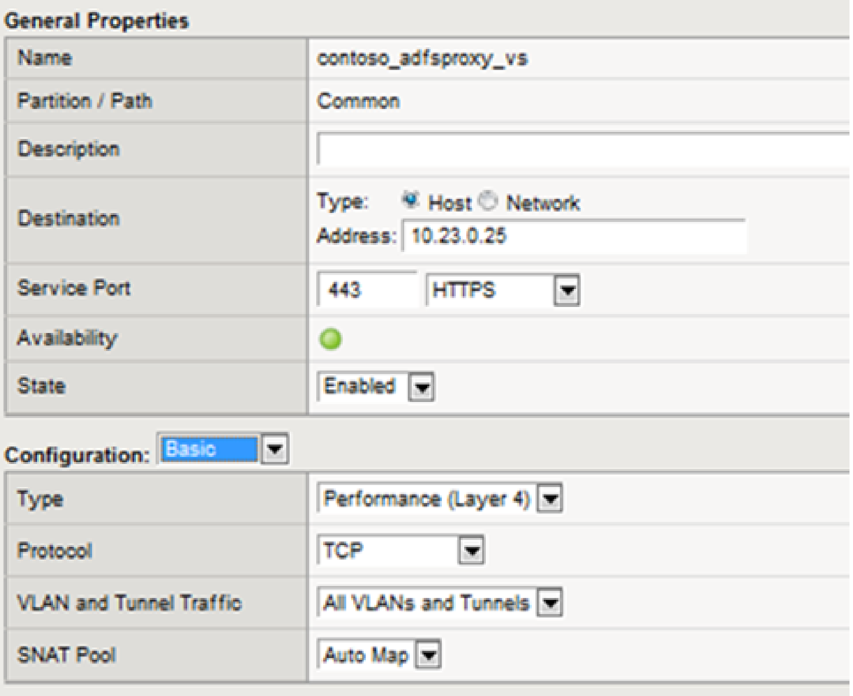
Configuration: Basic

Interval	Specify... 30 seconds
Timeout	Specify... 91 seconds
Send String	GET /\r\n
Receive String	
Receive Disable String	
Cipher List	DEFAULT:+SHA:+3DES:+kEDH
User Name	
Password	
Reverse	○ Yes ● No
Transparent	○ Yes ● No

"To SSL Tunnel or Not to SSL Tunnel"

When SSL tunneling is utilized, encrypted traffic flows from the client directly to the endpoint farm member. Additionally, SSL profiles are not used nor are SSL certificates required to be installed on the Big-IP. However, some advanced optimizations including HTTP compression and web acceleration are not possible when tunneling. Depending upon variables such as client connectivity and customization of ADFS sign-on pages, an ADFS proxy deployment may benefit from these HTTP optimization features. The following two options, (SSL Tunneling and SSL Bridging) are provided.

***SSL TUNNELING -** In this instance Big-IP profiles requiring packet analysis and/or modification, (ex. compression, web acceleration) will not be relevant. To further boost the performance, a Fast L4 virtual server will be used. Below is an example of the Fast L4 Big-IP Virtual server configuration in SSL tunneling mode.*



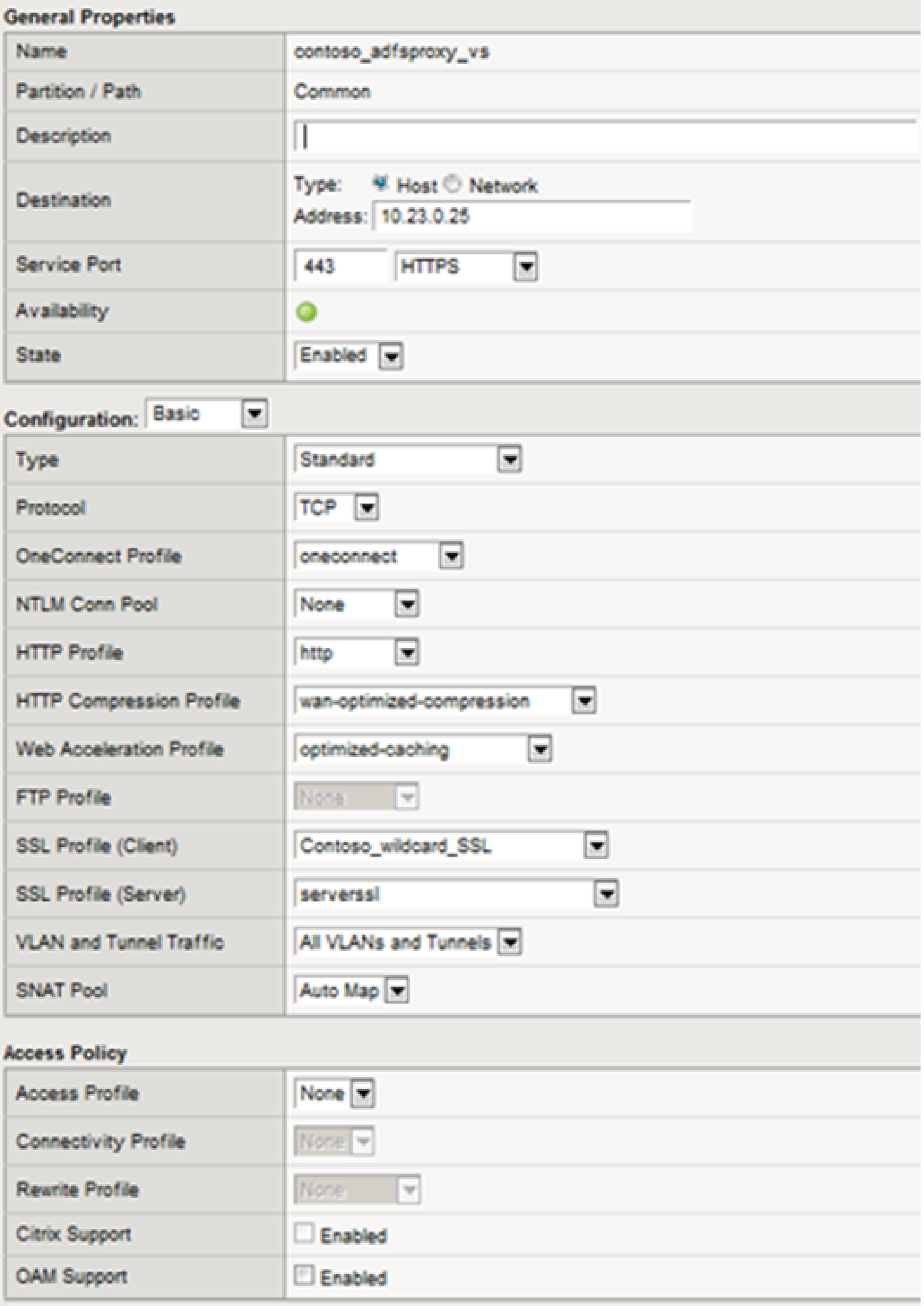
General Properties

Name	contoso_adfsproxy_vs
Partition / Path	Common
Description	
Destination	Type: ● Host ○ Network Address: 10.23.0.25
Service Port	443 HTTPS
Availability	●
State	Enabled

Configuration: Basic

Type	Performance (Layer 4)
Protocol	TCP
VLAN and Tunnel Traffic	All VLANs and Tunnels
SNAT Pool	Auto Map

SSL BRIDGING – *When SSL bridging is utilized, traffic is decrypted and then re-encrypted at the Big-IP device. This allows for additional features to be applied to the traffic on both client-facing and pool member-facing sides of the connection. Below is an example of the standard Big-IP Virtual server configuration in SSL bridging mode.*



General Properties

Name	contoso_adfsproxy_vs
Partition / Path	Common
Description	
Destination	Type: ● Host ○ Network Address: 10.23.0.25
Service Port	443 HTTPS
Availability	●
State	Enabled

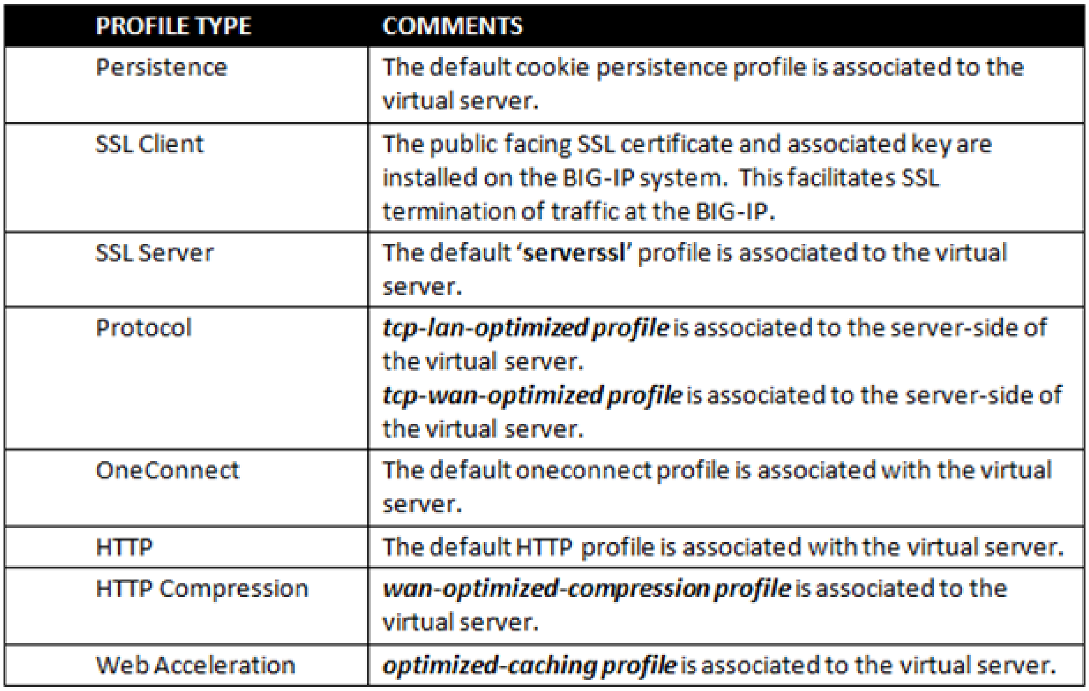
Configuration: Basic

Type	Standard
Protocol	TCP
OneConnect Profile	oneconnect
NTLM Conn Pool	None
HTTP Profile	http
HTTP Compression Profile	wan-optimized-compression
Web Acceleration Profile	optimized-caching
FTP Profile	None
SSL Profile (Client)	Contoso_wildcard_SSL
SSL Profile (Server)	serverssl
VLAN and Tunnel Traffic	All VLANs and Tunnels
SNAT Pool	Auto Map

Access Policy

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

Standard Virtual Server Profiles - *The following list of profiles is associated with the AD FS proxy virtual server.*



PROFILE TYPE	COMMENTS
Persistence	The default cookie persistence profile is associated to the virtual server.
SSL Client	The public facing SSL certificate and associated key are installed on the BIG-IP system. This facilitates SSL termination of traffic at the BIG-IP.
SSL Server	The default ‘**serverssl**’ profile is associated to the virtual server.
Protocol	***tcp-lan-optimized profile*** is associated to the server-side of the virtual server. ***tcp-wan-optimized profile*** is associated to the server-side of the virtual server.
OneConnect	The default oneconnect profile is associated with the virtual server.
HTTP	The default HTTP profile is associated with the virtual server.
HTTP Compression	***wan-optimized-compression profile*** is associated to the virtual server.
Web Acceleration	***optimized-caching profile*** is associated to the virtual server.

Well that’s it for Part 1. Along with the F5 business development team for the Microsoft global partnership I want to give a big thanks to the guys at Ensynch, an Insight Company - Kevin James, David Lundell, and Lutz Mueller Hipper for reviewing and providing feedback.

Stay tuned for ***Big-IP and ADFS Part 2 – “APM – An Alternative to the ADFS Proxy”.***

Additional Links:

Big-IP and ADFS Part 2 – “APM–An Alternative to the ADFS Proxy”

Big-IP and ADFS Part 3 - “ADFS, APM, and the Office 365 Thick Clients”

last modified: June 26, 2014

3 Comment(s):

ADFS3 is using SNI and F5 does not have any built-in support for SNI monitoring. You will need to create external check or do a limited monitoring at the host level (ie ICMP/TCP) .

5/1/2014 by Rianto Wahyudi 14

Hi,

really great article which helped me out a lot! Do you by chance know, if the Big-IP is also ADFS 2.0 and 3.0 certified?

Thanks,
Manuel

3/11/2014 by Manuel 81

Hello,