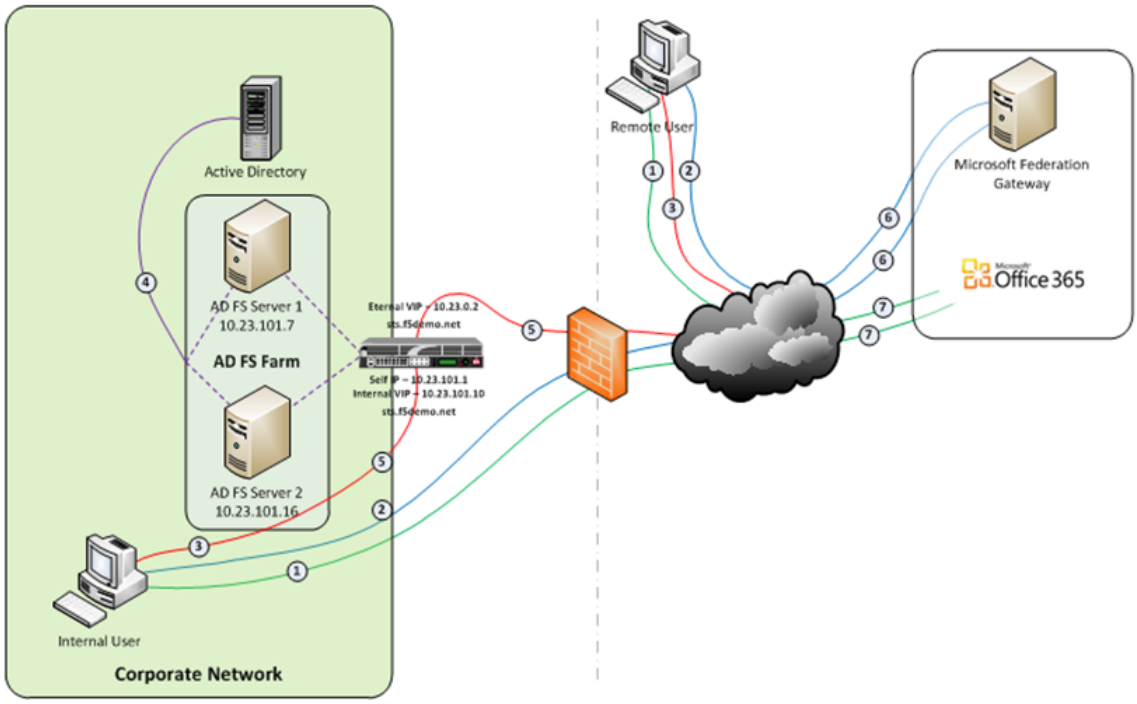
Big-IP and ADFS Part 2 - APM: An Alternative to the ADFS Proxy

Greg Coward, 2012-08-03

So let's talk Application Delivery Controllers, (ADC). In part one of this series we deployed both an internal ADFS farm as well as a perimeter ADFS proxy farm using the Big-IP's exceptional load balancing capabilities to provide HA and scalability. But there's much more the Big-IP can provide to the application delivery experience. Here in part 2 we'll utilize the Access Policy Manager, (APM) module as a replacement for the ADFS Proxy layer. To illustrate this approach, we'll address one of the most common use cases; ADFS deployment to federate with and enable single sign-on to Microsoft Office 365 web-based applications.

The purpose of the ADFS Proxy server is to receive and forward requests to ADFS servers that are not accessible from the Internet. As noted in part one, for high availability this typically requires a minimum of two proxy servers as well as an additional load balancing solution, (F5 Big-IPs of course). By implementing APM on the F5 appliance(s) we not only eliminate the need for these additional servers but, by implementing pre-authentication at the perimeter and advanced features such as client-side checks, (antivirus validation, firewall verification, etc.), arguably provide for a more secure deployment.

Assumptions and Product Deployment Documentation - This deployment scenario assumes the reader is assumed to have general administrative knowledge of the BIG-IP LTM module and basic understanding of the APM module. If you want more information or guidance please check out F5's support site, ASKF5. The following diagram shows a typical internal and external client access AD FS to Office 365 Process Flow, *(used for passive-protocol, "web-based" access).*



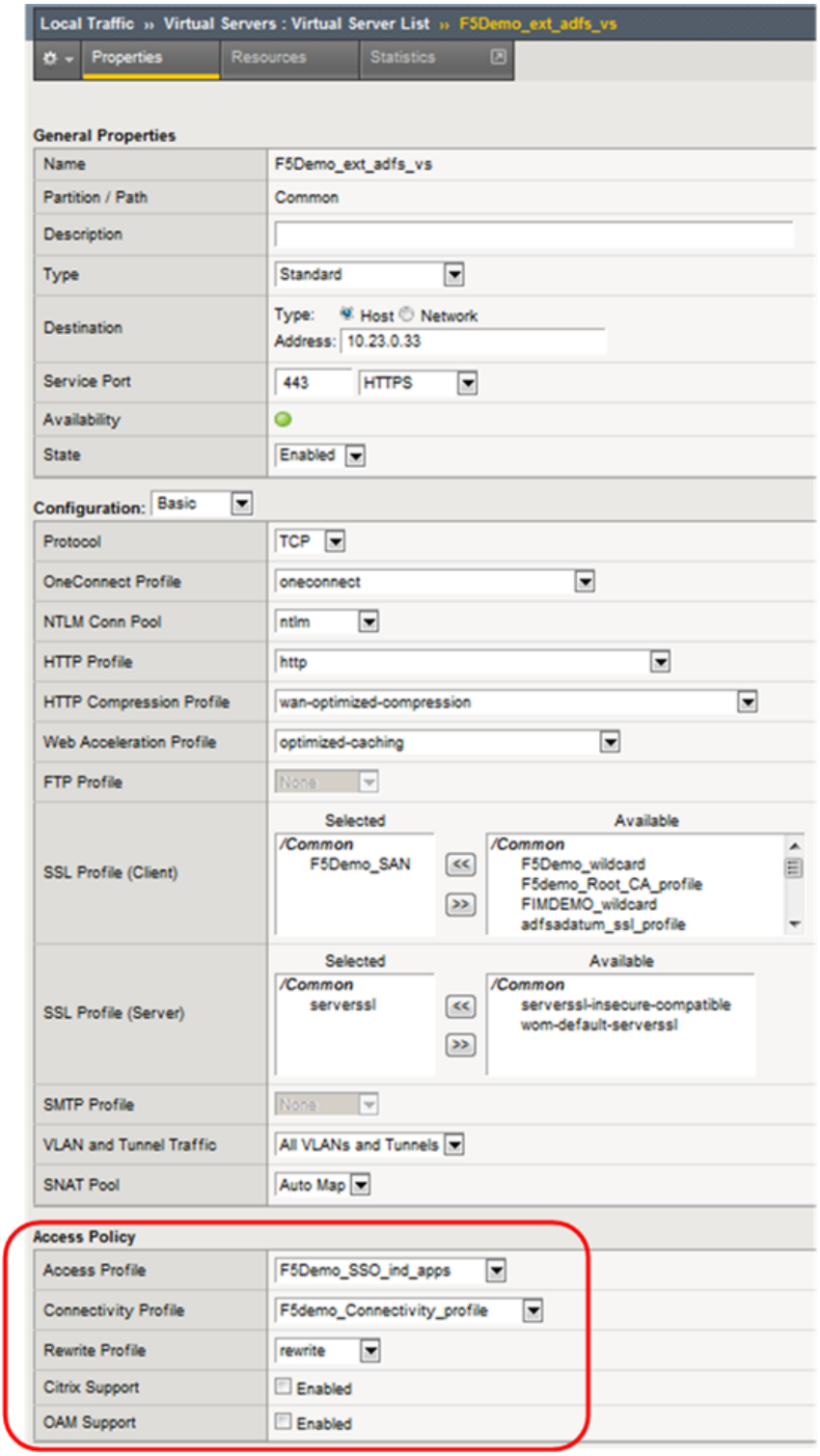
1. Both clients attempts to access the Office 365 resource;
2. Both clients are redirected to the resource's applicable federation service, (*Note: This step may be skipped with active clients such as Microsoft Outlook*);
3. Both client are redirected to their organization's internal federation service;
4. The AD FS server authenticates the client to active directory;
    - * Internal clients are load balanced directly to an ADFS server farm member; and
    - * External clients are:
        - * Pre-authenticated to Active Directory via APM's customizable sign-on page;
        - * Authenticated users are directed to an AD FS server farm member.

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 Microsoft Federation Gateway where the token and claims are verified. The Microsoft Federation Gateway provides the client with a new service token; and
7. The client presents the new cookie with included service token to the Office 365 resource for access.

Virtual Servers and Member Pool – Although all users, (both internal and external) will access the ADFS server farm via the same Big-IP(s), the requirements and subsequent user experience differ. While internal authenticated users are load balanced directly to the ADFS farm, external users must first be pre-authenticated, (via APM) prior to be allowed access to an ADFS farm member. To accomplish this two, (2) virtual servers are used; one for the internal access and another dedicated for external access. Both the internal and external virtual servers are associated with the same internal ADFS server farm pool.

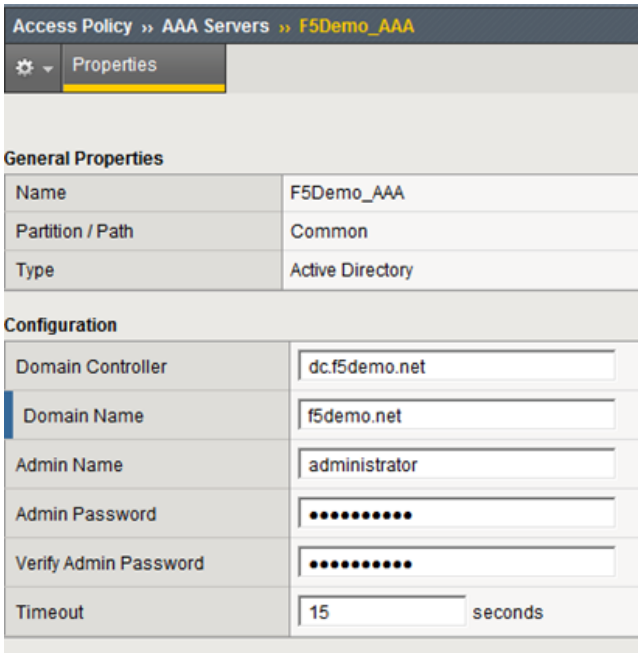
INTERNAL VIRTUAL SERVER – Refer to Part 1 of this guidance for configuration settings for the internal ADFS farm virtual server.

EXTERNAL VIRTUAL SERVER – The configuration for the external virtual server is similar to that of the virtual server described in Part 1 of this guidance. In addition an APM Access Profile, (*see highlighted section and settings below*) is assigned to the virtual server.

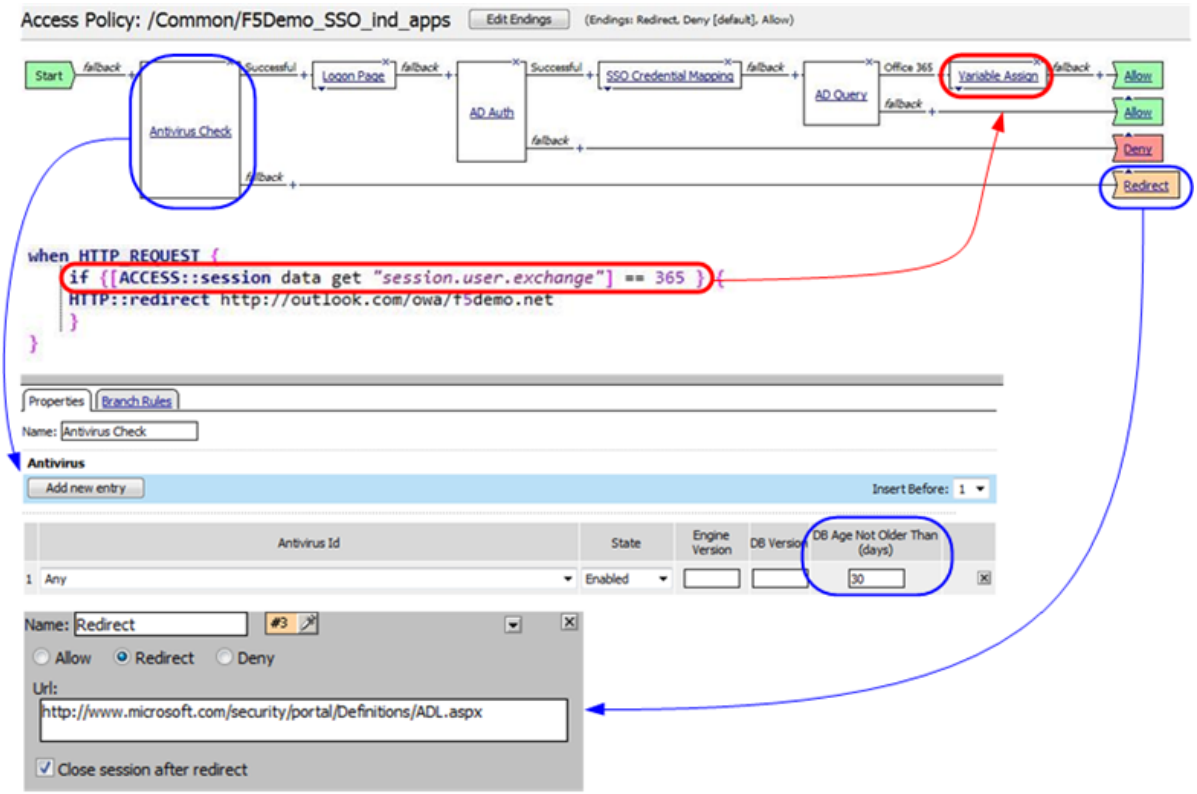


APM Configuration – The following Access Policy Manager, (APM) configuration is created and associated with the external virtual server to provide for pre-authentication of external users prior to being granted access to the internal ADFS farm. As I mentioned earlier, the APM module provides advanced features such as client-side checks and single sign-on, (SSO) in addition to pre-authentication. Of course this is just the tip of the iceberg. Take a deeper look at client-side checks at AskF5.

AAA SERVER - The ADFS access profile utilizes an Active Directory AAA server.

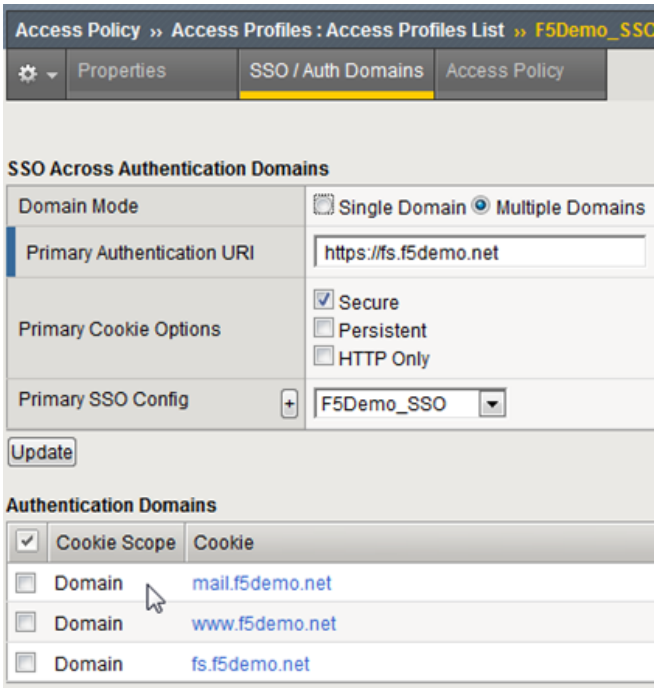


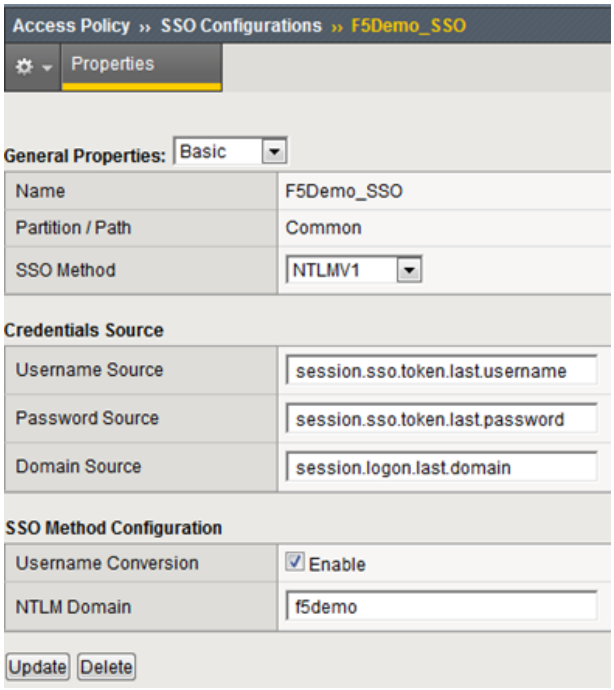
ACCESS POLICY - The following access policy is associated with the ADFS access profile.



- * Prior to presenting the logon page client machines are checked for the existence of updated antivirus. If the client lacks either antivirus software or does not have updated, (within 30 days) virus definitions the user is redirected to a mitigation site.
- * An AD query and simple iRule is used to provide single-url OWA access for both on-premise and Office365 Exchange users.

SSO CONFIGURATION - The ADFS access portal uses an NTLM v1 SSO profile with multiple authentication domains, (see below). By utilizing multiple SSO domains, clients are required to authenticate only once to gain access to both hosted applications such as Exchange Online and SharePoint Online as well as on-premise hosted applications. To facilitate this we deploy multiple virtual servers, (ADFS, Exchange, SharePoint) utilizing the same SSO configuration.





CONNECTIVITY PROFILE – A connectivity profile based upon the default connectivity profile is associated with the external virtual server.

Whoa! That's a lot to digest. But if nothing else, I hope this inspires you to further investigate APM and some of the cool things you can do with the Big-IP beyond load balancing.

Additional Links:

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

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

Latest F5 Information

- F5 News Articles
- F5 Press Releases
- F5 Events
- F5 Web Media
- F5 Technology Alliance Partners
- F5 YouTube Feed

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com