E Series FAQ: WAP Feature

Q: What is Web Application Proxy (WAP)?

A: WAP is a reverse proxy solution that publishes internal web applications for external access. The concept behind it is to streamline how users authenticate to web applications, and to provide a simple, integrated solution for both federation and remote access. In addition, WAP is designed to support consumer devices, BYOD initiatives, and Office application access.

Q: What are the requirements to deploy Web Application Proxy?

A: Infrastructure requires:

- Active Directory
- AD FS on separate hardware. The Celestix E Series solution can be configured for either role.
- DNS

Also, three types of certificates are required:

- Server Communication Certificate – an SSL certificate issued from a trusted third-party public CA is recommended, but an internal CA can be used.
- Token Signing Certificate – a self-signed certificate is created when AD FS is configured which is most commonly used, but a public or internal CA can also be used.
- Token Decrypting Certificate – a self-signed certificate is created when AD FS is configured which is most commonly used, but a public or internal CA can also be used.

Q: What kinds of devices can access published sites and applications? Are there additional requirements to facilitate some devices?

A: WAP allows nonmanaged computers, tablets, and smart phones to access published resources with no additional requirements.

Q: Does Web Application Proxy include an application firewall?

A: No. Recommended deployments should have edge security and a backend firewall.

Q: Does Web Application Proxy need to be joined to my corporate Active Directory domain?

A: Unless there are specific concerns or policies, the WAP server only needs to be joined to the production Active Directory when you are using Kerberos Constrained Delegation for application access.

Q. Can Web Application Proxy be deployed in a workgroup environment?

A. Yes.

Q: Where do I place the Web Application Proxy and federation (AD FS) servers?

A: Typically, the WAP server is placed in a DMZ segment to support external users while the AD FS server is installed in your internal network. This is subject to your organization's security policy.

Q: Will I need to have split DNS (same DNS namespace internally and externally?)

A: The short answer is yes. The federation server fully qualified domain name (FQDN) is the same for internal and external users. Internal users need to resolve the name to the internal AD FS server, whereas the external users need to be redirected to the external facing WAP servers. While there are methods to provide name resolution, for example adding a host record, split DNS is usually the recommended approach.

Q: Does Web Application Proxy support URL translation?

A: Yes, it supports translation of URLs from their external name to an internal name, as well as TCP ports. WAP also supports HTTPS, and HTTPS to HTTP bridging.

Q: Should we migrate from MSA or WSA?

A: If you are using either product for publishing internal applications, the WAP feature on the E Series could be a good fit. It offers new functionality that MSA does not have, namely the inclusion of federation services and enabling cloud application authentication.