White Paper

**Modernizing Microsoft Application Access with Web Application Proxy and Azure Active Directory Application Proxy**

**June 2015**

**Introduction**

*This document provides an overview of the features and benefits of using Microsoft Web Application Proxy and Azure Active Directory Application Proxy, which offers organizations a seamless way to secure their Internet-facing Microsoft applications including Exchange, SharePoint, and Lync.*

As the trends toward bring-your-own-device (BYOD) increase, Microsoft understands that remote/mobile access is a strategic area and continues to heavily invest in it. Our solutions for cloud and server technologies are an integral part of the Microsoft portfolio, with security continuing to play an important role in Microsoft’s overall management tool mindset.

On September 12, 2012, Microsoft announced the discontinuation of any further releases of certain Forefront branded solutions. Forefront Threat Management Gateway 2010 was one of those solutions. Mainstream support for Forefront TMG ended on April 14, 2015 and extended support will cease on April 14, 2020. In addition, mainstream support for another Forefront branded remote access solution, Forefront United Access Gateway (UAG), also expired on April 14, 2015, with extended support ending in on April 14, 2020. Widely deployed, there are a large number of organizations with active deployments of TMG or UAG as a security solution to protect internet-facing applications.

That said, for post end of life and end of support, organizations have other Microsoft solutions to address their reverse proxy needs. Microsoft Azure Active Directory (AD) Application Proxy and Microsoft Web Application Proxy can fill this role, while providing enhanced capabilities for integration with modern authentication and cloud-based technologies. Please see Table 1 for details on replacement options for the various roles and features offered by TMG and UAG.

**Comparing TMG/UAG Functionalities with Web Application Proxy and Azure AD Application Proxy Capabilities**

**TABLE 1. Microsoft Solution Evolution**

|  |  |
| --- | --- |
| **TMG/UAG Functionality** | **Web Application Proxy (WAP)/Azure AD Application Proxy (AADAP)** |
| Selective HTTP Publishing for Browser Apps | Available in WAP in Windows Server 2012 R2Available in AADAP today |
| ADFS Integration | Available in WAP in Windows Server 2012 R2 |
| Rich Protocols Publishing (e.g., Citrix, Lync, RDG) | Available in WAP in Windows Server 2012 R2Partially available in AADAP today – will be enhanced |
| Preauthentication for ActiveSync (HTTP Basic) and RDG | Will be available in WAP in Windows Server vNextWill be coming to AADAP |
| Portal | Use Intune / System Center for WAPUse AAD Access Panel or Office 365 App Launcher available for AADAP |
| Endpoint Health Detection | Use Intune / System Center |
| SSL Tunneling | Use Windows SSL-VPN capability |
| Layer 2/3 Firewall | Use Windows Server capabilities |
| Web Application Firewall | No current solution from Microsoft |
| Secure Web Gateway (Forward Proxy) | No current solution from Microsoft |

**Secure Access, Simple Administration: Azure AD Application Proxy and Web Application Proxy**

For organizations using Azure services or planning to, Azure AD Application Proxy gives remote or cloud users a simple and secure way to access on-premises web applications. Azure AD Application Proxy offers the following:

* Pre-authentication can now be accomplished using Azure AD before passing user requests across the proxy.
* Administrators can use Azure AD users and groups to grant access to on-premises web applications, such as SharePoint, Outlook Web Access, and IIS-based apps, with the ability to publish applications inside an organization’s private network.
* Deployment is simple and uncomplicated, with no demilitarized zone (DMZ) required.
* Users can easily access published web applications, on-premises and in the cloud, from a remote location using either home or mobile devices.

Microsoft Web Application Proxy for reverse proxy functionality is a remote access role service in Windows Server 2012 R2**.** Microsoft Web Application Proxy offers the following:

* Reverse proxy functionality for web applications inside the corporate network allows users on any device to access on-premises applications from outside the corporate network.
* Pre-authentication for access to web applications using Active Directory Federation Services (AD FS), and AD FS proxy functionality.

In addition, Microsoft Web Application Proxy in Windows Server vNext will offer the following capabilities:

* Ability to publish a specific domain name as well as an entire sub-domain for organizations that want to publish sites in bulk rather than one at a time. This is important when there is a need to publish SharePoint applications that use a special sub-domain for all applications. HTTP publishing for applications not using preauthentication ensures there is no leakage of sensitive information.
* HTTP to HTTPS redirection option reduces the risk of server spoofing and offers an improved user experience.
* Propagate client IP address to back-end application, adding to every request, “X-Forwarded-For” header that includes the address.
* Simplified Remote Desktop Gateway (RDG) publishing. AD FS can be used to perform preauthentication for Remote Desktop access using capabilities such as Multi-Factor Authentication and smartcards. Users receive the same experience as they do with their web applications. Admins have a convenient, single entry point to the system and a single authentication and authorization mechanism across all applications.
* Improved logging for better auditing and easier troubleshooting.
* Administrator UI enhancements include the ability to edit applications in the UI.

**Benefits of Microsoft Web Application Proxy**

Microsoft Web Application Proxy affords organizations all of the benefits of a secure network with a lower total cost of ownership (TCO) than hardware-based solutions for a number of reasons:

**A software-based solution that is simple to deploy, maintain, and scale:** Unlike most vendors that offer hardware-based solutions, Microsoft Web Application Proxy is software-based. With no additional appliances required, it is much easier to deploy, maintain, and scale than most hardware-based solutions.

**Favorable economics as part of Microsoft Windows 2012 R2:** Since Microsoft Web Application Proxy is software-based, startup and OpEx expenses are lower than those of a hardware-based system. This, in turn, provides organizations with a very low TCO.

**Consistent management with Windows workloads:** It’s not necessary to retrain existing workforce, or hire experts to publish applications. Users can manage them just as they would any other Windows workload. When it comes to publishing Microsoft Office servers (SharePoint, Lync, Exchange), Web Application Proxy provides all of the necessary capabilities. Web Application Proxy vNext will be available with the next version of Windows Server.

**Designed and built on modern security standards:** Most other vendors’ products are built on legacy protocol stacks using old security standards. Built from a fresh code base, the Web Application Proxy does not store passwords in memory, adding yet another secure layer to systems.

**The Hybrid Cloud and Microsoft Azure AD Application Proxy**

Over the last decade, keeping pace with new applications, supporting alternative endpoint devices, and maintaining security across a variety of networks has been challenging for businesses to successfully adapt. Organizations need to be agile to innovate and get to market quickly to stay ahead of the competition, while investing in long-term strategies that can easily adapt to change. This means being able to scale effortlessly and securely, reduce (if not eliminate) downtime, and consume minimal resources.

So how are organizations accomplishing this?

Many businesses are turning to the hybrid cloud, a combination of the public cloud and private cloud, to deliver the scalability, reliability, and protection they need to do business anytime, from any place.

The hybrid cloud provides organizations with:

**Easy scalability.** As needs change, organizations can quickly and seamlessly move data centers between public and private clouds, easily deploying workloads where it makes the most sense, and at no additional expense.

 **24/7 security**. The hybrid cloud provides organizations with a secure means of doing business, ensuring the security of web applications both inside and outside the corporate network—publishing, deploying, and managing applications without compromising security.

**Simple and efficient system administration.** Organizations can use a single pane of glass to see the entire hybrid infrastructure, offering IT central and comprehensive visibility into the corporate network and its data, applications, and files.

**Reliability and performance.** Businesses enjoy the same reliability and performance as they had with their previous system, using the same processes, tools, and resources.

**Cost containment and savings**. With the hybrid cloud, businesses can contain costs since they don’t require additional staff, retraining of existing staff, or purchasing, installing, and learning new management tools.

The hybrid cloud is a viable option that enables businesses to scale effortlessly, contain costs, and eliminate the burden of a substantial TCO. It also provides the reliability, performance, and level of security needed to ensure the protection of web applications, both inside and outside the corporate network.

**Enterprise Mobility Is Key to Staying Competitive**

Businesses today need a convenient and secure means for their workforces to access information anywhere, at any time, and from any place. While this may be second nature for the non-corporate user, there’s a great deal that the business must deal with—it’s about how organizations enable employees, customers, and partners to easily access the corporate cloud. And when you add BYOD to the mix—with the workforce using laptops, tablets, smartphones, thin clients, and other mobile devices—organizations need to get serious about how they’re going to protect the network, while giving those connected to it simple and intuitive access, and a seamless experience. Additionally, it’s essential that those devices and services used by the workforce are developed with a focus on ease of use and an improved and productive experience.

Microsoft believes that businesses must embrace mobile productivity to stay ahead of the competition. The Microsoft mobility platform provides office and collaborative solutions with mobile applications available for current lines of business, as well as custom-built applications that provide an enhanced user experience for any mobile device, corporate or personal, with a high level of security.

**Looking Forward**

Microsoft solutions enable IT to embrace a simplified software-based solution with a set of consistent management tools that IT administrators are familiar with. In addition, the economic efficiencies in Microsoft’s software-based approach enable businesses to federate user identity and access management, while at the same time protecting the data.

Though not direct replacements for the Microsoft Threat Management Gateway, Microsoft is offering its new solutions, Microsoft Web Application Proxy and Azure Active Directory Application Proxy, as those built from the ground up to ensure security, enhance the user experience, simplify system administration, and lower the total cost of ownership. Although both TMG and UAG have five more years of extended support, Microsoft recommends that its customers begin evaluating replacement strategies.

Microsoft is committed to the on-going development of Azure AD Application Proxy and Web Application Proxy. As such, we will be bringing out new features and functionality to support our vision, and deliver continued value to our customers so that organizations can continue their expansion into the cloud without compromising security.

**References –**

<https://msdn.microsoft.com/en-us/library/azure/dn768219.aspx>

<http://blogs.technet.com/b/applicationproxyblog/archive/2014/10/01/introducing-the-next-version-of-web-application-proxy.aspx>

[https://msdn.microsoft.com/en-us/library/windows/desktop/dn323740(v=vs.85).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/dn323740%28v%3Dvs.85%29.aspx)

<https://technet.microsoft.com/en-us/library/dn584107.aspx>

<http://channel9.msdn.com/events/Ignite/2015/BRK3864>