SAFE-T RSACCESS REPLACEMENT FOR MICROSOFT FOREFRONT UNIFIED ACCESS GATEWAY (UAG)

A RSACCESS WHITE PAPER

SAFE-T

Smart Security Made Simple.

1. Microsoft Forefront Unified Access Gateway Overview

Forefront Unified Access Gateway 2010 delivers comprehensive, secure remote access to corporate resources for employees, partners, and vendors from a diverse range of endpoints and locations, including managed and unmanaged PCs and mobile devices. Building on the secure remote access capabilities in Microsoft Intelligent Application Gateway 2007, Forefront UAG draws on a combination of connectivity options, ranging from SSL VPN to Windows® DirectAccess, as well as built-in configurations and user's identity based policies.

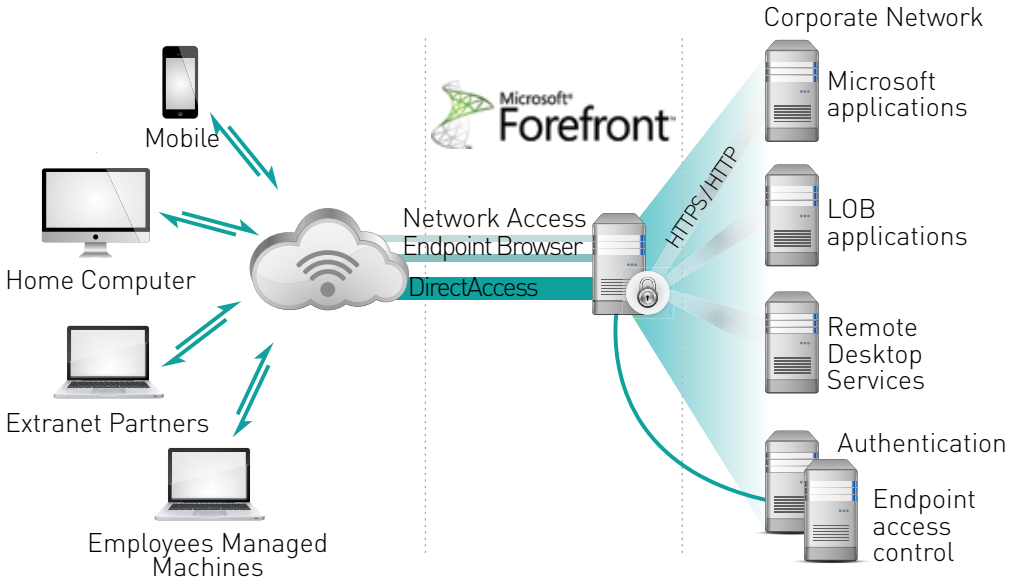

Figure 1 - Microsoft Forefront UAG Topology

In the following paper we will be addressing one of Microsoft Forefront UAG's main deployment scenarios, which is deploying Forefront UAG as a publishing server. In this deployment, internal applications and resources are published via Forefront UAG. And the applications can be accessed by remote client endpoints, either directly, or via the Forefront UAG Web portal.

On Dec. 17, 2013, Microsoft announced changes to the roadmaps of its Forefront identity & access products, including the discontinuation of Forefront Unified Access Gateway (UAG). According to Microsoft, it will continue to provide mainstream support for Forefront UAG 2010 through April 14, 2015, and extended support through April 14, 2020. For more details, read the article-
Important Forefront Roadmap Update.

2. Safe-T RSAccess Secure Front-end Overview

RSAccess is Safe-T's Secure Front-End and application publishing solution for securing the network from the outside. It removes the need to open any ports within the internal firewall and provides unmatched protection for enterprise data networks from the Internet and other public networks.
RSAccess Secure Front-End solution is a two tier TCP reverse-proxy solution:

1. External RSAccess Node – installed in the DMZ segment
2. Internal RSAccess Node – installed on a LAN segment

The role of the external RSAccess node is to act as a front-end to all services and applications published within the DMZ. It operates without the need to open any ports within the external firewall and ensures that only legitimate session data can pass through into the LAN.
It can be deployed in two main locations within the DMZ: The first is before the web/application front-ends, essentially replacing them completely. The second is after the web/application front-ends providing an additional layer of defense within the DMZ and preventing any attacks from being generated from within the front-end servers.

The role of the internal RSAccess node it to pull the session data into the LAN from the external RSAccess node, authenticate it using a variety of mechanisms, scan it using various security techniques including an application firewall, and then pass it to the destination application server.
For more information on Safe-T RSAccess, read the **Safe-T RSAccess white paper**

Figure 2 - Safe-T RSAccess Secure Front-end Solution Topology

3. Safe-T RSAccess Secure Front-end as a Microsoft Forefront UAG Alternative

3.1 General Comparison

With the announcement of the Forefront UAG discontinuation, enterprises are now in search for a replacement. As the next generation in application publishing, Safe-T's RSAccess is well positioned to replace Forefront UAG when it is used as a publishing server.
As can be seen in the table below, Safe-T RSAccess not only provides an adequate replacement for Forefront UAG feature set in the application publishing scenario, but it also provides additional benefits not provided by Forefront UAG.

	Safe-T RSAccess	Microsoft Forefront UAG
Forefront UAG Documented Features		
Publish Microsoft Applications	✓	✓
Publish non-Web Applications	✓	✓
Client Access	Directly	Portal / Directly
Anywhere access	✓	✓
Advanced authentication schemes	✓	✓
Secure Sockets Layer (SSL) termination	✓	✓
Application protection	✓	✓
URL inspection	✓	✓
HTTP filtering	✓	✓
Unique RSAccess Features		
Allows closing incoming ports in the Firewall	✓	✗
Provide reverse-proxy connectivity to DBs	✓	✗
Low Network Footprint	✓	✗
Built-in Open ID based authentication	✓	✗

3.1.1 Publish Microsoft and non-Web Applications

Similar to Forefront UAG, RSAccess supports publishing both Microsoft as well as non-web applications. This is done by configuring the RSAccess solution to take over the IP address of the published service, then any request to the service is routed to the RSAccess solution which handles it and passes the request to the relevant application server.

3.1.2 Client Access

The RSAccess solution provides direct access to clients to the published applications. Rather than accessing a portal via which the application is accessed, the client accesses the application's portal or login window directly through the RSAccess solution.
This allows publishing all types of applications, as discussed in the item above.

3.1.3 Anywhere Access

RSAccess is completely agnostic to the client end-point, supporting all types of end-points, including PCs, laptops, tablets, or smartphones.

3.1.4 Advanced Authentication Schemes

RSAccess supports a wide range of built-in authentication mechanism, to authenticate users accessing applications it front-ends (publishes). Authentication can be done using:

- The organization's LDAP or Active Directory systems.
- PKI or Token-based systems
- Open ID / SAML, allowing to authenticate users using the user's existing personal social network credentials. This feature is unique to RSAccess, see section 3.2.4, for additional information.

3.1.5 Secure Sockets Layer (SSL) termination

RSAccess supports terminating end user SSL connections, allowing to offload the SSL handshake from the application server, while providing a single point of management for certificates.

3.1.6 Application Protection, URL Inspection, and HTTP Filtering

To ensure protection of the published application, RSAccess provides the following layers of security protection

1. **Block Layer 3 and Layer 4 level attacks –** the main benefit of Safe-T's unique technology, which allows passing session data into the internal network without opening any inbound ports on the internal firewall, is that it allows the complete blocking of any network or Layer 4 based attacks such as port scanning, ICMP scanning, TCP bases attacks, etc from attacking the firewall and internal network.

2. **Block Application level attacks –** In case a hacker attempts to generate an application level attack such as application exploits, malware, etc, to traverse the RSAccess solution, the attack will be blocked by RSAccess's built-in application firewall. RSAccess built-in application firewall inspects and controls incoming traffic on the application layer to detect and mitigate attacks of RFC manipulation both on clear channels and encrypted channels such as HTTPS.

3. **URL inspection and HTTP filtering –** RSAccess built-in application firewall, also supports URL inspection and HTTP filtering capabilities, ensuring only the actual application URL and domain name is used.

3.2 RSAccess Unique Features

3.2.1 Allows closing incoming ports in the Firewall

For Forefront UAG to operate, the IT administrator must allow certain protocols to pass from the Forefront UAG located in the DMZ, through the internal firewall and connect to specific hosts in the internal network (e.g. TCP 80/443 for web or Microsoft SharePoint applications). With this configuration, Forefront UAG can access the internal network directly.
The fact that ports must be opened in the firewall, between the DMZ and internal network, means the

firewall and internal network become susceptible to a variety of L3-4 based attacks – Port scanning, IP Spoofing, Ping Flood, ICMP attacks, TCP bases attacks, etc.

However, as described above, RSAccess does not open any ports in the internal firewall in order to publish internal application, ensuring that the DMZ and LAN are totally separated environments, and preventing any attacks from targeting the internal firewall or network.

3.2.2 Provide Reverse-proxy Connectivity to Databases

While Forefront UAG supports publishing both web and non-web applications, it is still designed to publish applications rather than TCP protocols.
Contrary to UAG, RSAccess is a TCP based reverse-proxy solution, allowing it to publish and front-end any TCP based application and traffic including database traffic.
In scenarios, where the application's DMZ based tier includes both a front-end server and database server (e.g. Oracle EBS external web-tier or SharePoint), this ability of RSAccess allows migrating the database server into the LAN, preventing any hacker from attacking it, while ensuring the front-end server can still access it.

3.2.3 Low Network Footprint

Microsoft Forefront UAG runs on Windows Server 2008 R2, which means it has a visible network footprint, making it vulnerable to attacks, as was published in the Microsoft Security Bulletin MS12-026. The fact that Forefront UAG is vulnerable, means that if an external attacker compromises it, then it will be then able to get access into the company's internal servers, applications, and internal network.
Contrary to Forefront UAG, the external RSAccess node has a very low network footprint, making it much less vulnerable to hacking attempts, and taking control of it to initiate attacks.

3.2.4 Built-in Open ID Based Authentication

As opposed to Forefront UAG which requires 3rd party products to deliver the authentication mechanism, RSAccess supports a variety of built-in authentication mechanisms, including Open ID / SAML based authentication.
RSAccess enables authenticating either registered users or ad-hoc users using the user's existing personal social network credentials including all common social networks, such as Facebook, Google, Live ID, etc.
In addition RSAccess can also perform additional validations such as security questions (name of 1st pet, etc) after the user is authenticated by the social network provider. The validation questions can be verified by RSAccess itself or any other 3rd party data base.
The combination of the social network authentication with the additional validation, provides a unique three-way authentication mechanism. Which in addition to being more convenient for the user, provides high levels of security, and also greatly reduces the operational complexity of organizations, as there is no longer a need to store and manage large numbers of user credentials.

4. Conclusion

In conclusion, Safe-T RSAccess Secure Front-end, offers Microsoft Forefront UAG customers with a unique solution which offers not only the full set of publishing features provided by Forefront UAG, but also additional security features which enhance the security posture of the organization.
To learn more about RSAccess please - http://www.safe-t.com/rsaccess/