Forefront UAG DirectAccess Provides Anywhere Access to Corporate Resources for Mobile Workers

Situation

Over the past few years, advances in mobile computers and wireless broadband have enabled users to be more productive while away from the office. The changing structure of business puts more pressure on IT professionals to provide a high-performance infrastructure while minimizing costs. Traditional VPN networks cause connectivity delays and present challenges in maintaining security and managing remote users.

Solution

Microsoft IT implemented DirectAccess, a new feature in Windows 7 and Windows Server 2008 R2, to provide remote users with seamless access to internal network resources whenever they are connected to the Internet. Forefront UAG enhances DirectAccess to improve availability and extend the benefits of DirectAccess to IPv4-based corporate resources.

Benefits

* Improved end-user experience
* Improved remote monitoring for system health and management
* Seamless access to both IPv6 and IPv4 resources and servers
* Centralized Forefront UAG server array and DirectAccess client configuration management
* Potential cost-saving mechanism

Products & Technologies

* Microsoft Forefront Unified Access Gateway 2010
* DirectAccess
* Windows Server 2008 R2
* Windows 7
* IPsec
* IPv6
* Network Access Protection
* Smart cards

Published: June 2010

Microsoft Information Technology (Microsoft IT) deployed the DirectAccess feature in the Windows® 7 and Windows Server® 2008 R2 operating systems to enable employees to gain seamless remote access to corporate applications and data. The solution, which includes Microsoft® Forefront® Unified Access Gateway (UAG) 2010 and requires only Internet connectivity and credentials, significantly improves productivity and can reduce costs.

Today’s workforce is more mobile than ever. According to IDC, the third quarter of 2008 marked the point at which computer manufacturers began shipping more mobile computers than desktop computers worldwide (IDC Worldwide Quarterly PC Tracker, December 2008). IT professionals must provide an infrastructure to enable mobile workers to remain productive.

Although broadband services and Wi-Fi have dramatically improved in recent years, the connectivity experience for remote corporate users remains largely unchanged. Microsoft IT is the core group that is responsible for supporting the technology infrastructure at Microsoft. As such, it possesses firsthand experience in building and maintaining traditional network technologies from the perspective of both end users and IT administrators.

This case study describes Microsoft IT's use of Forefront UAG and DirectAccess (called Forefront UAG DirectAccess when implemented together) to improve the way employees connect to the Microsoft corporate network. This case study is intended for technical decision makers and network architects who are considering a similar solution. It assumes that readers have a basic understanding of corporate networks and networking technologies.

Situation

To maximize productivity, employees need to have access to intranet resources wherever they are. Providing this level of connectivity in a secure, manageable, and seamless way has been difficult with traditional virtual private networks (VPNs). Connecting to a VPN requires multiple steps, which causes delays while users wait for authentication. Two common challenges that remote workers have with traditional VPNs are:

* The manual effort and time required to establish a connection to the corporate network by using the appropriate gateway and tunnel type.
* The manual effort involved in resetting the connection each time the computer system is restarted or whenever the user moves to a different network access point or is otherwise temporarily disconnected from the network.

Because of these inconveniences, IT organizations sometimes choose to deploy application gateways in order to provide users with intranet access across a firewall. Although application gateways can be excellent point solutions, not all application access problems are solved through gateways; at times, users still may be unable to access intranet file shares or other important applications and resources. More significantly, the more end users are disconnected from the corporate network, the harder it is for IT professionals to manage the users' computers. This situation increases the risk of a computer becoming "unhealthy"—out of compliance with security guidelines.

Solution

To better support how the Microsoft remote workforce accesses the corporate network, Microsoft IT implemented the DirectAccess feature in Windows 7 and Windows Server 2008 R2. DirectAccess improves the user experience and worker productivity, enhances the manageability of remote client computers, and offers a more robust security model than is available in traditional VPNs. In addition, Forefront UAG DirectAccess allows for the consolidation of DirectAccess server roles in an easily managed load-balanced server array, and it includes Internet Protocol version 4 (IPv4) transition technologies to extend DirectAccess connectivity to older network resources. These capabilities enable Microsoft IT to provide comprehensive access, management, and support to all client computers at Microsoft, not just those connected directly to the corporate network.

Beyond the technological benefits, Forefront UAG DirectAccess is an important cost-saving mechanism that enables the Internet-connected branch offices at Microsoft to maintain efficient and security-enhanced connections to the corporate network instead of spending an estimated $250,000 US in initial capital costs to upgrade a single facility to a dedicated connection. (Such costs include purchasing racks, servers, network equipment, uninterruptible power supplies, cardkeys, cooling, and other infrastructure.) In addition, circuit maintenance for a dedicated connection costs about $50,000 per year per facility. Avoiding these expenditures saves an average of $300,000 per remote facility in the first year alone.

End-User Experience

DirectAccess uses Internet Protocol security (IPsec) for authentication and encryption to help provide a secure connection to the corporate network without using a VPN. Users can readily access corporate-network file shares, intranet Web sites, and line-of-business applications through DirectAccess wherever an Internet connection is available.

Always-on, Transparent Connection to the Corporate Network

From the user's perspective, DirectAccess is always on. It offers the same connectivity experience both inside and outside the office.

DirectAccess provides a communication channel through the Internet by using standard ports such as Transmission Control Protocol (TCP) 443. This ability translates to significant productivity improvements for remote workers at their customer sites or in other remote locations that have restrictive port or firewall policies. With DirectAccess, employees can access corporate resources from remote branch offices, extranets, or even while connected to a public Wi-Fi hotspot.

Organizations can configure DirectAccess in a variety of ways to provide a connection to the corporate network without requiring any user input (often called a transparent connection). When Microsoft IT enables DirectAccess, Windows 7 directs requests for resources such as e-mail, shared folders, or access to intranet Web sites on the corporate network without requiring users to connect to a VPN.

Separate Connections to the Corporate Network and the Public Internet

DirectAccess directs corporate traffic through a security-enhanced connection while allowing public traffic to connect directly to the Internet through the user's Internet service provider (ISP) without passing through the corporate network. This separation of private and public data streams, known as split tunneling, can provide a cost benefit because organizations do not need to pay for the bandwidth of Internet traffic being routed through the corporate network.

Split tunneling also helps organizations comply with international regulations for data transmission. Routing confidential data through the appropriate private network is especially important for remote users who are working in countries (such as France and Switzerland) that regulate how different types of data can be transmitted.

Manageability

DirectAccess enables Microsoft IT to better manage computer systems, such as laptops, that are frequently moved outside the corporate network. When a laptop with Internet connectivity is running DirectAccess, the laptop is always connected to the corporate network. From the administrator's perspective, this always-on connection:

* Promotes timely security scans
* Simplifies updates to Group Policy
* Allows the computer to download security and system updates as soon as they are required, even if the user is not logged on

This functionality enables Microsoft IT to service remote computers on a regular basis and helps ensure that remote users stay up-to-date with company policies. The remote computers at Microsoft that are not yet using DirectAccess are more challenging for Microsoft IT to manage.

The Forefront UAG array consists of up to eight servers. Microsoft IT manages the array as a single entity, as opposed to managing each server individually. Microsoft IT integrates Network Load Balancing (NLB) functionality provided by Windows Server 2008 R2 to scale the capacity of the array.

In addition to the built-in capability of Windows Server 2008 R2 to monitor DirectAccess by using the DirectAccess Monitoring snap-in, Microsoft IT deployed the Forefront UAG Management Pack for Microsoft System Center Operations Manager to monitor Forefront UAG arrays as a single entity. Together or separately, these tools provide the ability to monitor traffic activity and events, and to raise alerts if transport protocols or other services are not working.

System Design

The following figure illustrates the major components in the architecture of the Forefront UAG DirectAccess system that Microsoft IT implemented.



Figure 1. Architecture of Microsoft IT's Forefront UAG and DirectAccess implementation

The following sections discuss the connectivity and security technologies that Figure 1 summarizes.

Connectivity

Microsoft IT uses the following DirectAccess technologies to initiate and maintain a connection with the corporate network.

IPv6

DirectAccess clients maintain constant connectivity with the intranet, and Internet Protocol version 6 (IPv6) provides the end-to-end addressing necessary to accomplish this. Clients establish an IPsec tunnel over the IPv6 protocol to the Forefront UAG array, which acts as a gateway to the internal network. The preceding figure shows a DirectAccess client connecting to a Forefront UAG array across the public IPv4 Internet.

DirectAccess includes the following IPv6 transition technologies to enable IPv6 connectivity over the IPv4 Internet:

* Teredo (RFC 4380): Provides IPv6 connectivity across the IPv4 Internet for hosts that are located behind an IPv4 network address translation (NAT) device and assigned a private (RFC 1918) IPv4 address.
* 6to4 (RFC 3056): Provides IPv6 connectivity across the IPv4 Internet for hosts or sites that have a public IPv4 address.
* IP over Hypertext Transfer Protocol Secure (IP-HTTPS): A new protocol for Windows 7 and Windows Server 2008 R2. Allows hosts behind a Web proxy server or port restricted firewall to establish connectivity by tunneling IPv6 packets inside an IPv4-based HTTPS session. HTTPS is used instead of Hypertext Transfer Protocol (HTTP) so that Web proxy servers will not attempt to examine the data stream and terminate the connection. Performance of IP-HTTPS may be lower than that of the other DirectAccess connection protocols, due to additional protocol and encryption overhead.

Determination and Configuration of Network Location

To determine the reachability of intranet resources and a computer's proximity to them, the DirectAccess client requires several configuration settings. These settings are configured during the Forefront UAG DirectAccess setup process through the Forefront UAG Management Console. They consist of the following:

* The intranet IPv6 address prefix (if the intranet is native IPv6)
* The Domain Name System (DNS) name for intranet resources that are reachable through the infrastructure tunnel
* The IP addresses and fully qualified domain name (FQDN) on the external interface of the DirectAccess server that is reachable from the Internet
* The HTTPS-based URL for the network location server

The DirectAccess client uses this information to independently determine whether intranet resources are reachable and whether the client is connected to the intranet or the Internet.

Extension of DirectAccess to IPv4-Based Resources

DirectAccess requires end-to-end IPv6 communication between DirectAccess clients and the internal resources that they connect to on the corporate network. Many corporate resources cannot be directly accessed through IPv6, including computers that are not capable of running IPv6 or computers with services that are not IPv6 aware.

To extend the reach of DirectAccess, Forefront UAG uses integrated NAT64 and DNS64 IPv6/IPv4 translation technologies to enable clients to access IPv4-based resources in addition to IPv6-based resources. These technologies intercept DNS queries so that the replies can be modified to appropriately translated IPv4 and IPv6 addresses.

The servers in the Forefront UAG array receive the IPv6 traffic from DirectAccess clients and convert it into IPv4 traffic on the other side. The address conversion and conversation handling operate in a similar way to a traditional IPv4 NAT device. These integrated translation technologies enable DirectAccess clients to reach all resources on the entire corporate network in most cases, without requiring the purchase of additional network translation devices.

Security

DirectAccess supports a variety of complementary security components from which an organization can choose in order to conform to its security policies. In its current deployment, Microsoft IT is using the following set of security technologies with DirectAccess.

Two-Factor Authentication

Microsoft IT’s current implementation of DirectAccess requires two-factor authentication. Remote workers must use a smart card, in addition to a user ID and password, to access corporate resources.

IPsec

DirectAccess uses IPsec to provide encryption for communications across the Internet. IPsec provides true end-to-end security for data transmissions, helping to protect data all the way to the application servers. IPsec helps DirectAccess protect communication by allowing any two domain-member computers to communicate regardless of where those computers are or how they are physically connected to the network.

Network Access Protection

Network Access Protection (NAP) is a policy-enforcement platform built into Windows. NAP is a key component of Microsoft IT security requirements. DirectAccess also integrates well with NAP to perform these critical functions:

* Health evaluation: NAP provides a customizable definition of security and configuration health policy. Computers obtain NAP health certificates by contacting a NAP Health Registration Authority (HRA) and proving their compliance with a health policy that is located and evaluated on the NAP server.
* Network access control: DirectAccess requires proof of health certificate to control or restrict access to the network. While a computer is healthy, it has complete access to the corporate network. Unhealthy systems can access only remediation servers that may provide required updates to bring an unhealthy system up to standard.
* Automatic remediation: For computers that are unhealthy, the automatic remediation feature in NAP drives the computer to a healthy state by automatically correcting aspects of the computer's security and configuration that are not compliant. The system then automatically reconnects to the corporate network.
* Compliance reporting: NAP stores data about compliance with computer health policies, and related data, in a database. Administrators can use the data for reporting purposes to assess the compliance state of computers, groups of computers, or an entire organization.

Server and Domain Isolation

Server and Domain Isolation enables administrators to logically segment the Windows environment into more secure and isolated logical networks based on IPsec policy without costly changes to the network infrastructure or applications. This creates an additional layer of policy-driven protection and helps accomplish the following:

* Protects against costly network attacks
* Prevents unauthorized access to trusted networked resources
* Achieves regulatory compliance
* Reduces operational costs

Server and Domain Isolation is fully compatible with DirectAccess.

Deployment Considerations

Forefront UAG and DirectAccess provide a flexible solution that can be deployed in different ways to meet an organization's specific requirements. The options fall into three areas: the access model, the scalability model, and the deployment model.

There are two primary access models from which to choose:

* Full intranet access (end-to-edge): The full intranet access model allows DirectAccess clients to connect to all resources inside the intranet. It does this by using IPsec-based tunnel policies that require authentication and encryption and IPsec sessions that end at the IPsec gateway.
* Selected server access (end-to-end): This model is very similar to the full intranet access model. IPsec-based tunnel policies that require encryption to the IPsec gateway still help protect communication between the DirectAccess client and the IPsec gateway. However, this model includes an additional authentication mechanism. By creating an additional IPsec rule that requires Encapsulating Security Payload (ESP)+NULL or an Authentication Header (AH) from the client to the application server, the client’s communications will be encrypted to the IPsec gateway and authenticated at the application server. This helps ensure that the DirectAccess clients are communicating with the intended servers. Microsoft IT uses a combination of this model and the full intranet access model for DirectAccess implementation.

There are three deployment models from which to choose:

* Single server: In the single-server scenario, all of the components of Forefront UAG and DirectAccess are hosted on the same server computer. The benefit of this scenario is a relatively simple deployment that requires only one Forefront UAG DirectAccess server. The limitations of this scenario are a single point of failure and server performance bottlenecks that can limit the maximum number of concurrent DirectAccess connections.
* Multiple servers in a Forefront UAG array for high availability and load balancing: If high availability or capacity beyond a single server is a priority, the multiple-server Forefront UAG array configuration will reduce the chance of network outages and provide a means to scale capacity for greater numbers of client connections. An organization can configure up to eight servers as nodes in a single array. This is the model that Microsoft IT deployed, by using a seven-node Forefront UAG server array that the team manages as a single entity with integrated NLB.
* Multiple Forefront UAG arrays for additional scale: If an organization needs additional scalability beyond a single, eight-node array, it can deploy multiple arrays and combine them as one logical service by using round robin DNS.

An organization can use the following methods to deploy and configure Forefront UAG DirectAccess resources:

* Forefront UAG Getting Started Wizard: Forefront UAG provides a deployment wizard called the Getting Started Wizard that runs automatically after installation, to help configure network adapters and Microsoft Update settings. Microsoft IT used this wizard to create and configure the seven-node Forefront UAG server array.
* Forefront UAG DirectAccess Configuration Wizard: DirectAccess works for managed computers that are domain members. The Forefront UAG DirectAccess Configuration Wizard creates and deploys Group Policy objects (GPOs) that provide a policy-based method to create, distribute, and apply DirectAccess settings to clients. This allows for one-time and ongoing enforcement of DirectAccess settings. GPOs are used by DirectAccess Setup and may optionally be used in a scripted setup.

Deployment at Microsoft

Before the availability of Forefront UAG, Microsoft IT conducted a 100-user pilot on a single DirectAccess server based on the DirectAccess technology native to Windows. Microsoft IT then deployed four individual DirectAccess servers to provide DirectAccess to additional remote users. The team deployed DirectAccess to groups of users in one Active Directory® domain at a time, starting with the smallest domains.

When a beta version of Forefront UAG became available in July 2009, Microsoft IT deployed a seven-node Forefront UAG array. The team then migrated the DirectAccess users to the array by reconfiguring the DirectAccess client settings by using GPOs. With the availability of Forefront UAG, most organizations will be able to begin their implementation of DirectAccess with a Forefront UAG array, avoiding the need for even the simple migration activity that Microsoft IT performed.

By July 2009, 5,000 remote users were connected to the Microsoft corporate network through DirectAccess. That number increased to 11,000 by November 2009 and continued to grow from there. Microsoft IT expects to eventually deploy DirectAccess across the enterprise to more than 100,000 users.

Best Practices

Microsoft IT developed the following best practices for deploying a DirectAccess–based solution to give remote users transparent access to internal network resources:

* Deploy Forefront UAG in combination with DirectAccess to gain the added benefits of server-array scalability and manageability, and to extend the reach of DirectAccess to IPv4-based corporate resources.
* If possible, configure the intranet routing infrastructure to support native IPv6, or to be IPv6 aware, by using Intra-Site Automatic Tunnel Addressing Protocol (ISATAP). Computers running the Windows Vista®, Windows 7, Windows Server 2008, and Windows Server 2008 R2 operating systems are configured to use IPv6 by default. Native IPv6 transport allows for end-to-end IPsec between the DirectAccess client and the resource to which it connects.
* Deploy IP-HTTPS as soon as possible. IP-HTTPS is enabled automatically when an organization uses Forefront UAG DirectAccess. Microsoft IT has seen many ISPs, corporations, metropolitan area networks (MANs), and others block User Datagram Protocol (UDP) 3544 outbound, but TCP 443 (IP-HTTPS) is usually an open outbound port.
* Consider the challenges of split DNS infrastructures—where the same namespace is used with different records. DirectAccess clients are essentially forced to resolve either the internal or the external namespace via the Name Resolution Policy Table (NRPT); the DirectAccess clients cannot resolve both. For Microsoft IT, the internal namespace is the preferred choice, with NRPT exceptions for the external FQDNs that clients must be able to resolve.
* Treat the network location server as a very important part of the infrastructure for remote network access. Because of the network location server's mission-critical role, an organization should deploy it by using clustering on a high-availability network to minimize downtime.
* Use Group Policy to manage system configurations, and be sure to first perform a pilot test for all GPOs by restricting access to a security group for pilot users (and systems).
* Implement DirectAccess with NAP to enable system health monitoring and to support automatic remediation of computer health issues. Microsoft IT opted to deploy the NAP HRA and remediation servers on the Internet in order to provide the benefits of NAP to computers that are not running DirectAccess in addition to those that are.
* For additional security, require two-factor authentication with smart cards when using DirectAccess, and use encryption on all communication to and from DirectAccess clients.

Benefits

By implementing the Forefront UAG DirectAccess solution, Microsoft IT derived the following benefits for end users and administrators:

* Greater availability of resources, easier updates: Whenever the client computer is on the Internet, it has a connection to the intranet. This connectivity makes remote client computers easy to access and update, and it makes intranet resources always available.
* Increased user productivity: DirectAccess provides a consistent connectivity experience whether the client computer is local or remote. It enables users to focus more on productivity and less on connectivity options and process, which can result in decreased training costs for users and fewer support incidents. In addition, support of IP-HTTPS in DirectAccess improves client connectivity rates even when the deployment is behind firewalls and Web proxies. With Forefront UAG, DirectAccess clients can seamlessly access both IPv6-based and IPv4-based resources and servers by using NAT64 and DNS64 translation technologies.
* Greater security: The use of IPsec over IPv6 with two-factor authentication and the use of NAP and smart card authentication help ensure that computers are compliant with IT security and configuration requirements.
* Reduced manual input for configuration changes: Multiple Forefront UAG servers can be grouped into an array of up to eight nodes where all members share the same configuration, including DirectAccess settings. Administrators need to make configuration changes on only one server—the array manager—and those changes will propagate to all members of the array. Client connections are also natively load-balanced across the array members through integrated NLB.
* Easier enforcement policies: DirectAccess fully integrates with Server and Domain Isolation and Network Access Protection solutions. Because of this integration, policies related to security, access, and health requirements seamlessly integrate between computers on the intranet and remote computers.
* Easier remote management: DirectAccess is a bidirectional communication link that allows IT administrators to connect directly to clients to monitor them, manage them, and deploy updates, even when users are not logged on but have Internet connectivity. This can reduce the cost of managing remote computers by keeping them up-to-date with critical updates and required configuration changes.
* Cost savings: Forefront UAG DirectAccess enables Internet-connected branch offices at Microsoft to maintain efficient and security-enhanced connections to the corporate network instead of spending an estimated $250,000 to upgrade each facility to a dedicated connection and $50,000 per year to maintain circuits in each facility.

Conclusion

Microsoft IT is addressing the productivity and security needs of the Microsoft remote workforce by implementing Forefront UAG DirectAccess as the preferred technology for network access. By using Forefront UAG DirectAccess to replace traditional VPN solutions, Microsoft IT can offer end users a completely transparent connection to the corporate network wherever they have access to the Internet.

DirectAccess enables management of computer systems at all times, as if the computer were physically located on the corporate network. At the same time, remote computers running DirectAccess with NAP can be constantly monitored for system health. Administrators can update the system and automatically remediate computer health issues, even when the user is not logged on. In addition, the solution can save costs by enabling some offices to avoid upgrading to a dedicated connection.

Although Forefront UAG DirectAccess is in the early stages of use, Microsoft IT expects that it will handle more than 90 percent of Microsoft domain-member remote clients in the next three years.

For More Information

For more information about Microsoft products or services, call the Microsoft Sales Information Center at (800) 426-9400. In Canada, call the Microsoft Canada information Centre at (800) 563-9048. Outside the 50 United States and Canada, please contact your local Microsoft subsidiary. To access information via the World Wide Web, go to:

<http://www.microsoft.com>

<http://www.microsoft.com/technet/itshowcase>

<http://www.microsoft.com/directaccess>

<http://www.microsoft.com/forefront/unified-access-gateway/en/us/default.aspx>

© 2010 Microsoft Corporation. All rights reserved.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. Microsoft, Active Directory, Forefront, Windows, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.