Microsoft's Role in Remote Access VPNs

Version: 1.0, Jan 19, 2004

AUTHOR(S):

Dave Kosiur
(dkosiur@burtongroup.com)

TECHNOLOGY THREAD:

WANs and Provider Network Services

Conclusion

Microsoft now offers a full-featured solution for remote access virtual private networks (VPNs) using Point-to-Point Tunneling Protocol (PPTP) or Layer-2 Tunneling Protocol/IP Security (L2TP/IPSec), based on Windows Server 2003 and the VPN client software that was updated when Server 2003 was introduced. But this VPN solution will appeal most to Windows-only shops since many of the appealing features will not work with third-party VPN gateways.

BURTON GROUP 7050 Union Park Center · Suite 510 · Midvale, Utah · 84047
P 801.566.2880
F 801.566.3611
www.burtongroup.com

Publishing Information

Burton Group is a research and consulting firm specializing in network and applications infrastructure technologies. Burton works to catalyze change and progress in the network computing industry through interaction with leading vendors and users. Publication headquarters, marketing, and sales offices are located at:

Burton Group
7050 Union Park Center, Suite 510
Midvale, Utah USA 84047-4169
Phone: +1.801.566.2880
Fax: +1.801.566.3611
Toll free in the USA: 800.824.9924
Internet: info@burtongroup.com; www.burtongroup.com

Burton Group's *Network and Telecom Strategies* service provides objective analysis of networking technology, market trends, vendor strategies, and related products. The information in Burton Group's *Network and Telecom Strategies* service is gathered from reliable sources and is prepared by experienced analysts, but it cannot be considered infallible. The opinions expressed are based on judgments made at the time, and are subject to change. Burton offers no warranty, either expressed or implied, on the information in Burton Group's *Network and Telecom Strategies* service, and accepts no responsibility for errors resulting from its use.

If you do not have a license to Burton Group's *Network and Telecom Strategies* service and are interested in receiving information about becoming a subscriber, please contact Burton Group.

Table Of Contents

Synopsis

By including a virtual private network (VPN) client with its operating systems, Microsoft has the potential of providing a complete system to enterprises looking to install Point-to-Point Tunneling Protocol (PPTP) or IP Security (IPSec) VPNs for remote access. But, until the introduction of Windows Server 2003 and the upgraded VPN clients released at that time, the Microsoft VPN solution could not be considered competitive with systems offered by VPN vendors such as Check Point, Cisco, NetScreen, and Nortel.

Microsoft's latest VPN system, including Windows Server 2003 and the updated clients, includes such crucial features as standards-based Network Address Translation (NAT) traversal for IPSec and Network Quarantine for gauging the security of a remote client before access to corporate resources is granted. Also included are extensions to group policy for ease of client management and broader authentication options through the support of remote authentication dial-in user service (RADIUS) and protocols like the Extensible Authentication Protocol (EAP). The combination of all these features makes the Microsoft solution a competitive one, provided an enterprise is willing to proceed with a Windows-only solution. Enterprises already using third-party VPN gateways, such as those from Cisco, NetScreen, Nokia, and Nortel, will realize few advantages by switching to the new Windows VPN clients, because many of the new features—Network Quarantine and group policy extensions—only work when Windows Server 2003 is used as the VPN gateway.

Analysis

As the leading vendor of operating system software for personal computers, Microsoft is in the unique position of being able to influence the acceptance of virtual private network (VPN) protocols by including support for particular protocols in its software. Microsoft first did so by offering software clients for the Point-to-Point Tunneling Protocol (PPTP) as a service pack for Windows 95. However, the remote-access VPN market is largely driven by vendors of network hardware, who offer high-performance, highly secure VPN gateways and usually write off the cost of providing a software client for use with their hardware.

Many enterprises have found hidden costs associated with remote access VPNs using encrypted tunnel protocols like IP Security (IPSec), and these hidden costs reduce the projected savings of the VPN deployment over traditional remote-access methods. These costs largely stem from the distribution and management of the VPN client software that must be installed on each remote user's computer. Other unexpected costs arise from the complexities in the setup of the client and interactions between IPSec and foreign networks (involving firewall rules and Network Address Translation [NAT], for example). These interactions often lead to an increased load on corporate help desks. Additional problems with remote access VPNs include the complexities of the IPSec protocol and its accompanying key exchange protocol, Internet Key Exchange (IKE), interference between IPSec and NAT, and the security of the remote user's computer.

Partly because of their Windows-centric focus, Microsoft VPN clients have not been as widely used as those from network product and other VPN vendors. However, the feature set that Microsoft has developed for its latest VPN clients, combined with the features added to Windows Server 2003, has made Microsoft's VPN offering a more competitive one, and one that enterprises of various sizes should take another look at. Like many of the current IPSec clients (see the *Network and Telecom Strategies* report, " Securing Access for Remote Users and Small Sites"), Microsoft's VPN client solves many of the problems that have plagued deployments of IPSec for remote access.

Some of the salient features now included in the Windows IPSec VPN are:

- Improved NAT traversal for Layer-2 Tunneling Protocol (L2TP)/IPSec client using Universal Data Protocol (UDP) encapsulation
- Network Quarantine to ensure the security of remote users' machines before a secure connection is completed
- Improved authentication options, including a server and proxy server for remote authentication dial-in user service (RADIUS) in Internet Authentication Service (IAS)
- Support for more authentication standards, including Extensible Authentication Protocol (EAP) and Protected Extensible Authentication Protocol (PEAP)

IPSec VPN vendors still have a way to go in managing the security of the end node; that is, the remote user's device. A few vendors, such as Check Point and NetScreen, have coupled their VPN clients with personal firewalls so that the software can be managed via centrally defined security policies that are sent to remote nodes as necessary. Nortel has also introduced their TunnelGuard software for checking the security of the user's computer. But, Microsoft has the advantage of controlling its operating system, so it can tie together the VPN client and security monitoring software more closely than other vendors can. Microsoft's Network Quarantine is a step in this direction, but it is useful only when enterprises use Microsoft products (their VPN clients and Windows Server 2003) on remote clients as well as remote access servers.

An obstacle to the acceptance of such VPN or security server bundles from Microsoft is Microsoft's client support. As long as only an L2TP/IPSec client is supported, enterprises will be reluctant to use such products. Most enterprises work in a multivendor, multiplatform world, and they need clients for a wide variety of operating systems (OSs) and devices, including Linux, OS X, and Palm. If Microsoft cannot provide clients for these additional OSs and devices, network managers will continue to use VPN products from other vendors, even if the VPN clients are proprietary.

Even though Microsoft employs many standards for user authentication and VPNs in order to create a secure VPN solution, the company still has to deal with the current perception that the underlying operating system has many security holes. As Burton Group pointed out in the *Application and Platform Strategies* report, "Windows Server 2003: Microsoft's New Operating Platform for .NET and Web Services," Windows Server 2003 is the first product that seeks to address some of the security issues outlined by Microsoft's Trustworthy Computing initiative. To quote that report "Microsoft's fondest hope is that customers migrate quickly to its current generation of products (especially Windows Server 2003), and that the "Trustworthy Computing" features of these solutions work as advertised."

As noted in a recent Burton Group report (see the *Network and Telecom Strategies* report, "The Changing Face of SSL-based Remote Access"), the market for secure remote-access products has changed in the past few years with the introduction of products using the Secure Sockets Layer (SSL) protocol. Microsoft has focused on lower-layer encryption protocols such as IPSec for VPNs, and EAP for authentication and encryption. The market for secure remote access, however, is equally interested in using SSL, especially as an alternative to IPSec. Some of this interest stems from the desire to reduce the support requirements of VPNs by removing the need for distributing client software. Microsoft addresses the issue of client distribution in part by providing an L2TP/IPSec client with its Windows OS. But organizations are seeking tighter ties between remote user access and application control, which SSL provides. Microsoft provides numerous methods for SSL-based access, including terminal services and SSL-compatible applications (such as Outlook). But Microsoft has not yet delivered a coherent message on how the Windows products can easily be used together to provide secure connectivity via SSL. Their focus currently remains on PPTP and L2TP/IPSec, although it's likely that Microsoft will introduce some SSL-based solutions specifically aimed at remote access before long.

Market Impact

The current remote-access VPN market is dominated by network hardware vendors such as Cisco, NetScreen, Nokia, and Nortel. These companies provide VPN gateway hardware, client software for the Windows OS as well as other operating systems, gateway and client management software, and occasionally software for managing digital certificates. Network managers often buy these VPN gateways because of the high performance they provide, as well as the hardened OSs that they usually use.

Microsoft's solutions for remote-access VPNs now offer the same features as the leading VPN vendors, but only in software products. Thus, the question of the performance and security of Microsoft's solution is still open. Windows Server 2003 appears to be more secure than its predecessors, but it may not be as secure as some of the hardened OSs used by VPN vendors in their gateway hardware. It's possible that the performance of Windows Server 2003 as a VPN gateway running on the fastest Intel platforms (and with a cryptographic coprocessor card) can be comparable to that offered by some of the VPN hardware currently on the market, but Burton Group has yet to see any benchmark tests proving (or disproving) this assumption. Network managers looking for high-end VPN gateways, such as for large enterprises, may well shy away from Windows Server 2003 as a VPN solution for these reasons.

Microsoft has not yet formulated a clear marketing message for its networking products, including Windows Server 2003. It's clear from conversations with teams at Microsoft that they'd like to compete in networking markets such as remote-access VPNs, but they've yet to produce a strong market statement that focuses on network managers. The lack of such a strategy will likely delay the deployment of Windows Server 2003 as a VPN solution, since the purchase of the server software is currently more likely to be justified by application and systems managers than by network managers. Plus, network managers may well balk at the idea of using a Windows-based platform for networking functions like VPNs, just as they did when the introduction of Windows 2000 and Active Directory allowed enterprises to use AD for managing domain names and IP addresses. Many network managers continued to use Unix-based products for name and address management.

Microsoft's biggest impact in the VPN market is among the enterprises that have standardized on the Windows operating system. These Windows-only shops can now use VPN clients with advanced features—such as endpoint security and policy-based management—that have until now only been available from other VPN vendors.

The idea of using a single computer to act as the VPN gateway as well as a firewall, RADIUS server and perhaps an organizational directory (and possibly other functions) may appeal to some organizations, mainly small- to medium-sized ones. But, if too many users and too many functions are processed on a single server, it's likely that performance will suffer.

Recommendations

Microsoft's remote access VPN solutions, as described in this report, address many of the requirements posted in the *Network and Telecom Strategies* report, "Securing Access for Remote Users and Small Sites." These requirements included:

- Easy traversal of NAT devices
- Ease of client deployment and management
- Endpoint security

Enterprises looking to roll out new VPN remote-access services for Windows-only environments should consider using Microsoft's L2TP/IPSec client and Windows Server 2003, *provided* the enterprises can wring sufficient performance out of the WINTEL platform and are satisfied with the security of Windows Server 2003. When compared with products from other VPN vendors, the one advantage Microsoft's solution provides is the ease of client distribution, since the VPN client is part of the Windows XP operating system. Thus, as enterprises migrate their computers to Windows XP, they can provide a full-featured VPN using Microsoft's products. The migration is eased by Microsoft's support for older versions of the Windows OS, as Microsoft provides compatible VPN clients for Windows 98, ME, NT 4.0, and 2000.

But the Microsoft solution, as described here, is a less appealing solution in a multi-OS environment. Most of the appealing features in the Microsoft products—such as Network Quarantine and Group Policy—cannot be used when third-party VPN gateways are used or operating systems other than Windows must be supported. In such cases, it's still a wise course to deploy the VPN products from vendors such as Check Point, Cisco, NetScreen, Nokia, and Nortel.

The Details

Microsoft has been involved in the development of encrypted tunnel virtual private networks (VPNs) since the inception of the market, going all the way back to the formulation of the Point-to-Point Tunneling Protocol (PPTP) for remote access in 1995. Although Microsoft has done much to promote the use of VPNs by including various VPN clients (PPTP, Layer-2 Tunneling Protocol/IP Security [L2TP /IPSec]) in its operating systems, many enterprises have chosen to buy VPN systems for remote access from networking or security vendors such as Check Point, Cisco, NetScreen, and Nortel. These vendors offer VPN systems that not only provide the higher performance and security associated with hardware-based gateways, but also include more features in their VPN clients and offer clients for operating systems other than Windows.

But Microsoft has added new functionality with the introduction of Windows Server 2003 and upgraded VPN clients for various versions of Windows operating system (OS). These new functions now make Microsoft's offerings a more competitive solution for remote-access VPNs, especially for the small- to medium-size enterprise (SME) market. These features are available for Microsoft-only installations and do not extend to other OSs or VPN gateways. When Microsoft VPN clients are used with third-party gateways, many of the compelling features of Microsoft's software are not available. This section describes the components of Microsoft's VPN offerings and discusses what features are available in Microsoft-only shops and in mixed-vendor environments.

Microsoft's approach to VPNs is typical in providing user authentication, address management, data encryption, and key management. But, unlike networking product vendors, Microsoft does not market a hardware-based solution for VPNs, instead depending on personal computer (PC) manufacturers to offer hardware that furnishes sufficient performance.

Microsoft and VPN Protocols

Microsoft includes support for both the PPTP and L2TP for securing remote access in its operating systems.

PPTP uses a Transmission Control Protocol (TCP) connection for tunnel management and a modified version of Generic Routing Encapsulation (GRE) to encapsulate Point-to-Point Protocol (PPP) frames for tunneled data. The payloads of the encapsulated PPP frames can be encrypted and/or compressed. L2TP uses Universal Data Protocol (UDP) and a series of L2TP messages for tunnel management. L2TP also uses UDP to send L2TP-encapsulated PPP frames as the tunneled data. The payloads of encapsulated PPP frames can be encrypted and/or compressed. Figure 1 compares the structures of a PPTP packet and an L2TP packet.

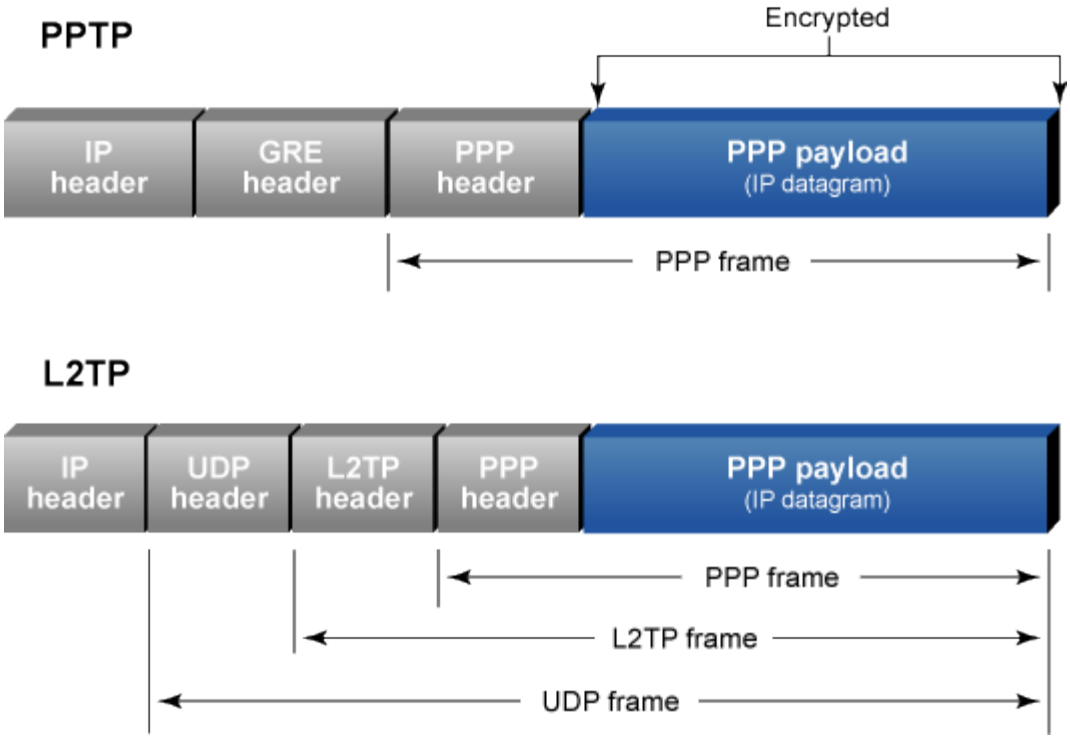

Figure 1:*Structure of PPTP and L2TP Packets*

Different objects are authenticated in VPNs, depending on which encrypted tunnel VPN protocol is used. PPTP and L2TP depend on only user authentication. IPSec authenticates the machine, not the user. One difficulty with setting up IPSec for remote-access users has been standardizing a method for authenticating the user as well as the machine so that the appropriate access rights can be granted once the user is connected to the VPN. Microsoft's approach has been to combine L2TP with IPSec. Although Microsoft originally developed the Microsoft Point-to-Point Encryption (MPPE) protocol to strengthen encryption in PPTP, Microsoft's implementation of L2TP does not use MPPE to encrypt the PPP payload. Instead, in the Microsoft implementation of L2TP, the IPSec Encapsulating Security Payload (ESP) is used to encrypt L2TP traffic. (For more details on IPSec's ESP, see the *Network and Telecom Strategies* overview, "VPNs: Types and Issues.") The combination of L2TP (the tunneling protocol) and IPSec (the method of encryption) is known as L2TP/IPSec. L2TP/IPSec is described in R equest For Comment (RFC) 3193, an informational RFC.

The result after applying ESP to an Internet Protocol (IP) packet containing an L2TP message is shown in Figure 2.

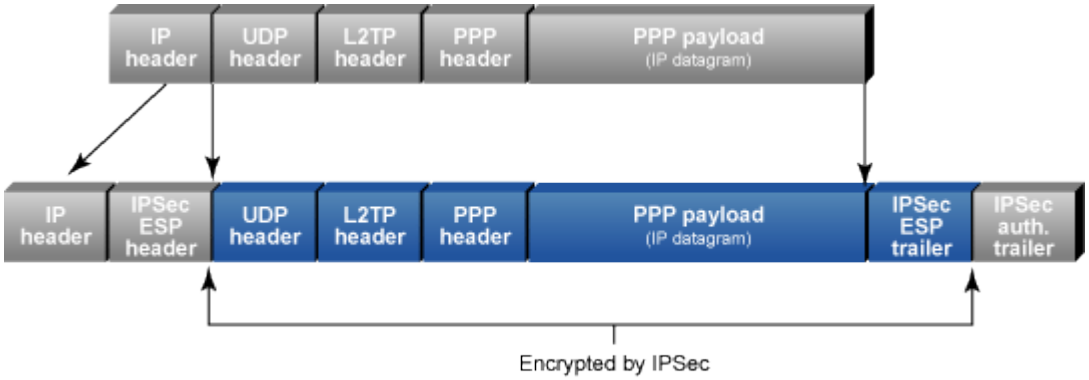

Figure 2:*Encryption of L2TP Traffic with IPSec ESP*

Although both PPTP and L2TP/IPSec use PPP to provide an initial envelope for the data, there are significant differences between the two protocols:

- With PPTP, data encryption begins after the PPP connection and PPP authentication are completed. With L2TP/IPSec, data encryption begins before the PPP connection process by negotiating an IPSec security association.
- PPTP connections use MPPE, a stream cipher that is based on the Rivest-Shamir-Aldeman (RSA) Rivest Cipher 4 (RC-4) encryption algorithm and uses 40-, 56-, or 128-bit encryption keys. In Microsoft's implementation, L2TP/IPSec connections use the Data Encryption Standard (DES), which is a block cipher that uses either a 56-bit key for DES or three 56-bit keys for 3-DES.
- PPTP connections require only user-level authentication using a PPP-based authentication protocol. L2TP/IPSec connections require the same user-level authentication as well as computer-level authentication using digital certificates.

Each protocol has its own set of advantages. The following are advantages of PPTP over L2TP/IPSec:

- PPTP does not require a certificate infrastructure. L2TP/IPSec requires a certificate infrastructure for issuing computer certificates to the VPN server computer and all VPN client computers.
- PPTP clients can be run behind a network address translator (NAT) if the NAT includes an editor for PPTP traffic. As we've mentioned in previous reports, an L2TP/IPSec-based VPN client cannot be run behind a NAT unless both the VPN client and server support some form of NAT traversal for IPSec, such as UDP encapsulation.

L2TP/IPSec has the following advantages over PPTP:

- IPSec ESP provides data origin authentication, data integrity, replay protection, and data confidentiality on a per-packet basis. On the other hand, PPTP provides only per-packet data confidentiality.
- L2TP/IPSec connections provide stronger authentication than PPTP by requiring both computer-level authentication through certificates and user-level authentication through a PPP authentication protocol.
- PPP packets exchanged during user-level authentication are always sent in encrypted form because the PPP connection process for L2TP/IPSec occurs after the IPSec security association is established. By encrypting the PPP authentication exchange, it's more difficult for an attacker to use PPP authentication data to perform offline dictionary attacks and determine user passwords.

Microsoft's Latest VPN Client

The VPN client that Microsoft released to coincide with the introduction of Windows Server 2003 includes the following features:

- NAT traversal by means of UDP encapsulation
- Endpoint security using the network quarantine feature of Windows Server 2003
- Support for new group policy extensions to coincide with Windows Server 2003

(The features that are implemented in Windows Server 2003 will be described in further detail in a later section.)

Traversal of NAT devices by IPSec-encrypted packets has been a problem for some time. IPSec typically requires unique addresses for both end devices, while NAT requires the capability to translate any part of the headers and packets that reference the addressing scheme. IP and TCP checksums need to be accessible, thus limiting the encryption of these areas. When the data is encrypted within the IP packets, NAT cannot perform the internal packet address translations.

Vendors have proposed solutions based on additional encapsulation of IPSec packets—using Hypertext Transfer Protocol (HTTP) or UDP, for example—but these solutions are vendor specific and not generally interoperable. The IPSec working group of the Internet Engineering Task Force (IETF) has been working on standardizing UDP encapsulation of IPSec packets for NAT traversal, and most network product vendors implemented the draft standard in 2003 as the proposed standard wound its way through the IETF standards process. The two IETF drafts of interest are "Negotiation of NAT-Traversal in the IKE" (draft-ietf-ipsec-nat-t-ike-07.txt) and "UDP Encapsulation of IPsec Packets" (draft-ietf-ipsec-udp-encaps-06.txt). The latter document should be approved as an IETF standard in the first half of 2004. Microsoft has also included support for UDP encapsulation of IPSec as a standard method for traversing NAT devices in its latest VPN clients. Readers of Microsoft documentation will often see the method referred to as NAT-Traversal, or NAT-T.

The Microsoft VPN client software is now available for Windows XP as well as older versions of Windows operating systems, including Windows 98, ME, and 2000. This wide availability simplifies the IT manager's task of deploying a remote-access VPN since many organizations have not yet migrated fully to the latest version of the Windows OS. It also allows many older computers to use the new security features found in Windows Server 2003. This includes support for Network Quarantine and Group Policy extensions, which will be described shortly.

However, Microsoft has not released VPN software clients for other operating systems, such as OS X, Linux, or Palm OS, and no vendor is known to have plans to do so. Thus, in order to take advantage of all of the VPN-related features that Microsoft has included in Windows Server 2003, an enterprise would have to use only devices running Microsoft operating systems.

Although various VPN vendors have included support for L2TP/IPSec in their VPN gateways, fewer vendors support L2TP/IPSec in their software clients. In today's multivendor, multi-OS world, L2TP/IPSec could achieve greater acceptance if support on other platforms, particularly the Palm and OS X platforms, were included.

Despite the security standards that Microsoft has used for its VPN package, there is still the problem that the underlying operating system has security holes. Although Microsoft is working to improve the security of its OS and applications, particularly through the Trustworthy Computing initiative, Microsoft still has to overcome the commonly held perception that its current OS is not secure. Any claims from Microsoft that it provides the most secure VPN client are for naught if the OS underlying the client is not considered secure, which is the current state of affairs. Enterprises using Microsoft's VPN client should do their utmost to ensure the security of remote users' computers, by using personal firewalls and virus scanners, for instance.

Because many of the interesting features of Microsoft's VPN solution are part of the Windows Server 2003 product, let's turn our attention to the server.

Microsoft's VPN Server Features

With the introduction of Windows Server 2003, Microsoft added functionality that not only improved control of the remote client, but also provided better support for standards-based user authentication. In the first case, this was accomplished by adding a feature called Network Quarantine and extending Microsoft's Group Policy Manager. For user authentication, Microsoft added a full-featured server and proxy server for remote authentication dial-in user service (RADIUS) to Server 2003, with support for a variety of authentication methods via the Enhanced Authentication Protocol (EAP, RFC 2284). In addition, Windows Server 2003 also provides policies for filtering remote-access packets.

Network Quarantine

Network Quarantine, or more properly Network Access Quarantine Control, is a new feature in the Windows Server 2003 family. The process examines the configuration of the remote-access computer and validates it against a manager-provided script before allowing normal access to a private network.

When Network Quarantine is activated and a remote computer initiates a connection to the remote access server, the user is authenticated and the remote access computer is assigned an IP address. However, the connection is placed in quarantine mode and network access is limited. An administrator-provided script is run on the remote computer. When the script completes successfully, it runs a notifier component that informs the remote access server that the remote computer complies with current network policies (as defined in the administrator's script). The remote access server removes quarantine mode, and the remote computer is now granted normal remote access.

In order to use Network Access Quarantine Control, a network manager has to deploy four components, as shown in Figure 3:

- A remote access server running Windows Server 2003 and a quarantine notification listener service
- A RADIUS server running Windows Server 2003 and IAS, configured with a quarantine remote access policy that specifies quarantine settings
- A Connection Manager (CM) profile created with the Windows Server 2003 Connection Manager Administration Kit (CMAK) that contains a network policy compliance script and a notifier component
- A Microsoft-provided remote access VPN client (as described previously)

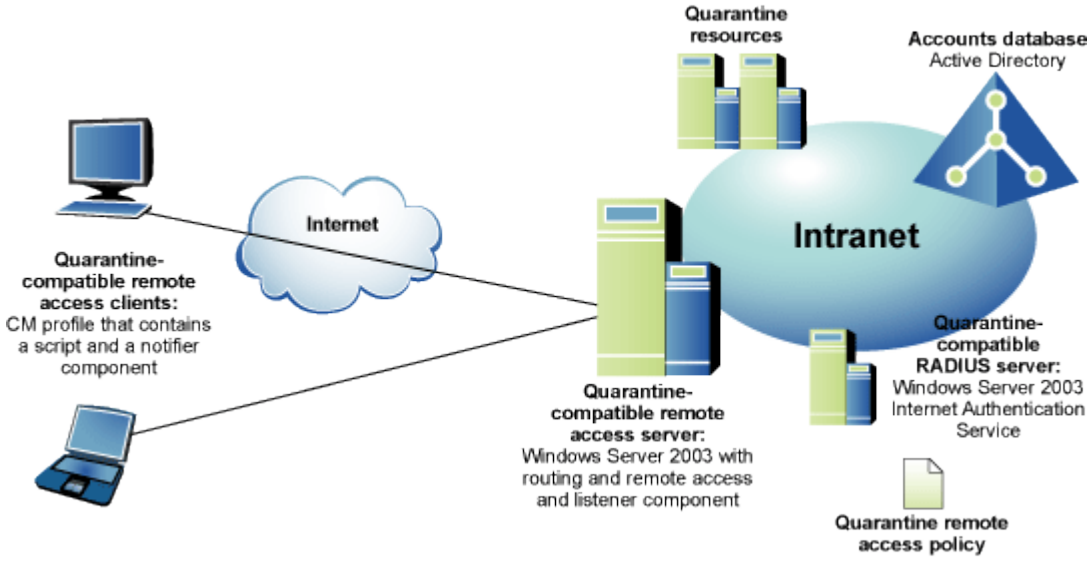

Figure 3: *Components of Network Access Quarantine Control (from Microsoft, 2003)*

Group Policies

As part of Windows Server 2003, Microsoft released a solution to unify management of group policy. In the past, administrators have been required to use several Microsoft tools to manage group policy, such as the Active Directory Users and Computers, Active Directory Sites and Services, and Resultant Set of Policy snap-ins. The Group Policy Management Console (GPMC) integrates the existing group policy functionality exposed in these tools into a single, unified console, along with several new capabilities. GPMC helps administrators manage both Windows 2000- and Windows Server 2003-based domains with the Active Directory service.

Windows Server 2003 also includes more than 200 new policy settings. According to the Windows Server 2003 document entitled “Group Policy Infrastructure,” the new policy settings allow administrators to control the behavior of (among other processes):

- System restore, error reporting, and PC health
- Terminal servers

- Networking such as Simple Network Management Protocol (SNMP), quality of service, personal firewalls, and dial-up connections
- Domain name server (DNS) and net logon
- Roaming user profiles and group policies
- Wireless configuration
- Software restriction policy

The software restriction policies are a valuable addition for use with Network Quarantine. The available software restriction policies let the network manager protect a computer from untrusted code by identifying and specifying which applications are allowed to run. With software restriction policies, a network manager can:

- Control the ability of programs to run on a system, such as allowing certain file types to run in the e-mail attachment directory of the e-mail program
- Permit users to run only specific files on multi-user computers
- Decide who can add trusted publishers to a computer
- Control whether software restriction policy settings affect all users or just certain users on a computer
- Prevent any files (such as those affected by a virus) from running on a local computer, organizational unit, site, or domain

Additionally, IPSec policy can be applied to the group policy object of an Active Directory object. This allows propagation of that IPSec policy to any computer accounts affected by that group policy object.

Windows Server 2003 also allows network managers to define packet filters that can be applied as part of a remote access policy profile. Remote access policies define authorization and connection constraints that are applied to remote access connections. When the connection is accepted, any packet filters that are part of the remote access policy define the types of IP traffic that are allowed into and out of the VPN client.

Control of accessible resources on an extranet is an example of the use of packet filters. By using remote access filtering based on policy profiles, the network manager can create a remote access policy that specifies that members of the partners group can access the Web servers at only specific IP addresses or on a specific subnet.

Network managers can also employ packet filtering to prevent VPN remote access clients from sending packets that the clients did not originate. In the Windows operating system, when a remote access computer creates a VPN connection, the computer creates a default route so that all traffic that matches the default route is sent over the VPN connection. If another computer forwards traffic to the remote access VPN client (treating the remote access client computer as a router) then that traffic is also forwarded across the VPN connection. This poses a security problem because the VPN server has not authenticated the computer that is forwarding traffic to the remote access VPN client. This would allow the computer that is forwarding traffic the same network access as the authenticated remote access VPN client computer.

User Authentication

Microsoft has strengthened the authentication options in its server products with the release of Windows Server 2003. The IAS component now includes a standards-based RADIUS server that is integrated with Active Directory. The links between RADIUS and IAS, and between IAS and Active Directory, improve the seamless management of authentication. As extensions to Active Directory's capabilities, these links also allow IT managers to view the management of user authentication for networking as part of the broader enterprise view of user authentication. They also allow the use of more advanced technologies to provide enterprise-wide authentication, such as meta-directories.

IAS also supports RADIUS proxy capabilities so that a network manager can configure the server to selectively forward authentication and accounting requests to other RADIUS servers, such as the connection to a service provider's RADIUS server for authentication of dial-in users. It's also possible to use Windows Server 2003's load-balancing capability to load balance RADIUS servers for better performance.

Windows Server 2003 and Windows XP support the following PPP authentication protocols:

- Password Authentication Protocol (PAP)
- Challenge-Handshake Authentication Protocol (CHAP)
- Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP)
- MS-CHAP version 2 (MS-CHAP v2)
- Extensible Authentication Protocol (EAP).

Authentication methods can be used in different ways by the VPN protocols. For example, IPSec tunnel mode only supports user authentication via user certificates or preshared keys. Since L2TP leverages the Point-to-Point Protocol (PPP) as the method of negotiating user authentication, L2TP can authenticate with legacy password-based systems through PAP, CHAP, MS-CHAP, or MS-CHAP v2.

Most implementations of PPP provide very limited authentication methods. EAP is an IETF standard extension to PPP that allows for arbitrary authentication mechanisms for the validation of a PPP connection. EAP was designed to allow the dynamic addition of authentication plug-in modules at both the client and server ends of a connection. This allows vendors to supply a new authentication scheme at any time. Microsoft's implementation of L2TP supports advanced authentication services through the EAP, which offers a way to plug in different authentication services without having to invent additional PPP authentication protocols. Thus L2TP gives network managers a common way to authenticate in an interoperable way while supporting the authentication services that most customers and vendors already have in place. All of this can be accomplished via integration with RADIUS- and Lightweight Directory Access Protocol (LDAP)-based directories in Windows Server 2003.

Other Noteworthy Server Features

In Windows 2000, the Network Load Balancing (NLB) service did not have the capability to manage IPSec security associations (SAs) among multiple servers. If a server in the cluster became unavailable, the SAs managed by that cluster were orphaned and eventually timed out, which meant that a network manager could not cluster L2TP/IPSec VPN servers. It was possible to use DNS round-robin to distribute the load across multiple L2TP/IPSec VPN servers, but there was no fault tolerance.

In the Windows Server 2003 product line, Microsoft enhanced the NLB service to provide clustering support for IPSec SAs. A network manager can now create a cluster of L2TP/IPSec VPN servers and the NLB service will provide both load balancing and fault tolerance for the L2TP/IPSec traffic. Note that this feature is only provided with the 32-bit and 64-bit versions of Enterprise Edition and Datacenter Edition. (For more details on Windows Server 2003 and its different versions, see the *Application and Platform Strategies* report, "Windows Server 2003: Microsoft's New Operating Platform for .NET and Web Services.")

Windows Server 2003 also provides several new network access control options. The server can be configured as a software-based Internet Connection Firewall (ICF) for local area network (LAN), dial-up, VPN, or Point-to-Point Protocol over Ethernet (PPPoE) connections, in conjunction with Internet Connection Sharing (ICS) or Routing and Remote Access Service (RRAS). When operating as an Internet Connection Firewall, Windows Server 2003 supports IPSec NAT firewall traversal using UDP encapsulation. Furthermore, the server's IAS can be configured to authenticate users on 802.1x wireless LANs (WLANs).

VPN Management

The two main components of Microsoft's VPN solution for remote access are the Group Policy Manager and the Connection Manager (CM). In Windows Server 2003, the Group Policy Manager has a new graphical user interface and combines the functions of a number of previous managers. The main improvement in the Group Policy Manager is the addition of more policy objects and actions that support remote users, and the introduction of Network Quarantine, discussed earlier in this report.

A network manager can use the Connection Manager to deploy the configuration of a large number of VPN remote access clients. The Connection Manager includes a client dialer, a CMAK, and Connection Point Services (CPS).

The Connection Manager dialer software is installed on each VPN client and presents a simplified dialing experience to the user. The dialer software limits the number of configuration options that a user can change, ensuring that the user can always connect successfully. Some options offered in the documentation for the Microsoft CM client dialer include:

- Select from a list of phone numbers to use, based on physical location (for an outsourced VPN solution).
- Use customized graphics, icons, messages, and help.
- Automatically create a dial-up connection before the VPN connection is made.
- Run custom actions during various parts of the connection process, such as preconnect and postconnect actions (executed before or after the dial-up or VPN connection is completed).

Microsoft refers to a customized CM client dialer package as a profile. A profile is a self-extracting executable file that is created by a network administrator with the CMAK. This CM profile can then be distributed to VPN users by means of CD-ROM, e-mail, website, or file share. When the user runs the CM profile, it automatically configures the appropriate dial-up and VPN connections. The CM profile can be used to configure connections for computers running Windows Server 2003, XP, 2000, NT 4.0, ME, and 98.

In Windows Server 2003, new features in CMAK allow the network administrator to:

- Provide more than one VPN access server for connections
- Enable end-user logging
- Control client-side split tunneling
- Configure pre-shared keys for L2TP/IPSec connections

CPS allows the network manager to create, distribute, and update custom phone books. These phone books contain entries for one or more points of presence (POP) and include complete POP information, so that users can connect to different organization or Internet access points based on location, rather than having to use a toll-free or long distance number.

CPS includes a phone book administrator for creating and maintaining phone book files, and a phone book server (a computer running Windows Server 2003 and Internet Information Services [IIS], including theFile Transfer Protocol [FTP] publishing service) that can process phone book update requests from the CM clients.

When a phone book is configured and published, a network manager uses CMAK to create the CM profile, which includes an action to automatically download phone book updates, the phone book file, and the name of the phone book server.

Interoperability of Microsoft's VPN Solution

When viewed as a total system, Microsoft's Windows Server 2003 and the latest VPN clients using L2TP/IPSec form a feature set that compares favorably with remote access VPN systems from networking vendors like Cisco, NetScreen, and Nortel, among others. (For more details on these competing products, see the *Network and Telecom Strategies* report, "Securing Access for Remote Users and Small Sites.") However, unlike the usual VPN products offered by these vendors, which include hardened hardware as the VPN gateway, Microsoft's package is a software-only solution. Users expecting a high-performance VPN should plan on using the highest performing PCs available and, if possible, including a cryptographic coprocessor card to handle IPSec encryption. But smaller sites with a few remote users may be able to get by with simply a high-performance PC as the server.

Many VPN vendors support Microsoft's implementation of L2TP/IPSec on their gateway hardware. This allows enterprises to use Microsoft's L2TP/IPSec client for Windows in conjunction with the higher performance hardware offered by the VPN vendors. In some cases in the past, this approach was a financially favorable one, since many VPN vendors charged extra for their own VPN client software. But that practice has pretty much disappeared. However, the only current advantage of this approach is the convenience of using a VPN client that's distributed with the operating system. All of the important features mentioned in this report, including group policy, Network Quarantine, and packet filtering, are not available when third-party VPN gateways are used. Although many VPN vendors have modified their gateways to support the Microsoft L2TP/IPSec client, none of these vendors have indicated that they will (or can) add support for other Microsoft-proprietary features that are part of Windows Server 2003.

Thus it only makes sense to use the Microsoft VPN clients in a Microsoft-only environment where Windows Server 2003 will also be deployed. As pointed out in a previous report (the *Network and Telecom Strategies* report, "Securing Access for Remote Users and Small Sites"), the major VPN vendors include a feature set (comparable to that offered by Microsoft), with the advantage of better gateway performance than that which Server 2003 most likely offers when running on an off-the-shelf PC.

Conclusion

Microsoft now offers a full-featured solution for remote access virtual private networks (VPNs) using Point-to-Point Tunneling Protocol (PPTP) or Layer-2 Tunneling Protocol/IP Security (L2TP/IPSec), based on Windows Server 2003 and the VPN client software that was updated when Server 2003 was introduced. But this VPN solution will appeal most to Windows-only shops since many of the appealing features will not work with third-party VPN gateways.

Author Bio

DaveKosiur

Senior Analyst

Emphasis: SSL and IPSec VPNs, QoS
Background: Freelance networking writer

Primary Distinctions: nternationally-known technical book author. Latest books are "Policy-based Networking" (John Wiley & Sons, January 2001), "Building and Managing Virtual Private Networks" (John Wiley & Sons, September 1998), "IP Multicasting" (John Wiley & Sons, April 1998), and "Understanding Electronic Commerce" (Microsoft Press, 1997). David Kosiur left Burton Group in April of 2004.