SANS Security Essentials
GSEC Practical Assignment
Version 1.2c

Author: Petteri Kaskenpalo

An Overview of Windows 2000 VPN Functionality and Comparison with Competing Solutions

With the introduction of Windows 2000 (Win2K), Microsoft has brought to the market an array of security tools. The operating system includes security tools like integrated Kerberos authentication protocol, public key infrastructure tools (PKI), support for smart cards, file encryption support, security configuration tools, and secure networking.

This article studies the secure networking functionality, or in other words IP security features of the Win2K operating system. The article gives an overview of the functionality, and compares it with similar products and also describes VPN performance benchmarks comparing various solutions.

The IP security features included in the Win2K operating system are the VPN functionality and IP traffic filtering. A VPN makes a connection over a public network, for example the Internet, and has three main goals: implement private communications, ensure data integrity and guarantee the authenticity of the transferred data.

The VPN functions included in Win2K are based on the IPSec [Ref. 1] standard developed by the Internet Engineering Task Force (IETF) as a secure protocol of the new IP version – the IPv6. IPSec can also be used as an extension to the currently used IPv4 protocol and can therefore be used with current applications and network equipment. The standard provides means for confidentiality and integrity to information transfer over IP networks. This is done on the network layer with device-based authentication. This type of protection will protect a network of man-in-the-middle, spoofing and, to some extent, denial of service attacks. The standard, however, does not define means for user based authentication or authorization, neither does it provide means for protecting data at rest while it passes intermediate systems in the network.

IPSec uses two methods of protecting IP traffic: the Encapsulating Security Payload (ESP) and the Authentication Header (AH). AH ensures the integrity of the IP packet data and headers. ESP guarantees the data confidentiality of the IP packet data portion.

A good summary of IPSec terminology can be found at:
http://www.vpnc.org/terms.html

VPN Types

IPSec has two operation modes: transport and tunnel mode [Ref. 2]. In transport mode the ESP and AH are applied to the original IP packet. This mode is used to provide end-to-end security between two communicating end systems. In tunnel mode the original IP packet is inserted into a new IP packet as data and the AH and ESP are applied to the new packet. The new IP header points to the end point of the tunnel. The original header still points to the original destination and this allows the tunnel end point to route the packet to its original destination. The tunnel mode can be used between two end systems, between an end system and a security gateway or between two gateway systems. Tunnel mode is especially useful in the last two cases where the data will be routed to a third system from the tunnel end point. In these two cases the original source or destination of a packet can be hidden. The gateway systems serving as tunnel end points can be specialized VPN gateways (tunnel servers), firewalls, or routers with VPN support.

Windows 2000 VPN Functionality

As mentioned above, the Win2K IP security builds on the IPSec standard [Ref 3]. What makes Win2K an interesting solution is that the architecture integrates Win2K domains and the Active Directory services. This enables linking of the IPSec functions to the policy-based, directory-enabled domains that allow policy configuration and distribution to Win2K domain members.

The Internet Key Exchange (IKE) implementation of Win2K enables the use of standard authentication methods to establish trust between computers. These are Kerberos v5, public/private key signatures using certificates, or passwords and pre-shared keys. Kerberos is provided by the Win2K domain infrastructure. The certificates can be issues by Win2K Certificate server or compatible third party certificate servers like Entrust, VeriSing, and Netscape. Once the system-to-system authentication is done, a session key is generated for encrypting the application data. The IPSec policy defines for example what level of encryption is required and how often the session keys will need to be refreshed.

The easiest way of deploying Win2K IP security is to use the Kerberos authentication. Certificates and pre-shared keys can be used between untrusted domains or achieving third party interoperability.

IPSec Policy

Security policy is the core of the Win2K IPSec. This contains the rules defining how IPSec module works; what type of traffic is allowed between systems, how data is to be protected and how communicating parties will authenticate each other. [Ref. 4]

For each host in the domain the administrator can configure if the IPSec protection is “requested but optional” or “requested and required”. Using these two approaches the hosts will have a default policy that describes how they are expected to respond to an incoming communication request.

Each host can also have specific rules for permitting, blocking or securing certain network packets. This is more difficult to configure and maintain as detailed knowledge is required of the type of network traffic and applications.

Each policy rule consists of five main components: IP filter list, filter action, authentication methods, tunnel settings and connection type. Defining a security relationship between two systems (or groups of systems) consist defining each of these components in the following steps:

1. **IP filter list** defines whom the computer can talk to. This is based on the IP source and destination, protocol and source and destination port numbers. The list can consist of one or more IP filters. The filers can consist of both allow and deny rules.

2. **Filter action** defines how communication that matches one of the filters is secured. This can define a number of different algorithms for both the data confidentiality and integrity. Level of protection can be configured differently for each IP filter.

3. **Authentication method** defines which of the three available protocols is used between two machines when the IPSec communication is established. Both systems must be configured to use the same protocol.

4. **Tunnel settings** are used to define gateway-based policies.

5. **Connection type** defines if the specific rule is to be used for Ethernet connection, dial-up connections or both.

Configuration Wizard will assist in walking through this process.

Win2K also provides several pre-configured security policies. These include for example a “secure server policy”, which will not allow unsecured communication between the server and the clients that do not have a trust relationship. Using these policies allows a fast deployment through an organization. Further configuration can be done granularly following the initial installation. Moving from an overall security policy to a detailed one also allows deployment that does not interrupt any network services.

Comparison with Other VPN Products

Comparing available VPN products is not an easy task. Globally, around 50 vendors provide VPN solutions that can all be considered high quality, industry standard security products. What criteria can be used to differentiate between these vendors? How can a match be made to suite the needs of a particular network? [Ref. 5]

The following discusses criteria for making the selection work easier, gives alternative product examples that perform especially well under each category, and explores how Win2K VPN compares to them.

Large vs. Small Scale and Complex vs. Simple

Certainly the requirements are different between a large enterprise and a small company. A few of the products require a fair amount of technical knowledge and deployment preparation. Large companies have a greater pool of IT staff and talent, and bigger IT budgets and thus has a greater range of VPN solutions available. They can set greater emphasis on functionality instead of price and ease of use. In contrast, smaller companies may like to consider solutions that offer one-stop, easy to use VPN gateway solutions bundled together with a firewall. Scalability is the key.

Of the software based VPN solutions two stand out as good options for the large corporation. Both the F-Secure VPN+ and Check Point VPN-1 are complex but compleat and competent security packages. Both companies also have several years of experience on the security software market. Both support very granular security policy configurations and provide powerful tools for large scale deployment and administrations. VPN-1 integrates seamlessly with the Check Point's industry leading firewall FW-1. VPN+ on the other hand has great client-rollout support. Both are very scalable and can support high availability as well as IP traffic load balancing.

For smaller companies there are solutions that are both easy to install and use. One of the software-based options is Gauntlet VPN, where as Sonic Wall provides an entry-level hardware option. Both of these are user friendly and also include extremely functional firewalls.

How does Win2K VPN compare with these solutions? Very well. As all software based solutions the initial investment does not need to be big. Attention must be paid to ensure that any chosen solution has potential to grow. Win2K supports active-active clustering with high availability and load balancing. This overcomes the hardware limitations of one system. The administration is integrated to the domain administration tools and the Active Directory. These features ensure Win2K VPN scalability to the largest of installations with thousands of simultaneous VPN connections. Any problems? Win2K VPN is a cheap option if the Win2K domain structure is already in place and working properly. If there are some NT 4.0 servers around or the NT domain has not yet been converted to Active Directory, then it might be advisable to consider other alternatives.

Type of Solution

Another important question is what type if VPN is required? Is it needed for network gateway-to-gateway connectivity, remote client to gateway connectivity, or client-to-client connectivity? Win2K VPN can be used in all of these configurations. Few other solutions provide this level of flexibility. Client-to-client functionality can only be found in products like F-Secure VPN+, Network Associates PGPNet and Netlock Technologies security suite, or in operating system level IPSec implementations like Sun Solaris 8.

Platform Coverage

This poses us to the third question: platform coverage. What operating systems does the VPN solution need to support? For example Win2K VPN solutions can be used only between Win2K systems as well as with earlier Windows 95/98/Me and NT operating systems. If only gateway-to-gateway solution is required this is not an issue as the gateways can operate on dedicated platforms. On client-to-gateway solutions it is important to consider if the VPN client software is available on required platforms. For example Macintosh clients are offered by only a handful of vendors. One example of Macintosh VPN clients is V-One's SmartPass solution. On client-to-client implementations the platform coverage is of greatest importance. In this type of solutions, secure communication is expected to be available between any two machines; between workstations and servers as well as between servers and servers, and workstations and workstations. Interoperability between clients on different operating systems may be required. True multi operating system support is available by vendors like V-One, Netlock and F-Secure. These solutions support communications between most of the commercial operating systems (including Windows versions, Macintosh, Solaris, HP-UX, Netware, IBM AIX, Linux, and hand held devices). Most hardware VPN gateway providers have a very limited platform support for remote access clients.

IPSec Interoperability

If IPSec is a standard, cannot all IPSec implementations work together regardless of the platform? Unfortunately the situation is not that simple. IPSec defines how the IP packets should look like and, in theory, any equipment or software that is IPSec compliant should work together. The problem is that the tools for managing the IPSec communications are not standardized. That means that a management tool for one IPSec implementation cannot control the systems using another implementation of the IPSec. Single nodes can be manually configured to work together, often by using pre-shared keys, but this is often not a secure enough, scalable or maintainable solution. Also VPN client software of two different vendors is not likely to work together through one VPN gateway.

More details on IPSec interoperability can be found at the following web page: http://www.vpnc.org/interop.html

Hardware vs. Software

Should the VPN gateway be software or hardware based? This topic relates to performance and availability. In most cases hardware based solution offers better performance for a large amount of concurrent VPN connections. They can also provide a higher level of availability, stability and speed. On the other hand they may offer a less flexible solution with less protection for the investment than a software solution.

As many of the software solutions, like Win2K, support hardware encryption accelerators the performance becomes less an issue. For example Intel and 3COM markets network interface cards that support offloading all IPSec operation from the Win2K host CPU. High availability solutions are more common in hardware-based solutions like in the high end offerings from Alcatel, CISCO, Lucent, Nokia, RAD Guard and Watch Guard. Many hardware solutions are targeted to the network providers and telecommunications companies and are of less interest here.

Central Management and Monitoring

Central management tools can be a key function when considering solutions for corporate use. Some of the key requirements for central VPN administration are: automated client deployment, configuration control of VPN relationships, key management, ability to configure traffic filtering, and possibility to collect security alerts and accounting information centrally.

Why are these important? The Network Associates PGP product family implements an opposite approach: philosophy of decentralized security control; leaving it to the end user to manage keys, setup VPN connections and configure port filtering. The PGP product family includes great functionality but gives very little control to the administrator. For example the security administrator cannot setup the VPN relationships between specific machines; each security association must be configured locally at each machine. This is of course neither a scalable solution nor does it support most security policies. There is also no central way to revoke keys from user's key rings. If, for example, an employee is fired, the security administrator would have to either manually remove the ex-employee's key from each machine, or give users instructions on how to do it themselves. This obviously can become an administrative nightmare for a larger company. On the other hand PGP does provide excellent tools for a loose group of individuals to communicate securely.

Win2K VPN functionality provides a natural compromise between these two approaches by allowing central configuration and control of all VPN relationships as well as traffic filtering for host in an Win2K domain, and on the other hand hosts outside the domain can be manually configured to use the Win2K IPSec and traffic filtering features.

Support for NAT

Network address translation is used at the edge of the network in two different modes, static one-to-one translation and dynamic one-to-many translation. As a principle rule it is not possible to use IPSec tunnel mode through a NAT while taking advantage of the automated key exchange. This is due to the incompatibilities between the IKE key exchange protocol and NAT. NAT is simply not considered in the IPSec standard.

Many VPN gateway vendors do support NAT in client-to-gateway communications. Some vendors, like CISCO and F-Secure, provide support for NAT also in tunnel mode. These IPSec implementations may include proprietary extensions to the IPSec standard and may create problems with IPSec interoperability.

General Considerations

The IPSec and IKE (Internet Key Exchange) are becoming standards in VPN communications. As open and well-tested standards are one corner stone for computer security, products based on these standards should be given priority when considering which VPN solution to select.

Available encryption algorithms can also be a key selection criteria. As most vendors today provide solutions with DES and 3DES encryption, this criterion does not really set the solutions apart. Some vendors are introducing AES based encryption and this may be worth looking into.

More details on the VPN feature comparison can be found at:
http://www.vpnc.org/features-chart.html

Windows 2000 VPN Performance

How does the different VPN solutions perform? How does Win2K compare?

Win2K VPN gateway's IP packet forwarding performance was evaluated by NSTL Inc, an independent hardware and software testing organization. They have tested a number of both hardware and software VPN products. The packet forwarding capacity is a widely used characteristic for comparing VPN solution performance. [Ref. 6] [Ref. 7]

The following summarizes the results of two tests, one focusing on hardware VPN vendors and the other on Win2K performance. In the tests the VPN devices were tested on a standard 100 Mbit/second Ethernet LAN using IPSec 3DES tunneling focusing on gateway-to-gateway functionality. Hardware based VPN gateways were: Xedia, VPNet, RadGuard, Lucent, RedGreek, Intel and Compatible Systems. The Win2K VPN was tested on a server with 4 Intel Xeon 550MHz processors, 1 GB of RAM and Intel network cards, which support IPSec/encryption offloading. Even if this configuration is getting close to be called hardware based as well, it still offers a cost effective comparison.

The reported maximum packet forwarding rates were as follows (Mbits/s or % of maximum throughput): Xedia (95), Win2K (70), VPNet (50), Lucent (40), Compatible Systems (25), RadGuard (10), RedGreek (10), and Internet Dynamics (8).

When evaluating VPN products performance of certainly not the only deciding factor. Overall security and manageability must be equally considered. This performance evaluation shows that Win2K offers a server based VPN solution that can be managed with powerful tools from a central location. Is also demonstrates that in terms of performance Win2K VPN features are comparable to leading hardware based VPN devices. How the Win2K VPN features perform in mid-range and low-end servers remains to be seen.

Summary

The combination of tools included in the Win2K operating system will allow security professionals to define scalable security policies for the largest of enterprises running Win2K or earlier Windows version. This can be done with granularity – from the entire organization to individuals. The IP security functionality enables, not only secure access to the servers and resources, but also between any individuals. Proven to be scalable and comparing well in performance benchmarks, IP security will be an important part of Windows network security.

While requiring detailed understanding of the underlying technology and ongoing support, the Win2K VPN services may not be the optimal solution for smaller companies with less dedicated IT personnel especially if they are not running a Win2K domain. They might like to consider less complex hardware based network appliances with easy to use configuration interfaces and simple client software.

References

[Ref. 1] RFC 2401. Security Architecture for the Internet Protocol
http://www.ietf.org/rfc/rfc2401.txt

[Ref. 2] Microsoft 2000 Server: Virtual Private Networking: An Overview
http://www.microsoft.com/windows2000/library/unzippeddocs/VPNoverview.doc

[Ref. 3] Configure a Win2K VPN, Windows 2000 Magazine, September 2000
http://www.win2000mag.com/Articles/Index.cfm?ArticleID=9650

[Ref. 4] Microsoft TechNet: Step-by-Step Guide to Internet Protocol Security
http://www.microsoft.com/TechNet/win2000/win2ksrv/technote/ispstep.asp

[Ref. 5] VPN Gateways – Tunnel your way to secure communications
Windows 2000 Magazine, April 2001
http://www.win2000mag.com/Articles/Index.cfm?ArticleID=20068

[Ref. 6] VPNs: Performance, Security and Management for All
NSTL, January 2000
http://www.nstl.com/downloads/NSTL_VPN.pdf

[Ref. 7] NSTL Lab Report: Windows 2000 VPN Testing, February 2000
http://www.nstl.com/downloads/NSTL%20Windows%202000%20VPN.pdf

Links to VPN vendors and products

3COM, Alcatel, Ashley Laurent, Assured Digital, Checkpoint, Cisco, Cloud Connector, Efficient, Ennovate, Enterasys Networks, eSoft, Extended Systems, Fortress Tech., F-Secure, Info Express, IBM, Lucent, Linksys, Microsoft, Netlock, Netopia, Netscreen, Network Associates, Nokia, Nortel, Novell, RadGuard, Red Creek, Secure Computing, SafeNet, Shiva, SUN, Symantec, Vircom, V-One, SonicWall, Tut Systems, Vpnet, WatchGuard, WindRiver, Xedia