

NET6 HYBRID-VPN GATEWAY

The First Complete Secure Remote Access Solution

by Goutham Rao, Chief Architect, Net6, Inc.

Caveats

The intent of this whitepaper is to discuss the advantages and disadvantages of current VPN and SSL VPN solutions as well as compare both to the Net6 Hybrid-VPN Gateway solution. The author assumes that the reader is familiar with the benefits of providing remote users access to the applications that he or she needs to maintain productivity, so the business case of VPN solutions is outside the scope of this document.

Additionally, the author provides high-level reference to the total cost of ownership business case of SSL VPNs when compared to IPSec VPNs, but assumes the reader has a rudimentary understanding of this cost savings. A Net6 representative can detail both business cases further. The whitepaper also uses the term “organization” as a general entity, but is meant to represent enterprises, businesses, government organizations, health-care institutions, financial services institutions, educational institutions, etc.

Contents

- “Summary” (1)
- “Background” (2)
- “Thick Client VPNs” (2)
- “SSL VPNs” (3)
- “IPSec versus SSL VPNs” (5)
- “The Net6 Hybrid-VPN Gateway: The First Complete VPN Solution” (6)
- “Summary” (9)

Summary

IPSec Virtual Private Networks (VPNs) revolutionized the way remote workers and business partners connected to an organization by establishing a secure tunnel between a remote worker or business partner and the organization to which they were connecting. IPSec VPNs enabled employees to attain immense productivity gains while reducing the costs for the employers.

Additionally, VPNs enabled a new world of Business to Business (B2B) productivity by connecting two different companies or organizations to facilitate and accelerate B2B transactions.

Unfortunately, VPNs prevent traveling users from connecting back to their corporate resources while behind the firewall at a customer or partner site. VPNs also bring along the administrative headaches and high costs of support and configuration primarily from the installation and updating of VPN clients.

Additionally, and becoming more of an issue on a daily basis, VPNs have become a prime traversal route for the spread of worms (since secured clients obtain a routable IP address on the private network), which have had a decimating impact on business.

A new form of secure remote access called “SSL VPN” was developed to solve the issues associated with IPSec VPNs and still provide the secure access required by remote workers and business partners. SSL VPNs primarily operate with web applications over an HTTPS connection. They achieve functionality by parsing web pages at runtime to ensure that every web navigation path is routable from the client computer. Since SSL VPNs provide a clientless way to access applications that are internal to an enterprise or organization network, they eliminate or reduce the administrative headaches and high support costs of IPSec VPN clients.

However, there are many limitations of SSL VPNs including lack of client-server application support without custom connectors, the inability to work with business applications that use binary object technology such as Java applets and ActiveX, and the inability to work with peer-to-peer applications such as soft-phones.

With each type of solution having distinct advantages and disadvantages, many vendors are now providing both types of solutions in their remote access portfolio and expecting their customers to deploy both types of solutions and use each type for different circumstances. Vendors that only have one of these two types of solutions are trying to migrate their solution to have the capabilities of the other type. While a “one box” IPSec plus SSL VPN solution provides a manageability advantage, the inherent problems of each technology remain. Clearly what is needed is a solution that has the combined advantages of both IPSec VPNs and SSL VPNs, but none of the shortcomings.

The Net6 Hybrid-VPN Gateway provides enterprises and organizations with the combined advantages of both IPSec VPNs and SSL VPNs with none of the shortcomings—replacing the need for IPSec and SSL VPN solutions. IPSec, L2TP, or PPTP VPN solutions provide network layer access and encryption. SSL VPNs provide application layer access and encryption. Net6 combines network layer access with application-level encryption in a hybrid technology. This drastically improves the end-user experience while significantly reducing the IT security administrator’s support overhead and security risks.

Similar to how SSL VPNs relieved enterprises and organizations of the administrative headaches and high costs of client management associated with an IPSec VPN, the Net6 Hybrid-VPN Gateway solution relieves enterprises and organizations from the burden of maintaining two separate VPN infrastructures because the Net6 solution provides the benefits of both.

Background

Organizations have a general problem of remote access to private networks for employees and partner organizations. Employees and business partners need to access information remotely, from another private or public network, and are potentially behind other security and firewall equipment themselves. Ordinarily, without any specific solution to address this issue, employees and partner organizations would not be able to access this information without being physically connected to the private network, for example, by obtaining a network address on the organization's intranet to physically connect to it.

Organizations seeking to solve this problem would like to provide access to trusted persons and organizations, and would like a mechanism to authenticate such users. Furthermore, since information would now be flowing from a private, and hence secure and trusted network, into a public or third-party network, organizations providing such access would benefit from having this information encrypted so as to not provide any valuable information to untrusted entities.

VPNs (Virtual Private Networks) were created to solve this problem. Over the years, organizations have deployed different types of solutions such as the following.

1. PPTP and L2TP VPNs use a technique known as GRE (Generic Routing Encapsulation). GRE is an Internet protocol that allows packets destined for a certain network to be encapsulated and sent, on a packet-by-packet basis, to a trusted server where packets are unwrapped and retransmitted on the private network. PPTP/GRE is an implementation by Microsoft that utilizes GRE and encrypts data using Microsoft algorithms.
2. IPSec also relies on GRE (IPSec/GRE) and another protocol known as ESP (Encapsulating Security Payload), where IP packets are encapsulated and encrypted. However, current implementations make IPSec more secure and robust compared to PPTP and L2TP due to the encryption algorithms chosen and supported.
3. SSL VPN allows only certain types of web-enabled applications to be made available over a secure web browser. It is limited to applications that use standard web authoring tools such as HTML and JavaScript. This technology parses each web page and ensures that all programmatic paths of navigation from that page get forwarded to the SSL VPN server over a secure connection.

Thick Client VPNs

For the purposes of this whitepaper, the PPTP/L2TP and IPSec solutions will be grouped because of their similarity, as they both use clients and rely on GRE. The IPSec version is the most widely deployed of the two versions, so we will refer to IPSec for the remainder of the document, but will imply the characteristics of both. As such, both have major drawbacks:

1. IPSec, PPTP, and L2TP (further referred to as just IPSec) solutions require the use of thick clients, which introduce administrative headaches and high support costs to an organization.

Thick client solutions require an organization to employ large support teams to aid end users with installation, maintenance, and troubleshooting.

2. GRE is not NAT (Network Address Translation) firewall friendly.

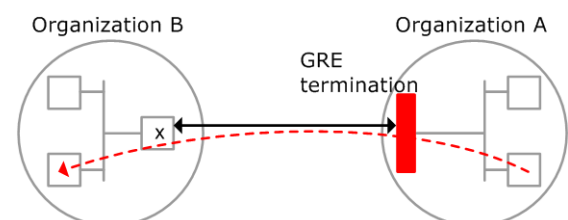
A NAT firewall is commonly used networking equipment that creates a private network for an organization, such that computers from the private network can instantiate connections with the public (or outside) networks and send and receive data, but new connections from the outside cannot typically come back in. NAT firewalls provide security and hide internal computers, thus protecting the organization from intruders and unwanted access to private information.

A NAT firewall requires that extensive measures be taken by partner organizations to allow a GRE client to operate and establish virtual circuits with the remote private network being accessed. This makes it extremely difficult to maintain and manage. Furthermore, it prevents the casual use of VPN by individuals who want to remotely connect to a private network from some other organization, where it is not possible to contact network administrators and request them to change firewall policies. This situation leaves many employees with the inability to access their company information from other organizations they may be visiting, limiting their access to information except when in a more unrestricted environment.

Many firewalls are incapable of tunneling GRE and ESP payloads, and in cases where they are able to tunnel such packets, system administrators traditionally turn this feature off in the NAT firewall to prevent employees from establishing a tunnel between the local trusted private network and another private network that the client is remotely accessing (the reason for this is explained below).

3. GRE assigns a private network IP address to the computer on which it is run. This IP address is visible to the private network the computer is connected to, thereby providing a major security breach.

As shown in the following illustration, a computer X in organization B would establish a GRE connection with organization A. A worm that is resident in organization A would now be able to copy itself on computer X over the GRE tunnel, since the IP address is visible on the private (infected) network of organization A. From computer X, the worm now has the ability to infect other computers within organization B, an undesirable behavior.



In the illustration, organization B has a private network of 10.10.0.0 and organization A has a private network of 192.168.1.0. Computer X which has established a GRE tunnel into organization A now gets a private IP address from the organization A, for example, 192.168.1.100. So computer X is now part of two private networks, and is capable of operating as a bridge between the two networks. A worm (shown as a dashed line in the illustration) can now reach IP address 192.168.1.100 (computer X) and from there, can reach other machines on the 10.10.0.0 network.

4. IPSec VPNs do not enable access to a private network from public computers such as kiosks.

SSL VPNs

To overcome all of the issues and problems associated with IPSec VPNs, a new category of remote access known as SSL VPNs were created. Essentially, this technology only allows web application access, which is a minor part of the remote access solution. SSL VPNs expose certain types of private web applications, over a secure connection known as HTTPS (HTTP over SSL), by recreating the navigation paths of the web application through the parsing and reconstruction of the web page in real time as requests are serviced. Essentially, SSL VPN solutions provide a web portal of access to a certain list of web applications.

Although SSL VPNs primarily work with web-based applications, a few SSL VPN vendors have written custom connectors that enable a limited number of client-server applications to also be accessed. Custom connectors that are sold by SSL VPN vendors are normally for applications that have a standard (non-customizable) client. An example of this type of application is Microsoft Outlook, which has a standard client (within releases). In other words, the Microsoft Outlook 2000 Service Pack (SP) 3 client is the same for company A as it is for company B or any other company. An example of an application that does not have a standard client is one that is customized for a particular customer. Examples of these applications are Sales Force Automation (SFA), Customer Relationship Management (CRM), Enterprise Resource Planning (ERP), and other applications from companies such as Siebel, Oracle, Remedy, Clarify, and SAP. These applications are customized for a particular company. In other words, a Siebel implementation at company A is much different than a Siebel implementation at company B or any other company.

For the SSL VPN vendors that do support limited client-server application access (only a few do), they approach these two types of applications differently. With an application that has a standard client (the Outlook example from above), they use the client that is on the users' PC. This approach involves the issues explained in the following table.

SSL VPN Issue

Explanation of Issue

Split DNS entries

The PC client is looking for an IP address or server name which cannot be seen outside the firewall (SSL VPNs do not provide access like IPSec VPNs), therefore the IT administrator has to set up split DNS entries.

For example, an Outlook client is normally set up to look for the server name where the Exchange Server is located. This server can be found and connected to by name if the PC is inside the network. However, for an outside client, this server's DNS name cannot be resolved as the server was intended to be connected to only from the inside. Even if the entry was published by the enterprise's public DNS server, the client would not be able to find a route to the private server.

SSL VPN vendors solve this issue by requiring an IT administrator to set up split DNS entries where, if the PC is on the network, it is routed to the Exchange server. However, if it is not on the network, it is routed to the SSL VPN loopback connector that is running on the PC (they accomplish this by specifying a loopback address like 127.0.0.1 as the IP address for the Exchange server).

Alternatively, some SSL VPN vendors will avoid loopback connectors by pointing PCs outside the private network directly at the SSL VPN server, however this also requires a split DNS entry (namely for PCs outside the network to resolve to the public SSL VPN server).

Additionally, each PC that uses the SSL VPN to access the application will have to change the server name in the client to point to the new, split DNS entry (at the time of SSL VPN configuration) or to the application connector, which is part of the SSL VPN Server.

This puts an undue amount of overhead on not only IT administrators, but also users who have to change the server name in their application clients.

SSL VPN Issue

Application performance

Explanation of Issue

When a PC client is accessing the server application over an SSL VPN, the performance of the application is significantly reduced. This is due to the protocol conversions that have to take place between the PC client and the SSL VPN clientless client and then between the SSL VPN server and the application. Of course, the opposite protocol conversions have to happen on the return trip of information from the application to the application client.

For example, an Outlook client would normally use a MAPI protocol to communicate with an Exchange server. When an SSL VPN is introduced, the Outlook client still communicates via MAPI to the SSL VPN clientless client. The SSL VPN clientless client converts this information into a custom protocol that it uses to communicate with the SSL VPN server. The SSL VPN server then has to convert this custom protocol back into a MAPI protocol that the Exchange server is expecting. The reverse set of protocol conversions happen on the return trip of information from the Exchange server to the Outlook client.

Application upgrades

Most upgrades to an application require a corresponding upgrade to the SSL VPN. If there are two applications, there will need to be an upgrade to the SSL VPN each time either of the applications are upgraded. The need to also upgrade the SSL VPN is because application upgrades nearly always have a change in the protocol that the application and application client use to communicate. Any time there is a change in this protocol, there has to be a change in the custom connector that the SSL VPN is using to convert protocols.

Returning to the Outlook example: If an organization upgrades the Exchange server from version 5.5 to 2000, the MAPI protocol used between the Outlook client and the Exchange server changes. Since the SSL VPN clientless client and server convert this specific MAPI protocol to the proprietary SSL VPN protocol, the corresponding protocol conversion of the SSL VPN server has to be upgraded. Furthermore, if the MAPI protocol between Outlook and the Exchange server is changed during a Service Pack upgrade (such as SP3 to SP4), the SSL VPN will also have to be upgraded.

For applications that do not have a standard client, the SSL VPN vendor can either create a custom connector (similar to the one explained above in the Outlook example) or bring in their Professional Services team to “webify” the product. To justify the cost of developing a custom connector, this connector would have to be able to be sold to many customers. Since these applications are customized for a particular organization (that is, SFA, CRM, ERP, etc.) and not a standard client (like Outlook), the cli-

ent will be specific to each customer. Therefore, an SSL VPN vendor will default to the customer using the SSL VPN vendor’s Professional Services organization to webify the application since a custom connector for a customized application cannot be leveraged across many customers. The following table lists the issues that will be discovered during or after this webification process.

SSL VPN Issue

Long implementation time and high cost

Explanation of Issue

Webification is purely a professional services exercise to provide browser access to a perfectly good client-server application just so it can be accessed through an SSL VPN.

An SSL VPN Professional Services organization will create an ActiveX, Java applet, or HTML representation of the application that runs in the PC’s web browser. This process will require an implementation of a web service that is able to translate the legacy server’s protocol and data to a web-friendly front-end.

If this webification takes ten days at a Professional Services rate of \$2000 per day, it would amount to a total of \$20,000 over and above the cost of the product, plus the additional travel and expense costs.

User interface changes

Employees grow accustomed to existing user interfaces. Developing unnatural browser interfaces for native applications will most likely change the look and feel of the application. This can require organizations to spend significant amounts of time reeducating unhappy users.

Inhibited protocol functionality (such as SMB)

Just as an unnatural user interface can have an affect on the efficiency of an employee using a webified application, the same can apply for some of the basic protocol conversions that may come with an SSL VPN.

One example is SMB (Server Message Block) Protocol. If a user is at his or her desk, mapped network drives are available for accessing or saving files right from even simple applications like Microsoft Word, Microsoft PowerPoint, Microsoft Excel, etc.

Forcing a user that is remote and using an SSL VPN to have to use a webified file-sharing protocol instead decreases the efficiency of that user, especially if he or she is not a power user.

After reading about the issues that SSL VPNs have with thick client-server applications as described in detail above, the reader may think that an organization can just develop and deploy the web interface available from many of the SFA, CRM, and ERP vendors. Unfortunately, SSL VPNs also cannot work with many of the “real business” web applications that organizations are deploying.

SSL VPNs are essentially a proxy technology and as such, have to parse and rewrite links to provide access to internal web applications. This means SSL VPNs can only work with web structures that are parsable. Java applets, ActiveX, Flash, and other web structures are executable binary code and therefore cannot be parsed. Unfortunately, many of the web interfaces from SFA, CRM, and ERP vendors contain these structures, which prevents them from being accessed through an SSL VPN.

Even if an SSL VPN could parse a Java applet, the Java security model would still prevent this because the Java applet has to

be launched from and run on the server where it resides. With an SSL VPN, a Java applet may be launchable, but it cannot be run.

For the web applications that can be used with an SSL VPN, there is a significant performance degradation. For every page of every internal web application that is accessed using an SSL VPN, the SSL VPN has to parse the web page into a DOM representation, identify navigation paths (such as URLs), rewrite and map navigations paths to externally accessible URLs, and then reconstruct all the web pages. This process also requires evaluating client-side script on the SSL VPN server because navigation paths can be programmatically computed. In addition, this technique does not always work since the SSL VPN server does not always have the information required to compute the end result that would supply a correct URL. In this case, professional services must be involved again.

Finally, there are some miscellaneous issues that affect SSL VPNs, as described in the following table.

SSL VPN Issue	Explanation of Issue
Real-time traffic (voice or video) is unsupported	SSL VPNs cannot support real-time traffic such as voice or video, which means users cannot take advantage of soft phones on their PCs or on-line or real-time video training sessions.
Kiosk modes can leave temporary files and cookies	The way an SSL VPN deals with kiosks is to run a clean-up script at the end of the session to delete any temporary files that may have been opened in e-mail and to delete any cookies. The problem with this approach is that it fails if the browser happens to crash during the session. If the browser crashes during the session, the clean-up script will not have a chance to work and all the proprietary information that was opened during the session is stored on the kiosk.
Deployment time can be inaccurately represented	SSL VPN vendors tout a significant reduction in the amount of time it takes to deploy an SSL VPN solution when compared to an IPSec solution. This, however, assumes that there is no customization or professional services work for the SSL VPN vendor to do. Even when using custom connectors, there are issues with split DNS entries that increase the deployment time with both the application and the client. Webification of an application increases the deployment time even more. In other words, this large reduction in deployment time will be the case when the SSL VPN can be installed with no application or client modification or professional services.

To summarize, SSL VPN solutions will work from most computers, even behind various firewall configurations. However, they have severe drawbacks:

1. SSL VPNs are not a complete remote access solution. They only work for certain types of web applications, and fail on advanced web applications that use binary object technology such as Java applets and ActiveX controls. They are completely incompatible for client-server applications without creating custom connectors or high-cost webification.
2. SSL VPNs are slow for the limited number of client-server applications they support: There are two protocol conversions for each trip, making a total of four for a round trip of an information request.
3. SSL VPNs are slow for web applications: The server-side logic involves parsing web applications.
4. SSL VPNs do not allow for peer-to-peer or real-time applications, where two applications need to open separate IP connections with each other to establish data paths so as to allow the peer-to-peer or even client-server protocol to work.

5. SSL VPNs provide unnatural, specific access to limited applications, instead of access that is similar to what employees experience when at their desk.

These serious limitations render SSL VPN remote access technology as one that falls very short of being able to address all remote access needs.

IPSec versus SSL VPNs

Until now, the secure remote access options boiled down to two choices: IPSec VPNs (first generation) and SSL VPNs (second generation). Both have strengths and both have weaknesses.

SSL VPNs primarily make browser-based applications available to remote devices. However, generally speaking, the more diverse the application mix, the less attractive an SSL VPN will be. It comes down to a trade-off between IPSec client installation and SSL VPN customization.

The extent to which applications can or should be “webified” is a wild card for SSL VPNs. The time and effort developing custom Java/ActiveX plug-ins could be more work than supporting an IPSec VPN.

Additionally, the term “clientless” isn’t entirely accurate for an SSL VPN. Although SSL VPN tunnels are launched from the user’s browser, often a desktop agent—a Java applet or ActiveX control—must be downloaded for access to thin client, client-server, or other applications that do not lend themselves to web page presentation (such as Citrix, IBM green-screen, Windows Terminal Services).

The bottom line is that the strengths of an IPSec VPN are the weaknesses of an SSL VPN and the strengths of an SSL VPN are the weaknesses of an IPSec VPN. Many vendors have recognized this and are providing both types of solutions to their customers. By doing this, these vendors can provide their customers with a complete solution that has the combined strengths of both types of VPN products and few or none of the weaknesses.

The burden now is placed on the enterprise or organization to accept the inadequacies and deploy only either an IPSec or SSL VPN, or implement and maintain both types of VPN solutions. Suddenly, the biggest advantage of an SSL VPN, the simple and low-cost administration no longer applies. By implementing both types of VPN solutions, the enterprise or organization not

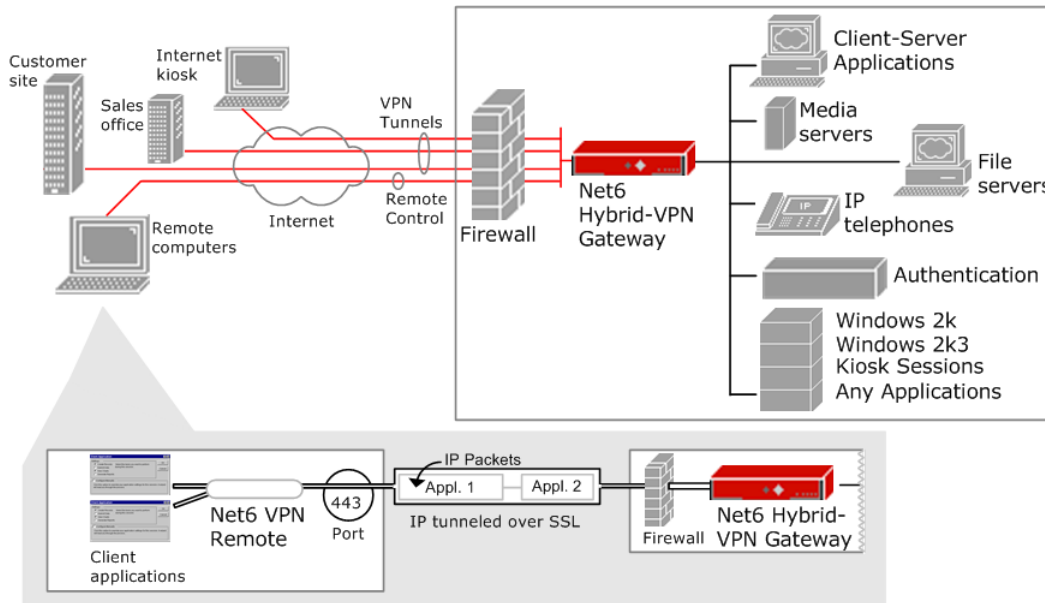
only has to implement and maintain clients on every PC, but also have to work around the inadequacies of the SSL VPN product as described in detail in the preceding discussion.

As supported by all of the issues with SSL VPNs and the known weaknesses, an organization that is deploying an SSL VPN will still need to deploy an IPSec VPN. In fact, TCO studies produced by many SSL VPN vendors to demonstrate the cost savings over an IPSec VPN still include a limited number of IPSec VPNs in their provisioning. If an SSL VPN was a complete solution, this would not need to happen.

The ideal case would be for an organization to replace both of these types of products with one that solves all of these issues.

The Net6 Hybrid-VPN Gateway: The First Complete VPN Solution

Net6, Inc. has developed a different approach to secure remote access that incorporates the benefits of both an IPSec VPN and an SSL VPN into one product: the Net6 Hybrid-VPN Gateway.



As shown in the above illustration, the Net6 Hybrid-VPN Gateway supports any application, thick client-server or industry strength web application, in its native form—no changes or development work whatsoever. It supports all protocols, traverses firewalls, and hides the IP addresses of the remote network to inhibit the traversal of worms. It is the best of both worlds when comparing the features of IPSec VPNs and SSL VPNs.

The Net6 Hybrid-VPN Gateway does this by bringing together the best parts of IPSec and SSL VPN solutions, with none of the shortcomings. IPSec VPN solutions provide network layer access and encryption. SSL VPNs provide application layer access and encryption. Net6 combines network layer access with application level encryption in a hybrid technology. This drastically

improves the end-user experience while significantly reducing the IT security administrator’s support overhead and security risks.

The unique Always-On™ feature enables users to work from anywhere, behind any firewall with auto reconnect. An employee can be connected at one location, disconnect from the network and be automatically reconnected when they get on-line at their next location. With the Hybrid-VPN Gateway, users simply access a secure website and use their normal authentication credentials. There is no need to worry about VPN client software or updates. Users remain productive by having the same network experience and application access available while sitting at their desk.

The following table notes the strengths and weaknesses of IPSec and SSL VPN solutions and how the Net6 Hybrid-VPN Gateway compares to both types of VPN products.

IPSec VPNs	SSL VPNs	Category	Net6 H-VPN Gateway
Yes	No	Desk-like network access experience?	Yes
Yes	No	All applications supported?	Yes
Yes	No	Peer-to-peer or real-time apps. (voice/video)?	Yes
Yes	No	Supports all protocols?	Yes
No	Yes	Low support costs?	Yes
No	Yes	Access through any firewall?	Yes
No	Yes	Hides network IP addresses (blocks worm traversal)?	Yes
No	Yes	Clientless kiosk mode?	Yes
No	No	Optimized (UDP) media and voice streaming?	Yes
No	No	ACLs at both network and application level?	Yes
No	No	Always-On Mode?	Yes

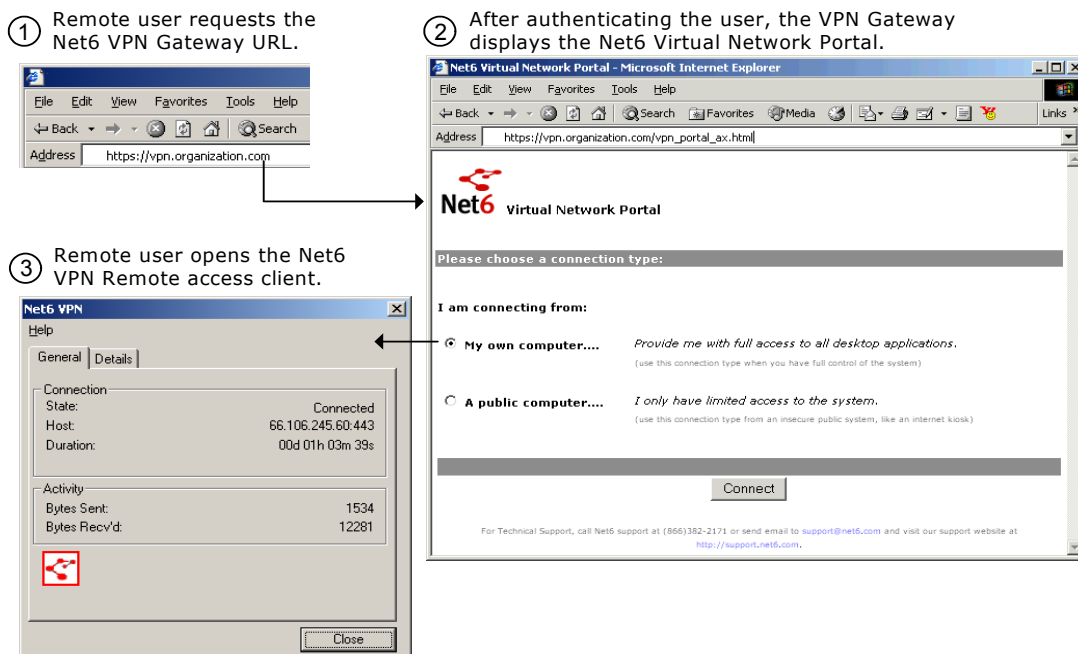
Enterprises and organizations can now just deploy one product for their secure remote access needs.

The Net6 Hybrid-VPN Gateway creates a virtual TCP circuit between the client computer and the Net6 Hybrid-VPN Gateway installed in the DMZ of the target private network. The Net6 Hybrid-VPN Gateway participates on two networks: a private network as well as a public network with a publicly routable IP address.

The virtual TCP circuit itself is encrypted using proven technologies such as SSL and TLS (Secure Socket Layer/Transport Layer Security). It is this circuit over which all packets destined for the private network are transported.

Launching the Net6 VPN Remote

Clients launch the Net6 VPN Remote access tool by simply accessing a secure web URL. This is typically the public name of the Net6 Hybrid-VPN Gateway, which prompts the user for authentication over HTTP 401 Basic, Digest or NTLM. The Hybrid-VPN Gateway then authenticates these credentials with an organization's logon server (such as LDAP or RADIUS) and if the credentials are correct, finishes the handshake with the client PC.



Establishing the Secure Tunnel

Once the VPN Remote has been launched, it establishes a secure tunnel over HTTPS port 443 (or any other configured port on the Net6 Hybrid-VPN Gateway) using TLS or SSL encryption. The client can be configured to test and validate client-side certificates if so configured by the Hybrid-VPN Gateway. In addition,

authentication information is sent to validate the tunnel. Once the tunnel is established, the Net6 gateway sends configuration information over to the Remote describing the networks that need to be secured and potentially an IP address if the administrator enables IP address visibility.

Tunneling Destination Private Address Traffic over SSL or TLS

Once authenticated, the Net6 VPN Remote is launched in the client computer, at which point all network traffic destined for certain private networks (which can be configured on a user by user basis, or organization basis) are captured and redirected over the secure tunnel to the Net6 Hybrid-VPN Gateway.

It is important to note that all IP packets, irrespective of protocol are captured in this manner and transmitted over the secure link. This in fact is what provides IPSec equivalent functionality to the Net6 Hybrid-VPN Gateway solution.

Consider TCP connections for example. Connections from local applications on the client computer are securely tunneled over to the Net6 Hybrid-VPN Gateway at which point the connections are re-established to the target server. Target servers view connections as originating from the local Net6 Hybrid-VPN Gateway on the private network, thus hiding client IP address (reverse NAT). Locally, on the client computer, all connection-related traffic (such as SYN-ACK, PUSH, ACK and FIN packets) are recreated by the Net6 VPN Remote so as to appear from the private server.

Terminating the Secure Tunnel and Regenerating Packets on the Private Network

The Net6 Hybrid-VPN Gateway terminates the SSL tunnel and accepts any incoming packets destined for the private network. If the packets meet the authorization and access control criteria, they are first fixed up (IP headers are regenerated to appear from the Net6 Hybrid-VPN Gateway private network IP address range, or the client-assigned private IP), then they are injected into the network. For circuit-oriented connections, the Net6 Hybrid-VPN Gateway maintains a port-mapped NAT table, so that connections can be matched and packets can be sent back over the tunnel to the client with the correct port numbers so they make it to the correct application.

Always-On™ Functionality

The Hybrid-VPN Gateway client continues to run in memory even when the laptop or PC is disconnected from the network. This advanced “Always On” functionality provides user benefits like auto-reconnect (the VPN connection is automatically restored when the network connection returns), application sharing, remote voice connectivity, remote control of user PCs by the IT department etc. This mode provides a powerful way to always ensure security over 802.11 networks with out having to deploy and maintain a WEP environment. This provides functionality is not currently available in either IPSec or SSL VPNs.

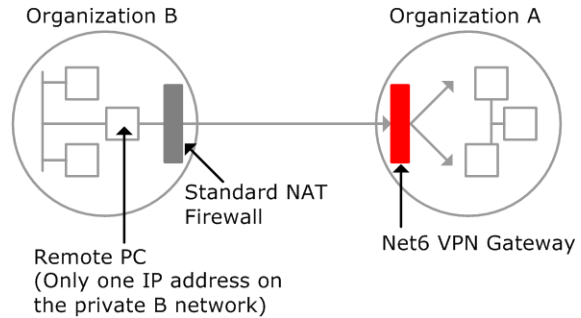
Handling Bi-Directional Protocols

It may be required for certain protocols that the server the client establishes a connection with in turn attempts to create a new connection with the client. In this case, the client sends its known local IP address over to the server by means of a custom client-server protocol. For these applications, the Net6 VPN Remote is able to provide the local client application a private IP

address representation, which the Net6 Hybrid-VPN Gateway will use on the internal network. Many real-time voice applications (and even FTP) use this feature.

Operation through NAT Firewalls and Proxies

A NAT firewall maintains a NAT translation table. The Net6 Hybrid-VPN Gateway maintains a reverse NAT table. VPN operation through the Net6 Hybrid-VPN Gateway is illustrated below.



The Hybrid-VPN Gateway tunnel is established using industry standard connection establishment techniques such as HTTPS, Proxy HTTPS, and SOCKS to name a few. This makes it firewall friendly and thus allows computers to access private networks from behind other organization firewalls with out creating any problems (these NAT firewalls can now create a mapping table that allows them to route secure packets from the Hybrid-VPN Gateway back to the client computer).

For example, the connection can be made via an intermediate proxy, such as an HTTP proxy, by issuing a CONNECT HTTPS command to the intermediate proxy. Any credentials requested by the intermediate proxy, will be in turn obtained from the end user (by using single sign-on information or by requesting the information from the end user) and presented to the intermediate proxy server. Once the HTTPS session is established, the payload of the session is encrypted and carries secure packets to the Hybrid-VPN Gateway.

Encryption Techniques

The Hybrid-VPN Gateway tunnel is encrypted using industry standard (and proven) technology such as SSL and TLS. Furthermore, each and every packet is encrypted, including any header information such as the IP header. This provides a very high level of security and does not provide anyone who gains access to the secure stream the ability to reconstruct any useful information.

The Hybrid-VPN Gateway supports 196-bit encryption, as well as higher or lower bit values set in the certificate. The Hybrid-VPN Gateway supports all OpenSSL ciphers: CAST, CAST5, DES, Triple-DES, IDEA, RC2, RC4, and RC5.

Performance and Real-Time Traffic

Many applications, such as voice and video, are real-time and therefore implemented over UDP (since TCP is not appropriate for real-time traffic due to the delay introduced by acknowledge-

ments and retransmission of lost packets). It is more important to deliver packets in real time than to ensure that all packets are delivered. However, with any tunneling technology over TCP, such real-time performances cannot be met.

The Net6 Hybrid-VPN Gateway overcomes this issue by routing UDP packets over the secure tunnel as special IP packets that do not require TCP acknowledgements. Even if the packets get lost in the network, there is no attempt made by either the client or the server applications to regenerate them, so real-time (UDP like) performance is achieved over a secure TCP-based tunnel.

Synopsis of the Net6 Hybrid-VPN Gateway Approach

The Net6 Hybrid-VPN Gateway provides secure remote network-level access to an organization's networks and all applications, over SSL/TLS. The Net6 Hybrid-VPN Gateway is appropriate for (i) employees accessing the organization remotely, (ii) for B2B access and transactions, and (iii) for intranet access from restricted LANs such as wireless networks.

The Net6 Hybrid-VPN Gateway has a remote software process running in it that performs the following functions:

1. Authentication
2. Terminating encrypted sessions
3. Access control (based on permissions)
4. Relaying data traffic (when the first three functions are met)

The Net6 Hybrid-VPN Gateway accomplishes remote access as follows.

1. The Net6 Hybrid-VPN Gateway exposes a secure web URL, accessible after authentication.
2. The Net6 Hybrid-VPN Gateway launches into the user's PC a per session Remote which resides in memory for the life of the session.
The Remote is a lightweight packet concentrator.
3. The Net6 Remote operates in conjunction with the Net6 Hybrid-VPN Gateway and maps application connections using a reverse NAT table.
4. During the session, the Remote resides in memory and operates at Layer 2 (between Ethernet and IP) during the session.
5. While the session is active, the Remote encrypts all network traffic destined for the organization's intranet and forwards the packets over an HTTPS session to the Net6 Hybrid-VPN Gateway along with user credentials.
6. All traffic is encrypted independent of port (potentially any port, not just port 443).

The Net6 Hybrid-VPN Gateway can handle real-time traffic, such as voice (RTP/SIP) with minimal loss in performance.

The Net6 Hybrid-VPN Gateway sits in an organization's DMZ with access to both the external network and internal network.

The Net6 Hybrid-VPN Gateway can also partition local area networks internally in the organization for access control and security between wired/wireless and data/voice networks.

The Net6 Hybrid-VPN Gateway is essentially acting as a low-level packet filter, with encryption. It drops traffic which does

not have authentication or does not have permission for a particular network.

The Net6 Hybrid-VPN Gateway has the option of making remote system IP addresses invisible. This adds security to source locations in B2B implementations. This is also valuable to secure the wireless network in a company for their users and visitors (a viable alternative to WEP).

Summary

IPSec VPNs and SSL VPNs both have inherent advantages and disadvantages. Organizations need the superset of advantages of both these types of products, with none of the disadvantages. The Net6 Hybrid-VPN Gateway provides organizations with the best of both worlds by providing the combined advantages of IPSec VPNs and SSL VPNs in a single product that is easy to install and maintain.

Advantages of today's IPSec VPN solutions

- Network to network communication.
- Desk-like network access experience.
- Protocol independent (network-level rather than transport-level).

Disadvantages of today's IPSec VPN solutions

- Do not work through firewalls (firewalls block all traffic except port 80 or 443).
- Difficult to deploy, maintain and manage.
- Unreliable or inconsistent operation (high cost of support and troubleshooting).
- Client IP addresses are visible from the accessed network (organization intranet)—a problem for B2B.
- Network bridging allows worm traversal.

Advantages of today's SSL VPN solutions

- Easy to deploy.
- Clientless.
- Client IP addresses are not visible from the accessed network.

Disadvantages of today's SSL VPN solutions

- Only work for web applications that do not use many of the more popular features like ActiveX controls and Java applets.
- Do not support native corporate applications (such as Microsoft Outlook) without creating custom connectors or performing high-cost webification.
- Degraded performance of client-server applications.
- Degraded performance of web applications.
- No support for peer-to-peer or real-time applications.
- Unnatural, specific access to limited applications, instead of access that is similar to what employees experience when at their desk.

Advantages of the Net6 Hybrid-VPN Gateway

- Complete network access—all applications including real-time Voice over IP are supported.
- Totally automatic invisible operation to the user, while securing 100% of applications.
- Successfully transverses all firewalls.
- Does not alter routing tables, thereby blocking worms.
- Flexibly can make IP addresses either invisible or visible to the accessed network applications, by application or host. The only IPSec alternative where peer-to-peer applications can work (where client IP addresses are visible to the application). This is a big advantage over IPSec for B2B implementations.
- Supports any routable protocol, including IP, IPX, AppleTalk and also Ethernet and RAS connections, not limited to TCP and UDP (e.g., it supports ICMP).
- Mobile device friendly.
- Ability to reconstruct Layer 4 protocols to analyze traffic.
- Lowest TCO—no IT department support required.
The Hybrid-VPN Gateway frees administrators from the hassle of installing, maintaining, supporting, and upgrading IPSec VPN clients. Every time a user accesses the secure VPN website, they receive the latest release of the VPN Remote. There is no need to webify any applications or call ahead to other organizations asking them to open a hole in their firewall. Using the Hybrid-VPN Gateway, the administrator's workload is decreased while employees' productivity is improved.
- Shortest deployment time.

Net6 and Net6 Hybrid-VPN Gateway are trademarks of Net6, Inc. All other trademarks and copyrights are the property of their respective owners.

The contents in this document are proprietary and confidential to Net6, Inc. This document cannot be reproduced or distributed, in any form, without the express permission of Net6, Inc.

All contents are Copyright 2004, Net6, Inc.

About Net6

Net6 provides solutions that enable employees, partners, and customers to securely access business applications regardless of their location or network. The Net6 Hybrid-VPN Gateway combines the best of VPN and IPSec features into a simple, secure remote access solution.

Net6 solutions are sold globally by Avaya, Cisco, NEC, Nortel Networks, Siemens and their resellers. With over 500 systems shipped, Net6 delivers value to Fortune 500 companies, hospitals, educational and financial institutions, manufacturers, and small and medium businesses. Net6 is a privately held company headquartered in San Jose, California. For more information, visit www.net6.com.