

White Paper



Accelerated, Scalable SSL VPN

Anywhere, Anytime Clientless Secure Remote Access

Table of Contents

Introduction.....	2
The Evolution of Remote Access.....	3
The NetScaler Solution.....	5
Conclusion.....	7
Contact NetScaler.....	7

Introduction

Enterprises are increasingly asked to provide access to corporate applications and data to employees and partners from outside the corporate perimeter. In order to do so in a cost-effective manner, enterprises are looking to leverage the Internet for providing remote access.

Today, most enterprises are using IPsec VPN technology to provide this access. Though robust and secure, IPsec VPNs have significant limitations. First and foremost, the administrative challenges in rolling out the VPN client software to thousands of remote access users, as well as managing and maintaining the client software, are not trivial. As a result, IT administrators incur significant incremental capital and operating costs. Furthermore, IPsec VPN technology has limitations in terms of access flexibility. Given the need for client software, corporate

users cannot access key resources from alternate endpoints, and their access from sites protected by firewalls is limited or in some cases, non-existent.

SSL-based VPN technology was developed to address some of the shortcomings of IPsec. However, most SSL VPN vendors have defined the problem statement too narrowly, and users are still searching for a solution that provides ubiquitous access to all applications in a secure, transparent and high performance fashion.

This white paper describes how NetScaler's solution represents the next generation of remote access technology, and describes how NetScaler's 9000 Series with SSL VPN capability delivers significant benefits in terms of application performance, application protection and return on investment for its customers.

The Evolution of Remote Access

To understand the issues involved when deploying existing remote access solutions and the unique advantages that NetScaler's Secure Application Networking solutions afford, it is important to look at the evolution of remote access and the underlying technologies.

Limitations of IPsec VPNs

The IPsec protocol operates at Layer 3 of the ISO OSI model, and essentially encrypts communication between two trusted parties. The IPsec VPN solution, while effective in providing high-performance encryption of data for site-to-site communications, has some significant limitations when used as a remote access solution.

The IPsec VPN solution requires client software to be deployed on the machine used for remote access. The need to deploy client software to thousands of corporate employees and partners is challenging from a software rollout, upgrade and maintenance standpoint. Training users on using separate client software for remote access is equally daunting. Furthermore, there are frequently situations where users need access to their applications and data from locations such as industry conferences, where they may not have or cannot use their own computers that have the IPsec client installed. This all-or-nothing IPsec client access proposition is too restrictive for peak productivity of today's mobile workforce.

Furthermore, as a Layer 3 protocol, IPsec encounters operational problems. IPsec exists as a separate protocol within the TCP/IP family, and as such is often blocked by firewalls since it is not among the commonly used protocols like HTTP, SSL, etc. This restriction often makes IPsec VPNs useless for users who

are guests at a facility and have no control over firewall rules. Firewalls that are performing network address translation (NAT) must also have special support for IPsec connections. These problems limit the range of locations where IPsec can be used successfully.

In addition, interoperability between manufacturers of VPN gateways and client software has always been an issue. Due to differences in implementation, not all client software works with all VPN gateways, thereby complicating the job of IT administrators in providing remote access to the user base.

And once access has been granted to the network, most VPN gateways have no way of limiting access rights—i.e., remote users can access everything. This can be a problem in situations where an IT administrator may want to enable access to a corporate partner, but wants to limit access to only certain servers or applications.

In summary, while IPsec is a proven, accepted solution for site-to-site communications, it has significant limitations when used for remote access.

Enter SSL VPNs

The Secure Socket Layer (SSL) protocol was originally created to secure Internet-based commerce, and hence all popular browsers support it. SSL-based VPNs have recently gained considerable momentum as a solution to overcome some of the challenges with IPsec VPNs.

Although originally created for securing Internet (HTTP) traffic, SSL is increasingly being used to secure other application protocols as well (e.g. SMTP, Telnet, LDAP, POP, and IMAP), and in some cases, has been used to secure more than just

TCP traffic. SSL VPN technology takes the underlying security provided by the SSL protocol, creates an encrypted tunnel between the client and the server and then adds granular authentication and authorization functionality to provide secure remote access to applications via the browser. This approach leads to significant benefits over IPsec VPNs:

SSL VPNs are Clientless

As mentioned earlier, a key limitation of IPsec VPNs is the need for deploying client side software on every access device, then training users on the client software and managing the ongoing upgrades for these devices. Since every client machine comes with a browser, and since every popular browser uses SSL, SSL VPN technology easily overcomes this issue. Valuable man-hours that would otherwise be spent administering VPN client software can now be used for more productive tasks.

Additionally, the learning curve for new users is negligible since most users know how to access content via a browser. SSL is highly interoperable too, since it is a well-known open standard in wide deployment.

SSL VPNs Can Be Used Anywhere

Another key limitation of IPsec VPNs is their inability to work seamlessly from behind client firewalls. Since SSL VPNs work not at the packet level, but at the application level, SSL VPNs do not have issues related to network address translation and reconfiguration when used behind a firewall. Because SSL traffic is allowed to pass by most firewalls, SSL VPNs can be used from almost any location.

SSL VPNs Have Granular Access Control

SSL VPNs are also flexible enough to provide granular access—based not only on user and role privileges and application types, but even on client access points. There are many useful applications of this capability. For instance, a user accessing the corporate network from a kiosk or Internet café could be restricted to access email applications only, while a user accessing from the home could be allowed broader access.

Secure Remote Access ≠ Secure Application Delivery

Clearly, SSL VPNs provide many advantages over IPsec VPNs for remote access. However, secure remote access is not the end goal of IT administrators. Rather, the goal is to achieve Secure Application Delivery, in which critical applications are accelerated, secured, and transmitted to end users. Remote access to the network is just one component of this concept.

In order to provide Secure Application Delivery, an SSL VPN gateway should include the following:

SSL VPNs Should Support Applications Transparently

Interoperability with existing infrastructure and applications is a key point to keep in mind when considering SSL VPNs. Most SSL VPN implementations cannot handle applications that dynamically generate URLs (e.g. JavaScript), dynamically change ports, or that use hard-coded IP addresses. This is a key limitation of SSL VPNs that severely restricts access to different kinds of applications by remote users. Another downside is that most SSL VPNs access one application per port, disallowing multiple logins by a user to the same application.

SSL VPNs Should Enhance Application Performance

Consideration should also be given to the overall performance of the SSL VPN solution. Remote users may dial-up on low-bandwidth connections and access applications that were never written for distribution over a wide area network. A poorly performing solution that makes remote users wait for page downloads reduces user productivity and the ultimate value of the application being accessed.

SSL VPNs Should Have Application-Layer Protection

According to some estimates, about 70% of all intrusion and hacking attempts occur through port 80 and 443. These ports are used for HTTP and Secure HTTP (SSL) traffic. Since firewalls are often configured to pass traffic on these ports, enterprises are vulnerable to attacks that can be tunneled through them. Worms such as Nimda and Code Red have exploited this weakness in the security architecture. Similarly, enterprises are vulnerable to range of denial of service (DoS) attacks, such as SYN floods. These attacks not only consume bandwidth and choke connections, they also bring down servers—resulting in a denial of service to legitimate users. For an IT administrator trying to provide remote access to a demanding employee base, a DoS attack can be a disastrous scenario.

| The NetScaler Solution

NetScaler's 9000 Series' secure remote access solution is a full-featured SSL VPN implementation that leverages NetScaler's proven application security and optimization capabilities to ensure high-performance, continuous, secure delivery of business-critical applications over the Internet and private networks.

Full-featured SSL VPN Solution

As a full-featured SSL VPN product, the NetScaler 9000 Series solution:

- Is clientless—i.e. does not require additional client software piece to be installed for remote access;
- Provides access to a broad range of applications including: email, native client/server applications, corporate intranets and shared file systems with a standard browser;
- Supports RADIUS, LDAP, Active Directory and other authentication schemes;
- Delivers comprehensive auditing and logging capabilities;
- Provides simplified management and monitoring via a command line or web-based graphical interface;
- Allows for granular access control by limiting user access on per user/group basis; and
- Integrates with end-station security components such as personal firewalls and antivirus software.

Achieving Secure Application Delivery

The NetScaler solution far outpaces the competition in other key areas critical to the goal of achieving secure application delivery.

NetScaler Supports Any Application

One unique feature the NetScaler 9000 Series provides in secure remote access is the capability to seamlessly handle applications which use dynamic port assignments or hard-coded IP addresses. Because of this, enterprises can support a much broader set of applications for remote access without

changing their existing network configuration or architecture. Remote users are not restricted to applications which were designed with remote access in mind.

NetScaler Accelerates Any Application

A key benefit of using the NetScaler solution in addition to security is performance optimization. The NetScaler 9000 Series of Application Delivery Systems is built on its patented Request Switching technology. The technology utilizes TCP offload, request multiplexing, and persistent connections with clients and servers to eliminate much of the overhead associated with TCP communication and speed applications and content delivery.

In addition, the NetScaler 9000 Series supports data compression for any application traversing the SSL VPN. This feature can even be used with applications which do not support encryption natively, such as e-mail or server file sharing. Compressing data for remote users has the effect of reducing download times by reducing the size of data transmitted, and is especially effective for users on low-bandwidth connections.

NetScaler's acceleration features also reduce costs. With a NetScaler system performing offload functions, application servers' capacity is maximized and the number of servers required can be reduced. This reduction in infrastructure results in lower operating costs since power consumption, cooling requirements, and administration tasks are all reduced. When compression is brought into the picture, NetScaler can provide bandwidth savings of more than 50%.

NetScaler Secures Applications

NetScaler is unique in its ability to prevent application-level attacks. NetScaler's Request Switching™ technology isolates servers from attacks such as SYN flood—preventing malicious denial of service to end users. Additionally, NetScaler's content aware intrusion prevention provides ability to create rules to block against specific traffic patterns, effectively blocking worms such as Code Red and Nimda, as well as GET flood and long URL attacks—ensuring that business-critical applications are available 24x7.

Conclusion

IPsec has many downsides when used for remote access. Client management and firewall problems keep this technology from being a widespread, easy to use remote access solution.

SSL VPNs solve many of the remote access problems associated with IPsec VPN solutions. SSL VPNs provide access via the browser and don't suffer from firewall issues. Since client software is not required, many more access options are available to remote users. Administrators are also freed of the burden of maintaining client software.

The NetScaler SSL VPN solution goes a few steps further. NetScaler's unique solution not only provides transparent access to any application, but also accelerates applications to provide a better remote access experience for users and enhance productivity. In addition, NetScaler's SSL VPN

provides the highest security for application servers as well as user data. These features combine to form a Secure Application Delivery system that enhances security, increases productivity, and reduces costs.

NetScaler's Request Switching traffic management represents a very significant advance in managing application traffic for a global infrastructure. By managing traffic at the request level and breaking the connection between the client and server, Request Switching provides optimal control over application traffic. Combining Request Switching's granular traffic management with advanced optimization and acceleration techniques delivers performance, flexibility, security, and manageability unmatched by any other solution. □

Contact NetScaler

NetScaler, Inc.
Corporate Headquarters
 180 Baytech Drive
 San Jose, CA 95134
 Phone: 408 678 1600
 Toll Free: 1 800 NETSCALER
 Fax: 408 678 1601

NetScaler Pvt. Ltd.
 #69/3, THE SIRIUS
 Millers Road
 Bangalore – 560052
 Phone: 91 80 51341000
 Fax: 91 80 51303000

NetScaler UK Limited
 1 Farnham Road
 Guildford
 Surrey GU2 4RG
 United Kingdom
 Phone: 44 1483 549440
 Fax: 44 1483 549441