Stratecast Partners | A Division of FROST & SULLIVAN

Addressing Enterprise Remote Access Challenges

Executive Summary

Ever since access to the Internet became prevalent, enterprises have been using it to remotely connect employees, business partners, and, for some, customers to internally hosted resources. Various alternatives have been developed to support this objective. However, each alternative has had its trade-offs in terms of security, cost, and flexibility. A more recent alternative, SSL VPN, is gaining rapid enterprise adoption because it overcomes many of the limitations that have plagued other alternatives. Nevertheless, no two SSL VPN solutions are the same so enterprises are wise to thoroughly assess SSL VPN solutions before making a selection.

This assessment can be a daunting task, as vendors do not portray their SSL VPNs in the same context. To that end, we believe that if one looks beyond a particular remote access technology and instead focuses on the core components that form an "Enterprise-Grade" remote access solution, this task becomes more manageable and produces a selection more tightly aligned with an enterprise's evolving remote access requirements.

In this paper, we will introduce and describe the three core components of an enterprise-grade remote access solution – Connectivity, Security, and Performance/Administration. We will also describe why these components are essential in an enterprise-grade remote access solution and how SSL VPNs, in general, are addressing them. In greater detail and in this same context, we will examine the FirePass SSL VPN appliance from F5.

Regarding F5's FirePass SSL VPN, it is important to note that prior to mid-2003 F5 was not known for its involvement in the SSL VPN market. This changed when the company acquired uRoam, an early developer of a SSL VPN appliance. F5 further expanded its product portfolio with the acquisition of MagniFire Websystems, a Web Application Firewall (WAF) vendor. The combination of three product lines – the company's flagship application traffic management BIG-IP product line, FirePass SSL VPN, and Traffic Shield WAF – all now sharing a common, high performance hardware architecture, is unique in the industry. No other SSL VPN vendor can claim a similar combination of complementary products. Furthermore, the company plans to create additional uniformity at the software level and eventually offer a blade alternative. With this blade alternative, enterprises can invest in a hardware chassis and plug in product blades to fit their current and future requirements. In our view, this chassis with blades approach further exemplifies the overlapping components of an enterprise-grade remote access solution and positions F5 well to be a leading provider of secure and performance-optimized application access solutions.

Introduction

The nature of remote access is continuously evolving. Originally, remote access was limited to a well-defined group of information-intensive workers with job functions that placed them beyond the perimeter of the enterprise network, but require periodic access to internal enterprise resources. Serving this need was traditionally accomplished through network-layer connectivity solutions, that is, solutions that temporarily redefined the boundaries of the enterprise network to include an external endpoint – primarily an enterprise-owned and managed device. While effective in creating a network connection, administrative effort was required to install and maintain a VPN software client on each remote access device and, as a network-layer connection, blocking at the remote network's perimeter security defenses could occur. In addition, remote access was limited to only devices where installation of the VPN software client was allowed.

Much has changed in terms of remote access. First and foremost, enterprises no longer singularly view remote access as a functional tool for a select number of end-users, but as a critical asset in advancing their strategic objectives – improved employee productivity, deeper business-to-business collaboration, and enhanced customer relationships. Second, Internet access alternatives are quickly broadening such that end-users can originate remote Internet-based access from any number of private and public locations: home, shared access sites (e.g., airport terminals, airplanes, convention centers, hotel lobbies, coffee shops, etc.), business partner locations, hotel rooms, and while mobile. Access devices are also broadening beyond desktop PCs and laptops to include PDAs and smartphones. Last, clientless, browser-based SSL VPNs have been instrumental in reducing administrative effort, expanding the range of accessing devices to include unmanaged devices (i.e., not owned by the enterprise), and improved end-user quality of experience. Consequently, previous obstacles in creating remote access connections between diverse endpoints and the enterprise over the Internet are quickly being erased.

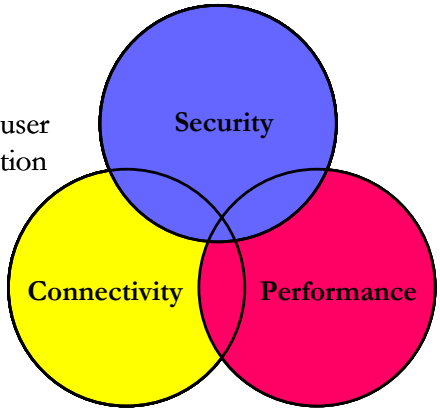
Enterprise-Grade Remote Access: More Than Connectivity

Connectivity, however, is only part of an enterprise-grade remote access solution. In our view and as demonstrated by developmental trends in SSL VPNs, the complementary functions of connectivity, security, and performance/administration are all required to deliver the full strategic benefits of remote access without compromising corporate security or incurring excessive administrative and infrastructure cost as the number and diversity of end-users, applications, and sessions increase. The figure below illustrates attributes of each functional component.

Functional Components of a Comprehensive Enterprise Remote Access Solution

Connectivity

- From anywhere
- Anytime
- Through any device
- By any authenticated end-user
- To any authorized application



Security

- Transmission privacy
- Enterprise network protection
- Granular and session-specific application access control
- End-point security & information protection

Performance/Administration

- Administrative-friendly without loss in functionality
- Interoperability with third-party solutions
- End-user transparent operation
- Optimized end-user application experience
- Throughput, scalability, and reliability

Source: Stratecast Partners

Connectivity

The access ubiquity of the Internet made possible through a combination of wired and wireless technologies means the first essential criteria for "anywhere" remote access can be met. However, as stated previously, traditional remote access VPN solutions restricted anywhere access to only devices that could support a pre-installed and configured VPN software client. Furthermore, perimeter security at the location of access origination could interfere in the establishment of a VPN session between the remote endpoint and the enterprise network. Consequently, traditional network-layer VPN solutions are insufficient for enterprises that need to support remote access from anywhere Internet access is available and from devices where a software client deployment is not possible (e.g., borrowed PCs and Internet kiosks) or not universally desired (e.g., employee home PCs).

SSL VPNs solve these limitations by relying on the ubiquity of Web browsers that are SSL-enabled. In essence, the Web browser becomes the standardized and readily available VPN software client. The need to deploy and configure a dedicated VPN software client is eliminated and remote access from nearly any Web browser-equipped device with any type of Internet access is supported. As a result, software client administration virtually disappears and the range of remote access devices is expanded. To be noted, the supported operating system of the access device is also a factor in unrestricted access. All SSL VPNs support multiple versions of Windows-based operating systems. Fewer numbers of vendors support other operating systems (e.g., Macintosh and Linux).

Regarding VPN session establishment, SSL VPNs are not a network-layer connectivity solution. Rather, they operate as a transport-layer connectivity solution and, as a result, do

not encounter the same challenges of creating a network-to-network connection. Moreover, since most network perimeter firewalls are configured with always-open ports for Web traffic (e.g., ports 80 and 443), blocking at the remote access network is minimized.

Not to be overlooked is the favorable attribute of network-layer VPNs of presenting any application in their native form. Network-layer VPNs, by design, are application agnostic. While simple browser-based access of SSL VPNs supports an ever-expanding number of Web-friendly applications, many enterprises require support for non-Web applications (e.g., client/server applications, terminal servers, Citrix MetaFrame). Fortunately, most SSL VPN vendors offer additional access modes to broaden supported applications. This is generally accomplished through a user-transparent download of a Java applet or Active X that runs locally on the access device during the VPN session. Full network access, similar to a network-layer VPN, through a SSL tunnel is another access mode available in many SSL VPNs. For the enterprise with non-Web applications, close attention to the availability, extensibility (i.e., which non-Web applications are reliably supported), and security associated with additional application access modes is recommended. The topic of security as it relates to application access modes, particularly the SSL Tunnel mode, will be discussed in the next section.

In the table below are F5's FirePass Connectivity features. Two comparative attributes relative to other SSL VPN solutions are:

1. Broad support of Windows and non-Windows operating systems, and
2. Multiple application access modes included as standard, not optional, features on the FirePass 4000/4100 - Portal Access, Application Access, and Network Access.

F5's FirePass Connectivity Features

Access originations supported – Allows access from managed and unmanaged endpoint devices behind perimeter firewalls and NAT devices.
Access devices supported – Windows, Macintosh, Linux, Pocket PC, and Solaris client operating systems with any of the major Web browsers.
Application access modes – Three access modes available in FirePass (4000/4100 platform), none require a pre-installed software client or configuration of endpoint or back-end resources: 1. ***Portal Access*** – internal Web servers, file services, and standards-based email servers. 2. ***Application Access*** –client/server applications in native form, terminal servers, remote corporate desktop control, Web-based collaboration, UNIX and Linux systems, and legacy hosts (e.g., VT100 and Telnet). 3. ***Network Access*** – any TCP and UDP-based applications.

Security

Connectivity without control constitutes a serious security gap. Unless specific security procedures and policies are created and enforced with remote access, enterprises jeopardize the integrity of their networks and the protection of sensitive information. Building regulatory and legislated directives aimed at tighter controls on information privacy and fair public disclosure further adds to the need for end-to-end security (end-user to application

server). In addition for SSL VPNs that support access from both managed and unmanaged access devices, vulnerabilities are greater versus VPN solutions that only support access from managed access devices.

Even with this greater level of vulnerability, several protection mechanisms exist with SSL VPN solutions to ensure the level of security risk can be adequately controlled; but as with connectivity features, enterprises should closely examine the security features of each vendor's SSL VPN solution before making a selection.

Following are six categories of remote access security enterprises should assess across SSL VPN solutions:

1. **Transmission privacy** – Since transportation over the Internet is in a shared network, payload encryption is essential to avoid information being sniffed while in transit. Support of both 3DES (Triple Data Encryption Standard) and AES (Advanced Encryption Standards) is desirable. FIPS certification is a useful gauge of solution strength.
2. **Enterprise network protection** – All Internet access devices are vulnerable to threats from Internet-based attacks and from worms and viruses carried in e-mails and file transfers. Spyware, programs that covertly record end-user activities and send them to un-trusted third parties, is also a growing threat category. While there are no guaranteed means to fully eradicate these threats in the open network environment of the Internet, the use of multiple security mechanisms can significantly reduce the risk. Those mechanisms include:
    - ***Assessing the security state of the endpoint as an integral step in determining end-user entitlements and permissions.*** If the endpoint is out-of-compliance with security policies (e.g., personal firewall in operation with correct policies, current anti-virus signatures and operating system patches, and no unauthorized applications operating), end-user access should be disallowed or restricted until compliance can be attained.
    - ***Directing end-users to a quarantine networks for policy remediation.*** To improve security policy compliance, end-users can be directed to specific sub-networks to download required anti-virus or personal firewall software and/or updates.
    - ***Filtering incoming e-mail attachments and files transfers for worms and viruses at the SSL VPN gateway.*** Even if the security state of the endpoint is in security policy compliance when the VPN session is initiated, worms and viruses can still be present in files and sent to the enterprise network. Filtering e-mail attachments and files augments efforts to slow the propagation of viruses and worms with other enterprise-connected endpoints.
    - ***Defending against split tunneling risk.*** Germane to the SSL Tunnel access mode are end-user circumstances of a VPN tunnel and general Internet access co-existing. Defense mechanisms to ensure Internet-based attackers cannot hijack the VPN tunnel are essential to protect the enterprise network with SSL Tunnel access mode.
3. **Granular and session-specific application access control** – A distinction of SSL VPNs attributable to being a transport-layer connectivity solution is the capability to

define and enforce granular access policies independent of the network infrastructure. Through this capability, IT administrators can be highly specific on the resources accessible for each end-user such that end-user access is restricted to only finely defined network resources; not a network of resources. Moreover, SSL VPN solutions that can dynamically assign end-user entitlements and permissions based on a combination end-user authentication method (e.g., single versus multiple factor), end-user group affiliations, type of endpoint device (e.g., public Internet kiosk, home PC, or corporate laptop), and endpoint device security state further enhances granular access control.

Session duration control is another important element of access control. Trusting the end-users will follow best practices is not 100% failsafe. End-users can and sometimes do leave an access device without closing the VPN session and, as a consequence, elevate the risk that an impostor could continue a legitimate session. Mechanisms to detect end-user inactivity and tear down the VPN session are crucial to defend against this risk.

4. **End-point security and information protection** – While several of the previously described security mechanisms are instrumental in endpoint security and information protection, other mechanisms are available with SSL VPN solutions and are listed below. As always, availability across SSL VPN solutions varies. These additional mechanisms include:

   - ***Session remnant purging*** – Identifying and removing specific VPN session remnants (e.g., cookies, downloaded files, and cache) from the endpoint device. Particularly with unmanaged access devices this is a valuable feature as the next user's trustworthiness is unknown.

   - ***Virtual desktop*** – An enhanced form of session remnant purging, the virtual desktop restricts all VPN session activities to a cordoned area of the desktop. At the end of the session, the entire virtual desktop is thoroughly purged or, depending on the SSL VPN vendor, saved in an encrypted file. With these capabilities, the need to specifically identify session remnants and the risk of under-identification are minimized. This virtual desktop feature also can be used to restrict saving of files outside the virtual desktop (e.g., on the hard drive or an external storage device).

   - ***File download control*** – Another element of granular access control is administrator-defined file download policies. For example, a policy that restricts downloading of highly sensitive files only to corporate-owned laptops by end-users who have been authenticated through a two-factor authentication method.

   - ***Virtual keyboard*** – The existence of spyware that records keyboard strokes, places end-user credentials are at risk of being captured and used by an un-trusted third-party. Techniques to obfuscate password entry such as mouse clicks can be an effective spyware defense.

5. **Application Security** – Whether malicious intent or out of curiosity, authorized end-users can engage in certain Web application behaviors that jeopardize information protection. Defenses against unacceptable user behaviors such as cookie manipulation, cross-site scripting, and SQL command injection assist in reducing this risk and improves compliance with industry regulations such as HIPPA (healthcare) and GLBA (financial services).

6. **Platform Security** – Closed systems with a hardened operating system (OS) and up-to-date vulnerability patches protect against OS-level security attacks. Trusted third-party certification and audits increase security assurance and compliance with various audit requirements. In addition, a platform design that features separate physical ports for quarantine network, shared DMZ network, and the internal network further adds to enterprise network security.

All SSL VPN vendors are continuously expanding and improving their security features. Consequently, enterprises will benefit by better security in whichever SSL VPN solution they select. Therefore, the more relevant SSL VPN comparison is a combination of: existing security features, distinctive features, and future security direction. In that regard, F5's FirePass contains a strong set of security features with market distinctiveness in e-mail attachment and file transfer filtering and application behavior blocking. The company's TrafficShield Web Application Firewall presents complementary capabilities for enterprises that need more comprehensive protection of their Web resources. As enterprises trend toward business Web applications and F5 executes on its chassis and blade architecture, the overall value of FirePass and TrafficShield expands.

F5's FirePass Security Features

Transmission Privacy
Encryption standards supported: 3DES and AES
FIPS-certified key storage and data protection
Granular and session-specific application access control
Granular access control based on user, device, and device security state
Administrative-defined session timeouts (session during and/or lack of keyboard or mouse activity)
Enterprise network protection
Safe split tunneling to protect against VPN tunnel hijacking and inadvertent Internet exposure.
Platform-based worm and virus inbound filtering
DoS (Denial of Service) defense
Web site and URL obfuscation
OS hardened platform
Packet filtering based on protocol, port, and destination
Granular and session-specific application access control
Granular access control based on user, device, and device security state
Administrative-defined session timeouts (session during and/or lack of keyboard or mouse activity)
End-point Security and Information Protection

File download blocking
Assesses security state of the endpoint and determines end-user entitlements and permissions based on that security state.
Secure Virtual Keyboard guards against keystroke loggers
Cache cleanup removes specific session remnants from endpoint device at session termination
Protected Workspace (i.e., entire session activity contained in cordoned space on desktop, no writing or saving outside, and entire session purged at session completion)
HTML content filtering. Blocks HTML buffer overflow, SQL command injection, cross site scripting, and cookie manipulation

Performance/Administration

As evidenced in the previous reviews of Connectivity and Security, SSL VPNs are highly sophisticated, feature-rich remote access solutions. This is logical conclusion considering the inherent complexity of remote access and the added burden of application support and heightened security vulnerabilities SSL VPNs must address in supporting access from unmanaged endpoints and through a Web browser. Consequently, if this sophistication is not translated into administrative-friendly tools and end-user transparency, the overall value of the SSL VPN solution is materially reduced. Similarly, the number and processing intensive functions placed in the SSL VPN gateway are considerable and, in our view, will continue to increase. Therefore, attributes of the gateway's hardware architecture and software pertaining to performance are also very relevant in an enterprise review of SSL VPN solutions.

For this review, we have grouped performance features into three categories: Administration, End-user Quality of Experience, and Gateway. Each will be discussed sequentially.

1. Administration

Granular access control, as described previously, is a distinctive and valuable capability of SSL VPNs in tightly controlling end-user entitlements and privileges. However, maximum control is only possible when several variables are combined to dynamically create the entitlements. To be efficient and accurate in combining all of the potential variables, administrators need object and group-based tools. Administration through objects minimizes the burden of managing enterprise resources by network addresses and/or server name, which have the potential to change, and grouping allows administrators to affect policy changes for subsets of end-users instead of completing the same task repetitively on an individual end-user basis.

Complementary to granular access control is seamless integration with exiting user authentication databases (e.g., RADIUS, LDAP, etc.). Without this capability, administrators would be required to replicate relevant portions of these databases into the SSL VPN gateway and on a continuous basis validate that these two databases match. Without this

integration, escalating administrator effort occurs as the complexity and size of the user community grows.

2. End-user Quality of Experience

For the end-user, performance is principally measured in terms of quality of experience. Being able to establish a connection in the circumstances most required by the end-user is a base requirement. To be expected in an information-intensive business environment, these required circumstances will expand. The browser-based attribute of SSL VPNs clearly broadens the circumstances in which a connection is supported relative to network-layer VPN solutions (i.e., non-corporate owned access devices). Supported access device operating systems is another factor in broadening connection circumstances. Beyond this base requirement, the next two characteristics of end-user quality of experience are the level and complexity of interaction required of the end-user to establish a connection and the extent the look and feel of a LAN connection is replicated in remote access.

3. Gateway

As with any other critical devices within an enterprise's network situated between end-users and back-end resources, the attributes of throughput, scalability, and reliability are relevant for SSL VPN gateways. For enterprises that have experimented with SSL VPN in a limited use scenario and are now prepared to expand and/or standardize on SSL VPN for remote access, these attributes are of utmost importance.

Contained in the following table are Performance features available in the F5 FirePass SSL VPN appliance. Areas of market distinctiveness include:

- Open API support of application auto launch,
- Broad traffic compression support, and
- SSL hardware acceleration for both SSL key exchange and data encryption /decryption.

Please note that the Open API and traffic compression also contribute to end-user quality of experience.

Last and similar to our comments on security, F5's flagship BIG-IP application traffic management product line is complementary to FirePass in providing customers of both enhanced means to optimize back-end resources and end-user quality of experience. As the company standardizes software and introduces a chassis and blade architecture, the combined value of these two products increases.

F5's FirePass Performance/Administration Features

Administration
Group-based policy management of users and resources
Importation of user information from external authentication servers
Authentication integration: RADIUS, LDAP, NTLM, Active Directory, various certificates, VASCO and RSA 2-factor authentication
End-User Quality of Experience

Auto launch applications (open API and SDK)
Automatic drive mapping
SSO support (Citrix, Web applications) and Netegrity integration
Login- and portal-page customization
Gateway
Application traffic compression (HTTP, TCP, UDP)
SSL Hardware acceleration of SSL Key exchange and data encryption/decryption
High availability stateful failover and clustering

Conclusion

Enterprise IT and security organizations face a constant struggle of providing access to enterprise resources by an increasingly larger and more diverse end-user community without subjecting the enterprise network infrastructure and its sensitive information to undue security risk. Compounding this struggle is enterprise applications are more complex, business critical, and performance demanding. In addition, the nature of Internet-based attacks is no longer limited to individuals seeking to demonstrate their technical prowess by disrupting network operations, but includes those who seek to financially profit by their exploits. Consequently, security threats are more sophisticated, originating from innumerable points of origin, and hidden within the data payload.

For all these reasons, enterprise-grade remote access solutions must seamlessly meld together the characteristics of anywhere/anytime connectivity, network and application layer security, and performance as measured from the perspectives of the administrators, end-users, and enterprise-grade gateway attributes.

In our opinion and as detailed in this report, F5's FirePass is a leading SSL VPN solution in melding all three of these components together. Furthermore, we view the company has a strong competitive position through full ownership of product lines in each of these components and the company's plans to build a chassis and blade architecture.

Michael Suby
Senior Research Analyst and Co-Program Manager, Communications Services Strategies and Opportunities
msuby@stratecast.com