

SSL VPN Application Access Technologies

An AEP Networks Functional Description

The benefits of web-based, on-demand access to centrally located applications – residing on Windows, Citrix, UNIX/Linux, mainframe or web servers - are well understood. By delivering mission-critical information efficiently and securely to a distributed workforce, companies can extend their reach across greater distances, bolster productivity, and realize a fast Return on Investment (ROI).

However, securing these application resources – particularly when access occurs over the Internet - remains a central challenge. This challenge grows more urgent in the wake of increasingly sophisticated network attacks (phishing, ID theft, man-in-the-middle attacks, Trojans, etc.) combined with expanding government guidance and mandates (GLBA, HIPAA, SOX, and others). The result: Companies have come to recognize data security as a critical business need. Fortunately, the emergence of SSL VPNs offers a simpler, safer, and less costly alternative to traditional access alternatives. SSL VPNs provide crucial network security for network-based applications, allowing organizations to extend their application resources with a surprising level of ease and confidence.

As with most technologies, not all products are created equal or provide comparable functionality. This document is intended to provide a brief technical overview of the application access technologies employed by the AEP Netilla Security Platform, a leading SSL VPN from AEP Networks.

Access Flexibility: Why AEP is Different

The NSP differs from other SSL VPN solutions by providing the choice of three application-access technologies in a single gateway device:

- Thin** ▪ Layer 7, application gateway access to applications residing on Windows Terminal Servers, Unix/Linux servers, and mainframe or AS/400 machines
- Web** ▪ Web Reverse Proxy access to web-based applications and intranet portals; Intelligent Port Forwarding for Windows Terminal Servers and Citrix Presentation Server
- Tunnel** ▪ Layer 3 (network-layer) access for any TCP/UDP-based applications via SSL tunneling

AEP's ability to elegantly integrate such a broad level of application flexibility into single security appliance architecture greatly distinguishes the NSP from competitors.

Thin/Application Gateway Access to Server-based Applications (Layer 7)

Applications residing on Terminal Servers - Windows, UNIX/Linux, and mainframes - form a vital core of the business applications used today. The challenge facing enterprises is to leverage these crucial applications in way that allows remote users to access these resources over the Internet in the most secure methodology available.

The NSP solves this dilemma, providing access to remote applications by incorporating Web-enabling technology directly within the platform. This integrated approach, unique to AEP among SSL VPN vendors, eliminates the need for enterprises to deploy and maintain server-based "middleware" — such as Citrix Secure Gateway — or remote-access clients, such as those required by IPSec approaches.





In this application-layer proxy model, the end user never directly connects to a “private side” network resource; instead, the NSP functions as a proxy, protecting application servers from direct Internet exposure. This approach eliminates the risk of viruses, worms and other exploits from passing from the end user to the network.

In the NSP’s Thin access model, the NSP initiates a session to the application server on behalf of the user, and presents a rendering of the session to the user’s web browser. This allows the user to interact with the application as if it were installed locally. An example using Microsoft Outlook is shown below.

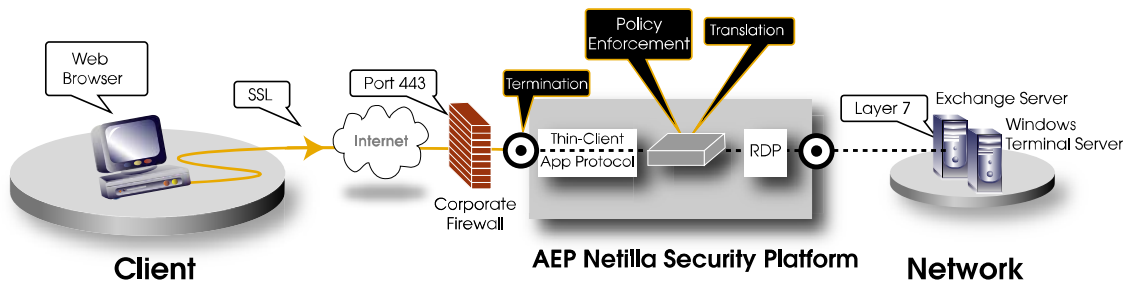


Figure 1: AEP Thin Access to Outlook

As Figure 1 shows, the NSP “intermediates” the connection between remote-client requests and the network server, terminating incoming connections at the application layer. Once the incoming request is terminated, the NSP processes and translates the data to the appropriate backend application protocol – in this case, RDP for the terminal server, which presents the Outlook application to the user. The NSP then resends the application data back to the user’s browser, in the form of HTTPS traffic via “screen scraping” technology. At no time is the enduser directly connected to a “private side” network resource.

AEP’s Thin access mode supports applications residing on Windows or Citrix, UNIX, Linux, and mainframe servers. By incorporating remote printing, client drive mapping, web-based file server access, this approach effectively recreates the main office environment from any authorized computer.

Web Reverse Proxy for Web Applications

In addition to Thin application access, the NSP also provides browser-based access to Web-based resources using Web reverse proxy technology. With this approach, a single point of entry over the Internet – the NSP itself – lets remote users access back-end, intranet Web servers securely through a Web browser.

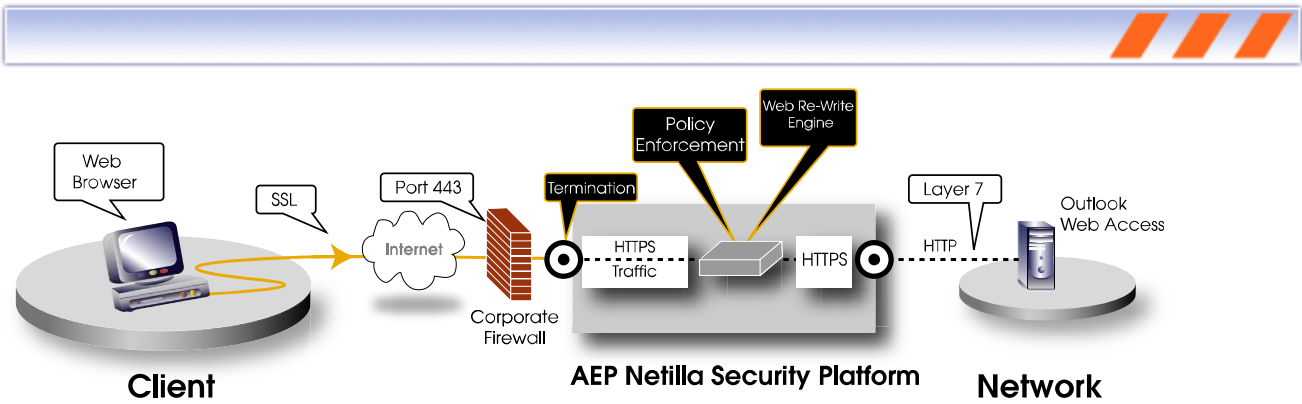


Figure 2: Outlook Web Access Through Reverse Proxy

As shown in Figure 2, a similar proxy approach used for Thin sessions is also well suited for Web-based intranet applications and portals. In this case, the NSP terminates, examines, and rewrites HTTP requests. Remote users are then presented with Web-application resources as allowed by corporate-defined security policy. For more complex web applications, the NSP employs a sophisticated Java applet re-write module, allowing smooth presentation of these applications.

Authorized remote users thus gain instant, clientless access to a wide range of internal Web applications from any location, allowing internal DNS addresses that do not resolve publicly to be accessed securely over the Internet. Company Web servers remain safe behind the firewall, in a highly secure portion of the private network, without the cost and maintenance of locking each server down for public access, while administrators gain granular access control to directories, servers, and paths on a user or group basis. At no time is the enduser directly connected to a "private side" network resource.

Windows and Citrix Access Alternative: Intelligent Port Forwarding

Organizations that prefer to use the Microsoft native RDP client or native Citrix ICA client, and whose user base typically accesses the network via corporate-issued machines and are employees of the company, can use AEP Intelligent Port Forwarding, which is included as part of the Web proxy functionality. This technique delivers a Java client that sits on a remote Windows machine and looks for the TCP port or ports that a particular application uses. As soon as data starts to flow, the client encapsulates and encrypts all the traffic in SSL and forwards it to the NSP gateway at the enterprise side of the network, where it can be deciphered and delivered to a terminal server or Citrix MetaFrame server.

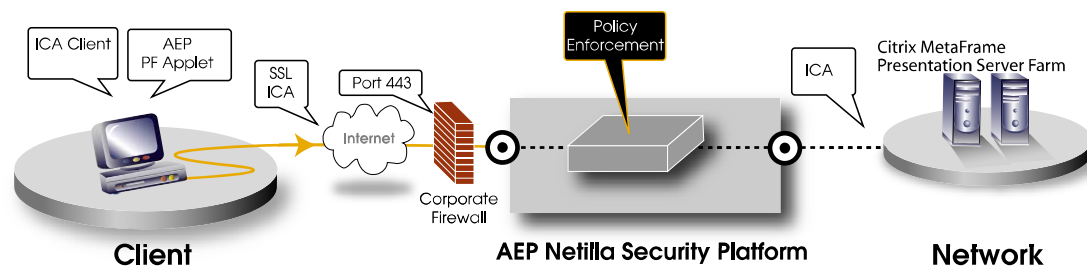


Figure 3: Port Forwarding for Citrix and Terminal Services



The NSP provides access to such environments with an automatic “client push.” When a user connects to the network for the first time, the NSP can package a Java applet that contains everything that particular client needs in order to connect to the network applications, whether they are running via Citrix (Java, ActiveX or Native clients) or via an RDP client. Administrators therefore do not have to send each user disks to install a driver onto the machine, and end users are not required to do anything other than click an icon; the NSP provides the appropriate client seamlessly and without administrative hassles.

In the case of Citrix, this functionality streamlines access and network complexity: Citrix applications can be published directly on the NSP webtop, giving users the same access environment remotely as when working at the office, while the NSP adds crucial security to the MetaFrame server farm without Citrix Secure Gateway or Web Interface. The NSP also enables organizations to avoid using Citrix Access Gateway, the Citrix VPN appliance that is severely lacking in security features and capabilities.

The NSP appliance supports the full Win32 Citrix ICA client via application-layer intelligent port forwarding technology, so users who already have the Citrix ICA client resident on their machines can access MetaFrame resources from any location.

Note that most SSL VPN competitors rely on 100% port forwarding to access terminal server applications, and do not offer the NSP’s application-layer Thin proxy model for the highest level of security. Port forwarding translates from one incoming TCP port to another, providing no opportunity to segregate public- and private-side data streams. This means that data passes through the SSL VPN appliance with fewer policy enforcement opportunities. This scenario often suits the needs of the majority of a company’s user base; yet only the AEP NSP provides the option to use both Port Forwarding AND a true Thin proxy access mode on the same appliance.

Network Layer Access to Client/Server Applications (Layer 3)

The third access mode option supported by the NSP allows access to client-server applications that require synchronization directly with the corporate server. The NSP provides this data transfer over a Layer 3 SSL tunnel, which is accomplished by using the browser as a conduit to install a virtual adapter. The virtual adapter negotiates the secure SSL tunnel via the user’s Web browser to the NSP, where each of these SSL tunnels is terminated as a PPP interface. Policy may be applied to these interfaces using the NSP’s integrated stateful packet inspection (SPI) firewall, facilitating a policy enforcement point similar to the NSP’s other access modes.

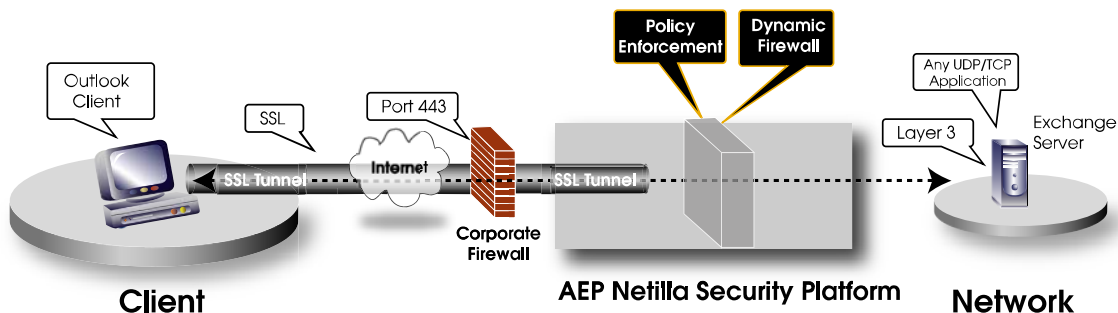


Figure 4: Fat Client Access Over SSL Tunnel



As shown in Figure 4, the NSP allows for applying dynamic policy over the layer 3 SSL tunnel. In this mode, the NSP's dynamic firewall is used to open and close specific ports. For the duration of each session, the administrator is able to grant access only to the Exchange server if required.

Ensuring Corporate Security Compliance

Protecting your network from outside threats is always a concern; such dangers grow larger when opening up your network for access from various locations outside of your IT department's control. Before you allow road warriors, partners and telecommuters to connect to your corporate network you must ensure against digital leakage and other threats. That's why the AEP Netilla Security Platform offers a wide range of security tools, including a deeply integrated endpoint security solution, with the flexibility to assign features on a per-V-Realm basis, creating customized protection for just those users who require it.

Client Integrity – Enforcing Corporate Compliance

Feature	Description	Benefit
Host Integrity Checking	Validates the presence and version of antivirus software, personal firewalls, service packs, patch levels, and custom objects on a polling basis throughout session	Ensures compliancy with corporate policy
Adaptive Policies	Checks pre-defined end station parameters; for example, registry entry or IP address	Confirms the identity and location of remote devices
Secure Desktop	Creates encrypted virtual workspace and performs DoD wipe at session end.	Prevents digital leakage and ensures the confidentiality of corporate information
Cache Cleaning	Deletes all traces of session data; for example, browser history or cookies	Removes the danger of sensitive data being left behind at remote locations
Session Timeout/Forced Periodic Re-authentication	Monitors inactivity and terminates session after elapsed time – can also force periodic re-entry of access credentials	Prevents data theft by terminating unattended sessions
Client Machine Identification Authentication (CMID)	Creates a unique profile (based upon CPU, memory, network card addresses and other information) to uniquely identify a specific corporate-issued computer.	Iron-clad method to limit access to pre-approved devices.
Certified security at the network edge	ICSA (Phase 2), VPNC, FIPS 140	Third-party security validation ensures the highest level of accreditation
Event logging and audit trails	Support for SNMP and SYSLOG	Helps achieve compliance by documenting security incidents and access histories.
Support for all leading authentication and policy databases	Seamless integration with MS ActiveDirectory, LDAP, RADIUS, Kerberos, RSA, and integrated VASCO server for 2-factor authentication	Ensures and enforces user authenticity



Trusted. Certified. Secure.



Conclusion: The Most Versatile SSL VPN Available

By merging three access technologies into a single appliance, the NSP provides a full-spectrum remote-access solution that meets EVERY application access type. The result is a powerful tool - one that delivers a high level of flexibility for network administrators, who can arm their remote users with a wide range of applications based on changing conditions and needs, while protecting the company's critical business assets.

Contact AEP Networks

info@aepnetworks.com

www.aepnetworks.com

U.S: 877-652-5200 x5207 • EMEA: +44 (0) 1442 458 640 • Japan: +81-3-3432-3336 • Hong Kong: +852 8199 0104

www.aepnetworks.com

© AEP Networks, Inc. All rights reserved. AEP Networks and the AEP Networks logo are trademarks of AEP Networks, Inc., with registration pending in the United States. Netilla, SmartGate, SmartPass and SmartAdmin are registered trademarks of AEP Networks, Inc. All other trademarks or registered trademarks contained herein are the property of their respective owners.