

End-to-End Security with Juniper Networks Secure Access SSL VPN

Ensure Your Remote Users and Devices Meet Stringent Security Requirements Before Granting Access to Corporate Network Resources

Challenge

As the global workforce continues to become more mobile, the need to access corporate network resources from various devices and locations becomes paramount. Enterprises must balance this demanding need for access while making sure users and devices have proper security credentials before getting into the network.

Solution

Juniper Networks Secure Access (SA) SSL VPN appliances provide comprehensive security measures against remote users and devices that can potentially harm the corporate network.

Benefits

- Protect the network from devices that don't meet proper security credentials
- Ensure network resources viewed by only those with proper authority to do so
- Confidently allow a wide array of devices and diverse audiences such as employees, partners, and contractors to access the network without security concerns
- Lower the total cost of ownership with no software to deploy or manage on devices

In today's global and mobile economy, it isn't uncommon to hear stories of companies incurring significant costs and exposing themselves to lawsuits due to corporate assets and data being compromised. At the same time, new risks for today's IT departments have emerged with the growing need for remote access to support mobile users, partners, and customers. Administrators in today's environments must constantly weigh the risks associated with providing remote access against the increasing demands for mobility.

Remote users require access to a company's applications and resources from anywhere and at any time, whether they are using a company issued laptop, personal home computer, mobile or handheld PDA device. IT departments face the challenge of opening the door to the exponentially growing number of mobile employees and partners, supporting their booming variety of devices and networks, while at the same time having the responsibility for ensuring that the company's data is safe from viruses and malware, disgruntled employees, or compromised devices that might trigger malicious threats on the company's applications or entire network.

Vulnerable security gaps in a remote access solution can lead to costly security incidents and public relations nightmares, if the right remote access tool with the best end-to-end security isn't in place.

The Challenge

A robust remote access solution must offer solid end-to-end security components. End-to-end security means having a variety of unique security features that protect access, from the end user to the internal server. While many companies may claim to have endpoint security features, more often than not, the feature set is lacking in one or more critical components, and security is only as strong as the weakest link in the chain.

Endpoint security features often include the ability to determine the security posture of the endpoint device in accordance with company policy, to check it for having the right virus protection, to scan for malware and other malicious agents, and to use that information to make informed decisions about the level of access provided to the end user for that specific session. Comprehensive end-to-end security includes ensuring that users have the right access to the data to which they have been granted access, whether that means providing access to the entire corporate network or access to only one file or application. End-to-end security includes safeguards for users accessing system resources from Internet cafés or kiosks by controlling that the data accessed is not inadvertently left behind for someone else to view or use.

Data in transition must also be secure. Ultimately, the SSL VPN device managing the traffic of users accessing a system must be secure from being compromised by outside users or malicious internal users.

Juniper Networks End-to-End Security with Secure Access SSL VPN

Juniper Networks Secure Access SSL VPN appliances offer a full spectrum of unique security features that protect access end-to-end, from the end user to the internal server.

Designed with security as the top concern, the Juniper Networks Secure Access SSL VPN platform provides important security benefits. Secure Access SSL VPN is a hardened security infrastructure that effectively protects internal resources and lowers total cost of ownership by minimizing the need to patch individual servers on an ongoing basis. The SA appliances will only run SSL VPN for remote access and no other services. There are no backdoors to exploit or hack. There is no interface, or interactive shell, or protocol to run on the machine. In fact, the platform has been audited and certified by several third-party security experts. Data storage is protected with AES 128-bit encryption.

Juniper Networks continually subjects Secure Access to third-party security audits in order to verify its security claims. In addition to having achieved iCSA Labs SSL/TLS Version 3.0 certification, third-party security audits have been conducted by ISEC Partners and CyberTrust (TruSecure). Secure Access was the industry's first SSL VPN product line to achieve Common Criteria certification, an internationally recognized verification of a vendor's security claims.

Features and Benefits

Host Checker

Prior to allowing an end user to start an SSL VPN session, the device from which that user is hoping to gain access needs to be assessed for an appropriate security posture. Endpoint defense establishes the trustworthiness of client hosts at VPN endpoints, the critical portion of the network that needs additional protection against malicious software and policy non-compliance.

The Juniper Networks SA SSL VPN Host Checker feature can be configured to assess the security posture of the endpoint device, to confirm that the user meets certain predefined security criteria, and to verify whether the machine should be considered trusted/managed or not. For example, the Host Checker can be configured so that the user is not even allowed to submit authentication credentials until the device has been scanned for updated antivirus software and an operational personal firewall.

Juniper Networks Host Checker capabilities include these components, which can be combined for a custom-tailored defense posture:

- Predefined Host Checker policies, available on all Juniper Networks SSL VPN appliances, enable point-and-click policy setup so that administrators can scan for a wide variety of third-party endpoint security packages on endpoint machines. Juniper Networks has provided predefined policies for the most commonly used antivirus, personal firewall, anti-spyware, anti-malware, and operating system types.
- In addition to predefined policies, administrators can configure custom Host Checker policies for increased flexibility in defining checks such as specific port activity, registry settings, processes running, and the presence or absence of specific files. Administrators can configure their own custom dynamic link libraries (DLLs) which can be integrated into the native functionality. Native Juniper Networks SSL VPN Host Check functionality combined with personal firewall, antivirus solutions, emerging malware detection agents, and virtual environments empower customers to leverage their existing investments in security, as well as easily deploy endpoint security solutions that fit their business needs. These policies allow administrators to verify the widest possible range of security applications or other attributes.
- Host Check application programming interface (API) provides integration with best-in-class security clients that include leading personal firewalls and antivirus solutions, verifying that these clients are installed, running, and in compliance with policy.
- Automatic remediation capability provides the ability to remediate (correct) any device that is found not to meet the corporate security policy. It includes the following capabilities.
- For all antivirus applications supported by Host Checker
 - Launching an antivirus process (if it's not already running)
 - Launching an antivirus scan
 - Downloading a virus definition file (if the antivirus definition file isn't recent)

- Invoking real-time protection (if not already enabled)
- Firewall auto-remediation for Microsoft Windows XP and 2000, and Microsoft Vista, turning the firewall on (if it's not running)
- Automatically modifying registry settings to pre-defined values as specified by policy for compliance
- Trusted Network Connect (TNC) support allows interoperability with diverse endpoint security solutions from antivirus to patch management to compliance management solutions. This enables customers to leverage existing investments in endpoint security solutions from third-party vendors.

The results of any Host Check are tightly tied with the Secure Access dynamic access privilege management policies (detailed later in this paper) and are documented in the SSL VPN logs. This enables the enterprise to easily integrate endpoint security into their remote access deployments and to track their overall security risk exposure. This is particularly critical when users are coming from unmanaged devices or from untrusted networks.

Dynamic Access Privilege Management

Juniper Networks SA SSL VPN dynamic access privilege management provides controlled, granular access based on endpoint security scan results, end user identity, state of the device, and trust level of the network. Based upon this information, and upon user credentials, SA dynamically assigns resource-level authorization for the session, specifying exactly which resources an end user can access. After a session has started, periodic endpoint security scans occur throughout the session to ensure that the security posture of the device has not changed, and to provide complete security to the company's resources. This role can change as the user moves around, logging in from different places, or even by time of day.

Juniper Networks SA SSL VPN provides relevant remediation and containment in the pre-authentication stage—if user attributes do not match minimum requirements, that user can be prompted to correct the situation before authentication, or be granted reduced access privileges.

Here is an example to demonstrate how dynamic access privilege management features work:

A saleswoman starts a travel day using her laptop on the corporate LAN to access resources protected by the Secure Access appliance. Since it is a managed device from a trusted network, she will probably get the most permissive access. The saleswoman then goes to the airport and logs into an airport kiosk to check her schedule. She is now accessing the network from an unmanaged device on an unmanaged network, and will likely get less permissive access than her access on the corporate LAN. At the end of the day, the saleswoman checks into her hotel and accesses the LAN from her room. Now she has a managed device coming from an untrusted network, and will likely get different privileges yet again.

In this example, Secure Access was able to dynamically grant different privileges for the same user, although she was accessing the SSL VPN appliance from the same URL. The difference in the variety of end devices and network connections resulted in different access experiences. The same concept can be applied to business partners, customers, and other non-employees who need to access the same network.

Connection Control

In order to fully protect corporate resources, some control must be exhibited over endpoint devices while they are connected to the SSL VPN gateway. Juniper Networks has implemented its Connection Control functionality to meet exactly that need. The predefined connection control Host Checker policy prevents attacks on Windows client computers from other infected computers on the same physical network. The Host Checker connection control policy blocks all incoming TCP connections. This policy allows all outgoing TCP and Network Connect traffic, as well as all connections to Domain Name System (DNS) servers, Windows Internet Name Service (WINS) servers, Dynamic Host Configuration Protocol (DHCP) servers, proxy servers, and SSL VPN . The result is that Secure Access can keep third parties from accessing the connected endpoint and potentially using the SSL VPN session for malicious purposes.

Cache Cleaner

Organizations frequently need to enable access to corporate resources from unmanaged machines, whether these are partner-owned laptops, shared machines in kiosks or Internet cafes, or home PCs. It is paramount that evidence of an SSL VPN session having occurred, along with details of that session, be deleted from the machine before others begin using the device. Cache Cleaner in Juniper Networks SA SSL VPN clears the temporary Internet directory, browser history, cookies, and other remnants of the user session from the user machine upon user logoff. Cache cleaning can also be conducted for administrator-defined directories and files (for example, temp). Cache Cleaner enables security administrators to extend the default policy that cleans temporary browser cache with realm, role, or resource-based policies that control the cache cleaning behavior on a host-by-host basis, or by specifying file and path names, enabling granular control over session information. Cache Cleaner executes on an explicit SSL VPN timeout if it encounters an abnormal termination, if the user session expires, or if a loss of connectivity with the server occurs. In all of these cases, temporary session data will be securely removed from the machine. Cache Cleaner utilizes a secure delete function to ensure that data cleanup is complete and comprehensive to protect from malicious attempts to recover erased data from disks.

Secure Virtual Workspace

Secure Virtual Workspace (SVW) provides complete control over corporate information that is downloaded to the local machine during an SSL VPN session. SVW is a client application that creates a sandbox within which a secure SSL VPN session is completely contained on an end user's PC, limiting the use of downloaded data to only the current SSL VPN session. The virtual workspace is created within the user's real desktop after validating the host integrity of the end user's machine. It provides a secure environment within which only administrator-specified programs can run, and where extremely strict control is enforced over user interactions with the data.

The registry and I/O access of these programs, their network communications, and the interactions with the resources and programs running on the real desktop are controlled entirely by the SVW module. All interactions with SSL VPN, and the backend resources protected by SSL VPN, occur within the sandbox. Any information stored on the disk or in the registries is encrypted on the fly using Advanced Encryption Standard (AES). At the end of the session, the sandbox is destroyed and all of the information pertaining to the virtual environment is permanently deleted from the endpoint. This ensures that users accessing data from a remote kiosk can be assured that their data is unavailable to any other user using the shared PC. The net result is that no data will have been saved locally, printing and clipboard operations are tightly controlled, and session specific-information is securely deleted from the endpoint. SVW is primarily used in kiosk and shared PC environments by organizations with strict information security policies. As deemed safe by administrators, SVW offers a persistent session capability which mandates that users select a shared secret at the end of the sessions that will be used to unlock the AES encrypted file once the user has begun a new SVW session. This enhances usability while still affording a high level of security.

The SVW is dynamically downloaded from the SSL VPN gateway and is installed on the endpoint when a user initiates a new session. SVW creates a virtual registry space, virtual file system, and a communication access control layer. The virtual file system and virtual registry are private spaces created by the SVW on the client desktop for use by programs running within the SVW module only. The communications access control layer monitors and controls all forms of inter-process and device communications between the programs that are running within SVW, and programs and devices that are running outside of SVW. This enables SVW to control keyboard operations, access to printers and removable drives, files shares, and so on. By default, all of these operations are disabled from within the SVW session for maximum security. SVW can install and run on endpoints with limited user privileges, making it optimal for the widest range of potential endpoints.

Coordinated Threat Control

The escalating volume and sophistication of threats from intentional and unintentional attacks contribute to the challenges for extended enterprise access. Granular access capabilities and endpoint security technologies provide the ability for IT to control access to applications and resources. However, while restricting access to only what a user requires is critical, it does not prevent attacks that can come from either unintentional or malicious authenticated users. Some examples include a disgruntled employee/partner or a hacker who has compromised the authentication credentials of a user.

A common way of adding security to a remote access deployment is to utilize intrusion prevention system (IPS) technologies. However, deploying IPS behind an SSL VPN can have limitations. When malicious traffic is detected, it can be difficult to correlate the malicious tunneled traffic to a specific user and sometimes impossible to identify a user with intermediated traffic. However, the identification of the user and the source of the malicious traffic are key in maintaining a secure network for the extended enterprise. A valid user whose remote access device may have been compromised must be notified and directed to “clean” their device as appropriate. A malicious user, on the other hand, must have their access blocked to prevent further network attacks. Containment and restricting any further access is imperative to safeguarding all resources.

Coordinated Threat Control technology enables Juniper Networks SA SSL VPN and Intrusion Detection and Prevention (IDP) appliances to tie the session identity of the SSL VPN with the threat detection capabilities of IDP to effectively identify, stop, and remediate both network and application-level threats within remote access traffic. With this technology, when IDP detects a threat or any traffic that breaks an administrator configured rule, it can, in addition to blocking that threat, signal Secure Access. SA uses the information from IDP to identify the user session that is the source of undesired traffic, and can take manual or automatic actions on the endpoint including: terminating the user session, disabling the user's account, or mapping the user into a quarantine role. Administrators can configure the quarantine role so that they can provide users with a lower level of access to resources, and inform the user of the reason they have been quarantined and what they should do in order to remove themselves from quarantine status.

Data Transit Security

To ensure that the data in transit is secure, Secure Access uses the Secure Socket Layer protocol (SSL) across the Internet. SSL utilizes encryption and decryption to secure private data across the public network.

Solution Components

The Juniper Networks SA 700, SA 2500, SA 4500, and SA 6500 SSL VPN appliances meet the needs of companies of all sizes requiring access for mobile users. Secure Access appliances use SSL (Secure Sockets Layer), the security protocol found in all standard Web browsers. The use of SSL eliminates the need for pre-installed client software, changes to internal servers, and costly ongoing maintenance and desktop support. Juniper Networks Secure Access appliances also offer sophisticated partner/customer extranet features that enable controlled access to differentiated users and groups without any infrastructure changes, demilitarized zone (DMZ) deployments or software agents.

The SA 700 appliance is specifically designed for very small enterprises as a secure, cost-effective way to deploy remote access to the corporate network. The SA 2500 SSL VPN appliance enables small-to medium-size businesses (SMBs) to deploy cost-effective remote and extranet access, as well as intranet security. The SA 4500 SSL VPN appliance is ideal for mid-to-large size organizations, while the SA 6500 SSL VPN is purpose-built for large multinational enterprises and service providers.

CORPORATE AND SALES HEADQUARTERS

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC HEADQUARTERS

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA HEADQUARTERS

Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
Fax: 35.31.8903.601

Copyright 2008 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Summary – The Most Feature-Rich Security Solution for Remote Access

While SSL VPN companies today often claim complete end-to-end security for remote access, their claims can be misleading if they are not offering a comprehensive solution. Security gaps in any remote access solution can lead to embarrassing news about compromised data, or information security breaches about the company and its customers, with devastating effects.

Juniper Networks Secure Access SSL VPN appliances offer the best in end-to-end security for remote access—from the hardened appliance itself to its rich feature set that enables IT departments to ensure the security posture of endpoint devices, networks, and users before allowing access into their systems.

Opening the doors to more users and the rising variety of devices can be quite a challenge for any IT deployment. Juniper Networks SA SSL VPN appliances are feature rich in providing a secure remote access solution. As the market leader in SSL VPN for remote access since the market's inception, Juniper Networks SA appliances are the top choice of IT departments worldwide for their best-in-class end-to-end security features.

Next Steps

Please contact a Juniper Networks representative or Juniper's global network of channel partners for any questions about the Secure Access SSL VPN appliances.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.

