

What's New in Juniper Networks Secure Access (SA) SSL VPN Version 6.4

This document lists the new features available in Version 6.4 of the Secure Access SSL VPN product line. This document assumes familiarity with the Juniper's IVE platform and the features of earlier releases up to version 6.3.

The document is organized into five sections, each describing a different functional area.

- I. UAC-SA Federation
- II. Authentication and Access Control
- III. Client Access Mode enhancements
- IV. Enhanced Manageability and Deployment Flexibility
- V. Endpoint Security
- VI. SA4500FIPS and SA6500FIPS hardware platforms

UAC-SA Federation

Unified Access Control – Secure Access Federation

Secure Access version 6.4 supports federation of user sessions between the Secure Access device and a Juniper Unified Access Control deployment (starting with UAC release 2.4). In many organizations where both a remote access solution and a Network Admission Control (NAC) solution have been deployed, remote access users frequently need to authenticate first into remote access, and then again into NAC in order to access the full range of protected resources. UAC-SA Federation adds the ability to seamlessly provision SSL VPN user sessions into UAC upon login, enabling a seamless end user experience in these types of environments. As Juniper is committed to supporting industry standards, UAC-SA Federation leverages an open standard from the Trusted Computing Group known as Interface for Metadata Access Protocol (IF-MAP).

Customer Benefits

- Federation of the Secure Access and UAC products provides remote users seamless access to corporate resources which are protected by UAC policies. This enables remote users to access such resources with a single login.

Availability

- Available on all Secure Access products and all Unified Access Control products.

Authentication and Access Control

Constrained Delegation and Advanced SSO Enhancements

In the area of web single sign-on through the Core Clientless access method, Secure Access 6.4 adds three new key enhancements - Kerberos SSO, NTLM v2 SSO and Kerberos Constrained Delegation. Both Kerberos and NTLMv2 SSO add new protocol support to existing Single Sign-On capabilities already provided by the Secure Access products.

Constrained Delegation is a new functionality that allows organizations to completely eliminate the need to manage static passwords in their environments. In recent years, many organizations have moved to strong authentications schemes such as One-Time Passwords (OTP) and X.509 Digital Certificates. One disadvantage of using these types of credentials in a clientless SSL VPN (or any "proxy" scenario) is that those credentials cannot be reused for SSO into backend resources and applications. Therefore, administrators must also collect static passwords from end users at login time to meet the need for SSO. Constrained Delegation (CD) changes that and finally allows organizations to free themselves from the time and expense associated with managing static passwords. With CD, when a user logs in to Secure Access with a credential that cannot be proxied through to the backend server, the Secure Access device will retrieve a

Mar 2009

Kerberos Ticket on behalf of the user from the Active Directory Kerberos infrastructure. That ticket will be cached on the SA and throughout the session, when the user accesses Kerberos-protected applications, the SA will use the cached Kerberos credentials to log the user in to the application without prompting for a password.

Customer Benefits

- Simplified User Experience – Remote access users can now seamlessly access corporate applications which require additional authentication via Kerberos or NTLM v2 protocols. The Secure Access appliance can automatically authenticate the remote user via Kerberos or NTLMv2 using user credentials, therefore avoiding the user having to enter credentials multiple times to access different applications.
- Ease of security administration – Corporate application administrators can enable authentication and access control for their applications via Single-Sign-On mechanisms or Kerberos Constrained Delegation. This provides easy administration of security policies while still maintaining strong security for critical applications.

Availability

- Available on all Secure Access products.

Support for Windows Domain Authentication through Windows Secure Access Manager (WSAM)

Windows Secure Application Manager (WSAM) in Secure Access 6.4 now supports the ability for a remote user's PC to authenticate to the Windows Domain. This will enable remote users to seamlessly login to applications that support Integrated Windows Authentication.

Customer Benefits

- With Secure Access 6.4, remote users can now access enterprise applications that use Integrated Windows Authentication through the WSAM access method. Such applications include Outlook, IIS-based web applications and remote file servers.

Availability

- Available on all Secure Access products.

Support for Windows Server 2008 Applications

Secure Access 6.4 supports interoperability with Windows Server 2008 applications including Windows Terminal Services. This release also supports authentication and access control against Active Directory on Windows Server 2008.

Customer Benefits

- Customers can seamlessly upgrade to Windows Server 2008 in their enterprises while their Secure Access products continue to support critical applications on Windows Server 2008.
- The Secure Access products now support clientless access to Sharepoint 2007, Outlook Web Access 2007 and also Terminal Services access on Windows Server 2008.
- Customers can use Active Directory on Windows Server 2008 to perform authentication and access control for their Secure Access deployments.

Availability

- Available on all Secure Access products.

Client Access Mode Enhancements

Client Access: Enhanced Credential Provider support with Network Connect

Credential Provider integration with Network Connect introduced in version 6.2 has been enhanced to work with 64-bit Windows Vista in addition to the 32-bit version and also to integrate with smartcards for authentication. As Windows Vista 64-bit is gaining popularity, this is an essential feature for most customers. In addition, smartcards are used widely so that passwords need not be remembered for authentication.

Customer Benefits

- Provides customers flexibility to choose the operating systems and authentication mechanisms best suited for their environment.

Availability

- Available on all Secure Access products.

Client Access: Extensions to usage of DHCP servers with Network Connect

The DHCP server usage with Network Connect has been extended to allow for passing the DHCP options of DNS Server, DNS Domain, and NetBIOS server from the server to the client. In addition, customers will be able to pass name/value pairs as DHCP options to the server. Customers will also be able to configure multiple (up to 3) DHCP servers for backup purposes.

Customer Benefits

- Provides customers an easy migration path from the traditional IPsec VPN clients to the SSL VPN based Network Connect by allowing for the familiar configuration options

Availability

- Available on all Secure Access products.

Host Checker for Network Connect and Windows Secure Application Manager Launchers

Customers can now leverage Host Checker functionality when using the standalone launchers of Network Connect and WSAM Access methods. Host Checker is now available for the standalone launchers of these access methods on Windows PCs. It is also available for WSAM on Windows Mobile platforms.

Customer Benefits

- This enables customers to enforce endpoint security on both Windows desktops as well as Windows Mobile devices using the Host Checker functionality while using standalone client launchers.

Availability

- Available on all Secure Access products.

Enhanced Manageability and Deployment Flexibility

XML Import/Export for Instant Virtual Systems (IVS)

Secure Access 6.4 extends programmatic support to configure and manage Instant Virtual Systems (IVS). This will enable Service Provider customers to integrate IVS management into their Operations Support Systems (OSS). It also enables Enterprises that use Instant Virtual Systems to leverage XML Import/Export capabilities for management of the individual Virtual Systems.

Customer Benefits

- Service Provider customers can now manage Instant Virtual Systems on their Secure Access appliances through their own Operations Support Systems (OSS).
- Customers can programmatically configure Instant Virtual Systems via XML, to create, edit and delete virtual systems on the Secure Access appliance.
- Customers can dynamically import or export XML configurations for Instant Virtual Systems into the Secure Access appliance.

Availability

- Available on all Secure Access products.

Enhanced Split Tunneling configuration for Network Connect Access Method

Customers can now configure a list of subnets or network hosts to be *excluded* from being tunneled through the Network Connect tunnel established between the remote desktop and the Secure Access appliance. In earlier releases, customers could only configure a list of subnets or hosts to be *included* in being tunneled through the Network Connect tunnel.

Customer Benefits

- This additional method of configuring split tunneling in Network Connect provides increased flexibility to the customer in specifying which subnets or hosts are to be included or excluded from being tunneled.

Availability

- Available on all Secure Access products.

Support proxy settings for download of virus signature and patch management files

The Secure Access SSL VPN Host Checker has been enhanced to allow for the configuration of a proxy server to be used to download Virus signature version monitoring and Patch Management Info monitoring files as many customers often use a proxy server to download frequent updates instead of downloading these updates directly from the Juniper Networks support site.

Customer Benefits

- Provides flexibility to choose how customers want to update the connecting users' endpoints for host checks.

Availability

- Available on all Secure Access products.
-

Endpoint Security

Auto-remediation of endpoints through SMS

Secure Access 6.4 now supports automatic remediation of non-compliant endpoints by updating software applications that do not comply to corporate security policies. Secure Access dynamically initiates an update of these software applications on the endpoint using the Microsoft SMS protocol.

Endpoints configured with SMS for software management typically poll for updates to software applications every 15 minutes (this time period is configurable). So when an endpoint remotely connects to the corporate network, it may have to wait up to 15 minutes before its software is updated as per latest corporate policies. This will prevent the endpoint from gaining full network access if the Secure Access is configured with a policy that requires software applications to have the latest updates. Secure Access 6.4 will now force the endpoint to update its software right after evaluating its software versions, so that the user does not have to wait for the next periodic software updates.

Customer Benefits

- Improves productivity of remote users who will gain immediate access to the corporate network without having to wait for periodic updates of software applications.
- Ensures compliance of remote endpoints to corporate security policies by facilitating an immediate remediation as soon as the endpoint connects to the corporate network.

Availability

- Available on all Secure Access products and all Unified Access Control products.

SA4500FIPS and SA6500FIPS hardware platforms

SA6500FIPS and SA4500FIPS hardware platforms now available

Juniper's industry-leading SSL VPN solution now includes two new FIPS platforms – the SA6500FIPS and the SA4500FIPS. These new platforms include the same functionality available on the rest of the Secure Access products, but include a dedicated FIPS 140-2 Level 3 certified hardware security module which handles all cryptographic operations.

The SA4500FIPS is an enterprise-level, purpose-built hardened security appliance that supports up to 1000 simultaneous users. It can be clustered in pairs for increased throughput and seamless failover.

The SA6500FIPS is built to meet the needs of the most demanding and complex government agency and secure enterprise environments. The SA6500FIPS can support up to 3,500 simultaneous users as a standalone device, scaling up to 10,000 users in a 4 unit cluster. It features dual mirrored, hot swappable power supplies, dual hot swappable fans, and dual redundant hot swappable power-efficient power supplies (second power supply optional, DC power supplies available). A four-port 10/100/1000 copper interface card is standard (upgradeable to fiber), as is a gigabit dedicated management interface.

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.

Copyright ©2009 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS and JUNOSe are trademarks 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.