

What's New in Juniper Networks Secure Access (SA) SSL VPN Version 6.5

Introduction

This document lists the new features available in Version 6.5 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 6.4.

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

- I. VDI Support
- II. Antispyware Support with Enhanced Endpoint Security (EES) Functionality
- III. Integrated WAN Acceleration (WX) Client Delivery
- IV. ActiveSync Expansion
- V. Network Connect Client FIPS Certification
- VI. User Record Synchronization
- VII. RDP Launcher
- VIII. Whitelist Security Enhancement
- IX. 2048-bit CSRs
- X. 64-bit platform support for Windows Secure Application Manager (WSAM)

Juniper Networks SA v6.5 New Feature Descriptions

VDI Support

Secure Access (SA) version 6.5 interoperates with VDI products, including VMWare's View Manager and Citrix's XenDesktop, enabling administrators to deploy virtual desktops alongside the SA series of SSL VPN devices. This allows the SA administrator to configure centralized remote access policies for users who access their virtual desktops.

Customer Benefits

- This provides a centralized point of configuration for administrators to configure remote access policies for virtual desktop access through leading virtualization products from VMWare and Citrix.
- SA 6.5 provides end users the VDI client to access the virtual desktop through, and provides flexible client fallback options thereby simplifying the deployment and management for administrators.

Availability

- Available on all Secure Access products.

Antispyware Support with Enhanced Endpoint Security (EES) Functionality

The number of just-discovered malware that can harm endpoint devices continues to grow, and quickly. According to the 1985-2008 AV-test.org report, there were over 7 million new programs discovered in 2008; it was just over 5 million in 2007. The threat and cost to enterprises from malware and particularly spyware are ever-increasing, as are the expenses around the quarantine and remediation of contaminated endpoints. SA v6.5 offers customers the ability to dynamically deploy an anti-spyware/anti-malware module from Webroot, the market leader in anti-spyware solutions. This module has been optimized for download size and efficiency, without compromising real time protection. This new capability is available on all currently shipping Windows Operating System versions. With this new capability, organizations can ensure that unmanaged and managed Windows endpoint devices conform to their corporate security policies before being allowed access to their corporate applications and resources. For example, potentially harmful key loggers can be found and removed from an endpoint device before the user enters sensitive information such as their user credentials.

These new anti-spyware/anti-malware capabilities, offered as part of SA's EES license, utilize a signature database to detect spyware and threats, facilitated and updated through an automatic download from Webroot's website, along with information on the definition version

and the date/time of the last successful download. This new antispyware capability is delivered to each device via an .msi package, downloaded to clients and silently installed.

If a customer has installed the commercially available version of Webroot's *Spy Sweeper* on their endpoints, SA's new anti-spyware/anti-malware protection can simply determine the device's real time protection status through that version. In this instance, no real time threat or remediation information is available to the SA since it will assume that *Spy Sweeper* is fully protecting the device from spyware and threats. Policy decisions for real time protection status will be determined by periodic queries (at intervals of 15 to 30 seconds) of the installed, commercially available *Spy Sweeper*.

Customer Benefits

- This enables customers to potentially enforce anti-spyware/anti-malware security protection on endpoints that are not corporate assigned assets.

Availability

- Available on all Secure Access products as part of the subscription-based, EES license.

Integrated WAN Acceleration (WX) Client Delivery

Secure Access version 6.5 allows customers to provide secure, accelerated remote connectivity to their corporate networks through the industry's first combination of SSL VPN and WAN acceleration clients. With this enhancement, customers who have Juniper's SA and WX devices in their data center can leverage the benefits of WAN acceleration along with the Layer-3 connectivity provided by Network Connect. Version 6.5 facilitates the dynamic, role-based delivery of the WX client to remote users when those users login to the SA appliance.

Customer Benefits

- Enables administrators to easily deploy WAN acceleration for remote users using their SA-series appliances.
- Enables users to experience 12x improvement on file transfers and 9x improvement on web apps in commonly seen configurations, optimized network access using Network Connect, for common TCP-based applications and downloading of large files.

Availability

- Available on all Secure Access products.

ActiveSync Expansion

Version 6.5 provides increased scalability for mobile devices connecting via ActiveSync, with support for up to 5000 simultaneous sessions on the SA6500. With this support, customers can leverage their existing remote access solution for their Window Mobile, Symbian, and iPhone mobile platforms. This capability allows mobile users to sync their Outlook and Calendaring applications with the backend Exchange server, allowing them to access corporate applications on their mobile phones.

Customer Benefits

- Enables administrators to allow ActiveSync usage to a large number of mobile users, to connect to their corporate applications through the SA device.
- Enables access using ActiveSync on market-leading Windows Mobile, iPhone, and Symbian phones that support the ActiveSync protocols.

Availability

- Available on all Secure Access products.

Network Connect Client FIPS Certification

SA 6.5 now includes a FIPS 140-2 Level 2 compliant Network Connect client on Windows 2000 and XP. For Vista operating systems, SA 6.5 includes a FIPS Level 1 compliant Network Connect client.

Customer Benefits

- Provides FIPS compliance for Layer-3 connectivity using Network Connect on Windows platforms.

Availability

- Available on SA4500 FIPS and SA6500 FIPS products only.

User Record Synchronization

Secure Access version 6.5 supports synchronization of user defined preferences and configuration across distributed Secure Access devices, even when not clustered together. Synchronized information includes user-defined Web bookmarks, File bookmarks, Terminal Services bookmarks, Persistent Cookies and User Preferences.

Customer Benefits

- Synchronization of user records provides a seamless experience for users who frequently connect to several non-clustered SA devices, such as when traveling or due to load balancing schemes.

Availability

- Available on all Secure Access products.

RDP Launcher

SA 6.5 simplifies the use of RDP sessions for end users without requiring them or administrators to create bookmarks.

Customer Benefits

- Simplifies ease of use for remote users to RDP into remote desktops by merely clicking a button or entering a hostname or IP Address of the remote computer.
- Simplifies the configuration for administrators and reduces the number of support calls from users who are unable to figure out how to RDP to remote computers.

Availability

- Available on all Secure Access products except the SA700.

Whitelist Security Enhancement

SA 6.5 introduces the Whitelist enhancement, to protect users from connecting to untrusted/rogue VPN gateways and having components launched without their knowledge. This provides a significant security advantage to address industry-wide growing concerns over malware and access to various untrusted systems.

Customer Benefits

- Users are prompted to trust new SSL VPN connections, which are then stored in the Whitelist file for future reference.
- Administrators can pre-populate the Whitelist file so that trusted hosts are listed ahead of time, preventing the users from ever being prompted for acceptance.

Availability

- Available on all Secure Access products.

2048-bit CSRs

SA 6.5 allows administrators to create Certificate Signing Requests with 2048-bit RSA keys. This allows customers to create a 2048-bit CSR for their cryptographic keys, enabling greater security than with 1024-bit keys.

Customer Benefits

- Allows customers with larger key length security policies to meet those needs
- Enables support with Certificate Authorities who only support 2048-bit CSRs.

Availability

- Available on all Secure Access products except the SA4000FIPS and SA6000FIPS.

64-bit platform support for Windows Secure Application Manager

Windows Secure Application Manager (WSAM) is now supported on 64-bit versions of supported Windows Operating Systems.

Customer Benefits

- Allows customers to use WSAM on 64-bit Windows Platforms.

Availability

- Available on all Secure Access products.

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.