What's New in Juniper's SSL VPN Version 6.2

This application note describes the new features available in Version 6.2 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 6.1.

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

I. Endpoint Security
II. Enterprise Mobility
III. Network Connect
IV. Terminal Services
V. Streamlined Manageability

I. **Endpoint Security –** As this segment of the market evolves, customers are now concerned about more than just basic antivirus and firewall policies on managed laptops. Today's enterprise environment must support a broad range of devices while simultaneously allowing customers to make access control decisions on a wide variety of variables. Customers also want to cut down on the number of calls in to their helpdesks related to end user compliance issues. Version 6.2 greatly extends Juniper's endpoint security offering in each of these areas as outlined below.

- **Endpoint Security - Automatic Remediation**

  Juniper Networks Secure Access v6.2 adds auto-remediation capabilities for non-compliant endpoints, enabling customers to remediate automatically those devices that do not meet policy prior to allowing them on to their network, minimizing support calls from users of non-compliant endpoints.

  Auto-remediation capabilities include:

  - 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 enough
    - Invoking real time protection – if it's not already enabled
  - Firewall auto-remediation for Microsoft Windows XP and 2000, and Microsoft Vista, turning the firewall on – if it is not running
  - Automatically modifying registry settings to pre-defined values as specified by policy for compliance

  Customer Benefits
  - Enables the solution to auto-remediate endpoints before allowing them on to the network, minimizing the support calls from non-compliant users.

  Availability
  - Available on all Secure Access products.

- **Endpoint Security - Pre-Defined Patch Management Checks**

Juniper Networks Secure Access v6.2 extends endpoint assessment capabilities to now include in the appliances the ability to support pre-defined patch management checks. Pre-defined endpoint patch management checks include the ability to inspect the endpoint for targeted operating system or application hot fixes, enabling SSL VPN customers to easily define policies that can be directly linked to the presence or absence of specific hot fixes for defined operating systems and/or applications. The pre-defined patch management checks can also be performed according to the severity level of the vulnerability (critical, high, medium, low, etc.) and can be used to enforce access to certain roles or deny access to certain roles.

Customer Benefits

- Enables customers to more easily define policies that ensure access control is tied to the presence or absence of certain critical hot fixes for operating systems and applications.

Availability

- Available on all Secure Access products.

- **Endpoint Security - Pre-Defined Host Checker Policy Enhancements**

Juniper Networks Secure Access v6.2 adds several enhancements to existing pre-defined host checker policies (in addition to automatic remediation and pre-defined patch checks). New features include:

- The ability to create policies that look for any endpoint security package from a specific vendor. Customers will be able to create policies that allow machines running any McAfee AV package, for example.
- The ability to create antivirus policies that look for virus definition files no older than X updates old, where X is anywhere from 1-10. This allows customers to create policies that are more flexible while still providing a reasonable level of security assurance.

Customer Benefits

- Allows customers to maintain assurance of endpoint integrity while simultaneously providing more flexibility to end users.
- Allows Secure Access devices to fit more seamless into existing security infrastructure.

Availability

- Available on all Secure Access products.

II. **Enterprise Mobility –** The reality of today's IT environment is that end users are increasingly demanding choice when it comes to the device(s) on which they do their work. This leaves IT managers with the responsibility to adapt and provide secure access from these varied platforms. Version 6.2 extends Juniper's reach and allows the Secure Access platform to continue as the standard for remote access across many of the world's top organizations.

- **Endpoint Security / Enterprise Mobility – Windows Mobile Host Checker**

Host Checker on Windows Mobile – as mobile deployments grow, customers have begun to look to Juniper to provide endpoint security functionality for their Windows Mobile devices, enabling them to ensure a strong endpoint security

posture, similar to what is provided on traditional endpoints. Version 6.2 adds Host Checker for the supported Windows Mobile platforms.

Customer Benefits

- Allows customers to ensure the same integrity verification capabilities for their mobile devices that they have deployed on their traditional devices.

Availability

- Available on all Secure Access products.

- **Enterprise Mobility - Clientless ActiveSync on Windows Mobile**

  The Clientless ActiveSync feature provides customers with a secure connection from a Windows Mobile device to the Exchange server with no client installation on the device. This allows customers that only wish to synchronize email a means to do so without requiring the Windows Secure Application Manager client on the mobile device.

  Customer Benefits

  - Allows customers to synchronize their email without authenticating to the SSL VPN device via a client such as WSAM or via the web browser, greatly simplifying the end user experience.

  Availability

  - Available on all Secure Access products other than the SA700.

- **Enterprise Mobility - Extended Support for Windows Mobile**

  Version 6.2 extends Juniper's support for Windows Mobile devices with several new features.

  - Windows Mobile 6.0 support – as new versions of Windows Mobile have been made available, Juniper has provided support across both the clientless access method, as well as WSAM. Version 6.2 adds support for Windows Mobile 6.0.
  - Windows Mobile Smartphone Edition – Version 6.2 extends supported Windows Mobile platforms from the PDA edition to also include the Smartphone form factor.

  Customer Benefits

  - Provides freedom for end users to purchase Windows Mobile devices running the latest OS versions and form factors, while still providing a secure connection to the corporate network.

  Availability

  - Available on all Secure Access products.

- **Enterprise Mobility - JSAM and Core Access Support for Solaris 10**

  Solaris 10 has been added as an additional supported platform for both the JSAM and the Core Clientless access methods.

  Customer Benefits

  - Further solidifies the Secure Access platform as the standard for remote access across an entire enterprise, regardless of the types of devices that must be supported.

Availability

- Available on all Secure Access products.

III. **Network Connect –** As organizations continue to replace their outdated IPSec VPN remote access gateways with the Juniper SSL VPN solution, Network Connect becomes a more popular option across these deployments. Version 6.2 responds to this popularity with several features that increase deployment flexibility and puts greater control over remote access security and performance in the hands of the administrator.

- **Network Connect – Windows Vista Credential Provider**

  With the introduction of Windows Vista, Microsoft has replaced its GINA functionality with a new feature known as Credential Provider. In the 6.2 release, Juniper Networks has Credential Provider functionality for Network Connect, providing a mechanism for creating a Network Connect tunnel when the user logs in to their endpoint. The Network Connect Credential Provider has been implemented as a Pre-Logon Access Provider (PLAP). Wherever possible, NC will attempt to provide Single Sign-On by using the same credentials provided for NC to attempt domain authentication.

  Customer Benefits

  - Allows end users to connect to the corporate network via Network Connect while they are logging on to their machine.
  - Allows a single set of credentials to be submitted for both SSL VPN authentication as well as machine/domain authentication.

  Availability

  - Available on all Secure Access products with Network Connect.

- **Network Connect – Bandwidth Management**

  Bandwidth management is the ability to control the rate of traffic sent or received on a network interface. It is performed by policing (discarding excess packets) and can be used to ensure that a peer is allocated a specified amount of bandwidth. Traffic that is less than or equal to the specified rate is guaranteed to be sent, whereas traffic that exceeds the rate may be dropped or delayed. Bandwidth management is configured per-role, per-IVS, and/or per-interface, with the ability to control both guaranteed minimum, as well as configured maximum bandwidth.

  Customer Benefits

  - Allows customers to manage the throughput of remote access connections, either for specific groups of users or across their entire Secure Access deployment, providing an additional level of service assurance across their user base.

  Availability

  - Available on all Secure Access products with Network Connect.

- **Network Connect – Windows Client Reconnect Behavior**

  This new feature will allow the Network Connect client to seamlessly recover from disconnect events. If Windows NC is disconnected for any reason other

than session timeout or Secure Access session termination, the client will continuously attempt to reconnect until a network connection is established, rather than timing out. The system tray icon will indicate that NC is attempting to reconnect, but there will be no other prompts to the end user. During this time, the user can Exit or Sign out of NC to stop the client from reconnecting.

Customer Benefits

- Ensures a seamless end user experience with improved response to network conditions and other network connectivity disruptions.

Availability

- Available on all Secure Access products with Network Connect.

- **Network Connect – 256-bit AES Support**

  Network Connect now supports 256-bit AES encryption, completing support for this level of encryption across the SSL VPN access methods.

  Customer Benefits

  - Allows security sensitive customers to increase the encryption levels used for their remote access connections.

  Availability

  - Available on all Secure Access products.

IV. **Terminal Services –** Terminal Services are in wide use across organizations of all sizes. Version 6.2 (as with most prior releases) focuses on adding new functionality supporting both Citrix and Microsoft Windows Terminal Services, ensuring that Secure Access SSL VPN appliances continue to be the functional leader in providing secure remote access to Terminal Services deployments.

- **Terminal Services - Citrix Published Application Support**

  Version 6.2 expands support for Citrix Terminal Services by allowing customers to display Citrix Presentation Server published applications directly to end users on the SSL VPN bookmark page. This enhancement makes it easier for end users to see exactly which applications they can access through their remote access session directly from their home page, regardless of whether those applications are accessed through Citrix or accessed directly.

  Customer Benefits

  - Improves the end user experience by displaying all application bookmarks on a single screen.
  - Saves on administration time by minimizing the task of configuring Citrix application bookmarks directly on the SSL VPN, as those bookmarks are pulled directly from Presentation Server.

  Availability

  - Available on all Secure Access products other than the SA700.

- **Terminal Services - Windows Server 2008 Support**

  In version 6.2, Juniper has added support for the latest version of Terminal Services, running on Windows Server 2008 (Codename: Longhorn).

  Customer Benefits

- Allows customers to test or rollout the latest version of Microsoft's Terminal Services functionality as soon as possible, providing deployment flexibility.
- Enables RemoteApp support to run seamless windows of applications when the client is running RDP 6.0 (or higher).

Availability
- Available on all Secure Access products other than the SA700.

V. **Streamlined Management** – As the size of Secure Access customer deployments have grown (both in the enterprise and the service provider space), so too have the management and administration needs of these organizations. Version 6.2 introduces several key new management features aimed at streamlining the manageability of the Secure Access devices.

- **Streamlined Management - XML Import/Export and Push Configuration**

  Version 6.2 adds additional functionality to the existing XML Import/Export and Push Configuration features, completing support for all SSL VPN policies. Additionally, these functions have been improved to minimize restarts that can result in service impact.

  Customer Benefits
  - Allows administrators further granularity in deciding which policies to synchronize between disparate devices or clusters.
  - Allows administrators to make configuration changes via XML Import and Push Config without worrying about service restarts, allowing greater management flexibility without any user impact.

  Availability
  - Available on all Secure Access products.

- **Streamlined Management - IVS Shared Authentication Services**

  This feature allows Instant Virtual Systems (IVS) customers to provide access to authentication services that can be shared across virtual systems. This enhancement allows the customer to place the authentication service on a particular VLAN and share that VLAN across all IVS on a given system or cluster.

  Customer Benefits
  - Allows Service Providers to host shared authentication services, such as RADIUS, in their networks as an additional value added service for each of their IVS/Shared Network-based SSL VPN services customers.
  - Allows enterprises utilizing IVS the ability to share a single authentication infrastructure across their entire user population.

  Availability
  - All Secure Access Products with the IVS license.

- **Streamlined Management – RADIUS Accounting NC Assigned IP Address**

  This enhancement allows customers the ability to send the IP address assigned by Network Connect, in addition to the user's source IP, to a RADIUS accounting server for auditing and billing purposes.

Customer Benefits

- Allows customers a better view into the activities performed by users on their network when connected via Network Connect, aiding in auditing and billing.

Availability

- All Secure Access Products with Network Connect.