

What's New in Juniper's SSL VPN Version 6.0

This application note describes the new features available in Version 6.0 of the Secure Access SSL VPN products. This document assumes familiarity with the Juniper's IVE platform and the features of earlier releases up to version 5.5.

I. Security Policy Enhancements to Meet The Needs of Today's Most Demanding Businesses

- **Support Trusted Network Connect (TNC) Standards on Host Checker**
Juniper is introducing support for the TNC-TCG industry standards which enables interoperability of the solution with diverse endpoint solutions, from antivirus to patch management to compliance management solutions that conform to the TNC-TCG specifications. The Trusted Computing Group (TCG) is a not-for-profit organization formed to develop, define, and promote open standards for hardware-enabled trusted computing and security technologies. Trusted Network Connect, a subgroup of the TCG that comprises more than 60 members, is responsible for defining an open architecture for network operators to enforce policies regarding endpoint integrity during network connections established by users/endpoints. By introducing this support, Juniper Networks is extending its endpoint assessment capabilities, in addition to what is supported in SSL VPN today, by providing interoperability and deep integration with solutions that support these standards. These standards are also supported on Juniper's Unified Access Control solution, allowing customers to create similar security policies for remote and local access control deployments.

Customer Benefits

- Enables customers to leverage their investments in existing endpoint security solutions.
- Standards-based, open APIs provide flexibility to customers, providing tight integration with a wide array of third party security products as part of the endpoint security assessment on every remote access session.
- Allows customers to create a unified endpoint security policy that can be deployed across both their remote access (SSL VPN) and their local access (UAC) deployments.

Availability

- All Secure Access Products

- **Support for remote Integrity Measurement Collectors (IMC) – Integrity Measurement Verifiers (IMV) for TNC conformant solutions developed by third party vendors**

Juniper Networks is adding generic support for any endpoint vendor who develops TNC compliant solutions for integration into SSL VPN. By providing this support, customers can enable IMVs from 3rd party solutions and use SSL VPN to gather the relevant information from the endpoint (IMC), pass this information to the IMV for endpoint status, and leverage the results back from the IMV for network and application based access control.

Customer Benefits

- Enables customers to customize their SSL VPN deployments to meet the exact needs of their business.
- Gives customers the flexibility of zero-day support for new endpoint security solutions as third party vendors add support for TNC standards.
- Accelerates the integration of diverse endpoint solutions into SSL VPN by providing a common, standards-based framework for integration.

Availability

- All Secure Access Products

- **Host Checker Support for Machine Certificate Authorization**

Juniper has extended Host Checker to now include support for X.509 machine certificates, including validation via OCSP/CRL. This allows customers to perform authorization based on whether or not the machine itself is trusted, in addition to end-user authentication and authorization.

Customer Benefits

- Allows customers to create authorization and role mapping policies based on whether or not an end-user's device is a corporate managed asset, leveraging Juniper's industry-leading dynamic access privilege management capabilities.

Availability

- All Secure Access Products

- **Certificate Authentication with Network Connect Launcher**

Juniper's advanced PKI capabilities have now been extended further with support for certificate authentication via the Network Connect command line launcher.

Customer Benefits

- Extends support for certificate authentication across all access methods.

Availability

- All Secure Access Products with Advanced License

- **Selectable Cipher Suites**

With 6.0, Juniper allows the selection of specific bulk encryption ciphers for SSL connections. For example, customers can choose to allow only ciphers using AES and 3DES, for more secure deployments.

Customer Benefits

- Provides greater flexibility to customers in creating policies to match their corporate security policies.

Availability

- All Secure Access Products

- **Extended custom endpoint assessment capabilities to include checks for Mac address and NETBIOS**

Juniper Networks is extending the custom endpoint assessment capabilities to incorporate checks for Mac Address of endpoint and whether the endpoint is a NetBIOS machine or not. SSL can then vary the user's level of access as a consequence of these checks.

Customer Benefits

- Provides greater flexibility to customers in defining custom endpoint assessment checks and leveraging them for granular access control.

Availability

- All Secure Access Products

II. Anytime, Anywhere Access Through Enhanced End-User Browser, Platform, and Application Support

- **Support for OWA, Sharepoint, and Office 2007 through the Core Access Method**

Version 6.0 of the SSL VPN products adds support for Outlook Web Access 2007, Sharepoint 2007, and the Office 2007 suite of application through the core clientless access method. Juniper continues to provide support for the widest possible set of web applications by providing support soon after these new applications have been released. Resource profile templates are provided for Sharepoint 2007, as well as OWA 2007.

Customer Benefits

- Completely clientless support for the 2007 versions of Microsoft business productivity applications, for ubiquitous availability through only a web browser

Availability

- All Secure Access Products 2000 and Above and SA700 with Core Access license

- **MySecureMeeting**

MySecureMeeting adds support for Reservationless, Fixed-URL Secure Meeting deployments. With this feature, customers can create fixed URLs or "meeting rooms" for their end-users based on predefined strings, username, or directory/session variables. When joining these types of meetings, attendees specify the fixed meeting URL, their name, and the meeting password. Administrators can specify URL format and can choose whether or not they want to allow end users to create additional meeting URLs for other purposes. Password options such as complexity and expiry can also be set by administrative policy.

Customer Benefits

- Allows the use of static, configurable meeting URLs for ease of use. Makes it easier to join meetings and to remember meeting URLs.

Availability

- All Secure Access Products 2000 and Above with Secure Meeting License
- **Citrix Terminal Services (CTS) – Intelligent Client Delivery and SSO**
Allows customers to run published applications available on the Citrix Web Interface using the SSL VPN Gateway's embedded Citrix Terminal Services Client. With this enhancement, CTS will automatically launch and run if the IVE receives an ICA file. If Web Interface delivers a Java applet, traffic is tunneled through the Java rewriter. In addition, the native IVE CTS client now supports Single Sign-On using domain credentials, for seamless authentication. Through this feature, users can access published apps without the use of JSAM or WSAM, improving usability, security, and avoiding client installation issues.

Customer Benefits

- Improved usability, as all that the end user has to do to start the application is click on the bookmark or the icon for the published application in the Web Interface.
- Strong security, as users cannot write their own ICA file and gain access to applications that have not been published on the Web Interface.
- Ubiquitous access, as the IVE Citrix Terminal Services proxy does not require administrator privileges for installation. For users with the Citrix client already installed on their machine, there is no need for advanced privileges to access published apps.

Availability

- All Secure Access Products 2000 and Above with SAMNC License
- **CTS Proxy Auto-Client Reconnect and Session Reliability**
These two enhancements optimize uptime and reliability if connections to the Terminal Server are lost. Session Reliability keeps the remote desktop running and available until the connection is restored (via auto-client reconnect) or the session is cancelled.

Customer Benefits

- Enhanced usability and reliability through robust session maintenance capabilities

Availability

- All Secure Access Products 2000 and Above with SAMNC License
- **ICA Client Policy-Based Access Control**
The Citrix ICA client can provide access to local printers, local drives, COM ports and clipboard sharing to applications running remotely over ICA sessions. Many customers do not want to provide all of these capabilities all of the time, particularly if end users are coming from what they deem to be insecure machines. This feature allows granular control of those options at the role level.

Customer Benefits

- Granular access control over access to local resources, ensuring that corporate security policies can be met by varying access based on trust level of remote endpoints.

Availability

- All Secure Access Products 2000 and Above with SAMNC License

- **Terminal Services RDP/JICA Fallback**

Many SSL VPN customers must provide access from a broad range of managed and unmanaged machines, resulting in a wide range of installed software and end user privileges. With this enhancement to both Windows Terminal Services and Citrix Terminal Services, the IVE will attempt to launch several different versions of each client in order to maximize likelihood that a user can connect. In the case of WTS/RDP, the IVE will first attempt to launch the native RDP client. If that fails, the IVE will attempt to install the ActiveX control and use that to launch WTS. If that fails, the IVE will automatically launch the configured WTS bookmark using the uploaded Java RDP applet. In the case of Citrix, an installation of Citrix consists of an ActiveX control and an executable. If an installation is not already present, the IVE will attempt to download the Citrix installation based upon configured role options. If this fails the IVE will fall back to the JICA applet to launch the CTS bookmark.

Customer Benefits

- Ensures that end users can access their Terminal Services sessions in nearly all cases, regardless of what is installed on the endpoint PC.

Availability

- All Secure Access Products 2000 and Above with SAMNC License

- **Windows Terminal Services Session Directory Support**

Session Directory is a Windows Terminal Services (WTS) feature that allows session persistence for terminal services farms. If a connection is lost for any reason, when the user attempts to reconnect, session directory will reconnect them to the same terminal server, bypassing normal load balancing that would likely direct the user to another server. This feature adds support for Session Directory to the Juniper Windows Terminal Services Client.

Customer Benefits

- Enhances productivity, as users do not lose any unsaved work by being directed to a different terminal server after a reconnect.
- Improves end user experience as the user can disconnect a TS session without logging off, and then reconnect later, continuing where they left off.

Availability

- All Secure Access Products 2000 and Above with SAMNC License

- **Windows Terminal Services Usability/Experience Enhancements**

Version 6.0 of the SSL VPN software includes several new enhancements aimed at improving WTS usability and the overall end user experience. The first enhancement allows the use of a universal printer driver through the WTS proxy,

avoiding the need to install numerous third party printer drivers on terminal servers for every user's local printer. Additionally, a new enhancement was added to control the end-user's access to local resources such as local printers, drivers, COM ports, and clipboard (copy/paste) sharing between the host computer and the terminal server. Finally, several new display options make it easier to personalize WTS sessions and to optimize performance for users on low bandwidth networks. These display options include desktop background selection, menu and window animation, use of Windows Themes, font smoothing, and several more (outlined in Administrator's guide).

Customer Benefits

- Reduced management as administrator's no longer need to worry about installing a large number of printer drivers on their terminal servers.
- Enhanced security for insecure environments through control of local resource access.
- Improved end-user experience and performance via control of display options and personalization at the role level, allowing administrator's to optimize depending on the user's connection.

Availability

- All Secure Access Products 2000 and Above with SAMNC License

III. Mobile Device Support Enhancements

- **Standalone WSAM Launcher for Windows Mobile Devices**

Standalone WSAM Launcher provides a browser-less mechanism for users to authenticate to the Secure Access gateway. The WSAM launcher includes an auto-connect and storage of authentication information in encrypted form. This feature makes it extremely easy for end users to successfully connect to the SSL VPN and establish their session.

Customer Benefits

- Provides a way for users to launch and end their WSAM session with the use of Internet Explorer and without entering their login credentials on login

Availability

- All Secure Access Products 2000 and Above with SAMNC License

- **Clientless File Browsing on Windows Mobile**

Provides file browsing capabilities through the web browser with no client (i.e. WSAM) to download to the mobile device

Customer Benefits

- Provides access to the widest possible range of content with no client to dynamically download to the mobile device.

Availability

- All Secure Access Products 2000 and Above

- **Certificate Authentication Support for Windows Mobile Devices**
Provides support for certificate authentication on Windows Mobile Devices. If certificate auth is required and one is present on the device, user can automatically establish WSAM connection with no need to enter username and password. If multiple certificates are present, the user will be prompted to select the appropriate certificate.

Customer Benefits

- Allows customers to leverage their PKI/strong authentication infrastructure across all devices connecting to their networks, including mobile devices.

Availability

- All Secure Access Products 2000 and Above with Advanced License

- **Seamless Roaming Support for WSAM on Windows Mobile**
Allows WSAM to stay connected when roaming between different connections including between cellular and Wi-Fi connections.

Customer Benefits

- Provides seamless connectivity to end users as they move from one network to another

Availability

- All Secure Access Products 2000 and Above with SAMNC License

- **Localization of SSL VPN End-User UI on Windows Mobile Devices**
Localizes SSL VPN User Interface on Windows Mobile devices for the Core and WSAM access methods to all 7 languages support by Secure Access

Availability

- All Secure Access Products 2000 and Above

IV. Administration Flexibility and Ease of Deployment

- **MSI Packaging for Installer Service**
The Juniper Installer Service has now been repackaged into an MSI file for easier deployment via group policy in Windows enterprise environments. Package is available in .MSI or .EXE formats.

Customer Benefits

- Allows customers to push Juniper Installer Service deployment via SMS, leveraging their existing deployments of management infrastructure.

Availability

- All Secure Access Products with SAMNC License

- **IVS Configuration Templates**
Juniper's Virtual Systems capabilities have been extended to allow creation of

new virtual systems through configuration templates. Customers can use either un-configured or existing virtual systems from which to create templates. These templates can then be used as a basis for new virtual systems and further customized as necessary.

Customer Benefits

- Simplifies management by allowing administrators to create copies of existing virtual system configurations for deployment of additional virtual systems.

Availability

- All Secure Access Products with IVS License

- **IVS Oversubscription**

This new feature allows customers to configure an IVS to burst beyond its user limit configuration, up to the overall concurrent user license capacity of the Secure Access device. Customers simply configure a minimum guaranteed and maximum allowed user limit for each IVS.

Customer Benefits

- Allows large enterprises and service providers to create service level agreements on number of concurrent users supported for a user group.
- Allows bursting capabilities during periods when a particular system is not fully utilized.

Availability

- All Secure Access Products with IVS License