

What's New in Juniper's IVE Platform Version 5.2

This application note describes the new features available in Version 5.2 of the IVE platform for all Secure Access SSL VPN products. This document assumes familiarity with the Juniper's IVE platform and the features of earlier releases up to version 5.1.

Highlights of this Release

Juniper Networks enables enterprises and service providers to converge all of their secure access needs to provide a secure and assured communication experience with version 5.2 of the IVE platform:

I. Administration Flexibility and Ease of Deployment

- Integrated Malware Protection Capabilities
- Pre-Defined Host Checker Policies
- User Account Management Capabilities
- Authentication Flexibility
- Configuration/Deployment Options

II. Enhanced End-User Access

- Extended Cross Platform Support
- Emerging Application Support
- Access Enhancements
- Secure Meeting Enhancements

III. Virtual System Enhancements

- Virtualization of Code Signing Certificates
- Virtualized SSL Encryption Settings

I. Administration Flexibility and Ease of Deployment

• Integrated Malware Protection Capabilities

Juniper Networks provides integrated endpoint containment capabilities to protect users and devices from keyloggers, Trojans, remote control applications and monitoring applications. The technology, licensed as part of a deal with Whole Security (now Symantec) enables the Juniper SSL VPN platforms to support 3 sub policies – Category I threats (key loggers and Trojans) and Category II threats (Remote Control applications and monitoring applications) for signature based detection and elimination of known threats to the network and behavior blocking technology for behavior-based detection and elimination of threats to the endpoint. All 3 sub policies can be tied to the access management framework of the SSL VPN platforms and applied by the administrator to meet the security needs of the network. The signature based and behavior blocker policies can be configured in 2 modes: User involvement mode where users can selectively disable specific actions on threats identified by the malware protection module on their endpoint or silent mode where the network administrators can disable end user involvement in securing the endpoint. In silent mode, the malware protection detects and removes threats to the endpoint without giving the end user the choice to disable the actions being taken. In both modes, administrators can enforce these policies in

evaluate or enforce mode and appropriately control access regardless of end user actions on their endpoint.

Customer Benefits

- Enables customers to provision endpoint containment capabilities and secure the endpoint either prior to granting access or during the user session for comprehensive network protection

Availability

- Advanced Endpoint Defense: Malware Protection license available for all Secure Access products (25 user license ships free on all secure access products)

- **Pre-Defined Host Checker Policies**

Juniper Networks is introducing the ability to leverage pre-defined Host Checker policies to setup endpoint security checks for policy enforcement on the SSL VPN platform. By leveraging these checks, administrators can select from a wide range of pre-defined checks for antivirus, firewall or spyware applications to easily ensure that the selected applications are installed and running before granting access to users needing corporate access.

Customer Benefits

- Enables customers to easily leverage investments in third party vendor solutions by leveraging the pre-defined checks without the need for manually setting checks
- Simplified and intuitive configuration of endpoint security checks as administrators do not need to have knowledge on how to set up checks for their endpoint security applications.

Availability

- All Secure Access Products

- **User Account Management Capabilities**

- **RADIUS Accounting Data Statistics**

With IVE v5.2, Juniper Networks has extended its support for RADIUS Accounting with the addition of sent/received byte count for all access methods (Core, Network Connect, JSAM, WSAM). The IVE already supports recording of user session duration with session Start/Stop messages and interim updates.

Customer Benefits

- Allows better integration into existing RADIUS accounting/billing infrastructures
- Provides customers the ability to support usage-based billing in addition to time-based billing

Availability

- All Secure Access Products

- **Disabling Local Accounts**

Allows locally authenticated user accounts to be enabled/disabled temporarily. This functionality allows administrators to temporarily

disable a user (e.g. on a leave of absence) and then easily enable that user later without having to recreate the account. When the account is disabled, the user will not be able to login to the SSL/VPN device and an error message will be displayed stating that the account was disabled by the administrator. If a user is logged in when the account is disabled, they will be forced out with the same error message.

Customer Benefits:

- Enhanced security – questionable accounts can be disabled
- Ease of use – reduces user account administration tasks.

Availability

- All Secure Access Products

- **One-Time Use Accounts**

One-time use accounts are single-use, locally authenticated user accounts that are automatically disabled after one successful login. Once the account has been disabled, subsequent login attempts will result in an error message. The administrator has the option of re-enabling the account at any future time.

Customer Benefits:

- Enhanced security and ease of use

Availability

- All Secure Access Products

- **Account Last Access Statistics**

This feature displays statistics related to the last time a user logged in to the IVE on the Admin UI. Statistics shown include IP Address, agent name, and last login time. This provides administrators the ability to view recent user statistics at a glance, without looking through the User Access log.

Customer Benefits

- Streamlined manageability and troubleshooting

Availability

- All Secure Access Products

- **Authentication Flexibility**

- **SAML Authentication Consumption**

Juniper Networks has extended its support for the SAML (Security Assertion Markup Language) protocol by adding the ability to accept authentication assertions from another SAML system. This feature allows users to login to a resource protected by another access management product and then have single sign-on to a resource protected by the Secure Access product. The Secure Access (SA) products can accept SAML assertions through the Artifact Profile method. Previous support allows the SA to accept outside authorization assertions and to generate authentication assertions to send to another SAML system.

Customer Benefits

- Flexibility and enhanced ease of deployment (user login experience can remain the same)
- Improves end-user experience through single sign-on

Availability

- Secure Access Products 1000 and above with Advanced license

- **Variable-based Certificate Realm Restrictions**

This feature allows the customer to compare variables on a client certificate to expected variables that have been pulled from the authentication server at login. If there is no match or if there is no value for the attribute, the match is considered failed and the end-user will not be mapped to that role.

Customer Benefits

- Improves flexibility and functionality of role mapping
- Enhanced ease of deployment in existing environments.

Availability

- All Secure Access Products

- **Resource-based Control of NTLM and Basic Auth Intermediation**

With this feature, administrators can configure policies to control NTLM and Basic Authentication intermediation on a resource by resource basis.

Specifically, administrators can author a resource policy that determines NTLM Single Sign-On (SSO) behavior. Options include: intermediate without SSO, intermediate with SSO - IVE default/current behavior, intermediate with SSO with configurable username/password credentials and deny direct login to a particular NTLM protected resource if a configured SSO behavior fails.

Customer Benefits

- Greater flexibility in deployment of applications

Availability

- All Secure Access Products with Core Clientless Access

- **Configuration/Deployment Options**

- **Out-of-Band Management Ethernet Port**

With IVE v5.2, Juniper Networks has added an out-of-band management Ethernet port, enabling administrators to have always-on management (configuration, monitoring, etc) access to the SA appliance through a dedicated port.

Customer Benefits

- Always-on management access
- Seamless integration into dedicated management networks

Availability

- Secure Access 6000 and Secure Access 6000 SP

- **Selective Rewriting for Java Applets**

Juniper has extended the selective rewriting feature to Java applets. Administrators can now create a rewriting rule for specific jar files, allowing a Java applet to bypass the IVE rewriting engine.

Customer Benefits

- Enhances applet delivery flexibility and troubleshooting

Availability

- All Secure Access Products with Core Clientless Access

- **Citrix Server Farm Load Balancing Support**

In this release, we provide load balancing support for Citrix server farms for Citrix Terminal Services sessions that use a custom ICA file. The Citrix Terminal Services feature enables terminal emulation session on a Citrix Metaframe server using an ICA file downloaded from the IVE.

Customer Benefits

- Enhanced supportability of Citrix server farm deployments

Availability

- Secure Access products 1000 and above with SAMNC license

II. Enhanced End-User Access

- **Extended Cross Platform Support**

- **SuSE Linux support on IVE Platform**

With this release, Juniper Networks has introduced support for SuSE Linux platforms with Network Connect, Host Checker, JSAM and Cache Cleaner

Customer Benefits

- Enables customers to leverage existing Win 98 and SuSE Linux deployments.

Availability

- All Secure Access products with SAMNC license
 - Host Checker is available on all Secure Access Products

- **Emerging Application Support**

- **Multicast support on Network Connect**

With this release, Juniper Networks introduces support for applications that require multicast with the Network Connect access method. This includes support for applications in the areas of video conferencing, distance learning, corporate communications, distribution of software, etc., where data needs to be streamed to a select group of receivers and not broadcast over the entire network.

Customer Benefits

- Enables customers to support leading edge applications that require selective streaming of data to a group or groups of users across the IP network using Network Connect.

Availability

- All Secure Access products with SAMNC license
- **DiffServ Marking Preservation on Network Connect**
This feature enables Network Connect to preserve diffserv or ToS markings made by applications such as VoIP soft phones to ensure that any downstream infrastructure can continue to offer differentiated services.

Customer Benefits

- Enables customers to continue to use Network Connect for encrypted data transport and still be able to offer differentiated services to applications/users

Availability

- All Secure Access products with SAMNC license

- **Access Enhancements**

- **File Sorting**

This feature allows end users to sort files by clicking on the Owner, Size, Type and Modified column headers. On the first click of a column header all entries on the page will be sorted in the ascending (for Size column), lexicographic (for Name, Owner and Type columns) or chronological (Modified column) order. A subsequent click on the same column header will sort the file entries in the descending, reverse lexicographic or reverse chronological order.

Customer Benefits

- Improves and simplifies end-user experience

Availability

- All Secure Access Products with Core Clientless Access

- **Auto-launch of Windows Terminal Services at Login**

The admin will now have the ability to auto-launch one or more Terminal Services session (both Windows Terminal Services and Citrix Terminal Services). From an End-user perspective, after the end-user enters his credentials on the IVE login page, the first Terminal Services page will be displayed in a new window. If multiple Terminal Server bookmarks are configured to auto-launch then the end-user will see multiple Terminal Server windows show up in new windows. The original browser window will display either the custom start page, if configured, or the IVE home page

- **RDP Client Upgraded to Windows 2003 Version**

With IVE v5.2, Juniper has upgraded the RDP client that the IVE installs on end-user's devices to the Windows 2003 Server version. This upgrade allows customers to take advantage of usability (ex. the remote desktop

now fits on the terminal without the need for a scroll bar) and basic security improvements in the Windows 2003 client.

Customer Benefits

- Improves and simplifies end-user experience

Availability

- Secure Access Products 1000 and above with SAMNC license
- **Internal VIP Stays Active During External VIP Failure**
In an Active/Passive cluster environment, this feature allows the Internal VIP to remain active when the External VIP loses connectivity. With this functionality, if the external VIP goes down, internal users can continue to access IVE protected resources through the internal interface. This behavior is administrator configurable. The external VIP will never be up on its own at any node.

Customer Benefits

- Increased accessibility for internal users as they can continue to access resources, even if the external network is down.

Availability

- Secure Access products 1000 and above with Clustering License
- **Guaranteed Number of Concurrent Users per Realm**
In addition to the maximum number of concurrent user sessions per realm, IVE v5.2 has added support for a guaranteed minimum number of concurrent user sessions. This feature assures administrators that the specified number of users for a realm will always be allowed to sign-in to an IVE session. Guaranteed minimums for a realm can range from 0 to the size of the user license on the appliance.

Customer Benefits

- Ensures access for specified groups of end-users (e.g. Admins, Executives)
- Allows Instant Virtual System (IVS) customers to guarantee minimum service levels to groups/customers

Availability

- All Secure Access Products
- **Simultaneous User Warning**
With this feature, if a user attempts to access the IVE, but is already logged in on another session, they are given the option of continuing with the new session or canceling their attempt to login again. If the user chooses to continue with the new session, the older session will automatically be logged out. The logged out user will get a warning message stating why they were logged out and which IP address overtook their session, allowing them to report unauthorized use of their credentials (if their username/password were somehow taken by a third party).

Customer Benefits

- Added security – users are warned if another person tries to login with their credentials.
- Enhanced user experience - they can continue to login, even if they have forgotten to close their session on another device.

Availability

- All Secure Access Products

- **Utilization of Existing XP Terminal Services Clients**

With this feature, if the user has a Windows XP machine with a bundled RDP client, then the IVE will use this client instead of downloading the IVE's RDP client. As a result, Windows XP users will not require administrative rights in order to use the Terminal Services functionality.

Customer Benefits

- Reduced administrative privileges required for Windows XP Terminal Services users

Availability

- Secure Access Products 1000 and above with SAMNC license

- **Java Rewriting Engine Performance Improvements**

The IVE now caches rewritten Java applets. This eliminates the need to re-instrument the applet each time it is accessed and thus improves end-user response time when the user requests the applet.

Customer Benefits

- Improves Java application performance

Availability

- All Secure Access Products with Core Clientless Access

- **Custom Sign-in Pages Accept-language Header Support**

This feature provides the ability for administrators to create custom sign-in pages in several languages. The accept-language header is automatically checked by the IVE when the user points their browser to the sign-in page. If a custom page specific to that language has been uploaded to the IVE, that page is served to the customer. If the administrator has not created a page corresponding to the header value, the default sign-in page is served to the end-user.

Customer Benefits

- Enhanced localization – end-users are provided content in their preferred language.

Availability

- Secure Access Products 1000 and above with Advanced license

- **Secure Meeting Enhancements**

- **Private Chat**

In addition to group chat, an attendee can now chat privately with other Secure Meeting attendees.

- **Filtered Chat**

Filtered chat allows users to hide messages from selected attendees in a chat. This enables attendees to be more selective in their communications during meetings.

Customer Benefits

- Greater meeting productivity

Availability

- Secure Access Products 1000 and above with Secure Meeting license

III. Virtual System Enhancements

- **Virtualization of Code Signing Certificates**

This feature enables importing code-signing certificates into each individual Instant Virtual System (IVS). As a result, signed Java applets that are intermediated by an IVS are re-signed by the IVS using the certificate. This function helps to avoid the browser security warning that is displayed when a user accesses a signed Java applet through the IVS, as the hostname on the certificate will match the hostname of the originating entity, so warnings will not be displayed.

IVS is the end-to-end virtualization framework with Application Layer, Network Layer and Access Management virtualization enabling administrators to provision 255 logical independent SSL VPN gateways within a single appliance / cluster. Each virtual SSL VPN gateway represents a customer of a Managed Service Provider or a group within an enterprise providing complete segregation of traffic belonging to those customers/groups.

Customer Benefits

- Enhanced virtualization capabilities, allowing highly customized settings tailored for individual customer/group needs.
- Enhanced user experience by elimination of the warnings

Availability

- Secure Access products 3000 and above with Instant Virtual System license

- **Virtualized SSL Encryption Settings**

IVE release 5.2 further extends support for end-to-end virtualization by virtualizing the IVE security options. Options for allowed SSL and TLS version as well as allowed encryption strength are now supported at the individual IVS level. Virtualization of these features enables configuration of customer / group specific browser security settings for each Virtual System.

Customer Benefits

- Enhanced virtualization capabilities, allowing highly customized settings tailored for individual customer/group needs.

Availability

- Secure Access products 3000 and above with Instant Virtual System license



What's New in IVE v5.2