

What's New in Juniper's NetScreen IVE Platform Version 5.0

This application note describes the new features available in Version 5.0 of the NetScreen IVE platform for NetScreen Secure Access, Remote Access and Secure Meeting products. This document assumes familiarity with the Juniper's NetScreen IVE platform and the features of earlier releases including versions 4.1, 4.1.1 and 4.2.

Highlights of this Release

Juniper Networks enables companies to converge all of the access needs for their extended enterprise to provide a Secure and Assured communication experience with the 5.0 version of the IVE platform:

I. Introduction of Juniper Networks Next Generation Network Connect, a Hybrid VPN Client for Fast Network Access and High Availability

- **Dual Mode Functionality – Browser Based Provisioning or Stand Alone Client**
- **GINA Integration with Network Connect Client**
- **Cross Platform Support with Network Connect Client**
- **Enhanced Logging and Auditing Support for Network Connect Client**

II. Enhanced Ease of Use, Management and Support

- **Redesigned End User Bookmarks Page and Enhanced Customization Options**
- **RADIUS Accounting Support for NC and SAM**
- **Configurable IP Lockout for Failed Logins**
- **Factory Rollback in Administrator UI**

III. Increased Ease of Deployment

- **Web Rewriter Support for XML and Flash Content**
- **Client/Server Applications on Pocket PC Devices Support**
- **Mac OS 10.4 ("Tiger") Support for Web, Files, Telnet/SSH, and JSAM**
- **Solaris 8, 9 Support for Web, Files, Telnet/SSH, and JSAM**
- **Dynamic Policy Evaluation**

- **Netegrity SiteMinder Support Enhancements**
- **External Terminal Services Launcher**
- **Dynamic Intermediation of Web Proxy Authentication Challenges**
- **Java Applet Delivery Infrastructure**
- **Citrix Client Upload Capability (ActiveX)**
- **Multiple Virtual Source IP Addresses Support on IVE Backend**
- **Juniper End Point Defense Initiative (J.E.D.I.) Enhancements**
 - **Policy Specific Remediation**
 - **Conditional Evaluation of Host Checker Policies**
 - **Custom Remediation Actions for Host Check Policy Failures**
 - **Enabling of Third Party Client/Server Communication**
 - **Firefox Browser Support**
 - **Introduction of Endpoint Connection Control**
 - **Cross Platform Host Checker**

I. Introduction of Juniper Networks Next Generation Network Connect, a Hybrid VPN Client for Fast Network Access and High Availability

Juniper Networks introduces Next Gen Network Connect, a new hybrid VPN client that leverages the strengths of IPSec style data transport for maximum performance and also retains its SSL mode as a fallback transport mechanism, ensuring both maximum performance and high availability. When the user attempts to log in, Network Connect is auto provisioned if the user has authenticated, his end point compliance checks completed and he qualifies for network access (exactly like in the Juniper SSL VPN solution today). When the user tries to connect to a network resource, the client attempts to provide IPSec Style connectivity where possible for fast LAN type performance and, oblivious to the end user, seamlessly fails back to SSL mode of data transport in environments where IPSec style connectivity is not possible due to network environments that block IPSec based transport.

Customer Benefits

- Enables customers to converge around Juniper SSL VPN platforms for all their remote access needs, from core access for partners and vendors to Network Connect Access for power users/administrators
- Enables corporations to provide LAN style performance for a subset of their users, while still being able to leverage the strengths of a SSL VPN platform, namely dynamic provisioning of client and granular enabling of network level access.

Availability

- All Secure Access Products with a Network Connect License

- All Remote Access Products

1. Dual Mode Functionality – Browser Based Provisioning or Stand Alone Client

With this feature, Juniper Networks has extended the ability for the Network Connect access mode on the SSL VPN client to either be provisioned by the browser (exactly the same as today) or exist as a stand alone client on the end-point. Users can use the stand alone client to establish a tunnel to the corporate network and log in without opening their browser to establish such a connection. If the user logs in using a standalone client, the client upgrades automatically to the latest version, thereby ensuring that every customer is updated with the latest version of the Network Connect client.

Customer Benefits

- Enables end users and administrators to be flexible in their ability to deliver the Network Connect Client
- Provides an option to corporations to migrate their IPSec deployments for remote access to SSL VPN, while still providing a seamless user experience for customers used to launching VPN clients for tunnel access from their machines.

Availability

- All Secure Access Products with a Network Connect License
- All Remote Access Products

2. GINA Integration with Network Connect Client

With this feature, Juniper Networks has extended support for domain end-points to establish a connection to the network, map network drives or file shares before presenting the user with his/her desktop. This option is administrator configurable per role and the administrator can either force Network Connect in GINA mode or allow the user to enable this option.

Customer Benefits

- Enables administrators to easily support domain laptops while using the SSL VPN platform to provision network level access
- Enables end users accustomed to using IPSec clients to enjoy the same functionality while using their Network Connect Client for network access, thereby enabling a seamless end user experience

Availability

- All Secure Access Products with a Network Connect License
- All Remote Access Products

3. Cross Platform Support with Network Connect Client

With this feature, Juniper Networks has extended support for its Network Connect access method to Linux and Mac platforms. With this release, Juniper Networks will support Network Connect on RedHat Linux 9.0 and Mac OS X 10.2 and 10.3 releases

Customer Benefits

- Enables administrators to more easily deploy network level access on SSL VPN platforms across the multiple platforms deployed in their existing infrastructure

Availability

- All Secure Access Products with a Network Connect License
- All Remote Access Products

4. Enhanced Logging and Auditing Support for Network Connect Client

With this feature, Juniper Networks has added extensive client side logging and diagnostics capabilities for easy troubleshooting and ability to trace sessions and pinpoint problems. Users also have the ability to easily send detailed client side logs to the support teams for troubleshooting. Administrators will also have the capability to log packets based on source IP, destination IP, source and destination ports as well as application protocols. Administrators also have the ability to set up detailed rules to filter and selectively log a subset of the logging capabilities depending on the security needs of the network.

Customer Benefits

- Enables administrators to more intelligently manage their support infrastructure and reduce their costs of providing access to their customers using SSL VPN platforms

Availability

- All Secure Access Products with a Network Connect License
- All Remote Access Products

II. Enhanced Ease of Use, Management and Support

1. Redesigned End User Bookmarks Page and Enhanced Customization Options

In 5.0, the end user bookmarks page has been redesigned in three major ways. First, all the end user bookmarks can now be placed directly on the bookmarks or home page including terminal sessions, terminal services, client applications/SAM and Network Connect. As a result, users will require only one click to start a terminal session or Network Connect. As part of this redesign, the bookmarks have been reorganized into panels. In addition, the navigation bar on the left side of the bookmarks page has been removed and the bookmarks that didn't go directly into a panel, Meeting and Preferences, have been moved to a new framed toolbar on the homepage.

Second, administrators now have greater ability to customize their end-users experience. Administrators now have the ability to:

- Configure placement of all the panels in various single and double column formations
- Choose between putting "client application sessions" panel which contains NC, JSAM, WSAM or Email either on bookmarks page or on the toolbar
- Hide preferences on framed homepage toolbar
- Choose color of headers and sub-headers (headers available earlier)
- Point help link to another page (existing feature)
- Use standard, framed or no toolbar (existing feature)
- Show personalized greeting (existing feature but greeting is now in panel form and thus can be moved around)

All of these features are available on a role basis and panels will only show up if an administrator has configured a relevant bookmark in the end users role. Note that an existing feature also allows the administrator to provide an end user a custom start page.

Third, end-users now also have greater ability to customize their environment as they are able to configure the placement of their panels in addition to existing features such as adding and sorting their own bookmarks. In addition to these features, in 5.0, we also allow the administrator to create a bookmark that will start MS outlook using the URL handler function in Internet Explorer. Thus administrators can create a bookmark using [outlook:inbox](#), which will start MS Outlook when clicked in IE.

Furthermore, the Browsing Toolbar has been enhanced to include the following features:

- Visible session timer
- Icon that links to a custom-defined home page
- Ability to bookmark a page while browsing
- Ability to collapse the toolbar in order to increase the viewing area around it

Customer Benefits

- Faster, more familiar and easy-to-learn user interface
- Greater administrator customizability
- Greater end user customizability
- Flexibility to direct users to a custom home page

Availability

- All Secure Access and Remote Access Products

2. RADIUS Accounting Support for NC and SAM

Enhancing our RADIUS Accounting support (based on RFC 2866), Juniper now sends RADIUS Accounting Start and Stop messages for user activity (login and logout) on SAM and NC. RADIUS Accounting is the standard way to provide details on the end user activity through the NAS (Network Access Server) device in traditional remote access solutions.

Customer Benefits

- Enhanced interoperability with existing customer RADIUS Accounting infrastructure enabling reporting and billing based on the information on the RADIUS Accounting server.
- Enables actionable reporting on IVE user activity in environment with RADIUS servers.

Availability

- All Secure Access and Remote Access Products

3. Configurable IP Lockout for Failed Logins

With this feature, Juniper Networks provides the ability to configure the lockout algorithm for failed logins. The IVE protects the backend systems in case of a Denial of Service, Distributed Denial of Service (DDOS) or Password Guessing attack against the system. Now

the algorithm has been enhanced to be more flexible and configurable so the users can better fit its behavior to their specific environment requirements. Administrators can now configure the rate of failed attempts, the trigger for failed attempts and the lockout period.

Customer Benefits

- Increased security and protection against DOS, DDOS and Password Guessing attacks.
- Increased flexibility allows for enhanced integration with unique user environments.

Availability

- All Secure Access and Remote Access products

4. Factory Rollback in Administrator UI

Factory rollback is now available in the Administrator GUI on the UI platforms page. Previously, this feature was just available through the serial console.

Customer Benefits

- Makes factory rollback function easier to use

Availability

- All Secure Access and Remote Access Products

III. Increased Ease of Deployment

1. Web Rewriter Support for XML and Flash Content

This feature extends the sophistication of Juniper's market-leading web rewriting engine to support intermediation of XML and Flash content, including dynamic rewriting of internal web links during an access request.

Customer Benefits

- Enables end users to securely access web applications with XML and Flash content through the Secure Access appliance, protecting internal web servers while providing an experience as if the user is connected to the internal servers directly

Availability

- All Secure Access Products

2. Client/Server Applications on Pocket PC Devices Support

With this feature, Juniper Networks introduces support for client/server applications on Pocket PC devices running Windows Mobile 2003.

Customer Benefits

- Enables customers to extend their ability to provide access to their customers on PDA devices, thereby increasing the value of their SSL VPN deployment

- Increases the access options available to end users on PDA devices to include client server applications like Outlook, thereby increasing their productivity

Availability

- All Secure Access Products with a Secure Application Manager License

3. Mac OS 10.4 (“Tiger”) Support for Web, Files, Telnet/SSH, and JSAM

With this feature, end users running Mac OS 10.4 (code named “Tiger” and expected to be generally available in April 2005) will be able to securely access web applications, file shares, and telnet/SSH sessions via the Secure Access appliance. End users will also be able to run static TCP port client/server applications through the Secure Access appliance using JSAM running on Mac OS 10.4. Mac OS 10.4 will be tested with the Safari 2.0 browser (Mac OS 10.4 is packaged with Safari 2.0)

Customer Benefits

- Enables end user access from the latest version of the Mac OS

Availability

- All Secure Access Products (with a Secure Application Manager License for JSAM support)

4. Solaris 8, 9 Support for Web, Files, Telnet/SSH, and JSAM

With this feature, end users running Solaris 8 or 9 will be able to securely access web applications, file shares, and telnet/ssh sessions via the Secure Access appliance. End users will also be able to run static TCP port client/server applications through the Secure Access using JSAM running on Solaris 8 or 9.

Customer Benefits

- Extends ubiquity of access to end user machines running Solaris 8 or 9

Availability

- All Secure Access Products (with a Secure Application Manager License for JSAM support)

5. Dynamic Policy Evaluation

The IVE will have the capability to dynamically evaluate resource policies as configuration changes occur. Administrators can activate the policy evaluation on demand or configure a re-evaluation frequency for periodic dynamic evaluations. When re-evaluation occurs, the IVE will evaluate policies for all active users including role mapping rules, role definitions (capabilities and restrictions) and resource policies. If a user’s access has been revoked his session will be terminated and he will not be able to access the revoked resources. Dynamic resource policy evaluation will take place for Web, JSAM, WSAM, NC, Telnet, SSH, Windows Terminal Services and Citrix.

Customer Benefits

- Increased security due to administrators' configuration and time-based changes taking effect immediately for active users.

Availability

- All Secure Access and Remote Access Products

6. Netegrity SiteMinder Support Enhancements

With these enhancements, Juniper Networks provides advanced support for SiteMinder as an Authorization Server. This will allow administrators to use SiteMinder user attributes for authorization decisions in role mapping. Furthermore, SiteMinder's error codes returned during authentication and authorization will now be displayed in the IVE User Access Log.

Customer Benefits

- Enhanced granularity in role mapping allowing advanced network security design and configuration.
- Increased interoperability with SiteMinder environments.
- Enhanced and comprehensive logging capabilities.

Availability

- All Secure Access Products with an Advanced License

7. External Terminal Services Launcher

With this feature, customers can establish "bookmarks" on their own web pages that, when clicked, launch a terminal services application dynamically proxied through the Secure Access appliance. The end user experience when clicking the external bookmark is identical to the experience when clicking a terminal services bookmark on the Secure Access home page.

Customer Benefits

- Enables the use of custom portal pages to launch secure terminal services sessions dynamically proxied by the Secure Access appliance

Availability

- All Secure Access Products with a Secure Application Manager License

8. Dynamic Intermediation of Web Proxy Authentication Challenges

With this feature, the Secure Access appliance will intermediate authentication challenge requests (HTTP 407) presented by web proxy servers that reside between the Secure Access appliance and internal web application servers. If the web proxy server sends a Basic or NTLM challenge, the Secure Access appliance will prompt the user for authentication credentials. For subsequent web proxy authentication challenges, the credentials can be securely cached on the Secure Access appliance and be used for single-sign on through the web proxy server.

Customer Benefits

- Supports flexible use of web proxy server architectures
- Provides seamless user experience in environments with web proxy servers that require authentication

Availability

- All Secure Access Products

9. Java Applet Delivery Infrastructure

With this feature, customers can utilize the Secure Access appliance to host and deliver Java applets of their choice. Once an administrator obtains an applet(s) of choice, the applet(s) can be uploaded to the Secure Access appliance, and then dynamically provisioned to end users during the SSL VPN session based on real-time access requests and privileges.

Customer Benefits

- Enables secure delivery of client-side Java applets to end users without the need for a separate internal hosting server
- Enables seamless and secure access to emulation environments (e.g. TN3270/5250, Citrix, Hob) via Java applets of customer choice

Availability

- All Secure Access Products

10. Citrix Client Upload Capability (ActiveX)

This feature allows an administrator to securely upload a Citrix ActiveX ICA web client to the Secure Access appliance, after which the ICA ActiveX client can be dynamically provisioned to end users as part of an access request to a Citrix-based application.

Customer Benefits

- Provides a mechanism to provision a standard Citrix ActiveX ICA client without relying on a separate internal hosting server and without requiring internal internet connectivity to the Citrix download site
- Extends flexibility of options for provisioning the Citrix ICA client to end users

Availability

- All Secure Access Products with a Secure Application Manager License

11. Multiple Virtual Source IP Addresses Support on IVE Backend

This feature allows an administrator to configure multiple virtual source IP addresses on a role basis on IVE internal interface for Core and SAM access methods. One or more roles could be configured with a virtual source IP address by the administrator. For all incoming end-user sessions that get mapped to these roles, the configured virtual IP address will be used as the Source IP for corresponding traffic going out over the IVE backend.

Customer Benefits

- Enables IVE to work seamlessly with IP address based access control lists / security policies configured in the network

Availability

- All Secure Access Products

12. Juniper End Point Defense Initiative (J.E.D.I.) Enhancements

12.1 Policy Specific Remediation

With this feature, Juniper Networks has introduced the ability for administrators to specify Host Checker Policy specific remediation instructions in the event of a hostchecker policy failure. When a user fails a subset of the host checker policies, he/she will have the ability to receive a customized remediation page that only lists the Host Checker Policies that have failed and the remediation instructions specific to the failed policy as provided by the administrator

Customer Benefits

- Enables end users to more easily identify the specific policies that have failed on their end point and remediate appropriately
- Provides administrators the ability to provide detailed information to the end user on the specific policies that failed and targeted remediation instructions, thereby minimizing administrative support costs and time

Availability

- All Secure Access and Remote Access Products

12.2 Conditional Evaluation of Host Checker Policies

With this feature, Juniper Networks has introduced the ability for administrators to specify the conditional evaluate of Host Checker policies. For e.g. administrators can evaluate if a PC is a managed PC or not using a single Host Checker policy and if the user fails the policy, then evaluate or enforce a secondary policy that can be used for remediation actions. For e.g. an administrator could setup a Host Checker policy that checks if the user is authenticating from a managed PC and if that policy fails and Host Checker detects that it is an unmanaged PC, the user can be forced into a Virtual Desktop that ensures that corporate data is protected by confining the user to a sandbox on his/her endpoint.

Customer Benefits

- Enables administrators to more intelligently run and enforce Host Checker policies, depending on the status of their Host Checker policies

Availability

- All Secure Access and Remote Access Products

12.3 Custom Remediation Actions for Host Check Policy Failures

With this feature, Juniper Networks has enabled the ability for administrators to launch remediation actions in the event of a host check policy failure. These actions are specific to the policy that is failing. For e.g. administrators can now selectively launch cache cleaner on a PC if they detect that the end-point is not a managed device

Customer Benefits

- Enables administrators to more intelligently deploy targeted actions on the end user's endpoint and ensure that the end point is compliant with the security needs of the network before granting access

Availability

- All Secure Access and Remote Access Products

12.4 Enabling of Third Party Client/Server Communication

With this feature, Juniper Networks has added the ability for third party clients to be able to communicate with their policy servers, obtain latest virus definitions and remediation instructions to automatically remediate the clients

Customer Benefits

- Enables administrators to enable the full functioning of any 3rd party compliance clients they have installed on their endpoints that require access to their policy servers residing in their corporate network, thereby leveraging their investments in 3rd party compliance checking solutions

Availability

- All Secure Access and Remote Access Products

12.5 Firefox Browser Support

With this feature, Juniper Networks introduced support for the Firefox browser across the J.E.D.I. components, Host Checker and Cache Cleaner and Access Methods, Secure Application Manager and Network Connect

Customer Benefits

- Enables administrators to deploy Juniper SSL VPN solutions across different types of browser types

Availability

- All Secure Access and Remote Access Products

12.6 Introduction of Endpoint Connection Control

With this feature, Juniper Networks introduces support for a connection control module that can ensure that all incoming connections to the endpoint are blocked except for trusted communication from the SSL VPN platform. The module is a part of the Host Checker download and can ensure that all connections on the physical interfaces, other than from the SSL VPN gateway can be monitored and disallowed as a precursor to providing access to the user.

Customer Benefits

- Enables administrators to deploy tighter policies around connections to and from an endpoint to ensure that malicious users cannot use incoming connections on IP interfaces to mount a U-Turn attack on the corporate network
- Enables administrators to dynamically increase security controls, particularly while provisioning network level access from an SSL VPN platform

Availability

- All Secure Access and Remote Access Products

12.7 Cross Platform Host Checker

With this feature, Juniper Networks had added the ability to support J.E.D.I. Assessment and Containment Capabilities on MAC and Linux platforms. With this release, Juniper Networks will support Host Checker on RedHat Linux 9.0 and Mac OS X 10.3 releases

Customer Benefits

- Enables administrators to deploy comprehensive endpoint assessment and containment functionality in varied environments

Availability

- All Secure Access and Remote Access Products