

What's New in Juniper SSL VPN Version 7.0

Introduction

This document lists the new features available in version 7.0 of the SA Series SSL VPN product line. This document assumes familiarity with the Juniper's SA gateway and the features of earlier releases up to version 6.5

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

- I. [Support for Junos Pulse](#)
- II. [Multiple Sessions per user](#)
- III. [Ability to present legal disclaimer pages before and after user authentication](#)
- IV. [Certificate Authentication to backend servers](#)
- V. [Extended mobility support with IPSec/IKEv2 VPN and Client Cert Auth for ActiveSync](#)
- VI. [Logging of Network Connect Transport Mode on the Admin UI](#)
- VII. [Bridge CA Support](#)
- VIII. [Support for Microsoft AJAX through the Rewriter \(Core Access\)](#)
- IX. [Support for Outlook Web Access 2010 through the Rewriter \(Core Access\)](#)
- X. [Kerberos Debugging Tools](#)
- XI. [FIPS Performance Enhancements](#)
- XII. [RDP 7 support](#)
- XIII. [Embedded Java RDP Applet](#)
- XIV. [2-Phase Upgrade](#)
- XV. [Ability to display banner messages to remote users](#)
- XVI. [Virtual Appliances and License Server](#)

Support for Junos Pulse

SA 7.0 introduces support for remote access features using the new Junos Pulse client. This client provides secure, authenticated access for remote users to corporate resources via the SSL protocol. More details about the Junos Pulse client and its remote access features are in the website referenced below:

<http://www.juniper.net/us/en/products-services/software/junos-platform/junos-pulse/>

Feature differences from Network Connect

- Junos Pulse is designed to provide forward compatibility with versions of the SA gateway beyond 7.0. Pulse 1.0 (released along with SA 7.0) will support two (2) versions of the SA gateway beyond version 7.0.
- Pulse has a brand new User Interface, designed with simplicity and ease of use in mind. The new Pulse UI is easier to use, automatic wherever configured by the administrator and reduces the need for the end user to be savvy about networking or technical issues.

- Junos Pulse 1.0 includes the Location Awareness feature, which enables administrators to configure flexible rules that indicate when to automatically trigger remote access to the SA gateway. Pulse will use these rules to automatically trigger connectivity to the SA without needing the end user to manually start the client each time. For example, a simple rule might enable the Pulse client to automatically connect to the SA gateway upon detecting that the user is on a home network, and not on the corporate LAN.
- Junos Pulse 1.0 also allows the administrator to pre-configure a list of SA gateways to end users, who can then simply click on one of the gateways to connect to. This allows administrators the flexibility to pre-configure a list of globally deployed enterprise SA gateways, so that end users can easily choose which gateway they want to connect to.
- Pulse 1.0 also includes the Session Migration feature. This feature enables customers who have both the SA and IC to leverage the combined value of both solutions. This feature enables seamless migration of the user's authenticated session to the SA if the user is already authenticated to the IC, and vice-versa. This enables a user who may be authenticated with an SA gateway remotely, to seamlessly login to an IC when they arrive within corporate premises. This simplifies the user experience without needing them to manually switch between a LAN access client and a remote access client.

Multiple sessions per user

SA 7.0 allows remote users to launch multiple sessions to the SA gateway. The maximum number of sessions per user is configurable by the administrator per realm and defaults to 1. This allows remote users to have secure VPN connectivity from more than one computer at a time.

Customer Benefits

- Remote users often need to have multiple authenticated sessions open at the same time, often using each session for a particular need. This feature allows the users to do so, without needing them to terminate earlier sessions.

Ability to present legal disclaimer pages before and after user authentication

Some corporate IT policies require that end-users accept a license agreement before they sign in remotely into the enterprise network. A legal notice must be presented to the user at the time of logging in, and access should be granted only if the user accepts the terms and conditions of the notice. This feature implements this requirement.

This feature can also be utilized to display a "message of the day" (MOTD) to the user when they login. MOTD's typically do not require an explicit end-user acceptance to let the user use the system. Configuring two buttons ("Accept" and "Decline") makes the feature function in the EULA mode, while a single button ("Accept" or "Proceed") supports the MOTD mode.

Administrators have the option of presenting the notice

- Before authenticating the user (pre-auth) or
- After the user credentials are collected and evaluated by the server (post-auth) or

- In both situations above.

In the post-authentication case, the content displayed to the user can be associated with the role assigned to the user.

Administrators also have the option to configure the “look and feel” of the notice, either through Web UI, or by uploading (an enhanced) custom sign-in package. Furthermore, the notice can be displayed in multiple languages.

Customer Benefits

- This feature enables several customers to enforce corporate legal policies, before allowing access to remote users. Customers often need remote users to read, understand and accept corporate policies before letting them access to privileged resources in the data center.
- The ability to customize the content and presentation style of the disclaimer pages allows the administrator tremendous flexibility in customizing the page as per specific needs and requirements.

Certificate Authentication to backend servers

This feature enables customers to enforce client authentication on their secure backend servers, and allows the SA gateway to present an admin-configured certificate to these servers for authentication. Several customers need backend servers to require strict access control, including the usage of client certificates for SSL establishment. This feature allows the SA gateway to present a certificate to such a backend server, thereby conforming to these SSL policies. The SA gateway can be easily configured to present a client certificate to one or more secure backend servers.

Customer Benefits

- This feature enables customers to mandate strict SSL policies on their backend servers by configuring client authentication.

Extended mobility support with IPSec/IKEv2 VPN and Client Cert Auth for ActiveSync

The SA gateway has offered best-of-breed features enabling mobile users to access corporate resources and applications securely. This feature further extends the mobility features with the following enhancements:

- SA 7.0 allows remote users to connect to the gateway using IPSec/IKEv2 clients. This allows users to connect remotely from devices such as PDA's, mobile devices and smartphones which support IKEv2 VPN connectivity. The administrator can also enable strict certificate authentication for access via IPSec/IKEv2.
- SA 7.0 also extends ActiveSync support by enabling Client Certificate authentication for ActiveSync access. Any mobile device capable of supporting ActiveSync (push e-mail) along with client side certificates can now be challenged by the SSL VPN for a valid client certificate before being allowed access to the ActiveSync server, thereby providing greater assurance than only properly authenticated mobile devices can reach the corporate email services. Client certificate authentication will be supported on the internal port, external port, and virtual ports defined on the internal or external ports.

Customer Benefits

- The IPSec/IKEv2 feature extends the leading mobility and access control features of Juniper's SSL VPN solution to a broad range of devices and OS platforms that support IKEv2 VPN connectivity.
- The administrator can enable strict mobile authentication policies for ActiveSync access, requiring client certificate authentication. The SA gateway is the only solution in the industry enabling such granular mobile access control, combined with strict authentication policies such as client cert authentication.

Logging of Network Connect Transport Mode on the Admin UI

SA 7.0 enables the administrator to view granular user access information, such as the Network Connect transport mode, logged on the Active Users page in the Admin UI. This enables the administrator to view the type of connectivity each end user has, that may be useful for troubleshooting or support purposes. Network Connect can transparently adapt its transport mode to suit the user's environment, by dynamically failing over to SSL in case UDP is blocked in the user's network by a firewall. This information is now available for administrators to view on the admin UI.

There are two changes provided by this feature:

- User Access Log will clearly indicate whether a Network Connect user is connected via SSL or ESP protocol;
- A new column is added to the Active User page to indicate whether the Network Connect session is using SSL or ESP protocol.

Customer Benefits

- This feature allows the administrator to troubleshoot user access issues more easily with more information logged on the admin UI.

Bridge CA Support

SA 7.0 supports Certificate Path Building and Path Validation compliant with RFC 3280 standards. This standards-compliant certificate path processing enables the SA gateway to process name constraints, certificate policies, policy constraints and policy mappings, in addition to basic constraints and key usage. The administrator can configure the initial-explicit-policy, user-initial-policy-set and initial-policy-mapping-inhibit inputs to ensure standards-compliant processing of the certificate policy extension during certificate path validation, conforming to the behavior outlined in RFC 5280.

This feature is critical to ensure correct certificate validation in advanced PKI deployments, such as deployments including the usage of a Bridge Certificate Authority (CA). A Bridge CA is a special purpose CA that enables trust between separate PKIs. Through a process called cross certification, the Bridge CA links PKIs from various organizations. This linkage enables the users of all these organizations to validate certificates and signatures made by each other in order to facilitate the secure exchange of data with each other.

Customer Benefits

- This feature enables customers who use advanced PKI deployments to deploy the SA gateway to perform strict standards-compliant certificate validation, before allowing data and applications to be shared between organizations and users. The lack of such strict certificate validation could lead to unintended trust or exposure of information to users who lack the privileges to see the data being accessed.

Support for Microsoft AJAX through the Rewriter (Core Access)

SA 7.0 introduces support for applications written using Microsoft AJAX to be delivered via Core Access through the Content Intermediation Engine (a.k.a. Rewriter). Support for Microsoft AJAX natively in the Rewriter provides high-performance rewriting for these applications without needing custom filters.

Customer Benefits

- Full native support for rewriting applications written using Microsoft AJAX
- Higher performance of rewriting applications that are written using Microsoft AJAX than with custom filters

Support for Outlook Web Access 2010 through the Rewriter (Core Access)

SA 7.0 introduces support for Outlook Web Access 2010 through the Content Intermediation Engine (a.k.a. Rewriter).

Customer Benefits

- This feature enables customers to upgrade their Exchange environments to 2010 and enable web-based access to emails through the Rewriter.

Kerberos Debugging Tools

This feature simplifies the deployment and troubleshooting of Kerberos and Constrained Delegation environments for administrators. Using this feature, the administrator can:

1. Probe Kerberos infrastructure, especially the DNS infrastructure, to check the validity of Kerberos realms and defined credentials.
2. Inspect the Kerberos ticket cache.
3. Invoke command-line Kerberos operations, either by admin or by support team via remote debugging, to investigate Kerberos and NTLM issues.

Customer Benefits

This feature reduces the complexity involved in deploying Kerberos Constrained Delegation and provides valuable tools for troubleshooting and debugging setup issues. Deploying Kerberos and Constrained Delegation can become challenging for IT administrations due to the following reasons:

- There is a plethora of SSO methods: Basic Auth, NTLM, Kerberos and Constrained Delegation. The backend application can require any one of these SSO methods to authenticate.
- The admin for the SA gateway is often not in the same functional group as those responsible for enterprise authentication infrastructures.

FIPS Performance Enhancements

SA4500 FIPS and SA56500 FIPS platforms have been enhanced to provide additional performance to web server (Core Access) operations.

Customer Benefits

- FIPS platform users enjoy much improved page response times.

RDP 7 support

With this release, the Juniper Terminal Service client supports the latest Remote Desktop Protocol, RDP7.

The following additional features of RDP7 are not currently supported using the Juniper Terminal Services Client, although they will work if used with NC or WSAM along with the standard Microsoft RDP7 client.,

- True multi-monitor support
- Bi-directional audio support

Customer Benefits

- Improved terminal services experience for users running RDP7 clients.

Embedded Java RDP Applet

Juniper has partnered with Hobsoft to bring the Hob RDP Java applet to the Juniper SSL VPN as an embedded feature, thereby providing development, quality assurance and support benefits to customers who require quality java applet support for remote desktop connections. Complex HTML configurations have been replaced by simple admin configuration options, such as screen size, color depth, and single sign-on. All Juniper SSL VPNs will ship with 2 concurrent user licenses, after which customers will be required to purchase subscription licenses to expand to additional user counts.

Customer Benefits

- Integrated licensing for simple administrative deployments
- Multiple monitor support
- Enterprise-class features
- No admin rights requirements
- Cross-platform: Windows, Mac and Linux

- Single-source Juniper (JTAC) support

2-Phase Upgrade

Uploading an upgrade package to the SSL VPN can take a significant amount of time, especially when the target device is located across a WAN. This feature allows administrators to push (stage) the package ahead of time so that the upgrade itself can instead be triggered at a later date and time.

Customer Benefits

- Reduced downtime during upgrades, as upgrades can be immediately executed upon command rather than having to push an upgrade at the beginning of the downtime window.
- Ability to script large scale distribution and deployment of upgrade packages using DMI.

Ability to display banner messages to remote users

SA 7.0 introduces the ability to set banner messages to be displayed to remote users who connect to the SA gateway using Network Connect. These messages may be customized by the admins to indicate regular maintenance timeframes, or other critical information that they may need users to know about. The admin-configured message is then displayed to the remote user in a separate dialog box.

Customer Benefits

- Remote Users who use Network Connect can now be informed about downtimes, system maintenance events or other admin-related information when they launch a VPN connection to the SA. This enables administrators to reach remote users to communicate useful information to them.

Virtual Appliances and License Server

Virtual appliances are being introduced to support large-scale service provider deployments, whereby service providers can deploy the SSL VPN as individual virtual appliances to customers. As virtual appliances can run on various hardware platforms and configurations (typically blade servers), the virtual appliances themselves come at no cost. Instead, subscription licenses are also being introduced as the new method for licensing virtual appliances, as a service provider will simply install all licenses on the SSL VPN license server and then assign licenses at various levels to the virtual appliances.

Customer Benefits

- Licensing that conforms to service provider business models and operations
- Flexible hardware configuration options
- Virtually unlimited scalability

Corporate and Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airsides Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

Copyright 2010 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, 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.

June 2010