What’s New in Juniper SSL VPN Version 7.1

Introduction

This document lists the new features available in Version 7.1 of the Secure Access SSL VPN product line. This document assumes familiarity with the Juniper’s SA gateway and the features of earlier releases up to version 7.0.

Junos Pulse client enhancements are addressed in the most recent “What’s New in Junos Pulse 2.0” document.

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

Enterprise Leased Licensing

Enterprise leased licensing provides the ability for administrators to lease excess licensing capacity from one appliance in order to use that capacity on another appliance.

Example Use Case: An administrator who manages 80 SA gateways would generally not want to manage licenses across all systems and would also not want to buy enterprise licenses up front if the less expensive per-device licenses would suffice. But at the same time it can be assumed that at some point at least one of those boxes might end up having a large surplus of licenses from which one or more other devices could benefit, such as 5,000 surplus licenses on one system with a desire to lease 2,500 to two other systems. In this case the license server can be implemented quite narrowly (across just 3 systems instead of all 80) and only when it is needed, thereby saving the organization excessive up-front planning and, quite possibly, excess spending for a condition which might never arise.

Requirements:

- **License Server**: Any hardware appliance capable of running this version (7.1) can be used as a license server. It is important to note that the license server itself is only required for the lease operations rather than serving as a centralized license distribution point such as a DHCP server would be. In this way the license server can tolerate very lengthy downtimes, thereby preventing the need to deploy servers throughout multiple network segments.
- **License Server Activation License**: Simply a license to enable the hardware appliance to fulfill the license server role.
- **License Server Membership Licenses**: Licenses that are only applied to the active appliances that need to participate in leased licenses.

Customer Benefits

- Provides the ability to buy enterprise licensing incrementally and as-needed rather than all up-front.

Common ACCESS Licensing

Common ACCESS licensing is being introduced to serve both SA Series SSLVPN and IC Series UAC appliances. While the existing licenses will remain as an available option, newer deployments will favor the common licensing as they are able to work with either appliance.

Customer Benefits

- Works well with the new license server option to allow licenses to be leased between SA and IC appliances.
- Simplifies the licensing model across both SA and IC implementations, resulting in generally lower costs, especially in mixed environments.

SAML 2.0

SAML support has been upgrade to support version 2.0 (in addition to existing support for SAML 1.X), enhancing the SSL VPN's ability to securely integrate single sign-on (SSO) authentication and authorization with external applications, such as cloud application providers. As with the 1.X implementation, the SA can act as a SAML producer or consumer.

The SA Series SSLVPN can be deployed in any of the following SAML 2.0 scenarios:

- SA as a SAML Service Provider (SP): This deployment involves another access management system being used as an Identity Provider (IdP), with the SA being configured to use the authentication result from that IdP.
  As a Service Provider, the SA also supports the Single Logout feature of SAML 2.0, to force the user to be logged out from all sessions at the same time.

- SA as a SAML Identity Provider (IdP): This deployment involves the user authenticating to the SA using any supported authentication mechanism. Subsequently, the user can access any resource or application that is protected as a SAML SSO resource policy. The SA generates and sends SAML assertions to the protected resource or application.
- SA as a Policy Enforcement Point (PEP): In this deployment type, the user authenticates to the SA and accesses a resource that is protected by a SAML Access Control List. The SA generates the SAML 2.0 user authorization request and grants or denies access based on the response from the Policy Decision Point (PDP).

Customer Benefits

- Standards-based SAML 2.0 support enabling Single Sign On access to resources or applications protected by SAML 2.0 policies.

ActiveX Self-Upgrade

ActiveX is a common deployment method for various client software on Microsoft platforms, typically when using Internet Explorer (IE). However, since both installing and upgrading ActiveX components require administrative privileges, users with locked-down systems are unable to receive upgraded versions of the ActiveX installer unless the administrator had previously installed the Juniper Installer Service (JIS). Until now, the only reliable way to upgrade this component was for the administrator to push out the new JIS package, which included this control.

Customer Benefits

- Customers no longer need to deploy the latest JIS version when upgrading from SA 6.5 or 7.0, to 7.1 or future releases. Likewise, customers no longer need to deploy latest JIS versions while upgrading from 7.1 to future releases either.
- End users will only be prompted when a new ActiveX version exists, but the process itself is intuitive and only requires the user to accept the action so that the install may begin.
- Administrators no longer have to push the JIS update in order to update the ActiveX installer. Note, however, that the JIS feature is still required on locked down workstations if the user is to run the update themselves.

Sharepoint 2010

SA 7.1 provides extensive support for Sharepoint 2010 when accessed through the SA Rewriter (Core Access). Support covers popular features in Sharepoint 2010 such as Office integration, Collaborative content and remote access from mobile devices, such as smartphones and tablets.

In particular, the support for Sharepoint 2010 includes the following features:

- Cross browser support – IE7, IE8, Firefox, Safari
- Microsoft Office integration
- SharePoint web experience
- Collaborative content, social feedback and organization, User Profiles, MySites
- Content management – Large lists, libraries, Enterprise Metadata, Document sets, Web Publishing including Digital Asset Management, Governance and Record management
- Search – Interactive search experience, relevance, people search
- Browser based administrative tasks
- SharePoint Mobile Access
- Silverlight support only through PTP

The following features are not supported through Core Access (rewriter):

- Silverlight – Workaround: Filter to disable silverlight
- OneNote, Visio and Excel REST
- People connections – interaction with Outlook and Office Communicator

- Activity (RSS) feeds
- Business Connectivity Service – connect to Exchange, LotusNotes, Documentum, FileNet, etc.
- SharePoint Designer
- SharePoint Workspace Groove
- InfoPath Forms Service
- Access Service
- Office Web Apps
- Fast search

Customer Benefits

- Provides remote users with comprehensive support for Sharepoint 2010 when accessed through the Rewriter.
- Delivers stable functionality and performance for end user access.

Peak Load Monitoring

As part of ongoing performance monitoring and management across heavily loaded systems, it is important for administrators to have ready access to both current and historical data so that proactive calculations and adjustments can be made. This feature provides the following to further assist in those endeavors:

- Cockpit Graph: A new graph has been included on the admin home page to illustrate the total and successful login rate (commonly called the ramp rate) as well as the total and current NC and HC launch rates. Under peak load and spike conditions, such as a an emergency situation where remote users are connecting at higher-than-usual rates, this graph can aid in the overall understand of the resource utilization as compared to the non-peak conditions.
- Enhanced Logging: NCP and JCP connection counts are now included in the event logs as a way to provide improved historical data around client connection loads over time.

Customer Benefits

- Improves the administrator's situational awareness concerning system load, providing more opportunities for more thorough capacity planning over time and abnormal events.

IKEv2 EAP Support

IKEv2 support allows any standard IKEv2 supplicant to connect to the SSL VPN as a layer 3 VPN client, thereby allowing full network access without requiring any Juniper client software to be installed on the remote workstation/device. However, prior to this release only certificate authentication was supported.

Starting with 7.1 this has been extended to now include username/password authentication through EAP (Extensible Authentication Payload), whereby IKEv2 provides a "tunnel" mechanism for EAP authentication.

Specifically, the following EAP protocols are now supported:

- EAP-MSCHAPV2
    - Supported auth servers: Local, Active Directory / Windows NT
- EAP-MD5
    - Supported auth servers: Local

Customer Benefits

- This feature greatly expands the remote access client possibilities to include any IKEv2 standards-based connection.

Certificate Revocation List (CRL) Download through a Proxy

At times when a CRL Distribution Point (CDP) is on an external network to the SSL VPN and hosted on an HTTP or HTTPS server, certain environments may require that all outbound access go through a proxy server. This feature addresses this need by allowing administrators to configure a proxy server as part of the CRL configuration.

Customer Benefits

- Customers with restrictive policies that require all external communication to first go through a proxy server no longer need to seek an exception for CRL downloads.
- Authenticated proxy access is supported using basic authentication (username + password).

Mobile-friendly SSL VPN Login Pages

SA 7.1 includes pre-defined html pages that are customized for mobile devices, including Apple iPhones and iPad, Google Android, and Nokia Symbian devices. This enables mobile device users to authenticate to the SA and be presented with webpages that are customized for their device types and screen resolutions.

Customer Benefits

- Users who login to the SSLVPN from mobile devices, including smartphones, have a simplified and enhanced user experience with webpages that are customized for their device types.

Endpoint Auto-Remediation

While Host Checker has the ability to scan workstations for security patch compliance using the Endpoint Security Assessment Plug-In (ESAP), remediation has required either Microsoft SMS/SCCM or a manual installation of any missing patches. This feature allows clients running Pulse 2.0 or higher to achieve auto-remediation directly from the SA Series SSLVPN gateway.

Customer Benefits

- End users see a process tracking in the UI so that the client has some understanding that a maintenance task is underway.
- This process utilizes the leading Shavlik patch detection and deployment engine and is enabled with a feature license such that only the required number of devices needs to be licensed. 2 concurrent user licenses are included for free.

VMware View 4.X Support

As both VMware View and Citrix Xen virtual desktop (VDI) environments are supported by the gateway, it is important for newer VDI versions to be enhanced as needed so that they may be delivered to their fullest potential. In this release the latest version of VMware View has been extended through rigorous development, quality assurance and support measures to ensure that newer VDI features and functionality are fully understood and supported as a common application rather than as an emerging and/or generic one.

Customer Benefits

- Administrators achieve a higher end-to-end level of support for VMware View implementations, including detailed logging of display protocol error conditions and support for the View client's Message Security Mode communication.
- Desktops can fall back to the RDP display protocol by default. But if this has been disabled by the administrator the desktop bookmark will be grayed out with an underlying message informing the user that the display is currently not supported on their system.

Citrix Web Interface 5.X Support

This feature provides upgraded support for the embedded Citrix Web Interface versions for simplified and rapid configuration of Web Interface profiles. This also reduces confusion as to which versions are "supported" as had been the case in previous releases that specifically called out .X versions, e.g. 5.1 or 5.2.

Customer Benefits

- Administrators can quickly configure any Citrix 5.X Web Interface versions, greatly reducing the need to manually configure various resource profile settings.
- Enhances the JTAC support experience.

Enabling DMI Logging

Customers using NSM for centralized management receive all logs within the management server as Juniper's Device Management Interface (DMI) protocol defaults to send. However, there are times when NSM (or any other management utility that has been configured with DMI) only requires management rather than logging, typically when other syslog servers are already being used for such purposes.

Customer Benefits

- Allows administrators to use NSM for management without duplicating the logging activity across both the centralized management and logging systems.

ActiveX Delivery Optimization

Whenever clients have to install ActiveX there is always a delay, as the installation always forces a break in what the user is doing which often leads to concerns over end-user satisfaction. However, by optimizing such delays to limit the exposure time while simultaneously keeping the users informed, overall satisfaction can be greatly improved.

Customer Benefits

- End user experience is improved by cutting the current delay prompt time by 50% with the addition of an on-screen countdown timer, informational messaging, help link, and the ability to skip the option altogether if the user knows they will not require this component.
- Administrators have the ability to customize the end user informational messaging in any of the supported languages.

Inheriting Policies from Root CA to Intermediate CA's

This feature provides the ability to inherit CRL and/or OCSP certificate status check settings from the root CA (Certificate Authority), to its intermediate CA's. This revocation check is performed during certificate chain verification, in most cases for client certificate authentication. This particularly benefits customers having a large number of intermediate CA's, which are imported automatically during client certificate authentication. For such intermediate CA's, customers can simply choose to inherit the certificate status check options from the root CA instead of having to configure settings for each intermediate CA.

Customer Benefits

- Enhances administrative ease and accuracy with flexible intermediate CA status checking configuration through auto-import.

Domain Based Security for Core Access (Rewriter)

Web browsers prevent content from one web site accessing content from another web site. But since content is all rewritten in a single domain (that of the IVE), all of the content appears to come from the same domain, which limits the browser's ability to enforce its own security model for those web pages that are being rewritten.

This features introduces the <localdomainsuffix> variable that can be used in any access control list (ACL) such that *.<localdomainsuffix>:*/* inserted as an ACL would enforce the DNS domains that have been entered under the system network settings.

Customer Benefits

- Provides a simple method for administrators to further enforce domain security for rewritten web applications.

LDAPS Certificate Authentication

SA 7.1 can be used to enforce certificate validation for LDAPS operations. For every connection the certificate is verified for:

- Hostname match to the server certificate name
- Trust by the IVE
- Expiration of the server certificate
- Expiration of the intermediate CA's in the certificate chain

If any of these conditions are not met, the LDAPS connection will be denied and logged.

Customer Benefits

- Provides increased security for LDAPS authentication.

Support for CA Siteminder R12

SA 7.1 extends authentication support for CA Siteminder Policy Server version R12 SP1. In addition to extending support for this Siteminder version, administrators can also configure options to exclude certain types of client requests from Siteminder session cookie validation.

Customer Benefits

- Supports rollout of CA Siteminder Policy Server R12.
- Periodic client traffic (example: Outlook Web Agent) that the administrator does not want to be considered for the purpose of managing session lifetime (e.g.: idle timeout) can be specified using HTTP methods or URL’s.

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
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

March 2011