JUNIPER NETWORKS PRODUCT BULLETIN

New Features and Functions of Junos Pulse 4.0, Junos Pulse Secure Access Service 7.4, Junos Pulse Access Control Service 4.4

Bulletin Date
February 12, 2013

Bulletin Number
8000023

Applicable to All Regions

Effective Change Date:
February 19, 2013

Introduction

This Product Bulletin describes the new features and functions available in Juniper Networks® Junos® Pulse 4.0, Junos Pulse Secure Access Service 7.4, and Junos Pulse Access Control Service 4.4. It assumes familiarity with Junos Pulse 3.x, Junos Pulse Secure Access Service, and Junos Pulse Access Control Service.

Junos Pulse 4.0 begins to address the requirements of government agencies and security conscious enterprises through support for Federal Information Processing Standard (FIPS), enabling Pulse Secure Access Service and Pulse Access Control Service to address stringent government requirements. Junos Pulse and Junos Pulse Secure Access Service continue to extend their support for IPv6, while continuing to address new and emerging industry standards such as HTML5. They also provide the most secure products for networks by extending support for SNMPv3 into Junos Pulse, Pulse Secure Access Service, and Pulse Access Control Service.

New Features for Junos Pulse 4.0, Junos Pulse Secure Access Service 7.4, and Junos Pulse Access Control Service 4.4

Federal Information Processing Standard (FIPS) 140-2 Level 1 Compliance

Federal Information Processing Standard (FIPS) is a requirement for most software run today by U.S. federal government agencies. FIPS is also a fast growing requirement for many security conscious industries such as financial services. Junos Pulse 4.0 supports FIPS 140-2. (FIPS 140-2 support is currently available for Junos Pulse clients for iOS and Android. Junos Pulse clients for Windows and Mac OS supporting FIPS 140-2 will be available in Q2 2013.)

The FIPS 140-2 standard requires Junos Pulse to use specific cryptographic algorithms approved and implemented by a certified cryptographic module. In addition, there is a requirement to support Suite B transport layer security (RFC 6460), which is implemented in the Transport Layer Security (TLS) 1.2 module.

Juniper Networks Junos Pulse client enables a VPN data channel to be FIPS-compliant, for even more stringent and secure communications. The option to establish a FIPS-compliant VPN data channel is provided by Juniper Networks MAG Series Junos Pulse Gateways running Junos Pulse Secure Access Service or the SA Series SSL VPN Virtual Appliances, once the Junos Pulse client successfully authenticates to the gateway or virtual appliance.

Junos Pulse also enables a layer 3 network connection—such as from Pulse Access Control Service running on a MAG Series gateway or Pulse Access Control Service Virtual Appliances—to be FIPS-compliant, as well as with clientless access (such as captive portal use cases) and in guest user account management (GUAM) scenarios. This addresses the need for FIPS compliance within Juniper Networks Unified Access Control solution as well.

Junos Pulse's FIPS support for mobile operating systems, such as Apple iOS or Google Android, makes use of a third-party, FIPS-certified library offered by SafeLogic (**www.safelogic.com**). The mode can change without shutting down the application, so that Junos Pulse can connect to one Juniper SSL VPN or UAC gateway, or virtual appliance in FIPS mode, and later connect to another Juniper SSL VPN or UAC gateway, or virtual appliance in non-FIPS mode.

FIPS ciphers will be utilized when Junos Pulse, in concert with SSL VPN and/or UAC, is deployed in FIPS mode. Among the ciphers supported are:

- Elliptic Curve Cryptography (ECC), which is a public key cryptosystem, especially useful in mobile (wireless) environments. It is comparable to RSA, offering equivalent security, but with smaller key sizes.
- Digital Signal Algorithm (DSA), the FIPS standard for digital signatures proposed by National Institute of Standards and Technology (NIST), which generates keys in two phases: phase 1, where algorithm parameters are shared between different system users; and phase 2, which computes public and private keys for a single user.

Both ECC and DSA are garnering a great deal of attention in the media and amassing a following in deployment, because they are secure and, at the same time, fast.

Additionally, Junos Pulse FIPS compliance supports Transport Layer Security (TLS) 1.2. TLS 1.2 is an important upgrade for Junos Pulse. TLS 1.2 (defined in RFC 5246) uses SHA-256, an upgrade from MD5-SHA-1. It also enables ciphersuite specific pseudorandom functions (PRFs) and hash algorithms to be used, as well as the ability to specify which hash and signature algorithms will be accepted. TLS 1.2 also supports expansion authenticated encryption ciphers, TLS Extension definitions, and the addition of Advanced Encryption Standards (AES) ciphersuites.

Junos Pulse FIPS supports Suite B cryptography. Suite B cryptography has been selected from cryptography that has been approved by NIST for use by the U.S. Government and specified in NIST standards or recommendations. Suite B Cryptography is formalized in CNSSP-15, National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems (March 2010). CNSSP-15 has been updated to address CIS and Suite B. In addition to AES, Suite B includes cryptographic algorithms for key exchange, digital signatures, and hashing, specifically:

- Encryption—AES-GCM, 128- or 256-bit block cipher
- Key Exchange—Ephemeral Unified Model and One-Pass Diffie Hellman (ECDH)
- Digital Signature—Elliptic Curve Digital Signature Algorithm (ECDSA)
- Hashing—SHA-256 and SHA-384

Suite B also mandates both TLS 1.2 and ECC ciphers.

Also, non-approved algorithms will be disabled when in FIPS mode.

With Juniper's SSL VPN FIPS deployment, Network Time Protocol (NTP) configuration is enhanced to optionally authenticate NTP traffic. An administrator may also choose not to enable NTP authentication. The NTP package for Juniper's SSL VPN has been upgraded to NTPv4, and is backward compatible with both NTPv3 and NTPv2.

HTML5 Support (Phase 1)

Junos Pulse Secure Access Service 7.4 provides support for HTML5 through Rewriter, with new elements, attributes, and APIs.

HTML5 support for Pulse Secure Access Service 7.4 is supported in Microsoft Internet Explorer 10, the latest Mozilla Firefox Extended Support Release (ESR), Apple Safari running on Microsoft Windows 7 and Windows 8, Apple Mac OSX 10.7 and Mac OSX 10.8, Linux Ubuntu, Android 4.0 (Ice Cream Sandwich), and Apple iOS 5.x.

Additionally, support for both audio and video multimedia traffic is available, and without the need for any additional plug-ins.

HTML5 support in Pulse Secure Access Service 7.4 can scale to thousands of users, which remains on a par with the standard support for Rewriter sessions.

Remote Desktop Protocol (RDP) access in Junos Pulse Secure Access Service 7.4 can be delivered over HTML5, via third-party RDP, through a WebSockets translator such as Ericom (www.ericom.com).

IPv6 Support (Phase 1.5)

For enterprise customers who are moving to an IPv6 network, Juniper has enhanced the Layer 3 VPN access method in Junos Pulse and Pulse Secure Access Service. (For more information on IPv6 support in Phase 1, please refer to the New Features Product Bulletin for Junos Pulse 3.1, Junos Pulse Secure Access Service 7.3, and Junos Pulse Access Control Service 4.3.)

Junos Pulse 4.0 and Pulse Secure Access Service 7.4 have been enhanced so that today, end users are now able to access IPv6 resources—along with IPv4 resources—from an IPv4 network, by simply using Junos Pulse to access Junos Pulse Secure Access Service 7.4.

The following describes a use case for this feature:

An enterprise has a number of home-based workers. The home-based workers are from different internal functions and groups, such as sales, engineering, finance, etc. Should home-based workers attempt to access their corporate network using Junos Pulse and Pulse Secure Access Service 7.4, they will still be connecting via an IPv4 network. However, if for additional security the enterprise mandates that home-based engineering workers must access the IPv6 network, it can use this feature to redirect the home-based engineers' traffic to its IPv6 network.

This feature enables customers to direct user traffic to either an IPv4 or IPv6 network, depending on need. In Phase 2, Junos Pulse accessing Pulse Secure Access Service 7.4 is the only method supporting access to IPv6 corporate resources.

The remaining access methods—including Junos Pulse Secure Application Manager (SAM), legacy Network Connect (NC) and Windows SAM, Rewriter, etc.—are not supported in this release. Junos Pulse Access Control Service is also not supported.

All other services, such as authentication, authorization, and accounting (AAA) servers, Domain Name System (DNS) servers, and Host Checker, must be on an IPv4 network.

Junos Pulse Enhancements

The ability to suspend or exit an SSL VPN tunnel set up by Junos Pulse Secure Access Service without losing session context is a feature currently supported in Pulse Secure Access Service's Network Connect, and it has now been added to Junos Pulse 4.0, working with Junos Pulse Secure Access Service 7.4.

Also, an event logging framework has been implemented in Junos Pulse 4.0, which captures operational events and which can be easily reviewed and understood by network administrators. This new event logging system is analogous to the Instant Virtual Extranet event logs that have provided important information about IVE.

More detailed information is usually captured in the debug log file, which can be interpreted by a Juniper support and development engineer. A framework similar to the debug log file is now integrated into the Windows event viewer.

SNMPv3 Support

Junos Pulse 4.0 and Pulse Secure Access Service 7.4 support the Simple Network Management Protocol version 3 (SNMPv3) standard, which provides a comprehensive authentication, authorization, and encryption mechanism, with support for extensions to the framework.

Juniper has chosen to support SNMPv3 to overcome security limitations found in SNMPv2c.

SNMPv3 delivers interoperable, standards-based network management, providing secure access to devices through a combination of authentication and encrypted packets. SNMPv3 provides message integrity by ensuring that a packet has not been modified or changed while in transit; authentication, by ensuring that the message source is valid; and encryption, securing the packet contents from unauthorized viewing. Additionally, SNMPv3 offers security models, and security levels within security models—a two-tiered approach that enables greater security. The combination of security model and security level determines the security means used for the SNMP packet. And, unlike SNMPv2c, which uses a common community string match for authentication, SNMPv3 leverages a username, as well as Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) for authentication. SNMPv3 is also a full Internet standard, as determined by the Internet Engineering Task Force (IETF).

Support for SAML Basic Attribute Profiles

Junos Pulse Secure Access Service (SSL VPN) 7.4 supports SAML Basic Attribute profiles as defined in the SAML standard (http://docs.oasis-open.org/security/saml/v2.0/).

Juniper Secure Access Service may now include SAML Attribute statements as part of the SAML Assertions it generates.

The Basic Attribute Profile specifies simplified naming of SAML attributes together with attribute values based on the built-in XML Schema data types.

A MAG Series Junos Pulse Gateway running Junos Pulse Secure Access Service (SSL VPN) may serve as a SAML Service Provider (SP), and consume a SAML assertion, resulting in a session on the gateway. The MAG Series gateway running Pulse Secure Access Service can obtain attribute data that was received as part of the incoming SAML assertion, and send the attribute data to a backend resource or application as part of a new (or separate) assertion generated by the same MAG Series gateway running Pulse Secure Access Service. The MAG Series gateway running Pulse Secure Access Service will also need to be configured as a SAML Identity Provider (IdP) in this use case to generate and send the new assertion. The new assertion can include attributes retrieved from the SAML assertion that the MAG Series gateway running Pulse Secure Access Service received in as a SAML SP, as well as any additional or new attributes that an administrator would choose to send as part of the assertion that is generated for and sent to a backend resource or application. For new attributes, the attribute-value information can be statically configured by the administrator or dynamically retrieved from an LDAP data store based on user authentication.

There is also a subset of the same use case, where the MAG Series gateway running Pulse Secure Access Service acts as a SAML Identity Provider (IdP), and generates SAML assertions with attribute statements included. The attribute-value may also be statically configured by the administrator or dynamically retrieved from an LDAP data store based on user authentication.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at **www.juniper.net**.

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
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: 31.0.207.125.700
Fax: 31.0.207.125.701

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

8000023-002-EN Mar 2013 Printed on recycled paper