Introduction

This Product Bulletin describes the new features and functions available in the following Juniper products:

- Juniper Networks Junos Pulse 3.0 for Microsoft Windows and Apple Mac OS
- Juniper Networks Junos Pulse 3.2 for Apple iOS and Google Android
- Juniper Networks Junos Pulse Secure Access Service (SSL VPN) 7.2
- Juniper Networks Junos Pulse Access Control Service (UAC) 4.2

This Product Bulletin assumes familiarity with Juniper Networks® Junos® Pulse 1.x and 2.x, as well as familiarity with the Junos Pulse Access Control Service (UAC) and Junos Pulse Secure Access Service (SSL VPN).

Please Note: Unless otherwise indicated, all features in this bulletin are supported on both physical and virtual appliance versions of Juniper Networks SSL VPN (including the Juniper Networks MAG Series Junos Pulse Gateways, SA Series SSL VPN Virtual Appliances, and legacy SA Series SSL VPN Appliances), and Juniper UAC (MAG Series Junos Pulse Gateways running Junos Pulse Access Control Service, or IC Series Unified Access Control Appliances).

New Junos Pulse 3.0 Features for Microsoft Windows and Apple Mac OS

Junos Pulse Secure Access Service (SSL VPN) 7.2 and Junos Pulse Access Control Service (UAC) 4.2 introduce support for Junos Pulse on Apple Mac OS, and enhanced SSL VPN and Unified Access Control/network access control (UAC/NAC) support, respectively, on Microsoft Windows. This section lists the new features introduced in Junos Pulse for Windows and Mac OS.

Junos Pulse for Apple Mac OS X

Junos Pulse for Apple Mac OS X has been designed from the ground up to deliver SSL VPN and UAC features, with an emphasis on simplifying the user experience. Junos Pulse on Mac OS X delivers secure, remote access by enabling users to connect to remote Juniper SSL VPN gateways or virtual appliances. It also delivers LAN and application access control via Juniper UAC gateways. Junos Pulse is supported on Apple Mac OS X 10.6 and newer versions. It extends Junos Pulse support to all major computing platforms, and helps ensure that users can seamlessly and securely access remote and local corporate networks. Junos Pulse on Mac OS X includes the following feature categories (which are also available in Junos Pulse on the Microsoft Windows platform):

- SSL VPN connectivity to all Juniper Networks SSL VPN gateways/appliances—including MAG Series Junos Pulse Gateways running Junos Pulse Secure Access Service, or SA Series SSL VPN Appliances and Virtual Appliances—via Encapsulation Security Payload (ESP) and SSL transport mode
- Layer 3 authentication to all Juniper UAC gateways/appliances—including MAG Series running Junos Pulse Access Control Service or IC Series UAC Appliances—with source IP enforcement
- Host Checker enforcement, supporting the following endpoint integrity checks:
  - Predefined antivirus, personal firewall, and antispyware
  - Process
  - File
  - TCP or UDP port

ESP Transport Mode (Junos Pulse Secure Access Service/SSL VPN)

Junos Pulse 3.0 on Microsoft Windows now includes support for SSL VPN ESP transport mode. UDP-based ESP transport mode provides higher throughput than the TCP-based SSL transport mode. Juniper’s dual-transport Junos Pulse client will attempt to establish the VPN tunnel over ESP transport mode by default. If this is unsuccessful, Junos Pulse will automatically attempt to set up the tunnel over SSL. A newly introduced administrative option in Pulse Secure Access Service (SSL VPN) 7.2 allows administrators to prevent the failover from ESP to SSL transport mode. If the administrator option is enabled, Junos Pulse attempts to connect only via the ESP transport mode.
Windows Only

schedule a meeting from one of the configured meeting servers. Users who are connected to a Juniper SSL VPN or UAC gateway may simply right-click on the Junos Pulse icon in their Windows taskbar to start or schedule a meeting from one of the configured meeting servers.

Credentialed Provider (for Microsoft Windows Only)

Junos Pulse 3.0 on Microsoft Windows supports Credentialed Provider for Windows Vista and Windows 7. It provides a mechanism for establishing a network tunnel upon login to the Windows device, ensuring corporate network connectivity during critical login processes. The Junos Pulse Credentialed Provider has been implemented as a Pre-Logon Access Provider (PLAP). Junos Pulse provides Credentialed Provider support for remote SSL VPN access, as well as for Layer 3 Juniper UAC access; however, Junos Pulse 3.0 does not provide Credentialed Provider support for 802.1X based connections.

Machine Authentication (for Microsoft Windows Only)

Junos Pulse 3.0 on Microsoft Windows supports machine-based authentication to a corporate network for both remote Juniper SSL VPN access as well as Layer 3 Juniper UAC access. It allows a corporate connection to be established based on the machine’s credentials instead of the user’s credentials, making it suitable for device-only network connectivity. Junos Pulse provides machine authentication support for remote Juniper SSL VPN access as well as for Layer 3 Juniper UAC access; however, Junos Pulse 3.0 does not support machine authentication for 802.1X based connections.

Session Extension

Junos Pulse 3.0 for Windows and Mac OS enables users to extend their current authenticated sessions prior to expiration of their existing sessions. Administrators can configure this optional feature on gateways running either Juniper SSL VPN or UAC. When enabled, this feature can be configured to display a session expiry warning dialog at a predefined time interval prior to a session’s expiration; or, allow users to extend their sessions manually by selecting a menu option in the Junos Pulse user interface. For each of these two options, Junos Pulse will prompt the user for valid credentials. Once authenticated, the user’s session is extended for a time period corresponding to the session time-out configured on the appropriate gateway.

Single Click Collaboration (for Microsoft Windows Only)

Junos Pulse 3.0 for Windows enables users to schedule and establish a Junos Pulse Collaboration meeting. Users who are connected to a Juniper SSL VPN or UAC gateway may simply right-click on the Junos Pulse icon in their Windows taskbar to start or schedule a meeting from one of the configured meeting servers.

New Junos Pulse 3.2 Features for Apple iOS and Google Android

Junos Pulse Secure Access Service (SSL VPN) 7.2 and Junos Pulse Access Control Service (UAC) 4.2 introduce support for new capabilities on the Apple iOS and Google Android mobile operating platforms. This section lists only the new features introduced in Junos Pulse for iOS and Android.

Host Checker for iOS and Android

Pulse Secure Access Service (SSL VPN) 7.2 and Pulse Access Control Service (UAC) 4.2 deliver Host Checker support for Apple iOS and Google Android mobile devices. This feature enables customers to restrict or prohibit SSL VPN or UAC/NAC access from devices that are not compliant with centrally-defined corporate security and access policies. This extends the endpoint integrity checks already offered on Windows and Macintosh platforms to iOS and Android platforms, which are now used widely in corporate environments. The security and access policies specific to iOS and Android include:

- **Version Restrictions:** Administrators can configure a Host Checker policy which limits VPN or UAC/NAC access to only iOS and Android mobile devices running specific mobile OS versions. For example, an administrator could decide to allow only Apple devices running iOS version 3.2 or higher; or devices running only Android 2.3.3 and higher. This enables organizations to ensure that only the latest, most secure versions of iOS and Android are running on mobile devices granted network access.

- **Jail-broken or Rooted Device Detection:** An administrator can configure a Host Checker policy preventing VPN or local network access from jail-broken iOS devices or rooted Android devices. Jail-breaking and rooting refer to a process whereby a user may gain privileged access on an iOS or Android device, respectively, bypassing restrictions imposed by the device manufacturer and carrier. Since jail-broken iOS devices and rooted Android devices are more prone to threats and malware exploit than non-jail-broken or non–rooted devices, organizations can protect their network from potential exploits by ensuring that only non-jail-broken iOS and non-rooted Android devices are granted network access.

- **Enforcement of the Junos Pulse Mobile Security Suite:** An administrator can configure a Host Checker policy enforcing the enablement of Junos Pulse Mobile Security Suite on the iOS or Android mobile device prior to granting the device remote or local network access. Pulse Mobile Security Suite is an additional product in the Junos Pulse mobility solution. It delivers on-device mobile security (such as anti-malware), mobile device management (including policy provisioning, remote alert/locate/track/lock/wipe, and backup and restore), and application control. With this policy enabled, iOS or Android mobile device users will not be able to gain access to the corporate network and resources without first enabling Junos Pulse Mobile Security Suite.
to protect and manage their mobile device. This feature ensures that iOS and Android devices attempting network, cloud, and application access, regardless if remote or local, are free of any potential malware exploits at access, and/or the device and its applications can be managed, and remain so throughout current and subsequent VPN sessions.

Full Layer 3 SSL VPN Access for Android 4.0
Junos Pulse 3.2 supports full SSL VPN tunneling on smartphones and tablets running Android 4.0, a.k.a. Ice Cream Sandwich (ICS). With Junos Pulse 3.2, users of devices running Android 4.0 are able to access their corporate network securely over an SSL VPN tunnel and have access to any areas of the organization’s network and applications to which they are authorized. This feature and these capabilities are available on all Android 4.0 enabled devices, regardless of vendor type or carrier. (Junos Pulse 3.2 for Android will also continue to support full VPN on pre-4.0 Samsung and Lenovo Android devices.) An administrator can configure policies on the SSL VPN gateway to allow specific roles for users to enable full VPN access and capabilities. When Junos Pulse connects to MAG Series Junos Pulse Gateways running Pulse Secure Access Service, or SA Series SSL VPN Appliances and Virtual Appliances, it determines the kind and level of access for which the user is authorized, and automatically enables the appropriate kind and form of network access. If full VPN access is enabled for a user by an administrator, the user’s device is assigned an IP Address, and all mobile apps running on the device are enabled to reach resources within the corporate network, as necessary.

If an administrator has enabled Core Access for the user’s assigned role and not full VPN access, then only a web SSL session is established between the user’s Android device and the Juniper SSL VPN gateway/appliance. In this case, only web-based applications are delivered over the SSL session through the SSL VPN gateway/appliance, preventing access to other apps from the user’s device.

Junos Pulse Collaboration (for Apple iOS Only)
Junos Pulse 3.2 allows Apple iPad and iPhone users to join online meetings “on the go” from anywhere, over any network, providing a simple, low-cost alternative for ad hoc, day-to-day online meetings—without having to pay a premium for rarely used advanced capabilities. Apple iPad and iPhone users can click on a link in their meeting invitation to join meetings via Junos Pulse Collaboration, view shared media, and actively chat with other meeting attendees. Shared content can be viewed in portrait or landscape mode, all with fully supported “pinch zoom” capability. The Chat feature allows participants to engage in a group conversation, or a private, one-on-one chat. Apple iPhone users can use the Dial option to view the teleconference details, and dial into an audio bridge (using the native phone application) from Junos Pulse*. The Meeting Info option allows attendees to not only view meeting details, but also forward those details to other parties via their e-mail client.

*Please Note: Devices on some carrier networks may not allow the use of data and voice at the same time. In those cases, users will lose the data connection if they dial into the audio bridge using the native phone application (carrier voice). These users will have to connect back to the meeting after disconnecting from the voice call.

Enhanced Programmability from Other Apps (for Apple iOS only)
Junos Pulse 3.2 for Apple iOS now provides an enhanced “junospulse:// URL” scheme for use when invoking Junos Pulse programmatically from other applications. This feature enhances Junos Pulse in the following ways:

• Allows the user to specify several parameters, including the Username, Realm, and Role when creating VPN configurations in Junos Pulse
• Uses the parameter values from the current VPN configuration to auto-fill login pages during web-based login
• Allows third-party applications to specify the parameters in “junospulse:// URL”, and use them to auto-fill login pages during login

The VPN configuration on iOS includes the following parameters:

• Server Address
• Username
• Password
• Realm
• Role
• Certificate

In previous versions, Junos Pulse for Apple iOS only allowed a user to specify the Server Address and Certificate. All other parameters were ignored if a VPN configuration was created using the iPhone Configuration Utility, or mobile device management (MDM) was used.

Please Note: The password field is only used when Junos Pulse is invoked via the “junospulse:// URL” scheme. The password value thus used is not saved anywhere on the iPhone file system. Even if the password value is set in a VPN configuration received from the iPhone Configuration Utility or MDM, it will not be used to establish a VPN connection.

New Juniper Networks Junos Pulse Secure Access Service (SSL VPN) 7.2 Features
Host Checker for Apple iOS and Google Android Devices
Please refer to the “Host Checker for iOS and Android” entry under the “New Junos Pulse 3.2 Features for Apple iOS and Google Android” section of this bulletin.

Cloud/Web Single Sign-On (SSO) via SAML
New in Junos Pulse Secure Access Service (SSL VPN) 7.2 is support for Security Assertion Markup Language (SAML) 2.0 that allows enterprises to easily and securely federate user identity with third-party Web applications, including cloud-based Software-as-a-Service (SaaS) applications such as Salesforce.com or Google Apps. Two options are available:

• Service Provider-Initiated SSO via SAML 2.0: When a user attempts to access a service provider resource protected by SAML (such as Salesforce.com or Google Apps), since the user is not authenticated on the service provider site, the service provider can transparently redirect the user to the Juniper SSL VPN gateway, which acts as the SAML IdP (Identity Provider). Once authenticated to the Juniper SSL VPN via the corporate enforced
authentication, the user's browser is redirected to the service provider resource, providing seamless SSO access. Enterprises can now provide simple and transparent SSO to cloud-based applications for remote users, while still enforcing standard corporate authentication and authorization policies configured on Juniper SSL VPN for applications hosted in the cloud.

- **Leveraging Existing Junos Pulse or Network Connect VPN Sessions:** When this unique option is enabled, the Juniper SSL VPN gateway (acting as the SAML IdP) checks for an existing Network Connect or Junos Pulse session when it receives a SAML request from a service provider resource. If the user is already connected via Network Connect or Junos Pulse, the Juniper SSL VPN gateway generates an SAML assertion (including Authentication Statements to the service provider resource), automatically authenticating the user. After the user has logged into Junos Pulse or Network Connect (SSO), the user will not be required to login again to any Web application that has been set up to work with this feature on the Juniper SSL VPN gateway.

**Junos Pulse Collaboration (for Microsoft Windows and Apple iOS)**

The Junos Pulse Collaboration service license option in Pulse Secure Access Service (SSL VPN) 7.2 includes a newly designed user interface for Windows users (Microsoft Windows XP, Windows Vista, and Windows 7), as well as increased scale. (User interfaces for Apple Mac OS and Linux continue to leverage the compatible, legacy Secure Meeting UI, renamed Junos Pulse Collaboration.) Pulse Collaboration allows organizations to enable their users to participate in meetings and collaborate anytime, anywhere, on-the-go regardless of their device, through a cost-effective online meeting, collaboration, and remote desktop sharing solution suitable for the majority of online meetings conducted by a typical enterprise.

For further information on Junos Pulse Collaboration for Apple iPad and iPhone, please refer to the “Junos Pulse Collaboration (for Apple iOS only)” entry under the “New Junos Pulse 3.2 Features for Apple iOS and Google Android” section of this bulletin.

The Juniper Networks MAG6610 and MAG6611 Junos Pulse Gateways running SM-360 service modules can now support up to 1,000 concurrent collaboration users, or 2,000 in a cluster. New 500 and 1,000 collaboration user license SKUs are also available. IT administrators can now offer a simple, secure, and cost-effective online meeting, collaboration, and remote desktop sharing application for their users. In addition, a plug-in for Microsoft Outlook 2007/2010 is now available, with iCal invitation capability that integrates with the calendar functionality on e-mail clients.

*Please Note: Devices on some carrier networks may not allow the user to use data and voice at the same time. In those cases, the user will lose the data connection if they dial into the audio bridge using the native phone application (carrier voice). These users will have to connect back to the meeting after disconnecting from the voice call.**

**Host Checker Enhancements**

Junos Pulse Secure Access Service (SSL VPN) 7.2 introduces several new ease of use enhancements for Juniper’s Host Checker. These enhancements increase the Quality of Experience for both end users and administrators, and also save administrative time and energy. The new features include:

- **Show Host Checker Progress:** Users can now see that Host Checker is progressing with its download in the background. This is particularly useful for situations where policy evaluation takes longer than a few seconds. This feature is only supported in Host Checker when running on Microsoft Windows based devices, as longer policy evaluations are typically encountered in more complex Windows policies.
- **Reconfigure Virus Definition Checks:** Host Checker now provides the ability to reconfigure the number of days for a virus definitions check and increase the support for the maximum number of updates to 20, allowing customers to create flexible policies for antivirus software signature updates published frequently.
- **Host Checker Status in Existing Active Users Table:** This feature presents the administrator details of the security policies and role mapping status for all active users on the Active Users page within Pulse Secure Access Service (SSL VPN) 7.2 and Pulse Access Control Service (UAC) 4.2.

**Support for Customized Variables**

Juniper Networks SSL VPN gateways/appliances support a standard set of system variables that can be used in role mapping rules, resource policy rules, and SSO parameter fields. In some use cases, however, these variables may need to be manipulated in order to accommodate the requirements of other devices and cloud services. Pulse Secure Access Service (SSL VPN) 7.2 allows administrators to specify Regular Expressions (Reg-Ex) on system variables to create new, custom variables. A set of predefined Reg-Ex macros are also provided.

Federal Agency Smart Credential Number (FASC-N) attributes, which are data objects in a Personal Identification Verification (PIV) card that uniquely identify the credential holder in user X509 certificates, are also now supported through a new set of system variables. These variables are used just as any other system variable.

**Support for 64-bit Secure Virtual Workspace (SVW) and 64-bit Internet Explorer Browsers**

Junos Pulse Secure Access Service (SSL VPN) 7.2 now includes support for 64-bit Internet Explorer 8 and 9 browsers, as well as support for Secure Virtual Workspace (SVW) on 64-bit Windows workstations.

**Silverlight Support for SharePoint, Office Web Apps, and Outlook Web Access**

Microsoft Silverlight widgets are commonly used within Microsoft SharePoint to upload documents or play video files created with Silverlight technology. Beginning with Junos Pulse Secure Access Service (SSL VPN) 7.2, these widgets can now be accessed through the SSL VPN Rewriter, allowing remote users to access the Silverlight widgets that are enabled on the SharePoint site. Silverlight is also now supported within Microsoft Office Web Apps and Outlook Web Access 2010, in which Silverlight is used for functions such as adding attachments to e-mails.
Access to Lotus Connections Through Rewriter
Pulse Secure Access Service (SSL VPN) 7.2 includes full qualification of Lotus Connections 2.5 and 3.0 through the SSL VPN Rewriter, which enables remote users to access Lotus Connections through a browser SSL connection.

User Record Synchronization (URS) Scheduled Backup
User Record Synchronization (URS) allows personal user bookmarks to be synchronized across all MAG Series gateways running Junos Pulse Secure Access Service (SSL VPN) 7.2, or SA Series SSL VPN Appliances and Virtual Appliances running SSL VPN 7.2, even when the gateways/appliances are not in a cluster. The integrity and availability of bookmarks has become critical for today's workforce; the URS capability assures that databases can be securely backed up, fully restored/imported, and archived to FTP and SCP servers using the standard archiving interface. The user database is now synchronized with user login credentials. This provides greater flexibility in backup and restore operations, and greater database security and privacy.

Virtual Appliance Service Provider Edition (SPE) Rapid Deployment
The SA Series SSL VPN Virtual Appliances, Service Provider Edition (VA-SPE), previously offered configuration scripts to aid in initial provisioning actions required to activate each system on VMware ESX through the VMware Console feature. With the newer ESXi hypervisor, however, the VMware Console feature is no longer available. The rapid provisioning feature of the SA Series Virtual Appliances Service Provider Edition has now been adapted to work with the OVFTool application. The entire configuration of the SA Series SPE Virtual Appliance can be scripted, with better performance achieved through the VMXNET2 driver. Rapid deployment functionality is no longer dependent on the VMware Service Console nor the Juniper Serial Console.

License Server Auto Leasing (a.k.a. Trust but Verify)
If a centralized license server should ever become unavailable, any gateways or appliances that require expanded capacity (subscription licenses meeting required minimum reserves) need to be able to work without interruption. With Pulse Secure Access Service (SSL VPN) 7.2, licensing clients can now auto-lease and expand their capacity on their own (Trust), with reconciliation occurring once connectivity to the license server has been restored (Verify). This feature enables a single license server to serve global organizations of any size with built-in resiliency to withstand prolonged connectivity issues. Detailed event logs provide history and tracking of centralized license server connectivity issues.

Traffic Segregation (SA Series Virtual Appliances)
In SSL VPN 7.2, authentication, authorization, and accounting (AAA) services such as Domain Name System (DNS), system logging, Device Management Interface (DMI), Lightweight Directory Access Protocol (LDAP), and RADIUS can now be placed on the management network or the subscriber's network, providing greater flexibility for SA Series SSL VPN Virtual Appliances in complex service provider networks. Also, it enables virtual ports on the administrative network to be assigned for service provider administrator logons.

Customized Landing Pages for Tablets
New in Junos Pulse Secure Access Service (SSL VPN) 7.2 is the ability to provide remote users of Apple iPads, Android tablets, and other tablets with a landing page that is customized to the size and screen resolution for the tablets (as opposed to smartphones), including the ability to display information such as Web bookmarks and VPN launching options. If the administrator enables a VPN button to be displayed and active, tapping it will launch a full VPN session through Junos Pulse on Apple iPads, Samsung Galaxy Tabs, and appropriate Android 4.0 (ICS)-based tablets, delivering an improved user experience based on the device's size, screen resolution, and other tablet nuances.

Customization of FIPS Options for Network Connect
A new administrative option in Juniper Networks SA4500 FIPS and SA6500 FIPS SSL VPN Appliances allows the FIPS mode in Network Connect to be enabled or disabled, with "enabled" being the default state. Previously, Network Connect functioned only in FIPS mode when connected to SA Series FIPS appliances. When FIPS mode in Network Connect is disabled, Network Connect will attempt to connect via ESP transport mode by default. When FIPS mode is enabled, Network Connect connects only via SSL transport mode. When FIPS mode is disabled, Network Connect will connect successfully to a FIPS appliance with a certificate chain that rolls up to a private certificate authority (CA), which is not deployed as a trusted certificate to the end user's device. In FIPS mode, however, Network Connect will reject such an untrusted certificate chain and prevent VPN access to the FIPS appliance. This capability provides users with flexibility in connecting to FIPS appliances from unmanaged devices like home PCs or Mac OS devices.

New Junos Pulse Access Control Service (UAC) 4.2 Features

Common Features
The following features, as previously covered in the Junos Pulse Secure Access Service section of this document, also apply to the Junos Pulse Access Control Service:
• Host Checker for Apple iOS and Google Android devices
• Host Checker enhancements
• Microsoft Credential Provider support

802.1X Support for Apple iOS and Google Android Operating Platforms
With Junos Pulse Access Control Service (UAC) 4.2, customers may now leverage Juniper UAC’s 802.1X support to deliver secure, identity-based network and application access control, leveraging the native 802.1X supplicants available on all Apple iOS and Google Android based mobile devices.

Captive Portal/Layer 3 Enforcement for Apple iOS and Google Android
In a prior Junos Pulse Access Control Service (UAC) release, the “Allow VPN through Firewall” feature was introduced. When enabled, Microsoft Windows, Apple Mac OS/X, and other computing device users can launch a browser, authenticate to Juniper UAC (MAG Series Junos Pulse Gateway running Junos Pulse Access Control Service, or IC Series Unified Access Control Appliances), and access resources protected by Juniper Networks ScreenOS® software on Juniper firewalls and/or SRX Series...
Services Gateways. Once the user has been authenticated, they no longer need to keep the browser page open to maintain a “heartbeat” with the backend Juniper UAC gateway/appliance. With Junos Pulse Access Control Service (UAC) 4.2, iOS and Android users can authenticate to the Juniper UAC gateway/appliance via captive portal. Pulse Access Control Service (UAC) 4.2 will authenticate the user, and push network resource access policies to the Juniper firewall(s) based on the mobile device user’s role.

Host Checker for Apple iOS and Google Android Devices

Please refer to the “Host Checker for iOS and Android” entry under the “New Junos Pulse 3.2 Features for Apple iOS and Google Android” section of this product bulletin.

Junos Pulse Access Control Service (UAC)—SRX Series Services Gateways Enhancements

Junos Pulse Access Control Service (UAC) 4.2 goes further to integrate identity-based access control with/within the SRX Series Services Gateways, introducing several new features:

User-Role Based AppSecure Policies

With Junos Pulse Access Control Service (UAC) 4.2 and Junos OS 12.1, administrators can configure application-aware firewall policies based on the Juniper UAC role of an authenticated user. The ability to configure application-aware firewall policies based on an authenticated user’s role empowers deployed SRX Series gateways to utilize the user’s role information in the application of granular polices for application access based on a specific user’s identity. This feature allows for the creation and deployment of identity enabled, application-aware firewall policies, delivering finer access control granularity.

No Agent or Reauthentication via Captive Portal Required

With Junos Pulse Access Control Service (UAC) 4.2 and Junos OS 12.1, any user who is authenticated to a Microsoft Active Directory (AD) domain can be silently provisioned to SRX Series gateways via Juniper UAC. Juniper UAC queries AD, acquires group membership information, and maps the user to a specific role before pushing any resource access policies to the SRX Series gateways. The entire process is completely transparent to the user. Users no longer need to launch a Web browser and reauthenticate to Juniper UAC (MAG Series gateways or IC Series appliances). This feature enables dynamic, identity-focused, role-based firewalls without user interaction.

Coordinated Threat Control with Branch SRX Series Gateways

Previous versions of Juniper UAC have supported Coordinated Threat Control with the standalone Juniper Networks IDP Series Intrusion Detection and Prevention Appliances, ScreenOS firewalls, and the high-end SRX Series gateways, specifically the Juniper Networks SRX3400, SRX3600, SRX5600, and SRX5800 Services Gateways. Junos Pulse Access Control Service (UAC) 4.2 now introduces support for CTC with the branch SRX Series gateways, specifically the Juniper Networks SRX100, SRX110, SRX210, SRX220, SRX240, and SRX650 Services Gateways. This feature allows the branch SRX Series gateways to send alerts to Pulse Access Control Service (UAC) if any attack or anomalous behavior is discovered emanating from user traffic. After receiving an alert of a potential or actual attack from the branch SRX Series gateway, Juniper UAC will take action based on established corporate policies that have been configured in Juniper UAC devices. Possible response actions can include the ability to quarantine the user/device, terminate a session, and prohibit follow-on authentications until an administrator manually allows reauthentication. This feature addresses potential insider threats in branch environments at the user/device level, halting attacks before they can propagate or multiply.

802.1X Support on Branch SRX Series

Junos Pulse Access Control Service (UAC) 4.2 supports branch SRX Series gateways (SRX100, SRX110, SRX210, SRX220, SRX240, and SRX650) as 802.1X RADIUS clients in a Juniper UAC environment. It also allows the branch SRX Series gateways to configure Juniper UAC as a RADIUS server. Once a user’s device has been authenticated via 802.1X, the switch port on the branch SRX Series gateway is open, allowing the user and device access to the network. This feature saves costs, as well as addresses 802.1X support for the branch domain.

Please Note: There are several limitations with the SRX100 gateway in this scenario. Not supported on the SRX100 gateway with Pulse Access Control Service (UAC) 4.2 are Dynamic VLAN Assignment, Guest VLAN, RADIUS Server Failure Feedback, and VoIP VLAN.

Transparent Mode Support

SRX Series gateways can be deployed in transparent mode with Junos Pulse Access Control Service (UAC) 4.2. Organizations can use SRX Series gateways simply as a Layer 3 enforcement point with Juniper UAC, enabling the SRX Series gateway in transparent mode to simply act as a “bump on the wire”. Operating SRX Series gateways in transparent mode with Juniper UAC eliminates the need for organizations to change the routing topology of their current network environment.

Junos Pulse Access Control Service (UAC)—EX Series Ethernet Switches Enhancements

Junos Pulse Access Control Service (UAC) 4.2 delivers and demonstrates tighter integration with the Juniper Networks EX Series Ethernet Switches. While continuing to provide support for third-party switches via standards-based 802.1X, these additional integrations and enhancements deliver additional value to Juniper UAC and EX Series customers. Among the features and functions being introduced in Pulse Access Control Service (UAC) 4.2 with EX Series switches are:

- Policy Orchestration and Dynamic Access Control List (ACL) Provisioning

This feature allows customers to manage all security and access control policies from a centralized policy server—Juniper UAC (MAG Series or IC Series), saving time and cost. Junos Pulse Access Control Service (UAC) 4.2 and Junos OS 12.2 enable EX Series switches to work as policy enforcement points (PEPs) in the Juniper UAC solution. At the time Juniper UAC and EX Series connect, Juniper UAC will push a role table and resource access policies to EX Series switches. Whenever an endpoint completes 802.1X or media access control (MAC) authentication, Juniper UAC will push down an authorization table entry to the EX Series switches. The EX Series switches in return will dynamically provision an access control list (ACL) to the switch port.
that particular device. This alleviates the need for corporate administrators to create hundreds of ACLs statically on individual switches, saving administrative time and expense. The Juniper UAC/EX Series integration follows the same model as the dynamic access control model that has been available with Juniper UAC and SRX Series gateways. EX Series switches connect to Juniper UAC in the same manner as SRX Series gateways and ScreenOS firewalls, with resource access policies expressed in terms of IP address ranges and MAC address lists, based on the user roles, with different actions such as “deny” or “allow.”

• Centralized Web Authentication

Junos Pulse Access Control Service (UAC) 4.2 and Junos OS 12.2 allow Web authentication to be managed from a single central policy server, saving time and cost. When users connect to an EX Series switch port that has been enabled for Web authentication and automatically launch a browser, the EX Series switch will perform a URL redirect to Juniper UAC (MAG Series or IC Series). In turn, Juniper UAC will return a captive portal authentication page to the user.

• EX Series Universal Port Support

When users connect to an EX Series switch port, they will go through an 802.1X process, with the Juniper UAC gateway/appliance (MAG Series or IC Series) acting as a RADIUS server. If the 802.1X authentication fails, the EX Series switch port falls back to MAC authentication with optional captive portal, depending on the MAC authentication policy. If the endpoint never sends HTTP traffic through port 80, the endpoint gains access based on MAC authentication policies. If the endpoint later sends HTTP traffic through port 80, a captive portal redirect will be used to reauthorize the port. Administrators no longer need to pre-provision ports to be dedicated for a specific purpose. Instead, all ports are configured with a shared policy, and the Juniper UAC/EX Series solution tailors authentication and access to whatever or whoever is attaching to the port, significantly increasing ease of usability and simplifying IT administration.

Host Checker for Apple Mac OS/X Devices

Junos Pulse Access Control Service (UAC) 4.2 introduces a version of Host Checker that now supports predefined security policies for Apple Macintosh platforms running Apple Mac OS/X through Junos Pulse, Juniper Networks Odyssey Access Client, and with clientless Juniper UAC deployments.

The following is an initial list of the Apple Mac OS/X security software categories, vendors, and products that are supported as part of this new Host Checker release:

### Antivirus products:

<table>
<thead>
<tr>
<th>Vendors</th>
<th>Host Check</th>
<th>Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Check RTP</td>
<td>Last Scan Time</td>
</tr>
<tr>
<td>ALWIL</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Software</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>ClamWin</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Computer Associates</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Eset</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Software</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Intego</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Kaspersky Labs</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>McAfee</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>PC Tools Software</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>SoftWin</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Sophos</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Symantec</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Trend Micro</td>
<td>√</td>
<td>√</td>
</tr>
</tbody>
</table>

### Personal firewall products:

<table>
<thead>
<tr>
<th>Vendors</th>
<th>Host Check</th>
<th>Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Is Firewall enabled?</td>
<td>Enable Firewall?</td>
</tr>
<tr>
<td>Apple Built-in Firewall</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Brian Hill</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>FreeBSD</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Haynet.com</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Intego</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Objective Development</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Open Door Networks</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Symantec</td>
<td>√</td>
<td></td>
</tr>
</tbody>
</table>

### Antispyware products:

Please Note: Since remediation is not supported for standalone antispyware products for Apple Mac OS, the following table does not have a column for Remediation.

<table>
<thead>
<tr>
<th>Vendors</th>
<th>Host Check (Check RTP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecureMac.com</td>
<td></td>
</tr>
<tr>
<td>Trend Micro</td>
<td>√</td>
</tr>
</tbody>
</table>
Host Checker Enhancements
For more information, please refer to the “Host Checker Enhancements” section of the “New Juniper Networks Junos Pulse Secure Access/SSL VPN 7.2 Features” section in this product bulletin.

Junos Pulse Support for Apple Mac OS/X Through Layer 3 Source IP Enforcement
Junos Pulse 3.0 now supports Apple Mac OS/X, provisioning endpoint access through Junos Pulse Access Control Service (UAC) and monitoring Apple Macintosh device posture assessment (via Juniper’s Host Checker). As with Junos Pulse running on Microsoft Windows-based devices, Junos Pulse 3.0 running on Mac OS/X-enabled devices consists of multiple modules (including Juniper Networks SSL VPN gateways/appliances). This reduces the deployment footprint by only implementing the components necessary to meet the networking needs of the endpoint, significantly increasing usability and simplifying IT administration.

Enterprise Guest Access License (for MAG4610, MAG6610, and MAG6611)
With previous releases of Juniper UAC, the Enterprise Guest Access license was only supported on the MAG2600 platform. Now, with Junos Pulse Access Control Service (UAC) 4.2, the Enterprise Guest Access license has been extended to support the MAG4610, MAG6610, and MAG6611 platforms. When the Enterprise Guest Access license is installed, customers can provision up to 200 concurrent guest users per platform. The concurrent guest users will be authenticated and resource access policies enforced natively in the platform without requiring any additional enforcement points, delivering fast, secure guest access from any MAG Series platform, and serving as an inline, all-in-one guest access policy server and enforcement point.

Junos Pulse Access Control Service (UAC) 4.2 on MAG2600
Previously, the MAG2600 platform only supported Enterprise Guest Access licenses. In Pulse Access Control Service (UAC) 4.2, the MAG2600 platform may be deployed as a complete Juniper UAC (NAC) appliance, with up to 200 concurrent user licenses, addressing network access control for small-to-medium sized businesses (SMBs), branches, or for small segments of larger enterprises.

Guest User Account Manager (GUAM) Enhancements
Both Junos Pulse Access Control Service (UAC) and Enterprise Guest Access solutions enable a Guest User Account Manager (GUAM) to create temporary guest user accounts. These guest user accounts are typically valid for a number of hours or days, allowing guest users to access the network for the specified time period. Two enhancements to GUAM that are new in Junos Pulse Access Control Service (UAC) 4.2 are:

- **Bulk guest user account creation**: Bulk account creation is useful when a nontechnical GUAM, such as an administrator or receptionist, must create a large number of guest user accounts. For example, if a corporation is expecting over 50 visitors for an open house the following day, it is much more efficient for a nontechnical GUAM to create the necessary guest access accounts a day earlier in bulk than to create them one at a time the day of the visit.

- **Guest user credentials via e-mail**: The ability to send guest user credentials via e-mail to an expected guest user simplifies guest account creation. The Juniper UAC Admin UI has a section for configuring the SMTP server and format of the guest user e-mail. Once this configuration is complete and the e-mail feature has been enabled by a corporate administrator, the option to send guest user credentials via e-mail to guests is available in the new/edit guest user page, alongside the Print option.

Management Interface Support (IC6500, IC6500 FIPS, MAG Series Junos Pulse Gateways)
The physical management port present in the MAG Series gateways, as well as the Juniper Networks IC6500 Unified Access Control Appliance and/or IC6500FIPS Unified Access Control Appliance (previously was not enabled), has now been enabled in software as part of the Pulse Access Control Service (UAC) 4.2 release. With the management port enabled, customers may now:

- Push Juniper UAC specific data to the Chassis Management Card (for MAG6610 and MAG6611) instead of using the internal port
- Push outbound traffic for SNMP, Network Time Protocol (NTP), push-config, archiving, system logging, and DMI services
- Allow administrators to login through the management port

The now operational management port allows an administrator to configure the port for use on a management network.

SQL as External Authentication Server
Customers may now utilize an existing Oracle user database as an authentication database with Junos Pulse Access Control Service (UAC) 4.2. This feature provides access only to Oracle databases through the Oracle Instant Client, and allows customers to create custom SELECT and EXECUTE SQL statements in order to access an existing database to retrieve information on various user attributes, including passwords. The feature supports multiple password formats: clear text, Message Digest 4 (MD4) hash, Secure Hash Algorithm 1 (SHA1)+Base64 hash, and salted SHA1+Base64 hash. Attributes returned by the SQL server can be used to make role mapping decisions, as well as RADIUS return attributes. The SQL server can be configured as either an authentication server or as a directory/attribute server for realm configuration, extending authentication support while saving administrative time and cost.

Support for 64-bit xSec FIPS in Odyssey Access Client
Prior to this release, OAC only supported a 32-bit FIPS module. But with Junos Pulse Access Control Service (UAC) 4.2, OAC FIPS now supports 64-bit xSec FIPS. xSec is a cryptographically secure Layer 2 tunneling network protocol with associated attribute negotiation and key agreement. xSec is used by U.S. government agencies, and thus requires the OAC FIPS module for encryption.

Enhanced User Messaging via Junos Pulse Client—Access Rejected by Firewall
Junos Pulse Access Control Service (UAC) policy may permit or drop user traffic based on the user role. When a user’s access has been denied, the client may be in a delay for a long period of time, causing user frustration. The long delay is due to the Juniper firewall acting as a Juniper UAC enforcement point—dropping traffic, which follows Juniper UAC policy. This feature introduces a new policy action called “Reject” which will deny user traffic and send a TCP RST back to the user.
Support for Active Directory (AD) 2008r2 and Machine Authentication via MSCHAPv2 and PEAP-MSCHAPv2

Junos Pulse Access Control Service (UAC) 4.2 introduces support for Active Directory (AD) 2008r2, in addition to previously supported AD 2003 and AD 2008r1 servers. Pulse Access Control Service (UAC) 4.2 also adds support for machine authentications via Challenge Handshake Authentication Protocol (MSCHAPv2) and Windows native supplicants via Protected Extensible Authentication Protocol (PEAP-MSCHAPv2).

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.