Pulse Secure®

White Paper

POLICY SECURE FOR UNIFIED ACCESS CONTROL

Enabling Identity, Role, and Device-Based Access Control in a Simply Connected Network

Table of Contents

Executive Summary

In today's dynamic and digitally connected world, users should have the freedom and the flexibility that businesses need to innovate and survive in the next-generation workplace. At the same time, technology leaders need to be able to operate their high-performance networks cost-effectively and keep them secure. Bring Your Own Device (BYOD) means that for the first time enterprise IT managers are being tasked with attempting to provide and enforce differentiated granular access control for end users connecting from non-corporate devices. Providing security in this mobile environment goes beyond simply securing network traffic—the security solution must provide differentiated network access based on policy and a combination of the user's identity, role, location, device type, and device integrity, for example. And, it must perform all of these activities quickly, transparently, and economically.

Although the transition to a mobile network presents challenges, it also offers an opportunity for businesses to streamline and simplify their network, improve employee productivity, and reduce operational costs and risk. Pulse Secure enables identity-, role-, and device-based access control in a Simply Connected network. Whether you want to unify your wired and wireless network or optimize your Juniper deployment, the Pulse Secure solution will enable your move to the mobile network. . Juniper's unified security and policy control "simply connects" as it protects and manages users, their devices, and their access from any device, anywhere.

Introduction

Today's enterprise has changed in ways that could not have been foreseen just a decade ago. The enterprise network evolved over the past decades based largely upon the specific tasks it was created to support. Advances in networking were typically led by particular applications or specific, repeatable use patterns. If the networks were considered "plumbing," the users, applications, and data were expected to flow where the pipes had been laid. The corporate LAN, for example, is where most users converged and where the highest bandwidth applications were used. Network performance, as expected, was optimal at corporate HQ.

Performance was lower in branch or remote locations, since a smaller percentage of users were located there. Mobile users, even so-called "road warriors," could only expect "best effort" network access when remote, because it was impossible to create or enforce any kind of standardized throughput. Brick and mortar data centers were expanded box by box, and as the demand for capacity increased, so did the overall appliance count. The wireless LAN (WLAN) moved slowly from a network of convenience to a more reliable alternative to the wired network. Overall, the enterprise network developed reactively in response to changes in user behavior and application development. Since changes were incremental rather than exponential, this reactive model sufficed.

In the last few years, however, everything has changed. With the development of new, high-performance mobile devices, the number of endpoints on the enterprise network has skyrocketed as users utilize their personal smartphones or tablets, in addition to their corporate laptops. The BYOD phenomenon means that a significant percentage of network traffic comes from unmanaged personal devices, stressing IT security and access control infrastructure. This consumerization of IT has raised end user expectations for both performance and innovation. In addition, advances in virtualization have enabled applications to be housed in the cloud, in the corporate data center, or both. Users don't want to have to think about how the increasingly complicated underlying network functions or what client-side software to use in a given situation; they simply want to be connected, anytime, anywhere, and from any device.

Pulse Secure' Response—The Simply Connected Network

Pulse Secure has addressed these challenges with the Simply Connected network. Juniper's Simply Connected portfolio of networking products provide innovative solutions for the data center and campus and branch networks of all sizes. Juniper ensures that the enterprise and its authorized users can make the most of new trends and businesses can capitalize on network innovations. The Simply Connected portfolio of products is designed to fit together into an automated, simplified architecture, offering high resiliency, orchestrated security, and performance at scale in a cost-effective package. The result is a superior quality of user experience that is simple for the user *and* easy for IT to support. In the context of today's enterprise paradigms, the goal of the Simply Connected network is to deliver user and device identification, simple device onboarding, complete security, and easy-to-use management and reporting.

Juniper's Simply Connected portfolio of products addresses wired, wireless and mobile devices and access, including:

- **Juniper Networks® EX Series Ethernet Switches**, which offer simplified switching architecture and a complete, feature-rich portfolio
- **Juniper Networks SRX Series Services Gateways,** with enterprise-class security that delivers application awareness, visibility and control at the user or group level
- **Juniper Networks WLC Series Wireless LAN Controllers and WLA Series Wireless LAN Access Points** for a wired-like experience on wireless, delivering superior resiliency and performance
- **Pulse Secure**, a comprehensive solution to securely connect, protect, and manage your users and devices

This white paper focuses on how enterprises can benefit from the BYOD trend using Juniper's Simply Connected network. User demand for BYOD tasks IT managers with providing and enforcing differentiated, granular access control for end users connecting from personally owned devices. Providing security in this environment goes beyond simply securing network traffic; the security solution must provide differentiated network access based on policy and a combination of the user's identity, role, location, device type, and device integrity. And perhaps most difficult of all, it must perform all of these activities quickly and transparently.

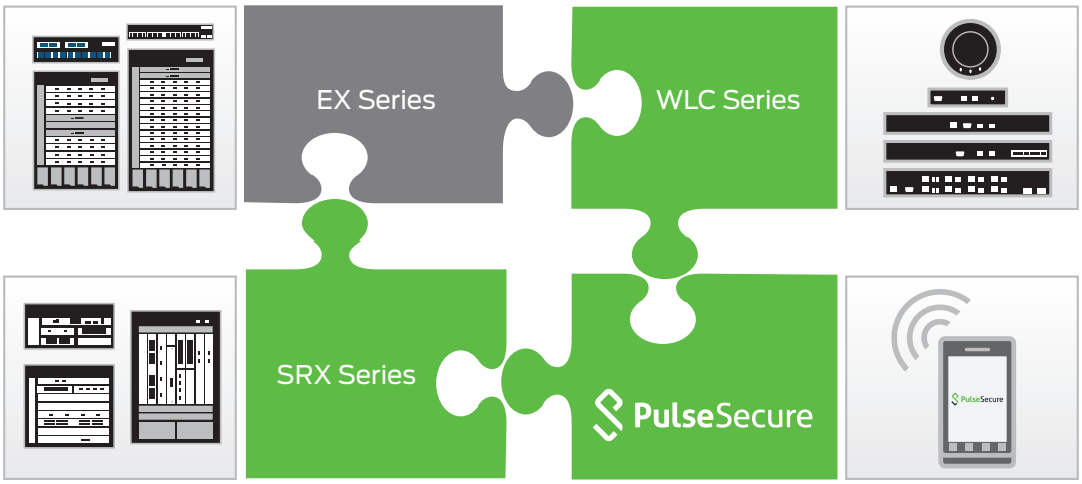

Figure 1: Elements of a Simply Connected network

Pulse Policy Secure/UAC

Pulse Policy Secure/Unified Access Control (UAC) is a standards-based, scalable network access control (NAC) solution that reduces network threat exposure and mitigates risks. This network and application access control solution protects your network by guarding mission critical applications and sensitive data, providing identity-aware network security, and delivering comprehensive NAC management, visibility, and monitoring.

Pulse Policy Secure/UAC reduces the cost and complexity of delivering and deploying granular, identity, and role enabled access control from the branch to the corporate data center. UAC addresses most network access control challenges, including insider threats, guest access control, and regulatory compliance.

Pulse Policy Secure/UAC is built on the industry-standard Trusted Network Connect (TNC) specifications from the Trusted Computing Group (TCG). The TNC model features a centralized gateway that distributes policy and links back to a network's authentication, authorization, and accounting (AAA) scheme, an end user software platform or portal that collects authentication and device information, and a variety of different policy enforcement points (PEPs). The Juniper UAC solution is comprised of:

- **Pulse Secure MAG Series Pulse Secure Gateways**: Modular, configurable gateways that address the secure mobile and remote network access (SSL VPN), LAN-based network access control (UAC), and application acceleration needs of enterprises of any size.
- **Pulse Secure client**: Juniper's dynamic, multiservice, multi-platform network client, available for all major computing and mobile device operating systems, collects user credentials and assesses device security state. Much of this same functionality is also available via UAC's agent-less mode.
- **Network enforcement points**: These policy enforcement points can include Juniper Networks WLA Series Wireless LAN Access Points, Juniper Networks EX Series Ethernet Switches; any Pulse Secure firewall platform, including the SRX Series Services Gateways, SSG Series Secure Services Gateways, and ISG Series Integrated Security Gateways; and standalone Juniper Networks IDP Series Intrusion Detection and Prevention Appliances; or any vendor-agnostic 802.1X-enabled wireless access point or 802.1X-enabled switch.

UAC is based on a robust foundation of industry standards (802.1X, RADIUS, and IPsec), as well as industry accepted open standards such as TNC specifications, including the TNC's open standard Interface to Metadata Access Point (IF-MAP), which empowers UAC to integrate with third-party network and security devices.

Pulse Policy Secure/UAC as part of the Simply Connected Network

As described above, Juniper built the Unified Access Control solution based on open standards. This is consistent with Juniper's stance on open standard solutions, which increase transparency and offer true customer choice. However, it is also true that including a UAC solution as part of a Juniper Simply Connected deployment will enable a number of unique capabilities. The easiest way to visualize the role of UAC in the Simply Connected network is to follow several end users through their work day. We will follow Joe, a sales executive at AcmeGizmo, as he moves from his home connection to his office, and later examine his onboarding of a new personal tablet. Then we'll look at Lisa, a guest user connecting to the AcmeGizmo network from inside the AcmeGizmo offices. We'll consider the addition of unmanageable devices such as voice over IP (VoIP) phones, and then look at how a marketing employee and a contractor can get differentiated, role-specific access. In the process, we'll look at most of the situations typically faced by enterprise IT, from wired connection of a corporate laptop to onboarding a user's own mobile device. As you will see in each scenario, the focus is on allowing users to simply and securely connect, and ensuring a consistently high quality of experience. End user intervention is minimized at every step, making the process easy—even as it becomes more secure.

Role-Based Access Control with Ethernet Switches and WLAN Systems

Scenario 1: Corporate Laptop on Wired Connection and Personal Device on Wireless Connection

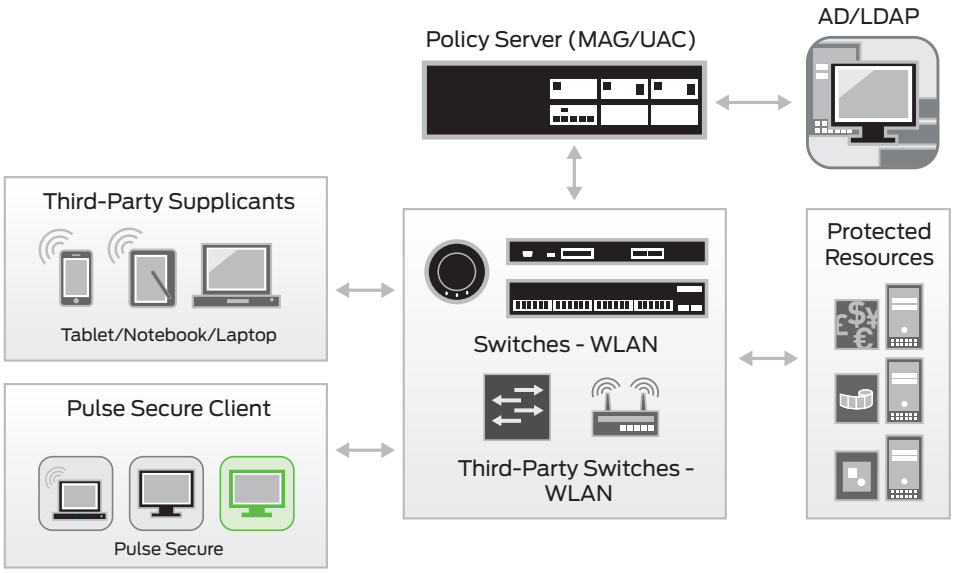

Figure 2: Access Control at Layer 2 (802.1X)

In our first scenario, Joe docks his corporate Windows laptop in his office at AcmeGizmo on Monday morning. He is connected via Ethernet to the AcmeGizmo network. The Pulse Secure client, which has already been installed, comes up and asks for Joe's user name, password, and secure token ID. Joe enters the information, and the device is joined to the appropriate domain. Joe now has access to network resources.

Later in the morning, Joe joins his colleagues in a conference room for an urgent meeting, taking his personal iPhone with him. Joe's iPhone connects to the secure wireless network at AcmeGizmo, and Joe is automatically connected to AcmeGizmo's 802.1X-enabled wireless network via the device certificate.

How Scenario 1 Is Enabled in the Network

From Joe's perspective, both of these transactions are straightforward and simple, thanks to a number of Pulse Secure services running in the network. When Joe's corporate laptop is docked and connected to the AcmeGizmo wired network, it is connected to a switch that is 802.1X-enabled. An Extensible Authentication Protocol–Tunneled TLS (EAP-TTLS) tunnel is constructed, which begins with an EAP-over-LAN connection between Joe's laptop and

the switch. The switch forwards authentication and authorization requests on behalf of the user via an EAP RADIUS connection between itself and MAG Series Pulse Secure Gateways or Juniper Networks IC Series Unified Access Control Appliances. The gateway could be either device; for the purposes of this description, we'll just call it a Pulse Secure gateway.

The Pulse Secure gateway first performs a host check to ensure that Joe's device is healthy and complies with corporate security policies. If Joe's device is deemed healthy and compliant, the process continues. If not, Joe's device may be quarantined and could be subject to automatic or manual remediation, depending on the situation or issue. Once Joe's device passes the host check, the Pulse Secure gateway communicates with AcmeGizmo's Active Directory server for authentication and authorization. Based on the user role assigned to Joe in Active Directory, the Pulse Secure gateway sends a RADIUS attribute back to the switch. This attribute could be a VLAN ID, a filter ID, or another attribute. The switch port is opened, and Joe has access to network resources.

In the iPhone scenario, the process works a little differently. Because the device is owned by Joe personally and does not have the Pulse Secure client installed on it, the entire 802.1X authentication process is done via the iPhone's native 802.1X supplicant. In this scenario, the WLAN controller acts as the authenticator (instead of the switch in the previous example) and the Pulse Secure gateway functions as the RADIUS server. The Pulse Secure gateway then receives the authentication and authorization information from AcmeGizmo's backend Active Directory server, and pushes the appropriate access control rules to the WLAN controller.

How does Pulse Secure add value on top of native 802.1x supplicants?

1. **Host Check Prior to Authentication**

   The Pulse Secure client delivered a full host check in the first scenario, before Joe was allowed to even enter his credentials. Pulse Secure enables a full host check including patch assessment/remediation, as well as a check for viruses, malware, and other threats before switch or WLAN controller ports are opened. This allows IT to ensure that an infected device has no connectivity to the Dynamic Host Configuration Protocol (DHCP) server or any other resource in the data center or on the network prior to the host check. Pulse Secure provides these capabilities via a Juniper EAP-JUAC plug-in.

2. **Layer 2 and Layer 3 Access Control via SSO**

   By using the Pulse Secure client, the enterprise can deploy 802.1X-based access control such as VLAN or filter assignments at Layer 2, and provide more granular Layer 3-based access control via internal firewalls. Once the Pulse Secure gateway authenticates the user, these credentials will be cached on the Pulse Secure client. Once the switch/WLAN controller opens the port and the device is part of the corporate domain appropriate to the user's role, the relevant resource access policies for the user will also be pushed to the Juniper firewall. This entire process is transparent to the end user, and can be achieved with a single sign-on (SSO) from the end user's perspective.

3. **Full Encryption**

   The Pulse Secure client can encrypt all LAN communications via an end-to-end IPsec tunnel. If a critical business application is hosted behind an internal Juniper firewall, the Pulse Secure gateway can dynamically launch an IPsec tunnel between the Pulse Secure client and the firewall when the end user is connecting to that specific application.

Scenario 2: Guest Users on Wired/Wireless Connections

In this next scenario, Lisa, our guest user, connects her laptop to a wired switch port or wireless access point from a conference room. Lisa needs Internet access and launches a Web browser. She is redirected to an authentication page for AcmeGizmo and enters her guest credentials. Once her credentials are verified, she is connected to the Internet.

How Scenario 2 Is Enabled in the Network

When Lisa launches a Web browser, the switch or WLAN controller sends an HTTP redirect to the Pulse Secure gateway, also called a captive portal. The Pulse Secure gateway launches an authentication page to Lisa's browser via the captive portal solution. Once Lisa presents her guest credentials, the Pulse Secure gateway authenticates her locally and sends appropriate access control rules to the switch or WLAN controller. In this case, the guest user role

Why use an EX Series switch in a UAC environment instead of a generic 802.1X-enabled switch?

1. **Free IT from creating manual ACLs**

   Hundreds of access control lists (ACLs) can be created and pushed onto the switches at runtime from the Pulse Secure gateway functioning as a centralized policy server. IT does not have to create/maintain ACLs on switches manually.

2. **No need to make manual changes**

   When a role changes for a particular user, IT does not need to delete the old ACL and create a new one on the switch port. A role change will automatically trigger a new policy to be pushed from the Pulse Secure gateway to the switch port.

3. **Higher scalability and performance**

   Higher scalability and network performance can be achieved since there is no need for Change of Authorization (COA) disconnect messages and triggering end user reauthentication when user roles change.

limits Lisa's access to only the Internet and nothing else. Lisa would be unable to access any portion or segment of the AcmeGizmo network.

Scenario 3: Unmanageable Devices on Wired/Wireless Connections

We've talked about an employee using a corporate device and a personal mobile device, and we've looked at what happens when a guest user accesses the network. Another common scenario occurs when an unmanageable device such as an IP-enabled phone, printer, or fax machine is connected to the network. In a network environment in which UAC has been deployed, the device simply connects to a switch port, joins the domain, and starts providing services to the network.

How Scenario 3 Is Enabled in the Network

When unmanageable devices are connected, a Media Access Control (MAC) request comes to the Pulse Secure gateway from the switch or WLAN device. The Pulse Secure gateway authenticates the unmanageable device via the MAC authentication bypass mechanism.

In addition, Pulse Secure gateways can push appropriate access control rules to switches, WLAN controllers, and Juniper Networks firewalls (such as the SRX Series Services Gateways) based on device profiling via a third-party device profiler and collector such as Great Bay Software's Beacon Endpoint Profiler. Security is achieved using standard-based Lightweight Directory Access Protocol (LDAP) between the Pulse Secure gateway and the unmanageable third-party devices.

Enabling Technology in the Network—Pulse Policy Secure/UAC and EX Series 802.1X Switches

Pulse Policy Secure/UAC solution is designed to work seamlessly with standard-based devices. If the enterprise has EX Series switches in place, however, network-based access control can go further while simplifying network operations for IT.

When a Pulse Secure gateway running the Pulse Policy Secure connects with an EX Series switch, a Juniper UAC Enforcer Protocol(JUEP) channel is established in addition to the RADIUS connection. Through the JUEP connection, the Pulse Secure gateway will publish a role table to EX Series switches based on Active Directory groups. When a user is authenticated via the Pulse Secure gateway, the appropriate access control list will be created and pushed down to the switch port based on the role of the user. For example, Joe, who is in sales, can have access to the Internet, the AcmeGizmo intranet, and to Salesforce.com, in order to look at corporate sales data. On the other hand, Sam, who is an engineer, will have access to the Internet, the AcmeGizmo intranet, and the software build server. This alleviates the

requirement for corporate administrators to create and maintain thousands of ACLs statically on individual switches. The Pulse Secure gateway functions as a centralized policy server, so administrators can manage all security and access control policies from a single point.

Role-Based Access Control with Internal Firewalls

Scenario 4: Corporate Laptop Connecting via Pulse Secure Client through the Internal Firewall

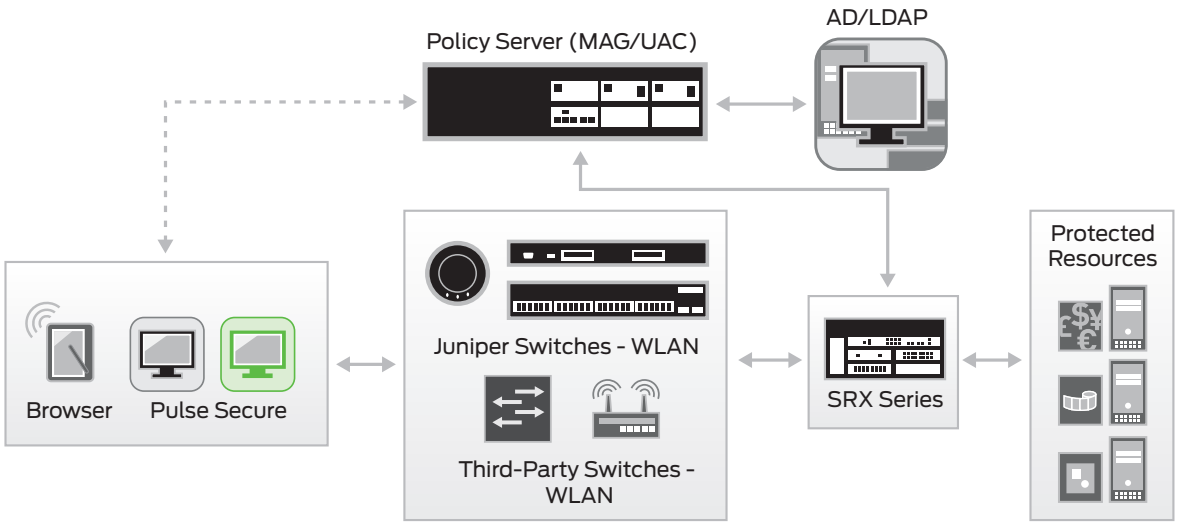

Figure 3: Role-based Access Control at Firewall

In the next scenario, Pat, a marketing employee, is connecting from his office to access the Business Objects application. The Pulse Secure client prompts Pat for his credentials. Once his credentials are supplied and verified, Pat can get to all of the business applications that he is authorized to access.

How Scenario 4 Is Enabled in the Network—Pulse Policy Secure/UAC and SRX Series Services Gateways
Behind the scenes, Pat is actually trying to get to a mission critical application protected by an SRX Series gateway. When the SRX Series connects with the Pulse Secure gateway at setup, it will send a role table to the SRX Series device. The administrator can then create an access policy, tying user roles to policy—for example, only users in a marketing role can access the Business Objects networked application, so marketing team members can research and analyze vital sales and revenue data. Note that this policy is created once, at setup.

The first step in getting Pat the access he needs is a full host check of his device, which is conducted to ensure that his device meets corporate policy. Next, the Pulse Secure client pushes credential information to the Pulse Secure gateway, which talks to the Active Directory server to perform authentication and authorization. Active Directory confirms that Pat is part of the marketing organization, and that role is pushed to the SRX Series. The SRX Series now maps Pat to a specific resource access policy, enabling him to gain the application access that he needs (in this instance, to Business Objects).

The interaction between Pulse Policy Secure/UAC and the SRX Series adds important functionality to this already award-winning solution. When combined with Pulse Policy Secure/UAC, the SRX Series firewall becomes identity aware—with vital functionality for enforcing application security policies on a per-user and role basis, and thus meeting compliance regulations when needed. This delivers fine-grained access control that is easily managed from a central location (UAC).

Scenario 5: Contractors Connect to Business Applications via Captive Portal/Web Authentication

In this scenario, we'll look at Dave, a contractor who doesn't have the Pulse Secure client on his device. He needs to get access to the Internet and some AcmeGizmo applications from inside the AcmeGizmo corporate office. Dave simply launches a Web browser and is automatically redirected to a captive portal, where he is asked to enter his credentials. He enters his credential, and is connected to the Internet, as well as to the appropriate applications.

How Scenario 5 Is Enabled in the Network—Pulse Policy Secure/UAC and SRX Series Gateways

Behind the scenes, Dave's access to the Internet from the corporate office is protected by an SRX Series gateway. As we saw in the previous scenario, user roles are sent from the Pulse Secure gateway to the SRX Series gateway at setup. One of the default roles in AcmeGizmo's Active Directory store is "Contractor." The administrator has created an access policy for contractors, allowing them access only to the Internet and a few restricted applications.

When Dave launched his browser, the request came to the SRX Series gateway, which did an HTTP redirect to the Pulse Secure gateway. Before authentication, a host check is performed to ensure that Dave's device meets minimum AcmeGizmo corporate security standards. The Pulse Secure gateway hosts a login page on the browser and asks Dave to authenticate. Dave presents his credentials, and the Pulse Secure gateway pushes an access control list to the SRX Series gateway. Dave is now allowed to go to the Internet and get access to a few corporate applications.

What does the Pulse Policy Secure/UAC deliver with the SRX Series gateway?

1. **Firewall policies incorporate user/role information**

   All firewall policies can be constructed with user and role information. For example, a user within the "Sales" role can access sales data, as opposed to a user within the "Engineering" role who can access a build server.

2. **Make the most of AppSecure and AppQoS**

   SRX Series AppSecure and AppQoS policies have full visibility into users and their roles on the network.

3. **Push dynamic policies vs. maintain static policies**

   Rather than creating and having to maintain hundreds of static firewall policies, all policies can be configured and pushed at runtime from a centralized policy server, in this instance, the Pulse Secure gateway/UAC.

4. **Higher security**

   When the end user is connecting to a critical application, a dynamic IPsec tunnel can be created from the Pulse Secure client to the SRX Series gateway to encrypt all LAN communications.

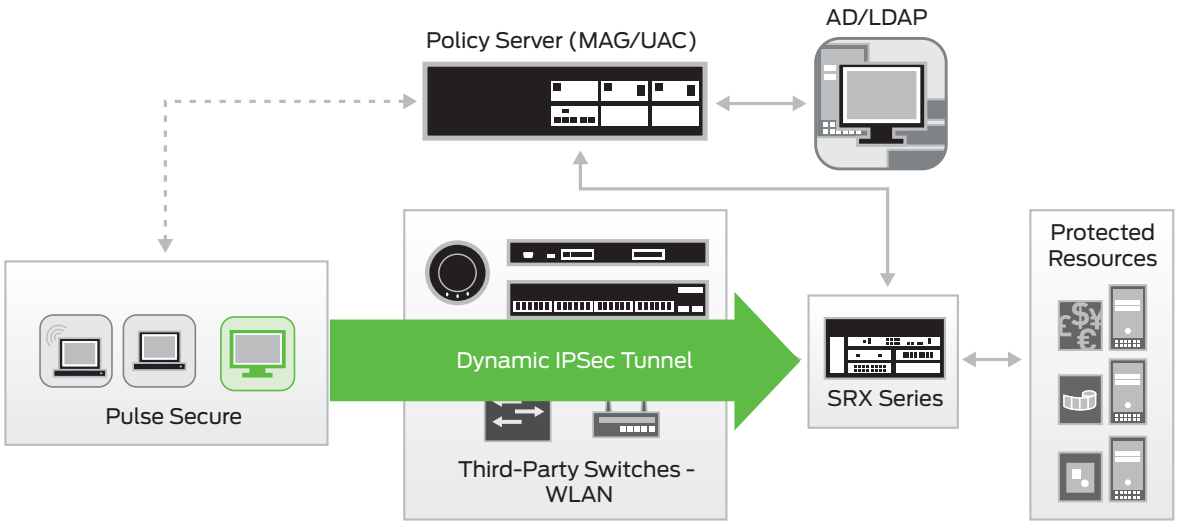

Figure 4: End-to-End Encryption

Role-Based Access Control in BYOD Environments

Scenario 6: Corporate Employees Using Personal Devices for Remote Access and LAN Connections

It's Sunday afternoon, and Joe has purchased a new iPad from an electronics store. He is enthusiastic about using his new tablet to catch up on work before he goes into the office on Monday. He downloads and installs the Pulse Secure client from the Apple App Store, then connects to AcmeGizmo's Pulse Secure Mobile Security Suite portal via a Web browser to get the applications and security protections that he needs. When the download is complete, Joe starts the Pulse Secure client, enters his credentials, and checks his e-mail. On Monday, he takes his tablet into the office, connects wirelessly, and accesses internal AcmeGizmo resources.

How Scenario 6 Is Enabled in the Network—Pulse Secure's UAC, SSL VPN, and Pulse Secure Mobile Security Suite with Pulse Secure's WLAN Offerings

Joe connects to AcmeGizmo's Pulse Secure Mobile Security Suite portal, which is hosted as a software-as-a-service (SaaS) by Pulse Secure. The hosted Pulse Secure Mobile Security Suite downloads Joe's VPN profile and the 802.1X configuration onto his new tablet.

Joe launches the Pulse Secure client, which connects to the Pulse Secure gateway at AcmeGizmo. This gateway is running both the Pulse Connect Secure (SSL VPN), as well as the Pulse Policy Secure (UAC) that we've seen in the earlier scenarios. The Pulse Secure gateway uses its location awareness feature to determine that Joe is not in the AcmeGizmo office. Joe is asked for his credentials, which are verified by the Active Directory server at AcmeGizmo. The Pulse Connect Secure (SSL VPN) is automatically launched, since Pulse Secure realizes that Joe is not in the office and connected directly, regardless if wired or wireless, to the AcmeGizmo corporate network. It then determines Joe's identity and role, and connects him to the resources that he is authorized to see and use on the AcmeGizmo network.

On Monday, Joe brings his tablet into the office, where the service switches from the Pulse Connect Secure to the Pulse Policy Secure. Joe's download from the previous afternoon has provisioned his Wi-Fi credentials, so he is connected to the WLAN. The native 802.1X supplicant authenticates Joe. Once the 802.1X authentication is done and the device has an IP address, the WLC Series controller does a MAC-IP link and sends this information to the Pulse Secure gateway via a RADIUS accounting message. This MAC-IP link triggers the Pulse Secure gateway to push a granular access control policy to a Juniper firewall, such as an SRX Series gateway, allowing Joe to connect to more business applications based on his assigned role in the network.

Conclusion

Pulse Policy Secure (UAC) is unique in the networking and security industry. With the simple addition of a MAG Series gateway (or legacy IC Series Unified Access Control appliance), you can enable centralized policy delivery that simplifies access for corporate devices and allows you to make the most of the BYOD trend. Because the Pulse Policy Secure is based on open standards, you are free to use the best-in-class solutions that work well in your environment or that meet your unique needs and requirements.

If you have Pulse Secure devices in your network, however, the addition of a MAG Series gateway running the Pulse Policy Secure delivers features that you won't get anywhere else. You can easily enable pre-authentication host checks so devices that don't meet your corporate security policies aren't even allowed on your network. Using the JUEP channel functionality, ACLs are automatically pushed to EX Series switches dynamically, freeing IT from the time-consuming and error-prone process of manual ACL entry, while ensuring that entries are updated as roles change. Finally, with Juniper firewalls, including the SRX Series gateways, you can enable dynamic Layer 3 policies that include information about users and their roles automatically.

Whether you want to unify your existing network or optimize your Juniper deployment, the Pulse Secure solution will get you there, at your pace. Pulse Secure' unified security and policy control simply connects, protects, and manages users, their devices and access, from any device, anywhere.

About Pulse Secure, LLC

Pulse Secure, LLC is a leading provider of access and mobile security solutions to both enterprises and service providers. Enterprises from every vertical and of all sizes utilize the company's Pulse virtual private network (VPN), network access control and mobile security products to enable end user mobility securely and seamlessly in their organizations. Pulse Secure's mission is to enable open, integrated enterprise system solutions that empower business productivity through seamless mobility.

Corporate and Sales Headquarters
Pulse Secure LLC
2700 Zanker Rd. Suite 200
San Jose, CA 95134
www.pulsesecure.net

WP001 Aug 2014