Juniper Networks and Pulse Secure Deliver Unified Secure Network Access

A comprehensive, standards-based solution for secure NAC

Challenge

Enterprises need to provide seamless and secure access to employees, contractors, and guests while balancing the need to secure corporate resources.

Solution

EX Series Ethernet Switches and SRX Series Services Gateways are fully integrated with Pulse Secure Policy Secure and Pulse Secure Profiler, delivering a complete 802.1X standards-based NAC solution with powerful pre- and post-admission access control management and enforcement.

Benefits

- Standards-based technology with fully validated integration helps customers avoid single vendor lock-in, provides immunity to price increases, and allows customers to select best-of–breed solutions.
- Automated discovery of unmanaged devices ensures the network can be fully secured while providing visibility to every IP-enabled device accessing the network.
- Frictionless access with centralized web-based captive portal and user-based QoS policies eliminates frustration while providing maximum performance for user applications and services.

As businesses move toward greater mobility with an increased emphasis on outsourcing, enterprises are pressed to employ a more mobile workforce, expand their use of outside contractors, and sustain an increasing number of vendors and partners. All of these users, as well as guests, require network and application access, which places tremendous stress on the enterprise network, its resources, and enterprise IT staff. Network and application access needs to be pervasive, robust, and secure. Yet as the demands and availability of network and application access increase, so do the risks to the network, applications, and the enterprise network's sensitive data.

Network access control (NAC) is a necessity for today's high-performance enterprise network, since it mitigates the risk and manages the threat threshold for enterprises and their networks. NAC manages access to the network and its applications based on user and/or device compliance against a series of enterprise-defined network and security policies. Criteria for network and security policies include user identity, device identity, device health, device security state, and/or network location, to name a few. Policy enforcement may include ensuring that users and their devices adhere to and maintain a minimum level of security or other criteria defined by the enterprise. Policies may also ensure that specific users and user roles receive the proper network and application access by enforcing established authorization levels. A NAC solution can enable authorized corporate as well as personal bring-your-own-device (BYOD) resources to access the network, while ensuring that the user and device follow all corporate authentication and security policies before network access is granted, as well as during an active network session.

The Challenge

Deploying network access control can be complex, costly, and time-consuming. Enterprises often fear that network and business disruptions could upset their management and frustrate end users. They are also concerned that ROI is outweighed by the time and cost of deploying NAC. Network administrators are looking for solutions that address these challenges and protect their network and application integrity, while providing the flexibility to evolve without disrupting business operations and leverage existing network infrastructure investments.

Selecting NAC based on industry standards accomplishes this. Standards are vital for enterprises, allowing them to:

- Avoid single vendor lock-in, which provides immunity to price increases and enables technologies to be open and accessible
- Increase ROI by leveraging existing networking infrastructure components
- Freely select network infrastructure and technology
- Ease integration with diverse technologies

Network access control requires a secure, strong, and flexible framework for authentication, access management, network security, and data privacy. The IEEE 802.1X standard for port-based NAC delivers that, as well as:

- Robust pre-admission and post-admission control enforcement
- A resilient authentication process
- Interoperability with new or existing heterogeneous network components
- Simplicity and speed in the deployment and integration of 802.1X standards-based components

A comprehensive 802.1X-based NAC solution addresses the challenges faced by administrators and their networks by protecting the network, delivering deployment simplicity and flexibility, leveraging existing network components, and ensuring network and application integrity.

Automatically discovering unmanaged devices using Pulse Secure Profiler allows for an all-inclusive solution, which ensures that the network can be completely secured while providing visibility into every IP-enabled device trying to gain access.

The solution also provides freedom of choice for network components and policy enforcement.

The Juniper Networks Pulse Secure Unified Secure Access Solution

Pulse Policy Secure (PPS) and Pulse Secure Profiler, deployed with Juniper Networks® EX Series Ethernet Switches, deliver a complete 802.1X standards-based network access control environment. The interoperable PPS and EX Series switches work together to deliver a single, seamless solution that provides powerful pre- and post-admission access control management and enforcement, protecting sensitive corporate data from unauthenticated access, attacks, and breaches. The integrated PPS and EX Series switches also give enterprises the freedom to select and work with diverse network components including, in the case of PPS, new or existing 802.1X-compatible switches and Juniper Networks SRX Series Services Gateways. The combined solution avoids the pitfalls usually faced with single-vendor solutions, while providing the benefits of working with one vendor for a comprehensive solution: easier and quicker deployment, value-added features and interoperability, and a single source for support.

PPS combines user identity and device security state information with network location to create a unique, session-specific access control policy for each user. PPS is based on industry standards, including 802.1X, Extensible Authentication Protocol (EAP), RADIUS, IPsec, and the Trusted Computing Group's (TCG) Trusted Network Connect (TNC) standards for endpoint integrity and NAC. Its foundation includes field-tested components, including Juniper Networks SA Series SSL VPN Appliances, Odyssey Access Client, and SBR Enterprise Series Steel-Belted Radius Servers that are deployed in thousands of networks worldwide and enable PPS to leverage your existing network environment.

With PPS, policy enforcement can be enabled at Layer 2 using the 802.1X standards, or at Layer 3 using an overlay deployment with SRX Series gateways. It can also be provisioned in mixed mode using 802.1X for network admission control and Layer 3 for resource access control. PPS reduces network threat exposure; delivers comprehensive control, visibility, and monitoring to surpass regulatory compliance; and decreases access control deployment costs and complexity while delivering the flexibility required for phased deployments. PPS extends access control to network traffic by implementing policy enforcement deeper into your network's core and outward to its edge, mitigating risks and protecting sensitive corporate assets.

Pulse Secure Profiler provides automated discovery and a comprehensive accounting of all network-attached endpoints. This inventory provides a real-time view of each network-attached device's location, media access control (MAC) address, IP address, identity, and behavior, as well as an historical view

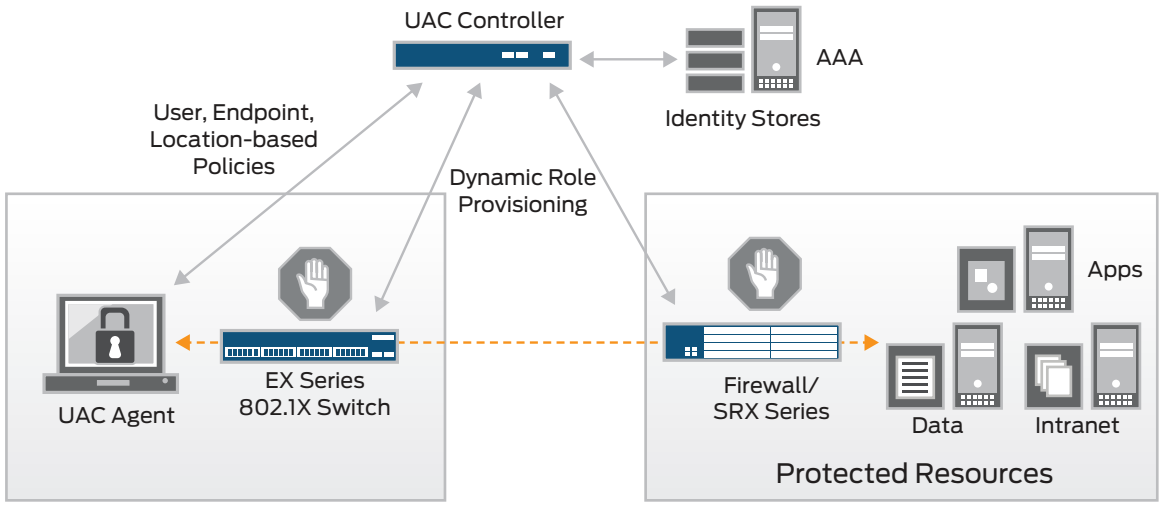

Figure 1: Integrated Juniper Networks Pulse Secure network access control solution

of these attributes. This information is used to facilitate the deployment of 802.1X access control by relieving the requirement to discover all enterprise endpoints manually. Policy Secure sends Lightweight Directory Access Protocol (LDAP) queries to the Pulse Secure Profiler software and performs MAC authentication based on the response. Thus, the information effectively stored within Pulse Secure Profiler is leveraged by PPS to authenticate endpoints that, for some reason, are not running an authentication client. Working in concert, these solutions provide authentication to the entire enterprise, avoiding the costly and unwieldy option of manually configuring all network ports.

The EX Series, including the EX2200, EX3300, and EX4300 lines of Ethernet Switches, combines the high availability and carrier-class reliability of modular systems with the economics and flexibility of stackable platforms, delivering a scalable solution for data center, campus, and branch office environments. By offering a full suite of Layer 2 and Layer 3 switching capabilities, the EX Series switches satisfy a variety of high-performance applications, including Gigabit Ethernet aggregation deployments. A single 24-port or 48-port EX Series switch can be deployed initially; as requirements grow, Juniper's Virtual Chassis technology allows multiple EX Series switches to be interconnected and managed as a single device, providing a scalable, pay-as-you-grow solution for expanding networks. Select models of EX Series switches include high availability (HA) features such as redundant, hot-swappable internal power supplies and field-replaceable, multi-blower fan trays to ensure maximum uptime. The EX Series switches include an integrated ASIC-based Packet Forwarding Engine, the EX-PFE, while an integrated Routing Engine (RE) based on existing, field-proven Juniper technology delivers all control plane functionality. This brings the same level of carrier-class performance and reliability to the EX Series that Juniper routers bring to the world's largest service provider networks. The EX Series switches also leverage the same modular Juniper Networks Junos® operating system, ensuring a consistent implementation and operation of each control plane feature across the entire Juniper infrastructure.

EX Series, Pulse Secure Profiler, and PPS work together to create a comprehensive 802.1X network access control solution that delivers rich policy enforcement capabilities. The EX Series switches are deployed as enforcement points within a PPS environment, using the 802.1X standard for port-level access control and L2-L4 policy enforcement. The user's identity, device posture, and location are used by PPS to determine network admission. If PPS grants network access, it will propagate that information to the EX Series switches, which will assign the user to a specific VLAN based on the appropriate authorization level. When deployed together, the EX Series switches and PPS can enforce and set user-based quality-of-service (QoS) policies for the prioritization of data, voice, and video traffic. PPS also leverages the intrusion detection capabilities of the SRX Series gateways to deliver broad visibility into application traffic, isolating threats to the user or device level and employing an applicable policy action via the EX Series against the offending user or device. PPS can also correlate user identity and role information to network and application access, better addressing regulatory compliance.

For managing guest users in the enterprise or devices which cannot use 802.1X, PPS and EX Series switches can work together to provide unified web-based captive portal authentication. When used in this way, the EX Series switches will offload the Web portal and authentication processes to PPS while remaining inline as the authentication enforcement point. This results in a simpler, more scalable system with a common guest user experience, regardless of device or location.

Features and Benefits

Together, EX Series Ethernet Switches, SRX Series Services Gateways, Pulse Secure Profiler, and Pulse Policy Secure deliver a comprehensive standards-based network access control solution that:

- Provides rich policy enforcement capabilities
- Uses the 802.1X standard for port-level access control and L2-L4 policy enforcement for robust network admission control
- Enforces user-based QoS policies that enable data, voice, and video traffic to be prioritized
- Mirrors user traffic to a central location for logging, monitoring, or threat detection by intrusion prevention system (IPS) products such as the SRX Series
- Isolates threats to the user or device and applies a suitable policy action against threatening users and/or devices, when used in conjunction with the SRX Series gateways
- Automates device discovery for added visibility
- Enables a common and consistent guest user experience with a centralized web-based captive portal

Solution Components

- EX Series Ethernet Switches
- SRX Series Services Gateways
- Pulse Policy Secure (PPS)
- Pulse Secure Profiler

Summary—A Fully Integrated Solution

Combining the flexibly deployed, best-in-class Pulse Policy Secure, visibility-enabling Pulse Secure Profiler, and the carrier-class reliability of EX Series Ethernet Switches and SRX Series Services Gateways enables organizations to quickly and easily deploy a network access control solution that delivers the performance, availability, and operational simplicity to meet the demands of today's high-performance enterprises.

When deployed together, Pulse Policy Secure, Pulse Secure Profiler, EX Series switches, and SRX Series gateways provide a complete standards-based NAC environment, delivering a seamless solution with powerful pre- and post-admission access control and enforcement. PPS, interoperating with EX Series switches, enables you to single-source a complete, standards-based, best-in-class NAC solution. This also allows you to enjoy value-added features when the products are deployed together, as well as economies of scale for support and service and the evolution of a complete access control environment. An integrated access control solution of PPS, Pulse Secure Profiler, and EX Series switches gives you the freedom to work with and choose diverse network components, helps you avoid vendor lock-in, and delivers simple and flexible deployment options while providing value-added features and a single source for support.

Next Steps

For more information on Pulse Policy Secure, please go to www.pulsesecure.net/products/policy-secure/, and for Pulse Secure Profiler, please go to www.pulsesecure.net/products/proflier/.

For more information on EX Series Ethernet Switches, please go to www.juniper.net/switching, and for more information on SRX Series Services Gateways, please go to www.juniper.net/us/en/products-services/security/srx-series/, or contact your Juniper Networks representative.

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.

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.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
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

3510551-001-EN July 2015