Juniper and Aruba Deliver Enhanced Protection for the Mobile IoT-Centric Enterprise

Securing Networks Through Identity-Based Policy Management and Firewall Perimeter Defense

Challenge

The increasing presence of smartphones, tablets, and other non-IT controlled devices in the workplace is leaving corporate networks vulnerable to threats, giving hackers more opportunities to access and exploit weaknesses.

Solution

Juniper's broad portfolio of security-focused solutions integrate seamlessly with Aruba Networks ClearPass Policy Manager, enabling enterprises to deploy consistent security policies across their wired and wireless networks.

Benefits

- Delivers a secure and consistent experience across both wired and wireless networks
- Effectively secures wired and wireless networks through intelligent policy management while acknowledging user and device context
- Protects against threats from outside the network perimeter

Organizations require greater control over the applications and traffic running on their networks to protect assets against attacks. This requires a solution that is not only efficient but also delivers high levels of security assurance.

In a mobile and IoT-centric enterprise, employee demands for flexibility are at an all-time high. Increasingly mobile and tech-savvy workers demand a consistent, high-quality experience whether they are using a company-owned device or their own personal smartphone. These demands are so prevalent that 74 percent of businesses have implemented BYOD policies that allow devices of all kinds to access the corporate network anytime, anywhere.[1] These personal devices represent a significant new source of security threats, and networks must be innovative and adaptive enough to respond.

The Challenge

Just a few short years ago, perimeter firewalls and deep packet inspection were sufficient to secure enterprise networks consisting exclusively of IT-controlled and IT-issued computers. As smartphones and tablets joined the enterprise, however, they provided hackers with additional avenues for finding and capitalizing on security weaknesses. Suddenly, these perimeter defenses were no longer enough.

Disparate security solutions must work hand in hand to ensure that both user and device context is used for accurate traffic inspection enforcement. Additionally, network access policy management must be able to ingest actions derived from the firewall to protect the network from new, potentially external, threats. Integration is essential in today's growing mobility and IoT environment.

Juniper Networks and Aruba Networks: A Secure Partnership

Juniper Networks® and Aruba Networks have joined forces to create a flexible and intelligent security system that delivers an exceptional user experience for today's highly connected workforce.

Organizations require greater control over the applications and traffic on their networks to manage usage and protect assets from attacks. They need a flexible and efficient solution that provides high levels of security assurance. Juniper Networks® SRX Series Services Gateways deliver next-generation firewall protection with integrated application awareness, intrusion prevention, role-based user controls, and best-in-class unified threat management (UTM) to protect and control your business assets—all centrally managed by Juniper Networks Junos® Space Security Director.

Meanwhile, Aruba's ClearPass Policy Management Platform provides access layer security for user authentication, policy management, and BYOD onboarding. ClearPass integrates with SRX Series firewalls to provide Layer 3 (L3) policy enforcement, while policy integration with Juniper Networks EX Series Ethernet Switches enforces network policy at the access edge. This integration results in protection at both the edge and in the middle

[1]Wearables, BYOD, and IoT: Current and future plans in the enterprise, Tech Pro Research, January 2015

of the network, leading to improved security with less downtime and much lower risk. Additionally, guest access is centralized and delivered consistently to both wired and wireless users.

The ClearPass Ingress Event Engine allows SRX Series firewalls to alert ClearPass about devices exhibiting malicious behavior or activity—information that ClearPass uses to invoke policies or enforceable actions such as blocking, quarantining, or sending messages to a specified device. For example, if a user connects with a device infected with malware, SRX Series firewalls immediately detect the threat and instruct ClearPass to quarantine the device.

Granular Enforcement of Employee Policy

The integration between Juniper and Aruba lets enterprises deploy consistent security policies across their wired and wireless networks. Enterprises typically see a variety of user groups and endpoints, resulting in multiple use cases that need to be addressed for secure access. Depending on the type of endpoint and how it is used, an endpoint might be verified by 802.1X authentication, MAC authentication, or captive portal authentication. The policy infrastructure should allow for any device to connect and be authenticated based on the device type, the user's authorization level, or both.

Consider the end-to-end deployment example depicted in Figure 1, where SRX Series firewalls and Juniper Networks EX Series Ethernet Switches integrate with Aruba ClearPass Manager. A user logging on to "Endpoint 1" and attempting to connect to the corporate network via the EX4300 LAN switch is redirected to Aruba ClearPass for authentication using 802.1X. Only users and devices providing valid credentials are permitted to access the network.

When Aruba ClearPass Manager completes the authentication, this user's identity and device information is passed to the SRX Series firewall. Advanced security policies either allowing or denying the user's access to the protected servers are enforced based on real-time context. In this example, a DHCP server allocates IP addresses to the authenticated endpoints.

Working together, Aruba ClearPass Manager, Juniper Networks SRX Series Services Gateways, and EX Series switches offer a best-in-class integrated solution that delivers both the carrier-grade scale and coverage necessary to protect against threats originating from unknown devices or within your network.

Summary: A Fully Integrated Solution

Organizations require greater control over the applications and traffic on their networks to protect their assets against attacks and manage bandwidth usage. They need a solution that is efficient yet still delivers high levels of security assurance.

Juniper Networks SRX Series Services Gateways deliver next-generation firewall protection with integrated application awareness, intrusion prevention, role-based user controls, and best-in-class UTM to protect and control your business assets.

Aruba's ClearPass Policy Management Platform provides access layer security for user authentication, policy management, and BYOD onboarding. ClearPass integrates with SRX Series firewalls to give you policy enforcement at L3, while policy integration with Juniper Networks EX Series Ethernet Switches enforces network policy at the access edge.

The integration results in protection both at the edge and the core of the network, leading to improved security with less downtime and less risk. Additionally, guest access is centralized and delivered consistently to wired and wireless users. Best of all, users experience seamless, easy access to all permitted network resources—UCC, e-mail, or cloud applications, for example—on any device and from any location.

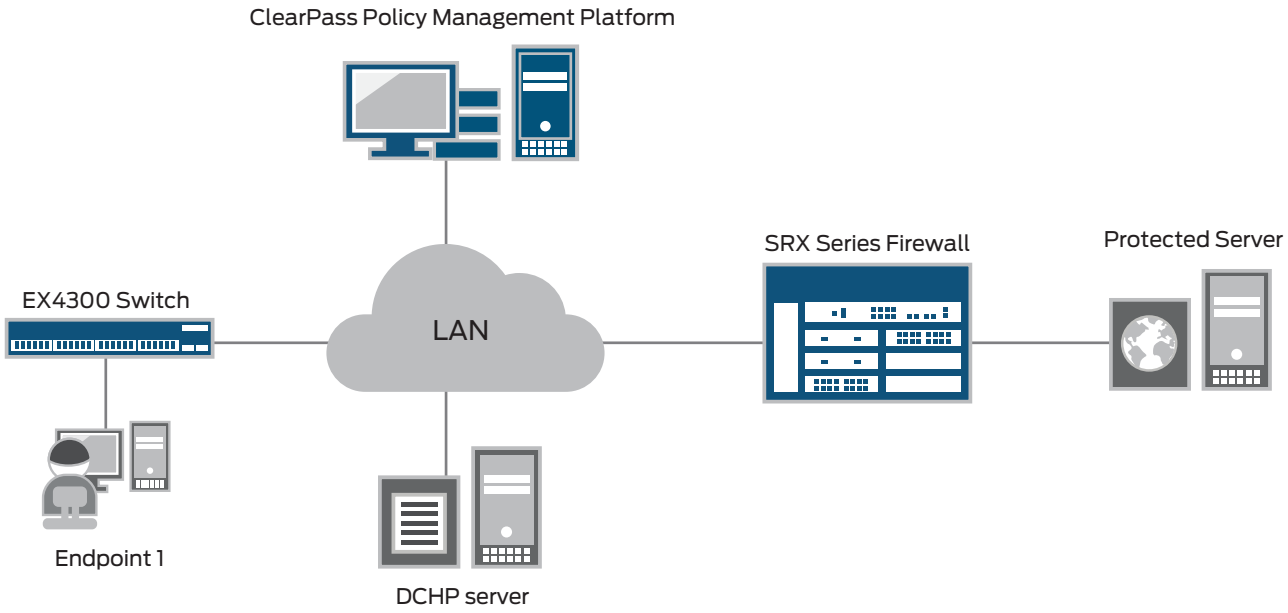

Figure 1: SRX Series firewall, EX Series switch, and ClearPass

Next Steps

For more information, contact your Juniper Networks or Aruba Networks representative, go to www.juniper.net, or visit www.arubanetworks.com.

About Aruba Networks

Aruba Networks is a leading provider of next-generation network access solutions for the mobile enterprise. The company designs and delivers Mobility-Defined Networks that empower IT departments and #GenMobile, a new generation of tech-savvy users who rely on their mobile devices for every aspect of work and personal communication. To create a mobility experience that #GenMobile and IT can rely upon, Aruba Mobility-Defined NetworksTM automate infrastructure-wider performance optimization and trigger security actions that used to require manual IT intervention. The results are dramatically improved productivity and lower operational costs.

About Juniper Networks

Juniper Networks challenges the status quo with products, solutions and services that transform the economics of networking. Our team co-innovates with customers and partners to deliver automated, scalable and secure networks with agility, performance and value. Additional information can be found at Juniper Networks or connect with Juniper on Twitter and Facebook.

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

3510584-001-EN July 2016