SOLUTION OVERVIEW

ENHANCED PROTECTION FOR THE MOBILE, IOT-CENTRIC ENTERPRISE

Aruba and Juniper identity based policy management and firewall perimeter defense

Just years ago, perimeter firewalls and deep packet inspection sufficiently secured enterprise networks consisting of IT controlled, and issued computers. As smartphones and tablets entered the enterprise, IT could no longer rely on perimeter defenses. Users freely download apps and connect from anywhere, which has provided hackers with new ways to capitalize on threats.

Disparate security solutions must now work hand-in-hand to ensure that user and device context is used for accurate traffic inspection enforcement. And when needed, network access policy management must be able to ingest actions derived from the firewall to protect the network from new threats, even outside of the network perimeter. Integration between solutions in today's growing mobility and IoT environment is a must.

JUNIPER SRX SERVICES GATEWAYS WITHIN AN ADAPTIVE TRUST DEFENSE

The Ingress Event Engine in ClearPass allows Juniper SRX Services Gateways to alert ClearPass about devices exhibiting malicious behavior or activity. In turn, ClearPass then utilizes this information to invoke policies or enforceable actions such as blocking, quarantining, or sending a message to a specified device. For example, if a user connects with a device corrupted by malware, Juniper SRX Series Gateways can immediately detect the threat and query ClearPass to quarantine the device from the network.

ATTRIBUTES COLLECTED BY CLEARPASS FROM THE USER AND THEN SHARED WITH JUNIPER FIREWALLS

Feature	Firewall
Source IP	✓
Username	✓
User Role	✓
Domain	✓
Device Type	✓*
Machine OS	✓*
Machine Name	✓*
Health/Posture	✓
Ingress Event Engine Support	✓

* The three attributes above are supplied to the SRX on a data-PULL. The API used is a generic ClearPass RESTful API and these attributes are included by default. However, at this time the SRX cannot enforce policy using these attributes.

GRANULAR ENFORCEMENT OF EMPLOYEE AND GUEST POLICIES

Aruba ClearPass Policy Manager is a policy management platform that provides role-based and device-based network access control (NAC) for any user, employee or guest, across any wired, wireless, and VPN infrastructure. Enterprises with Aruba wireless infrastructure typically deploy Aruba ClearPass to provide AAA, BYOD and guest services for their infrastructure. Enterprises that also deploy Juniper's EX Series switches in these environments can leverage the extensive RADIUS capabilities on EX Series switches to integrate with Aruba ClearPass.

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

In figure 1, an end-to-end deployment is presented where Juniper SRX Services Gateway and EX switch integrates with Aruba ClearPass. The user's endpoint attempts to connect to the corporate network, via Juniper's EX4300 LAN switch, which is then re-directed to ClearPass for authentication using 802.1X. Only users and devices providing valid credentials, are permitted to access the network. ClearPass provides Juniper SRX the flexibility to pull from an Active Directory, an internal database or elsewhere.

When the user is authenticated, this user's identity and device information is sent to the Juniper SRX. Advanced security policies will then be enforced based on real-time context to allow or deny the user's access to the protected servers behind it. A DHCP server is used in this example to allocate IP addresses to the authenticated endpoints.

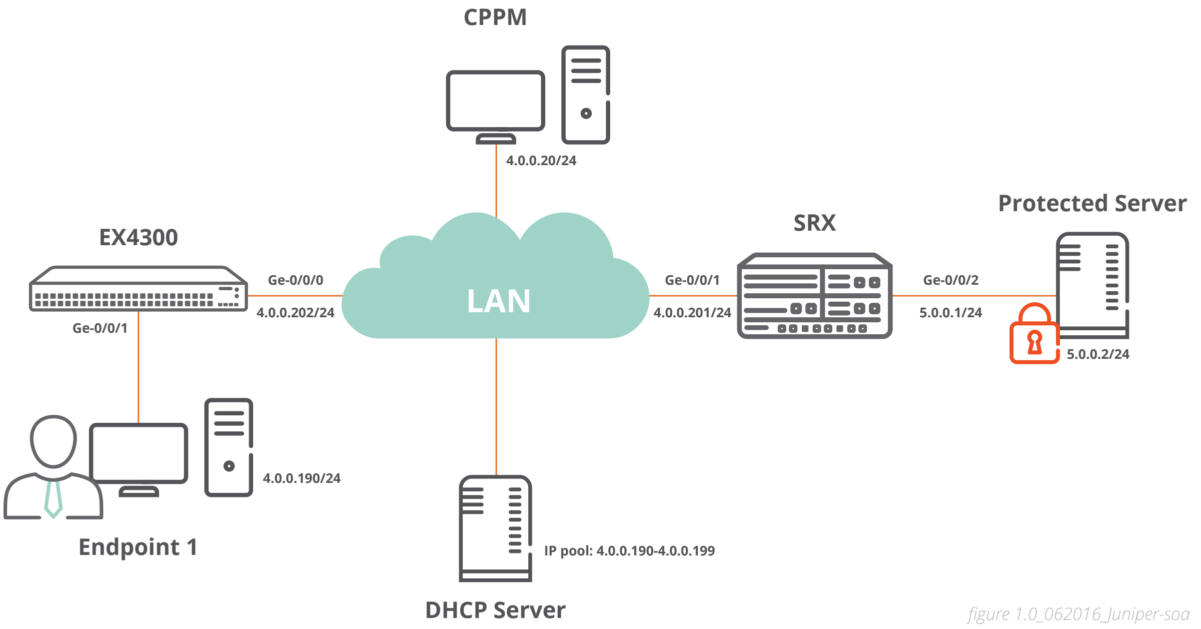

Figure 1. Juniper SRX, EX Switch and Aruba ClearPass

Juniper SRX Services Gateways protect against additional cybersecurity threats such as:

- Next generation firewall protection with application awareness
- Intrusion prevention
- Role based user controls
- Unified threat management

The combined ClearPass and Juniper SRX Services Gateway offers a best of breed integrated solution that can provide both the both the carrier grade scale and coverage necessary for threat protection and protection from unknown devices both on and within your network.

For more information:
www.arubanetworks.com/solutions/adaptive-trust-defense

ABOUT ARUBA, A HEWLETT PACKARD ENTERPRISE COMPANY

Aruba, a Hewlett Packard Enterprise company, is a leading provider of next-generation networking solutions for enterprises of all sizes worldwide. The company delivers IT solutions that empower organizations to serve the latest generation of mobile-savvy users who rely on cloud-based business apps for every aspect of their work and personal lives. For more information visit www.arubanetworks.com.

To learn more, visit Aruba at http://www.arubanetworks.com. For real-time news updates follow Aruba on Twitter and Facebook, and for the latest technical discussions on mobility and Aruba products visit Airheads Community at http://community.arubanetworks.com.

DATA EXCHANGED WITH OTHER NETWORK TOOLS

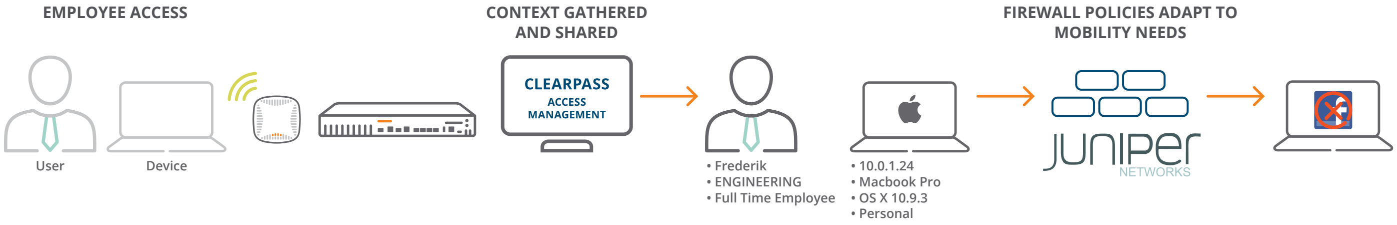

Figure 2. ClearPass Exchange Integration Workflow