ClearPass 6.1

Tech Note: Palo Alto Networks Integration with ClearPass 6.1

Overview

This document is intended to help field engineering, customers, and channel partners integrate Aruba Networks ClearPass 6.1.0 with Palo Alto Networks next-generation firewall and its central management system, Panorama. Customers can now leverage the Identity tracking features provided by ClearPass for known enterprise users using Active Directory and LDAP server, and for unknown guest/public user credentials that are used by Guest and HotSpot networks.

Why is this Integration Important?

Palo Alto Networks next-generation firewall offers contextual security for all users for a number of reasons – especially for safe enablement of applications. Simple firewalling beyond basic IP address or TCP port numbers only provides a subset of the enhanced security required for enterprises to secure their networks.

As an example, it's no longer acceptable to just 'deny Twitter' or 'deny Facebook' access. Many organizations use social networking Web sites to advertise their products, solutions, and activities. Social networking has become an accepted marketing tool and many companies now opt to use this as a mainstream part of their marketing efforts. As such, legacy firewalls are not able to differentiate valid authorized users from casual social networking users. So today's challenge to allow Facebook based upon contextual data such as username makes it almost impossible for legacy firewalls to implement granularity in security policy.

The Challenge

Historically, traditional firewalls make decisions based on Layer3/4 and some Layer7 information. For Web-based traffic, a decision would typically be based upon a domain or a URL string. Today, enterprises want to make decisions based upon the user and associated permissions, and, for this to happen, the firewall needs to correlate between the user and the assigned IP address. The challenge is finding meaningful sources of user information covering the full spectrum of network activity, including known users, guests, and non-enterprise configured users.

Background

One of the core features of the Palo Alto next-generation firewall is User-ID, which provides many methods for connecting to sources of identity information and associating them with firewall policy rules. For example, it has an option to gather user information from Active Directory or LDAP server. In the past, this functionality required the use of a User-ID agent running on a Windows workstation.

Similarly, an agent can be used to allow integration with a legacy Amigopod deployment to gather user information for the guest users. This integration allowed Amigopod to send user information to a Palo Alto Networks firewall via the User-ID agent running on a Windows workstation. In both scenarios above, the past approaches required an agent, which created dependencies that might not be easy to resolve in certain deployment scenarios. With the latest version of the Palo Alto Networks PAN-OS 5.0 and Aruba Networks ClearPass, a more seamless integration is now possible.

Next-Generation Solution

With the release of ClearPass 6.1.0, Aruba re-architected the integration between ClearPass Policy Manager and the Palo Alto Networks next-generation firewall to take advantage of the new XML APIs that were available in PAN OS 5.x.x. This simplified the solution significantly by making it more efficient and

streamlined. The requirement to download and configure a separate plug-in was eliminated and instead the solution was fully integrated into ClearPass' core product.

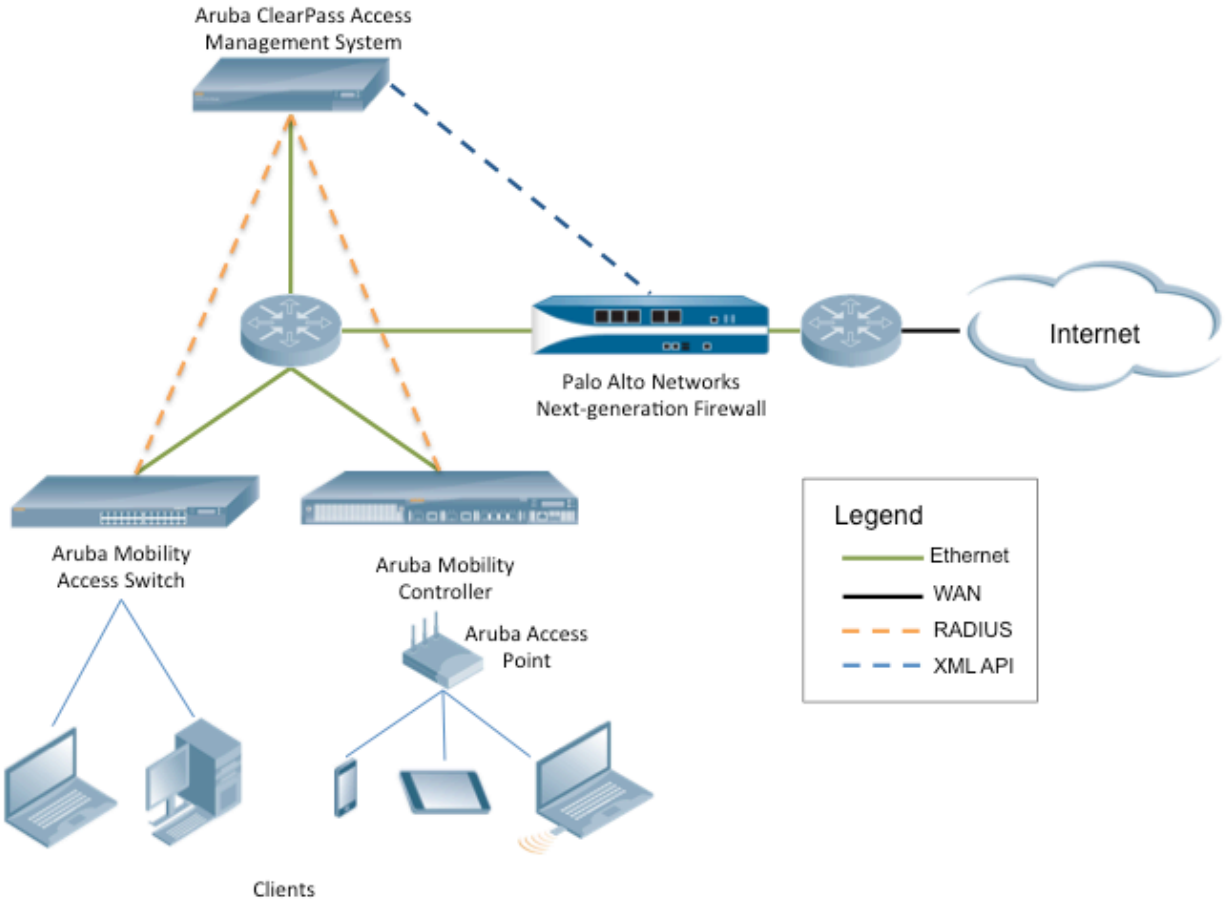

Figure 1 - ClearPass and Palo Alto Networks Integration Overview

Software Requirements

The minimum software version required on ClearPass Policy Manager is 6.1.0, which was released April 2013. The recommended minimum software version on the Palo Alto Networks firewall is PANOS 5.0.0, released in November 2012. However, it is recommended that you regularly review software updates to utilize the benefits from the latest fixes and feature updates.

ClearPass 6.1.0 Configuration

Configuring ClearPass for Palo Alto Networks firewall integration is a straightforward process. Step-by-step visual instructions are outlined in the following sections.

Adding Firewall Attributes

Under **Administration > External Server > Endpoint Context Servers > Add Context Server > Palo Alto Networks Firewall**, enter the required IP address of the Palo Alto Networks firewall, and a username/password pair that ClearPass will use to pass information to the required Palo Alto Networks firewall.

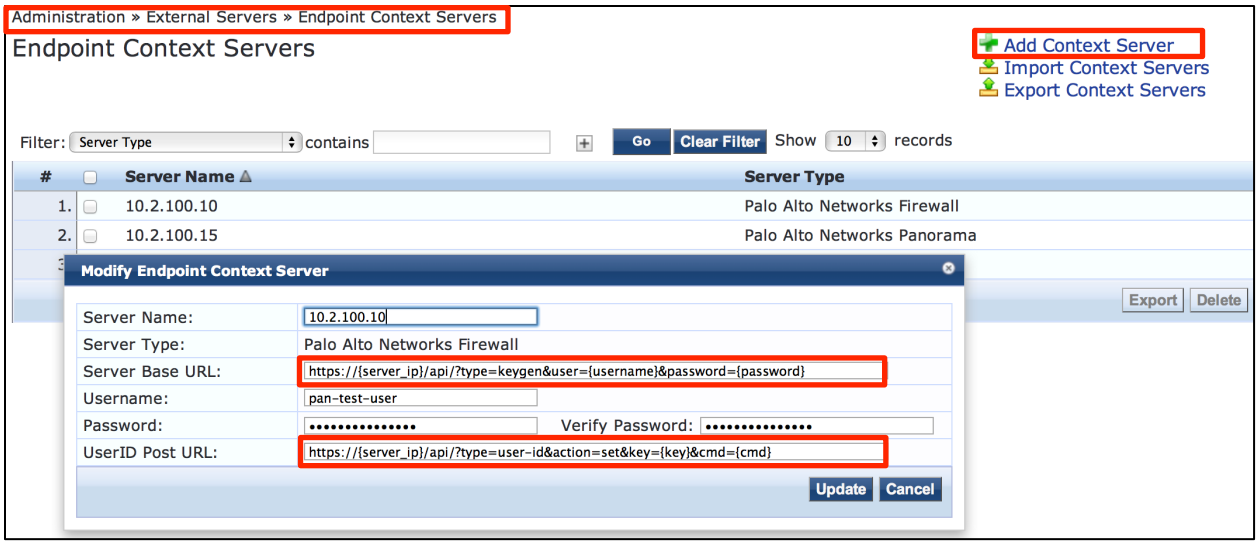

Figure 2 - Adding a Palo Alto Networks Firewall

Note: Do not change the Server Base URL or UserID Post URL. Although they are read/write fields, they are formatted to work with a Palo Alto Networks firewall running 5.x.x software. If there is a requirement to integrate with a Palo Alto Networks firewall running 4.x.x software, please contact your Aruba ClearPass specialist for advice.

Entering Panorama Values

Under **Administration > External Server > Endpoint Context Servers > Add Context Server > Palo Alto Networks Panorama**, enter the required IP address of the Palo Alto Networks Panorama server or an appliance, and a username/password pair that ClearPass will use to pass information to the required Palo Alto Networks firewall. In addition, it's very important that you configure the serial numbers of the Palo Alto Networks firewall under management of the Panorama appliance (as shown below).

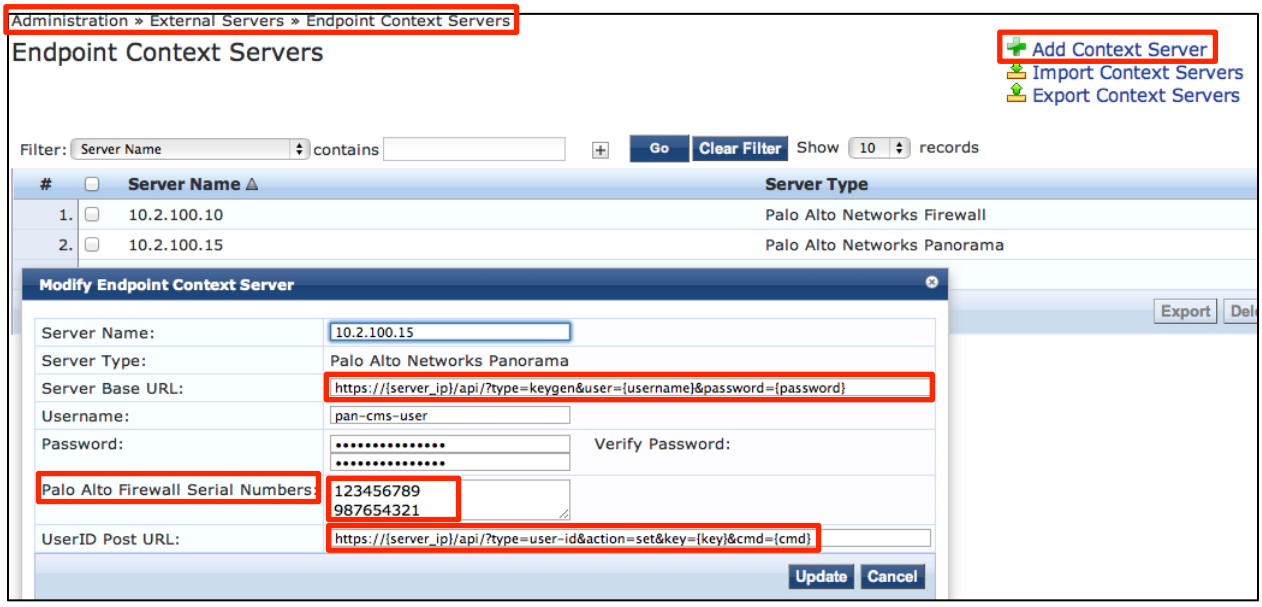

Figure 3 - Adding Palo Alto Networks Panorama

Note: Do not change the Server Base URL or UserID Post URL. Although these are read/write fields, they are formatted to work with Palo Alto Networks Panorama running 5.x.x software. If there is a requirement to integrate with a Palo Alto Networks firewall running 4.x.x software, please contact your Aruba partner or Aruba account team for advice.

How to Trigger Updates from ClearPass

After completing the steps in the previous two sections, there is only one final step required to ensure that, as users are authenticated with ClearPass, triggers are sent to the Palo Alto Networks firewall.

- This last process is done using a Post_Authentication Session Restrictions Enforcement profile.

Create a new Enforcement Profile as shown. Ensure this profile is created from the **Session Restrictions Enforcement** template.

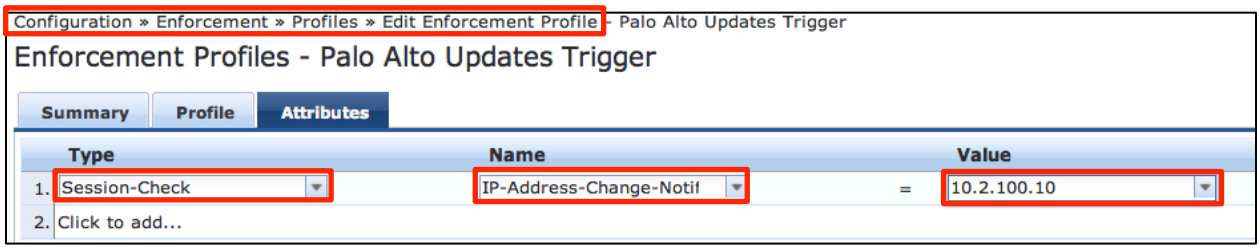

Figure 4 - Adding a Session Restriction Enforcement profile

Type = Name = *IP-Address-Change-Notification*

Value = *Palo Alto Networks endpoint*, previously added (this is a drop-down list field)

Note: If you don't see the Palo Alto Networks firewall, then you have missed a step in the earlier Adding Firewall Attributes section.

Associate Enforcement with a Service

After it is created, this Enforcement Profile needs to be associated with an access control policy in ClearPass before it will take effect. In the following example, we have associated the Enforcement Profile with a Secure Wireless service definition.

Adding the Enforcement Profile is performed under **Configuration > Services > Edit > Enforcement tab**.

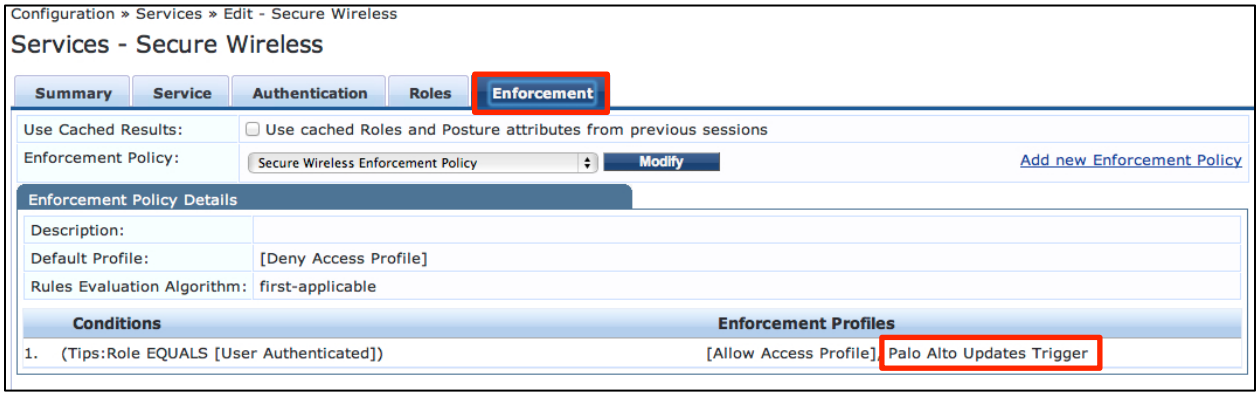

Figure 5 - Adding Enforcement Profile to a Service

Configuring Palo Alto Networks Next-Generation Firewall

Several steps need to be completed to take advantage of the integration we have developed. Many use cases exist in the scope of this integration to manage and control a user's access to different resources. We also documented the configuration on the firewall to allow Aruba's ClearPass to send data via Palo Alto Networks XML-based API.

Configuring a User to Allow CPPM to Communicate

For ClearPass to send data to a Palo Alto Networks firewall or Panorama, an account needs to be configured within Palo Alto Networks firewall/Panaroma. You could use the built in Admin account; however, we do not recommend this. Please create a new Admin account to be used solely for the purpose of ClearPass communicating with the Palo Alto Networks firewall.

Note: The account created here is what we configure in the endpoint context server when adding the Palo Alto Networks endpoints (see Adding Firewall Attributes).

The following screen capture displays the setup in the firewall. Panorama is very similar.

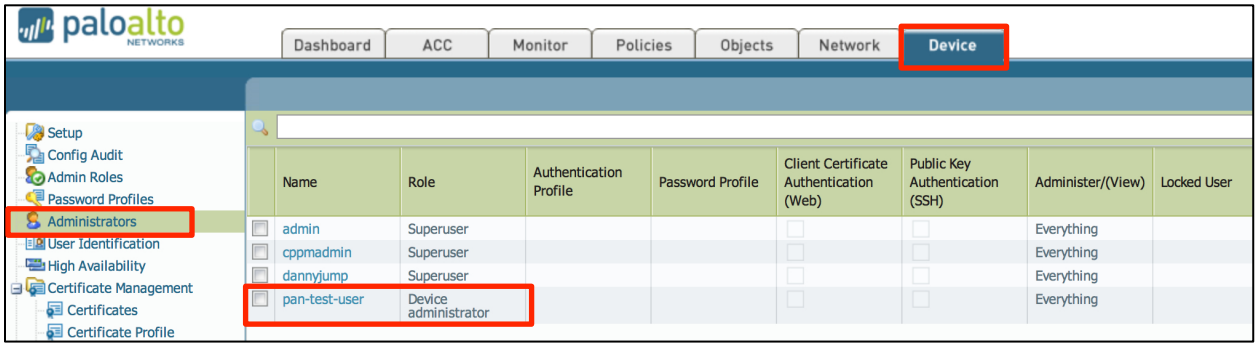

Figure 6 - Adding a User to Palo Alto Networks Firewall

In this example we have added a user 'pan-test-user' with a Role of 'Device administrator'. This matches the configuration described in the "Adding Firewall Attributes" section.

Configuring a Policy

A Palo Alto Networks firewall can build firewall rules using dynamic objects. A dynamic object is in essence an object type that is not tied to a fixed IP address. Aruba's ClearPass can complement a Palo Alto Networks firewall by supplying the dynamic object data.

- **UserID + Source IP address**
- **UserID + Device Type**

As of April 2013, we currently have to create the device types manually. In a future release we will extend our integration to allow ClearPass to push the discovered device types.

As a reference, the **device type** of someone that was authenticated in ClearPass can be viewed under **Administration >Dictionaries > Fingerprints.** The list below shows 211 device type groups. Shown are two lists, one generic and one more specific to Apple devices.

Administration » Dictionaries » Fingerprints

Device Fingerprints

Filter: Category contains SmartDevice Go Clear Filter Show 10 records

#	Category	Family	Name
2	SmartDevice	Apple	Apple iOS Device
3	SmartDevice	Apple	Apple iPod
4	SmartDevice	Apple	Apple iPad
5	SmartDevice	Apple	Apple iPhone
6	SmartDevice	Sony Ericsson	Sony Ericsson W800i
7	SmartDevice	Samsung	Samsung Device
8	SmartDevice	Samsung	Samsung S-Series
9	SmartDevice	Samsung	Samsung T-Mobile
10	SmartDevice	Windows	Samsung Windows
11	SmartDevice	LG	LG BL40

Figure 7 - CPPM Fingerprints, Name Column = Device Type

Administration » Dictionaries » Fingerprints

Device Fingerprints

Filter: Name contains apple Go Clear Filter Show 10 records

#	Category	Family	Name
2	Network Boot Agents	Apple	Apple Netboot
3	Router	Apple	Apple Airport
4	SmartDevice	Apple	Apple iOS Device
5	SmartDevice	Apple	Apple iPod
6	SmartDevice	Apple	Apple iPad
7	SmartDevice	Apple	Apple iPhone

Showing 1-6 of 6

Figure 8 - CPPM Fingerprint Device Type Just 'apple'

paloalto NETWORKS

Dashboard | ACC | Monitor | Policies | Objects | Network | Device

- Addresses
- Address Groups
- Regions
- Applications
- Application Groups
- Application Filters
- Services
- Service Groups
- GlobalProtect
  - HIP Objects
  - HIP Profiles
- Custom URL Category
- Dynamic Block Lists
- Custom Signatures
  - Data Patterns
  - Spyware

Name	Location	Type	Address
Android		Dynamic	Android
Apple_iPad		Dynamic	Apple_iPad
Apple_iPhone		Dynamic	Apple_iPhone
Apple_iPod		Dynamic	Apple_iPod
external interface		IP Netmask	192.168.1.200/24
HTC Android		Dynamic	HTC_Android
HTC_Android		Dynamic	HTC_Android
Linux_Computer		Dynamic	Linux_Computer
Mac_OS_X		Dynamic	Mac_OS_X
Samsung_Android		Dynamic	Samsung_Android
Windows_Vista_7		Dynamic	Windows_Vista_7

Figure 9 - Palo Alto Networks manually created 'dynamic' objects

Note: When creating definitions on the Palo Alto Networks firewall, a device type under ClearPass can use a space in the name. Ensure that on the Palo Alto Networks firewall, object definitions with a space are created with an underscore – for example, "Apple_iPad," not "Apple iPad"

After the objects are created, the power of the Palo Alto Networks Policy engine can be leveraged. A firewall rule that exploits this is shown below.

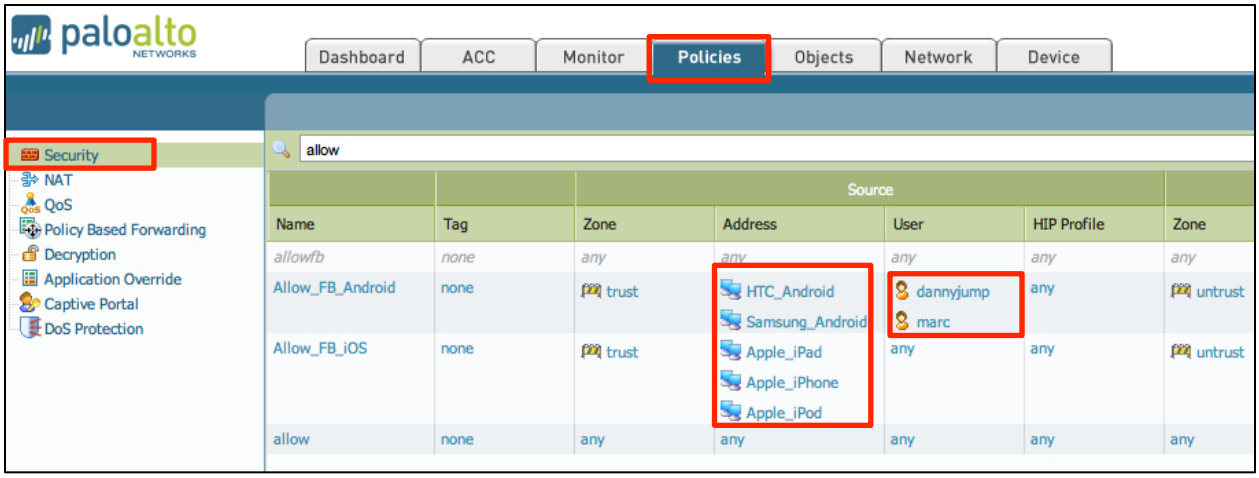

Figure 10 - Basic Firewall Rules

Historically, traditional firewalls classify traffic based on port number and IP address. However, port number is no longer a meaningful way to classify traffic, because any application can use any port number. The Palo Alto Networks next-generation firewall classifies traffic by application, and enforces policy based on the context of business elements such as application, user, and content.

The following rule shows the use of device types as a source address in the Trust zone.

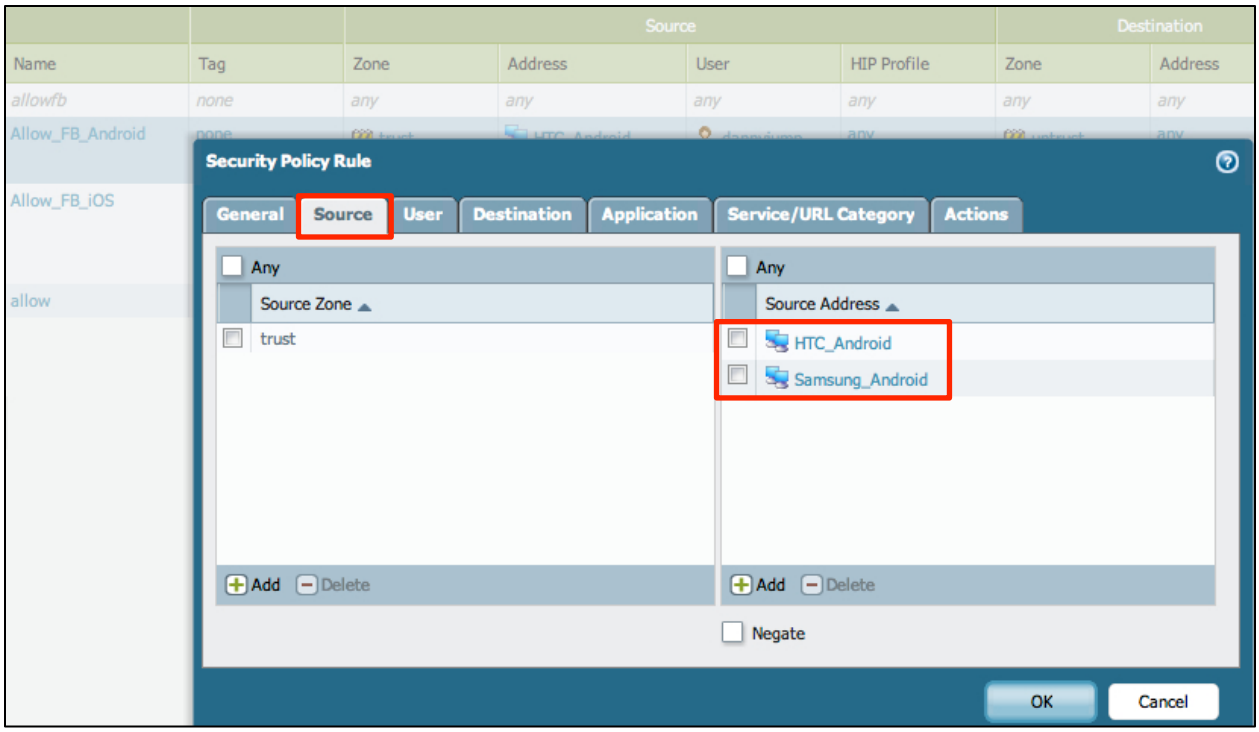

Figure 11 - Firewall Rule Based Upon a Source of a Device Type

In a similar way we can exploit the power of the Palo Alto Networks policy engine to make permit/deny decisions based upon a user name. In the example below, we are selecting the users 'marc' and 'dannyjump' in this particular policy.

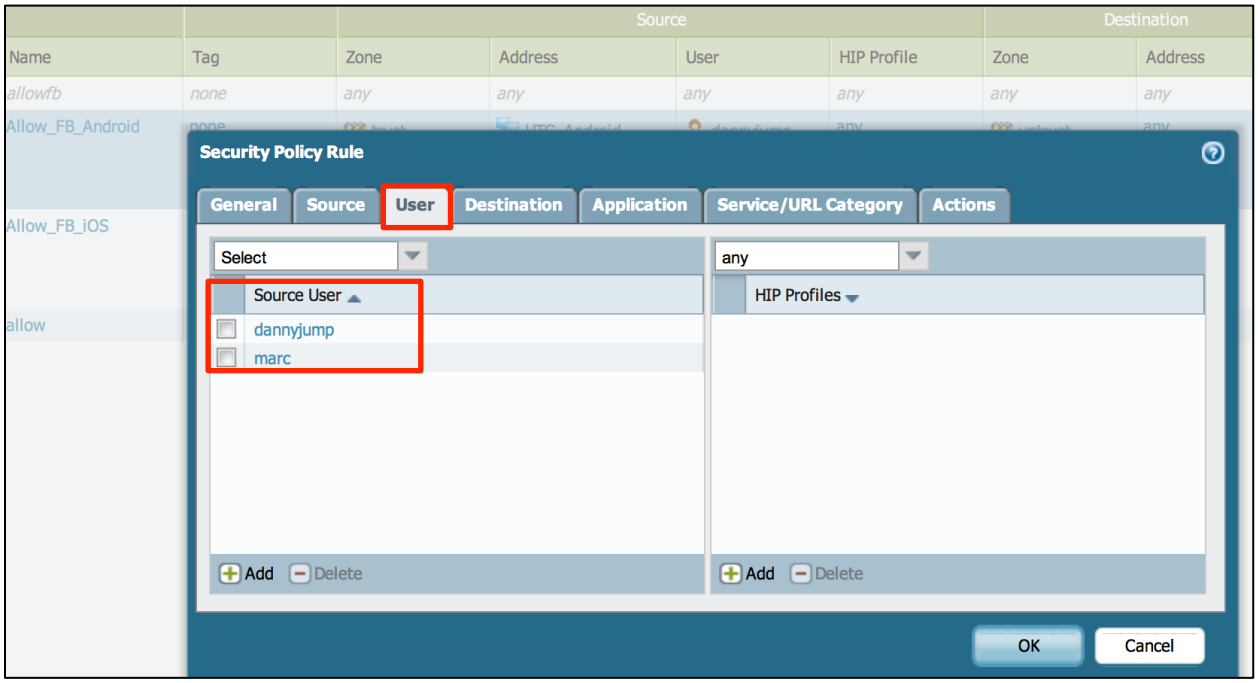

Figure 12 - Firewall Rule Based Upon a Source of a User Name

Conclusion

Aruba ClearPass in conjunction with Palo Alto Networks can provide administrators with full context and visibility about the users and devices on the network to deliver end-to-end safe application enablement.