TECH NOTE

PALO ALTO NETWORKS NEXT-GENERATION FIREWALL AND ARUBA WLAN INTEGRATION
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Overview</strong></td>
<td>3</td>
</tr>
<tr>
<td><strong>Why is this Integration Important?</strong></td>
<td>3</td>
</tr>
<tr>
<td>ARUBA Controller and Palo Alto Networks Firewall Integration Details</td>
<td>4</td>
</tr>
<tr>
<td>ARUBA Instant and Palo Alto Networks Firewall Integration Details</td>
<td>7</td>
</tr>
<tr>
<td>Appendix A – Sample Configurations</td>
<td>9</td>
</tr>
<tr>
<td>Appendix B – Verification Commands</td>
<td>16</td>
</tr>
<tr>
<td>About Aruba Networks, Inc.</td>
<td>22</td>
</tr>
</tbody>
</table>
OVERVIEW
This document is intended to help field engineering, customers, and channel partners integrate Aruba Networks Mobility Controllers and Aruba Instant Wi-Fi Access Points with the Palo Alto Networks next-generation firewall and its central management system, Panorama.

The document details the configurations required on the Aruba controllers and Instant Access Points to integrate with Palo Alto Networks firewalls. This document assumes that the reader has a working knowledge of the Aruba platforms.

WHY IS THIS INTEGRATION IMPORTANT?
Palo Alto Networks next-generation firewall offers a wide variety of contextual security for all users – including the safe enablement of applications. By looking beyond simple IP address or TCP port firewall rules to actual application payload, and taking into account who the user of the application is, Palo Alto Networks is able make intelligent, policy-driven decisions that adapt to today’s evolving network security needs.

As an example of safe application enablement, 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. Today, enterprises need to make decisions based upon users and associated permissions. For this to happen, the firewall needs to correlate the user with their assigned IP address. The challenge is finding meaningful sources of user information covering the full spectrum of network activity, including known users, guests and other non-enterprise classified users.

This is further compounded when considering enterprise mobility trends like bring your own device (BYOD), guest network access and the use of shared networked resources like Wi-Fi enabled printers, projectors, Apple TVs, lights and alarms. In most cases, security for these devices is handled differently than that of enterprise-owned devices making it even more difficult to get meaningful data.

The Aruba Palo Alto Networks integration aims to solve this problem. Through the integration with the Aruba Controllers and Aruba Instant Wi-Fi Access Points, Aruba provides mobile user context (usernames, IP addresses, and device types) to the Palo Alto Network next generation firewall for all authenticated users and guest as well as their devices including information gathered about shared resource devices like printers and scanners.

The Palo Alto Networks User-Id feature can now leverage this integration to resolve the username to IP address mapping for all wireless users from an Aruba WLAN solution (controllers and Instant Access Points), thus simplifying the deployment significantly by reducing the number of integration sources the firewall would ordinarily require to obtain the same set of information.

This integration also helps identify and secure guest users, devices like printers, projectors, scanners, and BYOD devices which would otherwise be undistinguishable from one another because of their transient nature and the lack of user information associated to them. Exposing this information to the Palo Alto Networks firewall allows security administrators to use more granular controls when securing today’s mobile enterprise networks.
ARUBA CONTROLLER AND PALO ALTO NETWORKS NEXT-GENERATION FIREWALL INTEGRATION DETAILS

Sample Network Topology

Software and Hardware Requirements

The minimum software version required on Aruba Mobility Controller is AOS v6.4. The recommended minimum software version on the Palo Alto Networks next-generation firewall is PAN-OS 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.

Note: The integration is not currently supported under the following conditions:

- On APs deployed in bridged forwarding mode
- On 600 series controllers or the model 3200 controller

Update Messages from the Aruba Controller to the Firewall

Using the PAN-OS XML API, the Aruba Controller sends the following update messages to the Palo Alto Network next generation firewall for every client that connects to the WLAN:

- Logon event when a client connects to the wireless network with the client username, IP address and device type if available.
- Login update event with client username, IP address and device type, if the controller determines a device type.
- “Keep alive” event if the user is active on the controller for more than 45 minutes. The age out time on the firewall is 45 minutes and the keep-alive messages are required to maintain the client entries on the firewall.
- Logout event with the client name and IP address when the client disconnects from the wireless network.

Figure 1: Aruba Networks Controller and Palo Alto Networks Integration Overview
The Palo Alto Networks next-generation firewall uses this information to associate the particular user and device with firewall policy. User-ID associates the user at a particular IP address and determines which applications the user may access. The device characteristics are mapped to a Host Information Profile (HIP) which is also used as part of the firewall policy criteria.

**Pre- configurations on the Palo Alto Networks Firewall**

Before the Palo Alto Networks integration is completed on the controller, the following configurations must be completed on the Palo Alto Networks firewall

- **Admin Account**
  
  An Admin account must be created on the Palo Alto Networks firewall to allow the controller to send data to it. The built-in Admin account can be used for this purpose but that is not recommended. It is better to create a new Admin account used solely for the purpose of communications between the controller and Palo Alto Networks firewall.

- **User-ID Support**

  To utilize the full potential of the integration, the firewall policies on the Palo Alto Networks firewall should be configured to accommodate user-names and/or user-groups.

- **Device-Type Based Policy Support**

  Pre-configuration of the Palo Alto Networks Host Information Profile (HIP) objects and HIP-profiles on the Palo Alto Networks Firewall are required to support device-type based policies on the firewall.

  The controller can identify a limited set of device types. The identified device type associated with each IP user will be sent to the Palo Alto Networks firewall in the client-version field with the host-info category of the HIP-report. In order to leverage the device type information on the firewall, it is necessary to create HIP objects, which filter the HIP-reports sent from the controller.

  The following table lists the HIP objects with specific Is Value in the Client Version field, which must be preconfigured on the Palo Alto Networks firewall for device-type based policies to work.

<table>
<thead>
<tr>
<th>HIP OBJECTS</th>
<th>Client Version Is Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android</td>
<td>webOS</td>
</tr>
<tr>
<td>Apple TV</td>
<td>Win 2000</td>
</tr>
<tr>
<td>BlackBerry</td>
<td>Win 7</td>
</tr>
<tr>
<td>Chrome OS</td>
<td>Win 8</td>
</tr>
<tr>
<td>iPad</td>
<td>Win 95</td>
</tr>
<tr>
<td>iPhone</td>
<td>Win 98</td>
</tr>
<tr>
<td>iPod</td>
<td>Win CE</td>
</tr>
<tr>
<td>Kindle</td>
<td>Windows</td>
</tr>
<tr>
<td>Linux</td>
<td>Windows Mobile</td>
</tr>
<tr>
<td>Nintendo 3DS</td>
<td>Windows Phone 7</td>
</tr>
<tr>
<td>Nintendo Wii</td>
<td>Win ME</td>
</tr>
<tr>
<td>Nook</td>
<td>Win NT</td>
</tr>
<tr>
<td>OS X</td>
<td>Win Server</td>
</tr>
<tr>
<td>PS3</td>
<td>Win Vista</td>
</tr>
<tr>
<td>PSP</td>
<td>Win XP</td>
</tr>
<tr>
<td>PS Vita</td>
<td>Apple</td>
</tr>
<tr>
<td>RIM Tablet</td>
<td>PlayStation</td>
</tr>
<tr>
<td>Roku</td>
<td>Nintendo</td>
</tr>
<tr>
<td>Symbian</td>
<td></td>
</tr>
</tbody>
</table>

Note: Please refer to the Palo Alto Networks next generation firewall configuration guides for additional information on how to configure the firewall.
Controller Configuration on AOS 6.4

Creating the Server Profile for Palo Alto Network on the Controller

The first step in configuring the Palo Alto Networks firewall integration is to create a server profile for Palo Alto Networks on the controller. This profile provides the controller with the information required for connecting to and interacting with the specified Palo Alto Networks firewall.

The Palo Alto Networks Servers profile has to be created on the Master controller. Multiple profiles can simultaneously exist on the master controller but only one profile can be active per controller at any given time. The profiles are activated locally on each controller.

Using Web UI:

To configure a new Palo Alto Networks profile,

1. Navigate to Configuration > Advanced Services > All Profiles > Other Profiles > Palo Alto Networks Servers
2. Type the name of the profile and click Add
3. Click on the name of the profile created to open the Profile Details window
4. Enter the Host (IP address or hostname) of the Palo Alto Networks firewall
5. Enter the Port (1-65535) of the Palo Alto Networks Firewall
   - Note: The port used by default is 443
6. Enter the Username of the Palo Alto Networks firewall.
   - The user name is between 1 and 255 bytes in length and must match the Admin Account previously created on the Palo Alto Networks firewall.
   - Note: Refer to section 3.3
7. Enter the Password of the username in Palo Alto Networks Firewall.
   - The password is between 6 and 100 bytes in length and must match the password used for the Admin account on the Palo Alto Networks firewall.
8. Re-enter the Password entered in the previous step
9. Click Add
10. Click Apply

In 6.4, each Palo Alto Network Server profile can support up to 20 Palo Alto firewall configurations

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host (IP or hostname)</td>
<td>The hostname or IP address of Palo Alto Networks Firewall</td>
</tr>
<tr>
<td>Port (1-65535)</td>
<td>The port used by the firewall (default value is 443)</td>
</tr>
<tr>
<td>Username</td>
<td>The username matching the Admin Account on the Palo Alto Networks firewall (1-255 bytes in length)</td>
</tr>
<tr>
<td>Password</td>
<td>Password match the password used for the Admin account on the Palo Alto Networks firewall</td>
</tr>
</tbody>
</table>

Using CLI:

(host)(config) #pan profile <profile-name>
firewall host <host> port <port> username <username> passwd <password>

Activating the Palo Alto Networks profile

Once a Palo Alto Networks Server profile has been created, the profile must be activated. Select profile you want to activate from the list of configured profiles. Although multiple profiles can be created, only one profile can be active at one time.

Note: This configuration must be completed on each local controller.

Using the Web UI

To apply a Palo Alto Networks Server profile on the local controller, complete the following steps:

1. Navigate to Configuration > Advanced Services > All Profiles > Other Profiles > Palo Alto Networks Active
2. Select Active Palo Alto Networks. To the right of this link, the name of the active profile is displayed.
3. Other configured profile can be selected from the Active Palo Alto Networks Profile > drop-down menu. To configure a new profile, select NEW from the drop down menu and complete the configuration details.
4. Once a profile is selected from the drop-down menu or a new profile is created, click Apply.

Using the CLI

(host)(config) #pan active-profile profile <profile-name>
Enabling the Palo Alto Networks Firewall Integration

Once the Palo Alto Networks Server profile is configured, it needs to be enabled on the AAA profile being used for the client authentication.

**Using Web UI:**
To enable a Palo Alto Networks firewall integration in the AAA profile:
2. In the AAA Profiles Summary, select the desired profile.
3. Check the PAN firewalls Integration check box.
4. Click Apply.

**Using CLI:**
(host)(config) #aaa profile <aaa profile-name>
pan-integration

Enabling Palo Alto Networks Profile Integration for VIA Clients

For VIA clients, the Palo Alto Networks firewall integration must be enabled on the VIA authentication profile that the client is associated with.

**Using Web UI:**
To enable Palo Alto Networks firewall integration for VIA clients:
2. In the profiles list on the left, click VIA Authentication and select the desired profile.
3. Check the PAN firewalls Integration check box.
4. Click Apply.

**Using CLI:**
(host)(config) #aaa authentication via auth-profile <profile-name>
pan-integration

Enabling Palo Alto Networks Profile Integration for VPN Clients

For VPN clients, the Palo Alto Networks firewall integration must be enabled on the VPN authentication profile that the client is associated with.

**Using Web UI:**
To enable Palo Alto Networks firewall integration for VPN clients:
2. In the profiles list on the left, click VPN Authentication and select the desired profile.
3. Check the PAN firewalls Integration check box.
4. Click Apply.

**Using CLI:**
(host)(config) #aaa authentication vpn default pan-integration

ARUBA INSTANT AND PALO ALTO NETWORKS FIREWALL INTEGRATION DETAILS

Sample Network Topology

Figure 2: Aruba Networks Instant AP and Palo Alto Networks Integration Overview
Software and Hardware Requirements
The minimum software version required on Aruba Instant AP is 6.3.1.1-4.0. The recommended minimum software version on the Palo Alto Networks next-generation firewall is PAN-OS 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.

Update Messages from the Aruba Instant to the Firewall
In a single AP environment, the Aruba Instant access point directly communicates with the Palo Alto Networks next-generation firewall using the PAN-OS XML API. However, in a multi-AP environment with more than one AP in a cluster, the virtual controller communicates with the Palo Alto Networks firewall using the API.

The following update messages to the Palo Alto Networks next-generation firewall for every client that connects to the WLAN –

• Logon event when a client connects to the wireless network with the client username and IP address
• Login update event with client username and IP address
• “Keep alive” event if the user is active on the controller for more than 45 minutes. The age out time on the firewall is 45 mins and the keep alive message is required to maintain the client entry on the firewall.
• Logout event with the client name and IP address when the client disconnects from the wireless network

Pre-configurations on the Palo Alto Networks Next-Generation Firewall
Please refer to section 3.4 on the pre-configurations required on the Palo Alto Networks firewall.

Instant AP Configuration on 6.3.1.1-4.0
To enable the API communication between the Aruba Instant AP and the Palo Alto Networks next-generation firewall, the following need to be configured on the Aruba Instant AP.

Using Web UI:

1. Navigate to More > Services. The Services window is displayed.
2. Click on the Network Integration tab. The Palo Alto firewall configuration options are displayed.
3. Select the Enable checkbox to enable the Palo Alto Networks firewall.
   A. Enter the Host (IP address or hostname) of the Palo Alto Networks firewall

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host (IP or hostname)</td>
<td>The hostname or IP address of Palo Alto Networks Firewall</td>
</tr>
<tr>
<td>Post (1-65535)</td>
<td>The port used by the firewall (default value is 443)</td>
</tr>
<tr>
<td>Username</td>
<td>The username matching the Admin Account on the Palo Alto Networks firewall</td>
</tr>
<tr>
<td>Password</td>
<td>Password match the password used for the Admin account on the Palo Alto Networks firewall</td>
</tr>
</tbody>
</table>

Using CLI:

(Instant Access Point)(config)# firewall-external-enforcement pan
(Instant Access Point)(firewall-external-enforcement pan)# enable
(Instant Access Point)(firewall-external-enforcement pan)# ip <ip-address>
(Instant Access Point)(firewall-external-enforcement pan)# port <port>
(Instant Access Point)(firewall-external-enforcement pan)# user <name> <password>
(Instant Access Point)(firewall-external-enforcement pan)# end
(Instant Access Point)# commit apply
APPENDIX A – SAMPLE CONFIGURATIONS

Network Topologies

Test topology used to validate the Aruba controller and Palo Alto Networks firewall integration

![Network Topologies Diagram]

**CLIENTS AND DEVICES USED IN TESTING THE SETUP**

<table>
<thead>
<tr>
<th>User Name</th>
<th>IP Address</th>
<th>Device Type</th>
<th>Auth Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>iphone-user</td>
<td>10.68.105.24</td>
<td>iPhone</td>
<td>802.1x-EAP-PEAP</td>
</tr>
<tr>
<td>ipad-user</td>
<td>10.68.105.26</td>
<td>iPad</td>
<td>802.1x-EAP-PEAP</td>
</tr>
</tbody>
</table>

Figure 3: Controller Setup
Test Topology used to validate the Aruba Instant and Palo Alto Networks firewall integration

1. Users are created in the Aruba Instant internal database
2. Users are authenticated by Instant using 802.1X EAP-PEAP (AAA Profile)

<table>
<thead>
<tr>
<th>User ID</th>
<th>User ID</th>
<th>IP Address</th>
<th>Device Type</th>
<th>Auth Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>User 1</td>
<td>User 1</td>
<td>172.31.99.107</td>
<td>iPhone</td>
<td>802.1x-EAP-PEAP</td>
</tr>
<tr>
<td>User 2</td>
<td>User 2</td>
<td>172.31.98.58</td>
<td>iPad</td>
<td>802.1x-EAP-PEAP</td>
</tr>
</tbody>
</table>
Configurations the Palo Alto Networks firewall to support the integration – Sample Setup

**Step 1.** Configuring the Admin Account on the Palo Alto Networks firewall (PAN-500, 10.2.100.10)

A. Logon to the Palo Alto Networks firewall WebUI using the root admin account
B. Navigate to Devices tab
C. From the menu on the right, select Administrators

d. Click Add and enter the Account information (name, password, role). In this example the username used was pan-test-user and the role selected was Device administrator

E. Commit the changes and logout

**Step 2.** Create the HIP Object entry on the Palo Alto Networks next-generation firewall

Manually create a HIP Object Entry for every Client Version listed in Table 1, Section 3.3

![Figure 5: Adding an Admin Account to Palo Alto next-generation firewall](image-url)
HIP objects can also be created using the CLI on the Palo Alto Networks firewall.

pan-test-user@PA-500> configure terminal
Entering configuration mode
[edit]
pan-test-user@PA-500# set profiles hip-objects
iPhone host-info criteria client-version is iPhone

pan-test-user@PA-500# set profiles hip-objects
iPad host-info criteria client-version is iPad

... 

Step 3. Ensure that User-Id support is enabled on the Palo Alto Networks firewall

Please refer to the Palo Alto Networks support site or configuration guides for User-Id support

NOTE: The first three steps are samples of the Palo Alto Networks configurations. Please refer to the Palo Alto Networks support site or the Palo Alto Networks firewall configurations guides for information on configuring the firewall.
Configuring the Aruba Mobility Controller – Sample Setup
Refer to Network Topology Diagram in Section 5.1.1

For the purpose of this example, only one controller was used. This controller serves the role of the master and local controller.

**Step 1.** Create a Palo Alto Networks Server profile on the controller for the Palo Alto Networks firewall PAN-500

A. Navigate to Configuration > Advanced Services > All Profiles > Other Profiles > Palo Alto Networks Servers

B. Type the name of the profile, PAN-500, and click Add

C. Click on PAN-500 to open the **Profile Details** window

D. Enter the Admin Account information created in Step 1, Section 4.2

   - Host: 10.2.100.10
   - Port: 443 (default)
   - User Name: pan-test-user
   - Password: **********
   - Retype Password: **********

**Step 2.** Activate the Palo Alto Networks Server profile on the controller.

In this example, the master and the local controller are the same, so the PAN-500 profile is activated on the **Controller-PAN-Test** Controller

A. Navigate to Configuration > Advanced Services > All Profiles > Other Profiles > Palo Alto Networks Active

B. Select **Active Palo Alto Networks**

C. Click on the drop down menu corresponding to **Active Palo Alto Networks Profile**

D. Select the **PAN-500** profile that was created in Step 1 Section 4.3

![Figure 7](image-url)

![Figure 8](image-url)
**Step 3.** Enabling the Palo Alto Networks firewall Integration on the active AAA profiles.

To ensure that the client information (username, IP address and device type) is passed on from the controller to the firewall, it is required to enable the **PAN firewall Integration** checkbox on all active AAA profiles used on the controller to authenticate the clients.

In this example, **PAN-Test-Employee-aaa_prof** is a preconfigured AAA profile used for user authentication on the **Controller-PAN-Test** Controller.

A. Navigate to the Configuration > Security > Authentication > AAA Profiles page.

B. In the AAA Profiles Summary, select the **PAN-Test-Employee-aaa_prof** profile.

C. Check the **PAN Firewalls Integration** check box.

In this example the VIA clients and VPN client support were not configured on this controller.
Configuring the Aruba Instant AP – Sample Setup

Refer to Network Topology Diagram in Section 5.1.2

For the purpose of this example, only one Instant AP was used.

**Step 1.** Create a Palo Alto Networks global profile on the Instant AP Virtual Controller (PAN-Test-Controller) for the Palo Alto Networks firewall

A. Navigate to More > Services

B. The Services window will appear, select Network Integration tab to enable the Palo Alto Networks integration and enter the Palo Alto Networks Profile information, as shown in figure 9 and 10 below.

C. Enter the Admin Account information created in Step 1, Section 2.2

   Host: 10.2.100.10
   Port: 443 (default)
   User Name: pan-test-user
   Password: *********
   Retype Password: *********

---

**Figure 9: Instant WebUI**

**Figure 10: Services Window “Network Integration” Tab**
APPENDIX B – VERIFICATION COMMANDS

Controller Verification Commands

show pan profile

The show pan profile CLI command lists all the Palo Alto Networks Server Profiles created along with the references to the profiles.

```
(Controller-PAN-Test) #show pan profile
Palo Alto Networks Servers Profile List
---------------------------------------
Name     References  Profile Status
---------     ----------  --------------
default      0
PAN-500     1
.PAN-VM      0
Total: 3
```

The output shows that there are three Palo Alto Networks Server Profiles created (default, PAN-500, PAN-VM) and PAN-500 has been referenced in another profile once.

The show pan profile command also takes a Palo Alto Networks profile name as input to provide additional information on the profile.

Ex:

```
(Controller-PAN-Test) #show pan profile PAN-500
Palo Alto Networks Servers Profile ”PAN-500”
--------------------------------------------
Parameter                    Value
---------                    ----- 
Palo Alto Networks Firewall  10.2.100.10:443 pan-test-user/********
```

show pan active-profile

The show pan active-profile CLI command lists the Palo Alto Networks Active Profiles that have been activated on the controller. In 6.4, only one active profile can exist per controller

```
(Controller-PAN-Test) #show pan active-profile
Palo Alto Networks Active Profile
---------------------------------
Parameter                          Value
----------------                        --------
Active Palo Alto Networks profile  PAN-500
```

The output shows PAN-500 has been activated on the controller
show pan state

The `show pan state` command is used to verify the connectivity with the Palo Alto Networks firewall. The connection state in the output needs to be set to UP and Established for the communication between the firewall and the controller to be operational.

```
(Controller-PAN-Test) #show pan state
Palo Alto Networks Servers Connection State[PAN-500]

Firewall  State
---------  ------
10.2.100.10:443 UP[01/23/14 09:56:01] Established
```

show pan statistics

The `show pan statistics` command lists the server communication statistics summary. The command output displays the total quantity of user messages – logins, logouts, and connection refreshes – that have been sent by the controller, along with stats for each configured PAN-OS receiver.

```
(Controller-PAN-Test) #show pan statistics
Palo Alto Networks Interface Statistics Summary
-----------------------------------------------
Login Reqts  Logout Reqts  Refresh Reqts
---------  ------------  ------------
5          2             4

Per-PAN server Statistics Summary
---------------------------------

PAN Server  User-ID Reqts  Sent  Skipped  Success  Failure  Last Error
----------  -------------  ----  -------  -------  -------  ----------
10.2.100.10:443  3              3     0        3        0
```

show pan debug

```
(Controller-PAN-Test) #show pan debug
Palo Alto Networks Interface Debug Information
----------------------------------------------
User Changed User Deleted Refresh Login Reqts Logout Reqts Refresh Reqts No UserName No Change No Deletion
---------  ------------  -------  -----------  ------------  -------------  -----------  ------------------
9          2             594      5            2             4              0            4          0

Per-PAN server Debug Information
---------------------------------

PAN Server  State            User-ID Reqts  Sent  Skipped  Success  Failure  Last Error
----------  -----             -------------  ----  -------  -------  -------  ----------
10.2.100.10:443  UP[01/23/14 09:56:01] Established  3              3     0        3        0

Work Factory Debug Information
-------------------------------
Mgmt Queue  Reqts Queue
---------  ----------
0         0(8192)
```

PAN Local UID-Table - total:2(2) cur:2 ref:3
**Aruba Instant verification commands**

**show summary**

The `show summary` command summarizes all the settings on the instant and include the Palo Alto Networks setting:

```
PAN-Test-AP# show summary
--- omitted ----
PAN Firewall IP Address    :10.2.100.10
PAN Firewall Port          :443
PAN Firewall User          :pan-test-user
PAN Firewall Password      :9b5545de650165121bea755e9fcfa73a
PAN Firewall Status        :Enabled
```

**show ap debug pan-key**

This lists the Palo Alto firewall key that is configured on the instant to enable communications with the Palo Alto Networks firewall:

```
PAN-Test-AP# show ap debug pan-key
pan _ firewall _ key :
LUFRPT0vN1lxelhBdFVWc09jVTk2emRDcG9CS29GQjA9aEcOyQjZPVGPWQ2RtGERPwU9t
UHVHN32sdHJEBdWURzFYSnFzQ0xzOx1wST0
```

**show log ap-debug**

The “show log ap-debug” CLI command can be used to check the statistics of the Palo Alto Networks global profile traffic exchange between IAP and Palo Alto Networks firewall.

```
PAN-Test-AP# show log ap-debug
Apr  8 10:39:18  awc[1546]: Message over SSL from 10.2.100.10, SSL _ read() returned 534, Message is “HTTP/1.0 200 OK” M Date: Tue, 08 Apr 2014 18:36:51 GMT” M Server: PanWeb Server/ - “M ETag: “c7bf-110-52aa2378” M Connection: close” M Pragma: no-cache” M Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0” M Content-Type: application/xml; charset=UTF-8” M Expires: Thu, 19 Nov 1981 08:52:00 GMT” M Set-Cookie: PHPSESSID=3ff675616b2abe7d58280041fdalc4ab; path=/; HttpOnly”M Set-Cookie: PHPSESSID=3ff675616b2abe7d58280041fdalc4ab; path=/; HttpOnly”M "M", AWC response: (null)
```

```
PAN-Test-AP# show log ap-debug
Apr  8 10:39:18  awc[1546]: Message over SSL from 10.2.100.10, SSL _ read() returned 69, Message is “<response status="success" result= "[]"/>”, AWC response: HTTP/1.0 200 OK” M Date: Tue, 08 Apr 2014 18:36:51 GMT” M Server: PanWeb Server/ - “M ETag: “c7bf-110-52aa2378” M Connection: close” M Pragma: no-cache” M Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0” M Content-Type: application/xml; charset=UTF-8” M Expires: Thu, 19 Nov 1981 08:52:00 GMT” M Set-Cookie: PHPSESSID=3ff675616b2abe7d58280041fdalc4ab; path=/; HttpOnly”M Set-Cookie: PHPSESSID=3ff675616b2abe7d58280041fdalc4ab; path=/; HttpOnly”M "M
```
Apr 8 10:39:18 awc[1546]: Message over SSL from 10.2.100.10, SSL_read() returned 0, Message is "", AWC response: HTTP/1.0 200 OK^M Date: Tue, 08 Apr 2014 18:36:51 GMT^M Server: PanWeb Server/ - ^M ETag: "c7bf-110-52aa2378"^M Connection: close^M Pragma: no-cache^M Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0^M Content-Type: application/xml; charset=UTF-8^M Expires: Thu, 19 Nov 1981 08:52:00 GMT^M Set-Cookie: PHPSESSID=3ff675616b2abe7d58280041fdalc4ab; path=/; HttpOnly^M Set-Cookie: PHPSESSID=3ff675616b2abe7d58280041fdalc4ab; path=/; HttpOnly^M Set-Cookie: PHPSESSID=3ff675616b2abe7d58280041fdalc4ab; path=/; HttpOnly^M <response status="success"><result>< ... 

Palo Alto Networks firewall verification commands

**show user ip-user-mapping ip &lt;ip address&gt;**

This command displays the username to IP address mapping for the client on the Palo Alto Networks firewall. This information is displayed only after the controller has updated the firewall with the username, IP address information.

```
pan-test-user@PA-500> show user ip-user-mapping ip 10.68.105.24
IP address: 10.68.105.24 (vsys1)
User: iphone-user
From: XMLAPI
Idle Timeout: 1559s
Max. TTL: 1559s
Groups that the user belongs to (used in policy)
```

```
pan-test-user@PA-500> show user ip-user-mapping ip 10.68.105.26
IP address: 10.68.105.26 (vsys1)
User: ipad-user
From: XMLAPI
Idle Timeout: 1554s
Max. TTL: 1554s
Groups that the user belongs to (used in policy)
```
WebUI support on the Palo Alto Networks firewall

The device type mapping to the IP address and User ID can be viewed on the Palo Alto Networks firewall WebUI.

- Device listings on the Application Command Center (ACC) tab
  
The device type to IP address mapping is listed in the HIP Matches section under the ACC tab

- For each HIP object listed in the above page, the details of the HIP object and the HIP report can be obtained by clicking on the object type. In this case, clicking on iPhone or iPad
• Information on the device type, username mapping, IP address and the receive time of the information can be see in the HIP Match section under the Monitor tab.
ABOUT ARUBA NETWORKS, INC.

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 Networks™ automate infrastructure-wide performance optimization and trigger security actions that used to require manual IT intervention. The results are dramatically improved productivity and lower operational costs.

Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, Africa and Asia Pacific regions. To learn more, visit Aruba at 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 Social at http://community.arubanetworks.com.