Tech Note:

ClearPass & Palo Alto Networks Advanced Deployment Use Cases

Copyright

Copyright © 2014 Aruba Networks, Inc.

Aruba Networks trademarks include AirWave, Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, Aruba Mobility Management System®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFProtect®, Green Island®. All rights reserved. All other trademarks are the property of their respective owners.

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

<table>
<thead>
<tr>
<th>Date</th>
<th>Modified By</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 2014</td>
<td>Danny Jump</td>
<td>Initial Published Version 1</td>
</tr>
<tr>
<td>July 2014</td>
<td>Danny Jump</td>
<td>Added Guest MAC Caching update</td>
</tr>
</tbody>
</table>
Table of Contents
Overview ........................................................................................................................................... 4
Deploying CPPM and PANW Overview ............................................................................................. 4
CPPM Config – A very short recap ...................................................................................................... 5
Brief review of CPPM / PANW exchanged attributes ...................................................................... 6
Advanced Deployment Scenario’s ...................................................................................................... 8
PANW Configuration to use AD Groups to enforce policy ............................................................... 8
Configure PANW to ingest AD Groups information ......................................................................... 8
Configuring PANW Rules to limit Access for AD Groups ............................................................... 10
PANW Configuration to use HIP Objects to enforce policy ............................................................ 13
Useful DEBUG/Info Commands for AD Group configuration on PANW ........................................ 16
CPPM Configuration to support Guest MAC Caching auth ............................................................. 18
Overview of this feature .................................................................................................................. 18
Technical Description of the problem and the resolution ............................................................... 18

Table of Figures
Figure 1 - Summary of CPPM configuration steps .......................................................................... 5
Figure 2 - HIP Objects Options ......................................................................................................... 6
Figure 3 - HIP OS Options ................................................................................................................. 7
Figure 4 - Adding an LDAP definition for AD ................................................................................... 8
Figure 5 - Defining PANW UserID Group Mapping server ............................................................... 9
Figure 6 - Adding AD Group’s to an Include Group list .................................................................... 10
Figure 7 - Firewall rule 'PLM-Block-Social' .................................................................................... 11
Figure 8 - Firewall rule 'PLM-Block-Social' detailed info ............................................................... 11
Figure 9 - User successfully authenticating against AD.......................................................... 11
Figure 10 - Details of user carlos in AD group plm.............................................................. 12
Figure 11 - PANW firewall logs shown allow and block for traffic........................................ 12
Figure 12 - Unauthorized access attempt shown to the user from the PANW......................... 12
Figure 13 - Create a HIP Object to match a device running Windows XP............................ 13
Figure 14 - Adding multiple HIP Objects to a HIP Report...................................................... 14
Figure 15 - PANW firewall policy denying XP endpoints based upon HIP Report.................... 14
Figure 16 - Details behind the deny rule.................................................................................. 14
Figure 17 - Traffic being denied based upon HIP Object data................................................ 15
Figure 18 - Example HIP Object sent to Palo Alto Networks............................................... 15
Figure 19 - CLI command to refresh AD group data............................................................... 16
Figure 20 – CLI command to show AD groups ingested from AD........................................ 16
Figure 21 - CLI command to show AD groups on firewall (short output)............................. 16
Figure 22 - CLI command showing actual users in AD groups (TME).................................... 17
Figure 23 - CLI command showing actual users in AD groups (PLM)................................... 17
Figure 24 – RADIUS Enforcement Profile with %{Endpoint:Username}.................................. 19
Figure 25 - CPPM enforcement profile for PANW endpoint prior to CPPM 6.3.1.................... 19
Figure 26 - Pre 6.3.1 Session-Check attributes.................................................................... 20
Figure 27 - Post 6.3.1 Session-Check attributes.................................................................... 20
Figure 28 - PANW enforcement profile PLUS MAC Cache required post CPPM 6.3.1.......... 21
Overview

The following guide has been produced to help educate our customers and partners in deploying ClearPass with Palo Alto Networks Firewalls. This guide is written to cover specific DEPLOYMENT solutions. Going forward this guide will be updated and republished to reflect new and improved functionality and designs we deliver/develop.

**Note:** Where you see a red-chili this is to signifies a *hot* important point and highlights that this point is to be taken as a best-practice recommendation.

This is the first in what we plan to be an ongoing update of deployment use-cases with ClearPass and Palo Alto Networks Firewall. How to setup basic CPPM and Palo Alto Networks integration can be found [here](#). The following guide discusses more advanced deployment scenarios.

Deploying CPPM and PANW Overview

In the following deployment use-cases, Company X already has deployed Microsoft Active Directory (MSAD) and has users and employees defined for authorization based on MSAD Group Membership.

Below we discuss how leveraging the integration between the two products allows us to solve common customer use cases and enhance network security. We are assuming that all of the necessary ClearPass configuration has been completed and that UserID’s are already being received on the PANW Firewall from CPPM via the UserID XML API.

We also assume that the firewall is running PAN-OS 6.x and that CPPM is running on a CPPM 6.3.x code release. Below is a brief recap of the steps required to configure Palo Alto Networks Firewall integration on ClearPass.
CPPM Config – A very short recap

Below is a VERY brief reminder on the steps required on CPPM to complete the Palo Alto Networks configuration. If you do not understand this part, please refer to this technote.

Ensure that Insight is Enabled
Administration -> Server Manager -> Server Configuration -> [Server Name] -> Insight Setting -> Enable Insight

Ensure that you have configured the Palo Alto Networks endpoints
Administration -> External Servers -> Endpoint Context Servers -> Add -> Palo Alto Networks Firewall

Ensure that Log Accounting Interim-Updates Packets is enabled on CPPM
Administration -> Server Manager -> Server Configuration -> [Server Name] -> [System Parameters TAB] -> Select Service [Radius server] -> Accounting -> Log Accounting Interim-Updates -> TRUE

Ensure that you have configured an Enforcement Profile
Configuration -> Enforcement -> Profiles -> Add -> Session restriction
Enforcement -> [Attribute Tab] -> Type -> Session-Check -> Name -> IP-Address-Change-Notification -> Value [PANW Endpoint]

Ensure that you have configured an Enforcement Policy
Configuration -> Enforcement -> Policy -> Add -> Enforcement-Type -> RADIUS -> RULES TAB -> BEYOND-THIS-DOC’s SCOPE -> Enforcement Profiles -> What was created above in previous section

Figure 1 - Summary of CPPM configuration steps

Ensure that you reference the Enforcement Policy created above within your RADIUS / 802.1X services definition, this triggers the sending of data to a Palo Alto Networks Firewall or Panorama system.

We also make the assumption that the necessary configuration has been completed on the WLAN controllers. Beyond ensuring that authentication and accounting are correctly configured and pointing at CPPM. Please also ensure that Radius Interim Accounting is enabled.

On Aruba Networks controllers this can be found under Security -> Authentication -> AAA Profiles, RADIUS Interim Accounting. Also ensure that for the AAA Profile, you have configured a CPPM node under RADIUS Accounting Server Group.
Brief review of CPPM / PANW exchanged attributes

As a summary CPPM 6.3.x can push the following data attributes to a PANW firewall.

**Source IP Address MSAD Username and Domain pair**

A Username is received from the RADIUS authentication request. We correlate this with the endpoint MAC address when we receive the IP accounting data from the NAS, which also contain the MAC address.

**Note:** If we don’t receive the DOMAIN within the authentication request we can’t send one to the PANW firewall. Some supplicants can be configured to have a default DOMAIN such as the 802.1x configuration within Windows. In other cases either the user must enter the full Domain\Username as part of their logon or for a Captive Portal WEB-LOGIN we can utilize javascript that adds a fixed domain to the username.

**IP Address and Device-Type pair**

Once we have received accounting data from the NAS we then have the IP address. Having the IP address of the endpoint we are then able to profile the device and obtain additional endpoint attributes, such as Device Category, Device Family and its Operating System, referred to in the Fingerprint DB as ‘Name’.

**HIP Data CPPM 6.3.x plus**

The above two data pairs are the basics of the Palo Alto Networks UserID API attributes we send. Starting in CPPM 6.3.x we enhanced the data we can share by utilizing HIP Objects. HIP Objects allow us to extend the data attributes we can send to the firewall to include but not limited to.....

- NT Domain
- Operating System
- Hostname

When defining HIP Objects utilizing the above attributes, fuzzy logic can also be used when creating your HIP object match rules, i.e. Contains, Is, Is-Not....

![Figure 2 - HIP Objects Options](image-url)
Domain and Hostname are entered as free input fields. For the OS attribute four options exist, Microsoft, Apple, Google and Other. For the first three, defined options exist as shown below, for Other it’s a free input field. An example of Other would be ‘Intermec Scanner’.

Figure 3 - HIP OS Options

Having covered the attributes we can send to the firewall lets now cover how we can configure the firewall to make use of this data and ensure the power of the policy engine can be fully exploited.
Advanced Deployment Scenario’s

PANW Configuration to use AD Groups to enforce policy

Having CPPM push the UserId attributes to the firewall is really powerful, but we need to ensure that the PANW Firewall can make policy decision around this data. The firewall can be configured to ingest AD information on a regular period. AD information is generally fairly static, so ingesting this data every 15 minutes should suffice for most customers, but your mileage and deployment environment may differ.

In conjunction with the **Domain\Username** received from CPPM and the AD Group membership, we can now apply policy utilizing this data. Let’s cover this configuration.

**Configure PANW to ingest AD Groups information**

In order to define security policies based on user or group, the firewall must retrieve the list of AD groups and the corresponding list of members from your directory server. To enable this functionality, you must create an LDAP server profile that instructs the firewall how to connect and authenticate to the LDAP directory server.

Add the Palo Alto Networks firewall to the MSFT Active-Directory Domain, this becomes the starting point for ingesting the AD Group Information.

Under **Device, Server Profiles, LDAP -> Add**

![LDAP Server Profile](image)

**Figure 4 - Adding an LDAP definition for AD**
After creating the server profile as shown above, we need to use the **Group Mapping** tab to define how to search the directory for the user and group information.

This is created under **Device, User Identification, Group Mapping Settings -> Add**

On the ‘**Server Profile**’ Tab under the dropdown ‘**Server Profile**’ you should see the LDAP server we previously added, here you can also set the update interval that data if refreshed from AD, note that this Update Interval is in seconds.

To explain their significance of the fields in the Group Mapping, Server Profile screen, please read below. Take special notice of the note on the Object Class field.

**Object Class** - Specify the definition of a group. For example, the default is objectClass=group, which means that the system retrieves all objects in the directory that match the group filter and have objectClass=group.

**Group Name** - Enter the attribute that specifies the name of the group. For example in Active Directory, this attribute is “CN” (Common Name).

**Group Member** - Specify the attribute that contains the members of this group. For example in Active Directory, this attribute is “member.”

**Object Class** - Specify the definition of a user object. For example in Active Directory, the objectClass is “user”, however ensure for this integration it is set to “person”.

**User Name** - Specify the attribute for user name. For example, in Active Directory, the default user name attribute is “samAccountName.”

---

**Figure 5 - Defining PANW UserID Group Mapping server**
Next we need to use the **Group Include List** subtab to limit the number of groups that are displayed when creating a security policy. Browse through the LDAP tree to locate the groups you want to be able to use in a policy. For each group you want to include, select it in the Available Groups list and click the add icon to move it to the Included Groups list.

Click the 📡 icon to remove groups from the list. Repeat this step for every group you want to be able to use in your policies and then click OK to save the list of included groups. In the below example we have selected that the *tme* and *plm* groups be included in this group mapping.

![Group Mapping](image)

**Figure 6 - Adding AD Group's to an Include Group list**

**Configuring PANW Rules to limit Access for AD Groups**

Following the setup above we can now create firewall policy rules utilizing the AD Group Membership for a user. This user will have authenticated against CPPM, which will have forwarded the **Domain\Username** to the firewall via the UserID XML API. In this example this user will be denied access to specific web sites based upon their AD group membership.
To demonstrate this restriction we defined a very simple policy, denying access to social-media sites for the users in the ns-tme\plm group, in our case carlos is our user in this group.

![Firewall rule 'PLM-Block-Social'](image)

**Figure 7 - Firewall rule 'PLM-Block-Social'**

From the detail below, you can see that we configured specific URL categories in this policy rule, the group social-networking is denied access for users in the ns-tme\plm group.

![Security Policy Rule](image)

**Figure 8 - Firewall rule 'PLM-Block-Social' detailed info**

We see the user ns-tme\carlos authenticating against CPPM and the auth source is AD.

![User successfully authenticating against AD](image)

**Figure 9 - User successfully authenticating against AD**
The below shows carlos as a user in Active Directory and a member of the PLM group.

![Image of carlos Properties](image)

Figure 10 - Details of user carlos in AD group plm

This user then tried to access multiple WEB sites. As can be seen from the below firewall logs ns-tme\carlos is blocked for access to social-networking sites twitter/facebook but general web-browsing is allowed.

![Image of PANW firewall logs](image)

Figure 11 - PANW firewall logs shown allow and block for traffic

Below shows the default message the firewall shows by default to a user when attempting to access prohibited sites.

![Image of Application Blocked](image)

Figure 12 - Unauthorized access attempt shown to the user from the PANW
PANW Configuration to use HIP Objects to enforce policy

Building on the previous example of utilizing the AD group membership policy, we will in this next example leverage a firewall policy utilizing the HIP Object data we are sending to the PANW Firewall.

In a very similar way as the previous example we can use HIP object data to make advanced policy decision based using the AD Group membership and HIP Objects. We will restrict users so that they cannot use devices running Windows XP, Microsoft has recently ceased supporting this OS. In our example we deem XP unsafe to use in our corporate environment specifically accessing the internet due to lack of vendor support.

Remember we discussed HIP objects earlier in the document and there is a pre-requisite that CPPM is running a minimum code revision of 6.3.x.

First we need to create some additional configuration to be able to reference the HIP Objects in the Policies.

Under Objects, GlobalProtect, HIP Objects, Add
Below we create a HIP Object that references Host Information. The below definition will create a match for any device that is running any version of Windows XP.

![HIP Object Configuration]

Figure 13 - Create a HIP Object to match a device running Windows XP
Next we need to build a HIP Report. Think of a HIP report as a hierarchical collection of HIP Objects. We created a new HIP report and then added as an example to demonstrate the possibilities with Boolean logic, two HIP Objects. The below example could be used for matching XP and OSX Devices. For the sake of this use-case we will only use the XP-DEVICE HIP Object.

![Figure 14 - Adding multiple HIP Objects to a HIP Report](image)

Having created the HIP Objects and added these to our HIP Report, we can make reference and write policy to perform the restrictions we desire. Below shows that the only real filter being used by the policy engine as a source is the HIP Report we created previously.

![Figure 15 - PANW firewall policy denying XP endpoints based upon HIP Report](image)

It is hard to see the details in the firewall rule, so the key portion of the rule is below....

![Figure 16 - Details behind the deny rule](image)
Looking on the monitor tab on the firewall when `ns-tme\danny` signs in and attempt to access WWW sites, the traffic is denied under the rule `stop-USERS-using-xp`. This deny is because the HIP Objects data CPPM sent to the firewall (desktop OS) which is then referenced in the above policy.

<table>
<thead>
<tr>
<th>Receive Time</th>
<th>Type</th>
<th>From Zone</th>
<th>To Zone</th>
<th>Source</th>
<th>Source User</th>
<th>Destination</th>
<th>To Port</th>
<th>Application</th>
<th>Action</th>
<th>Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/15 19:03:31</td>
<td>drop</td>
<td>trust</td>
<td>untrusted</td>
<td>10.2.100.149</td>
<td>ns-tme\danny</td>
<td>74.125.230.119</td>
<td>443</td>
<td>not-applicable</td>
<td>deny</td>
<td>stop-USERS-using-xp</td>
</tr>
<tr>
<td>05/15 19:03:31</td>
<td>drop</td>
<td>trust</td>
<td>untrusted</td>
<td>10.2.100.149</td>
<td>ns-tme\danny</td>
<td>74.125.239.119</td>
<td>443</td>
<td>not-applicable</td>
<td>deny</td>
<td>stop-USERS-using-xp</td>
</tr>
<tr>
<td>05/15 19:03:30</td>
<td>drop</td>
<td>trust</td>
<td>untrusted</td>
<td>10.2.100.149</td>
<td>ns-tme\danny</td>
<td>23.61.104.192</td>
<td>80</td>
<td>not-applicable</td>
<td>deny</td>
<td>stop-USERS-using-xp</td>
</tr>
<tr>
<td>05/15 19:03:30</td>
<td>drop</td>
<td>trust</td>
<td>untrusted</td>
<td>10.2.100.149</td>
<td>ns-tme\danny</td>
<td>23.61.194.192</td>
<td>80</td>
<td>not-applicable</td>
<td>deny</td>
<td>stop-USERS-using-xp</td>
</tr>
</tbody>
</table>

**Figure 17 - Traffic being denied based upon HIP Object data**

Below we show an example of a HIP Object, and the detail CPPM send to the firewall.

```
admin@PA-500> debug user-id dump hip-report ip 10.2.100.149 user ns-tme\danny computer xp-vm1
<?xml version="1.0" encoding="UTF-8"?>
<hip-report>
    <md5-sum>43771d52421c90bd36a3494f626cb1f2</md5-sum>
    <user-name>danny</user-name>
    <domain>ns-tme</domain>
    <host-name>xp-vm1</host-name>
    <ip-address>10.2.100.149</ip-address>
    <generate-time>15/05/2014 19:06:10</generate-time>
    <categories>
        <entry name="host-info">
            <host-name>xp-vm1</host-name>
            <domain>ns-tme</domain>
            <os>Microsoft Windows XP Service Pack 3</os>
            <os-vendor>Microsoft</os-vendor>
        </entry>
    </categories>
</hip-report>
```

**Figure 18 - Example HIP Object sent to Palo Alto Networks**

From the above HIP Report, you can see an example of the data (highlighted) that can be sent by CPPM to a Palo Alto Networks firewall, this is in addition to the basic UserID attributes we already send. The attributes are `host-name`, `domain`, `os` and `os-vendor`. These attributes can then be referenced in a policy when creating HIP Objects on the firewall.
Useful DEBUG/Info Commands for AD Group configuration on PANW

To force the firewall to refresh the AD user group-mappings, run this command via the CLI:

```
admin@PA-500> debug user-id reset group-mapping all
group mapping 'NS-GRP-MAPPING' in vsys1 is marked for reset.
```

**Figure 19 - CLI command to refresh AD group data**

**Note:** It will only fetch the delta values for the user-groups. The above is non-intrusive and shouldn’t affect any production traffic.

CLI commands to check the groups retrieved and connection to the LDAP server:

```
admin@PA-500> show user group-mapping state all
Group Mapping(vsys1, type: active-directory): NS-GRP-MAPPING
  Bind DN : cn=administrator,cn=users,dc=ns-tme,dc=com
  Base : DC=ns-tme,DC=com
  Group Filter: (None)
  User Filter: (None)
  Servers : configured 1 servers
    10.2.100.120(389)
      Last Action Time: 8 secs ago(took 0 secs)
      Next Action Time: In 52 secs
  Number of Groups: 2
    cn=plm,cn=users,dc=ns-tme,dc=com
    cn=tme,cn=users,dc=ns-tme,dc=com
```

**Figure 20 – CLI command to show AD groups ingested from AD**

Pay special attention to the group detail at the end of the command output.

```
admin@PA-500> show user group list
  cn=plm,cn=users,dc=ns-tme,dc=com
  cn=tme,cn=users,dc=ns-tme,dc=com
Total: 2
```

**Figure 21 - CLI command to show AD groups on firewall (short output)**
Very powerful command to show the users and their group mapping that the firewall has ingested from AD.

```
admin@PA-500> show user group name cn=tme,cn=users,dc=ns-tme,dc=com
short name: ns-tme\tme
source type: ldap
source: NS-GRP-MAPPING
[1 ] ns-tme\bob
[2 ] ns-tme\danny
admin@PA-500>
```

Figure 22 - CLI command showing actual users in AD groups (TME)

Very powerful command to show the users and their group mapping that the firewall has ingested from AD.

```
admin@PA-500> show user group name cn=plm,cn=users,dc=ns-tme,dc=com
short name: ns-tme\plm
source type: ldap
source: NS-GRP-MAPPING
[1 ] ns-tme\cam
[2 ] ns-tme\carlos
admin@PA-500>
```

Figure 23 - CLI command showing actual users in AD groups (PLM)
**CPPM Configuration to support Guest MAC Caching auth**

**Overview of this feature**

Starting in the CPPM 6.3.1 release we enhanced our functionality to support Guest MAC caching authentication with Palo Alto Networks. Previously if a user authenticated then left their device and it timed-out on the network, they hibernated their device or returned the following day to re-connect it was quite possible that the CPPM node they re-authenticated too would try to MAC-cache this endpoint. If this happened, then the endpoint would correctly match a known endpoint in the Local endpoint DB but then the underlying issue here was that the username sent to the Palo Alto Networks endpoint via the XMLAPI would be the device MAC address as the username. This then created an issue as the Palo Alto Networks endpoint would try and enforce a policy based upon the MAC address and not the UserID, this created an obvious policy mis-match. Now we have the ability to track these sessions and ensure during MAC Caching, the username of the logged-in user is updated in the Endpoint attribute.

*Note:* This process is not limited to just for Guest MAC Caching and should cover 802.1X, MAB, Guest Auth and MAB (MAC Caching flow).

**Technical Description of the problem and the resolution**

MAC Caching / MAC access Bypass (MAB) requests send the username in the RADIUS Access-Request as the **MAC Address** in the **RADIUS:IETF:Username** attribute. The Palo Alto Network User Id updates sent by CPPM use this attribute for updates to the PANW firewall. This mechanism works great in normal scenarios but breaks when used in conjunction with MAC Caching when the PANW rules are configured to enforce with a usernames not a MAC address. CPPM now exposes the flexibility of sending UserId updates with the actual user associated with the device in a MAC Caching flow. During MAC Caching, the username of the logged-in user is updated in the Endpoint attribute.

To implement this solution requires two key features. The first is to force the NAS device to send a username not a MAC address in the Interim Accounting Updates. For this to work make sure you send or append **Radius:IETF:Username = %{Endpoint:Username}** to the switch or controller as a part of MAB response. Ensure the switch/controller supports this attribute. This will enable accounting updates to carry the username instead of MAC Address and post auth will send the username in UID updates.

*Note:* If a new CPPM system is deployed, when you configure a MAC Caching service from the templates, this setting is added. If you already had a service configured on a pre 6.3.1 system you may need to manually add this configuration separately.
The second is to use a new **Session-Check** attribute, as part of the PANW UserID XMLAPI update enforcement profile. By using the new **Session-Check::Username** attribute we can substitute the default **RADIUS:IETF:User-name** (which would send the MAC address) attribute to use the Username sent by the Accounting Updates, forced by the above RADIUS enforcement profile. Ensure the two values below are defined within the post_auth profile.

```
Session-Check::IP-Addresses-Change-Notify = <IP@_of_PAN> {Existing-value}
Session-Check::Username = %{Endpoint:Username} {New-value}
```

Prior to CPPM 6.3.1 a typical Post Auth profile for PANW enforcement would have looked similar to the below example...... with a single entry identifying the Palo Alto Networks endpoint where we would forward the UserID/HIP data to.
Notice below the available Session-Check options available pre CPPM 6.3.1...

**Figure 26 - Pre 6.3.1 Session-Check attributes**

As explained above, adding the `Session-Check::Username = %{Endpoint:Username}` to the existing enforcement profile will allow CPPM to ensure that even if the endpoint is MAB/MAC authenticated we send the username, not the MAC address to the PAN endpoint.

As can be seen below we added in CPPM 6.3.1 the Username attribute as a Session-Check option....

**Figure 27 - Post 6.3.1 Session-Check attributes**
Example of required Enforcement Profile to substitute MAC address with Username.

![Enforcement Profile Diagram]

**Figure 28 - PANW enforcement profile PLUS MAC Cache required post CPPM 6.3.1**