Tech Note:

ClearPass 6.X. Services (V3)

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 2013</td>
<td>Danny Jump</td>
<td>Initial Version</td>
</tr>
<tr>
<td>June 2013</td>
<td>Danny Jump</td>
<td>V2 update, minor correction and additions</td>
</tr>
<tr>
<td>May 2014</td>
<td>Danny Jump</td>
<td>V3 Updates – minor corrections and minor updates to reflect changes in CPPM 6.3 and added my chili’s..!!</td>
</tr>
</tbody>
</table>
Table of Contents
Overview ........................................................................................................................................3
Background ....................................................................................................................................3
Caveats for RADIUS Request 6.0.x & 6.1.x and later ....................................................................4
Client to CPPM Route selection ..................................................................................................4
CPPM Background Traffic Route selection ..................................................................................4
  CPPM cluster traffic interfaces ..................................................................................................5
  CPPM cluster traffic TCP/UDP ports used ..................................................................................6
Onboard and Guest Portal Caveats ..............................................................................................6
OnGuard Caveats ..........................................................................................................................6
CPPM to Active Directory ............................................................................................................6
VIP Caveats - Physical v Virtual Caveats ......................................................................................7
Other Interface Rules / Suggestions ..............................................................................................7
  Interfaces in DMZ/Trusted firewall Zones ..................................................................................8
External Updates ............................................................................................................................8
Publisher/Subscriber Cluster ........................................................................................................8

Table of Figures
Figure 1 - appadmin CLI to define routes ..................................................................................5
Figure 2 - Configuring Application Access Control Rules ..........................................................7
Overview

The following guidance has been produced to aid field engineering, customers and partners to understand how ClearPass Policy Manager provides services on either the Data or Management Interface or both. This document will change over time as we develop the services, check back to ensure you always have the latest published version posted on Arubapedia.

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.

Background

ClearPass has the ability to support multiple physical Ethernet Interfaces. Commonly referred to as the ‘Data Port / Data Interface’ and the ‘Management Port / Management Interface’. We use the term port and interface loosely to mean the same thing. As we explain in this document, when both interfaces are configured the expected behavior as to which services listen on which interface and which interface is used to reply when a request is received is not always as expected. This document attempts to provide some clarity.

Note: Today CPPM only supports the use of two physical interfaces (CP-HW-500/5K), even though some of our hardware (CP-HW-25K) actually ships with four physical interfaces we only utilize a maximum of two today (May 2014). This restriction also applies for VM deployments, where a maximum of two supported interfaces can be configured.

Note: Starting in CPPM 6.3.x and specifically for the CP-HW-25K appliance ONLY we allow the configuration of a dedicated SPAN port on one of the two spare Ethernet port on the onboard 4-port card. This allows us to ingest DHCP Discover and Request packets for profiling, this helps remove the requirement to configure DHCP IP helpers across the entire network.

Note: CPPM can also be deployed using a single interface, this would be the Management Interface. However, the second interface (data port) should exist physically on the system and is optionally configured. This applies specifically to a VM deployment.

Aruba ClearPass engineering implemented some changes in the way our listening demons run and bind to interfaces starting in CPPM 6.1.x. As the product has advanced over recent revisions we have captured this in this document and this is detailed below.
Caveats for RADIUS Request 6.0.x & 6.1.x and later

**Under CPPM 6.0.x** you cannot configure the data port interface alone. In other words **management port is mandatory and data port is optional**. Once an Interface is given an IP address it in effect then becomes capable of receiving and replying to requests, be that RADIUS, Captive Portal, OnGuard etc. etc.

However, if you configure BOTH interfaces i.e. they both have IP address then ONLY the DATA interface will respond to RADIUS request. If you send a RADIUS request to the Management interface CPPM would ignore and drop this request.

**Under CPPM 6.1.x and later** you will not be able to configure the data port interface alone. In other words **management port is mandatory and data port is optional** however, RADIUS Authentications can be sent to both interfaces and we will reply with the RADIUS response on the interface we initially received the request on.

**Client to CPPM Route selection**

The following covers how route selection is chosen, **this covers Client <-> CPPM**.

- For network traffic that are received on the Management Interface, this interface is used as the return interface.
- For network traffic that are received on the Data Interface, this interface is used as the return interface.
- If the data interface is not configured all traffic will use the Management Interface.

**Note:** All of the above rules can be overridden by static routing from the ClearPass CLI using the **appadmin** UserID. An example of this is below in the next section.

**CPPM Auxiliary Traffic Route selection**

The following services follow the below rules in regard to how their route selection is chosen, **this specifically covers CPPM <-> CPPM communications**.

*Active Directory, LDAP, NTP, Network devices, CPPM Cluster Communications, Cloud updates, CRL, OSCP, CoA, Endpoint Context-Servers (PANW, MDM)*

When CPPM is configured with **both** interfaces, the following applies to route selection....

- If the destination network/address is in the management subnet then we use the management interface.
- If the destination network/address is in the data subnet then we use the data interface.
- If the destination network is not in either management or data subnets, then we use the data interface by default.
When CPPM is configured with a single interfaces, the following applies to route selection...

- When only one interface (i.e., management) is configured in CPPM, then the traffic goes through management port. This applies to all the network communication within CPPM

**Note:** If we attempt to communicate with the device through the data-interface and fail we will not try the management-interface unless the host-address or remote-subnet route has specifically been configured.

**Note:** All the above rules can be overridden by static routing from the ClearPass CLI using the `appadmin` UserID.

The following command example can be used to add routes as and if required. Make special notice of the option in the command syntax of “network ip add mgmt / data”

```
Failed to perform the network ip add operation
Usage:

network ip add <mgmt|data|greN> [-i <id>] [-s <SrcAddr>] [-d <DestAddr>] [-g <ViaAddr>]
```

- `greN` -- Name of the gre tunnel where N corresponds to the gre tunnel number ranging from 1,2,3...N
- `-i` -- Optional parameter. Id of the network ip rule. If unspecified the system will auto generate the Id
- `-s <SrcAddr>` -- Optional parameter. The source interface ip address or netmask from where the network ip rule is specified. The allowed values are valid IP Address or Netmask or '0/0'
- `-d <DestAddr>` -- Optional parameter. The destination interface ip address or netmask where the network ip rule is specified. The allowed values are valid IP Address or Netmask or '0/0'
- `-g <ViaAddr>` -- Optional parameter. The via or gateway ip address through which the network traffic should flow. The allowed value is valid IP Address

**Figure 1 - appadmin CLI to define routes**

**CPPM cluster traffic interfaces**

In reference to clustering traffic, the management IP address of the publisher needs to be accessible to all subscribers. The subscribers may reach the publisher’s management IP either through the subscriber’s management interface or data interface based on network routing set up.
**CPPM cluster traffic TCP/UDP ports used**

- UDP Port 123 NTP (Subscriber to Publisher)
- TCP Port 443 HTTPS (Bi-directional)
- TCP Port 5432 PostgreSQL for DB replication (Subscriber to Publisher)
- TCP Port 80 Bi-direction - change status queries between CPPM nodes.
- TCP Port 4231 NetWatch (Post Authentication module and the node where Insight is enabled)

**Note:** The CPPM DB sync for PostgreSQL. The sync is 99% Publisher to Subscriber. However there are bi-directional keep-alives between the DB's, please ensure if any firewalls exist between CPPM instances the firewall rules allow bi-directional traffic.

---

**Onboard and Guest Portal Caveats**

**Under CPPM 6.x** both Onboard and Guest Portal are supported on the Data and Management interfaces, separately and concurrently.

---

**OnGuard Caveats**

If Management and Data interfaces are configured concurrently, then OnGuard communicates with ClearPass through the Data interface.

- 6658 TCP for OnGuard client to communicate with CPPM. Otherwise client doesn’t appear in OnGuard Activity tab.

---

**CPPM to Active Directory**


The following is the list of services and their ports used for Active Directory communication:

- UDP Port 88 for Kerberos authentication
- UDP and TCP Port 135 for domain controllers-to-domain controller and client to domain controller operations.
- TCP Port 139 and UDP 138 for File Replication Service between domain controllers. (Probably not necessary for CPPM)
- UDP Port 389 for LDAP to handle normal queries from client computers to the domain controllers.
- TCP and UDP Port 445 for File Replication Service (Not necessary for CPPM)
- TCP and UDP Port 464 for Kerberos Password Change
• TCP Port 3268 and 3269 for Global Catalog from client to domain controller.
• TCP and UDP Port 53 for DNS from client to domain controller and domain controller to domain controller.

VIP Caveats - Physical v Virtual Caveats

Since the release of CPPM 6.1.1 you can configure VIP addresses pairs concurrently across the Management and Data Interfaces. Prior to 6.1.1 if the server had both Management and Data VIP configured, then the VIP will only work with the data interfaces.

VIP address can be used for the following services.....

• RADIUS
• Guest
• TACACS+
• WEBAUTH, this includes dissolvable OnGuard agent
  o OnGuard persistent agent always go to the Physical IP address

For other Services we use the Physical Interface IP address

• GRE
• SMTP

**Note:** If the VIP IP address is configured as the RADIUS server IP address in a switch/controller and if CPPM is expected to send CoA to the switch/controller, then the VIP IP address should be configured as the authorized RF3576 server in the switch/controller.

Other Interface Rules / Suggestions

The CLI can ONLY be accessed from the Management Interface. If a customer has concerns over ClearPass Policy Manager Admin UI access, you can starting in CPPM 6.1.x configure Application Access Control to restrict access. You will find this under Server Manager --> Server Configuration --> Network

![Figure 2 - Configuring Application Access Control Rules](image)
**Note:** If you inadvertently lock yourself out of the UI, we have supplied a CLI level command to remove all of the Access Control ACL’s. This will remove all of the Access Control ACL’s, you cannot just remove a single Application Control ‘ACL’.

To access this command, login to the CLI with the **appadmin** account and issue the following command:

```
system app-access-reset
```

DHCP Forwarded messages can be sent to either Management or Data Interface and we will update our fingerprint database accordingly.

**Interfaces in DMZ/Trusted firewall Zones**

If a deployment is such that an interface needs to be deployed into a ‘public’ environment such as a firewall DMZ, we recommend that you have the Data interface in the DMZ and the Management interface in the trusted zone. Secure access to the Data Interface through a combination of firewall rules that allows access to the DMZ and by the use of CPPM’s Application Access Control feature discussed previously.

**External Updates**

Every CPPM node requires HTTP(80) and HTTPS(443) to [clearpass.arubanetworks.com/webservice](http://clearpass.arubanetworks.com/webservice) for plugin updates.

**Publisher/Subscriber Cluster**

Finally, remember that any publisher or subscriber can process service requests on their Data or Management ports under the restrictions highlighted in this document.