

Cloudpath Integration with Palo Alto Firewalls

Supporting Software Release 5.2

Copyright Notice and Proprietary Information

Copyright 2017 Brocade Communications Systems, Inc. All rights reserved.

No part of this documentation may be used, reproduced, transmitted, or translated, in any form or by any means, electronic, mechanical, manual, optical, or otherwise, without prior written permission of or as expressly provided by under license from Brocade.

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader's responsibility to determine the applicable regulations and to comply with them.

Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN ("MATERIAL") IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. BROCADE and RUCKUS WIRELESS, INC. AND THEIR LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. BROCADE and RUCKUS RESERVE THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL BROCADE or RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

Trademarks

Ruckus Wireless, Ruckus, the bark logo, BeamFlex, ChannelFly, Dynamic PSK, FlexMaster, Simply Better Wireless, SmartCell, SmartMesh, SmartZone, Unleashed, ZoneDirector and ZoneFlex are trademarks of Ruckus Wireless, Inc. in the United States and in other countries. Brocade, the B-wing symbol, MyBrocade, and ICX are trademarks of Brocade Communications Systems, Inc. in the United States and in other countries. Other trademarks may belong to third parties.

Contents

- Integration with Palo Alto Firewalls.....4
- Palo Alto Firewall Prerequisites.....4
- Wireless Controller Configuration.....4
- Cloudpath Configuration.....6
- Palo Alto Output.....7

Integration with Palo Alto Firewalls

Cloudpath supplements data already captured by Palo Alto firewalls by adding mappings of the IP address to a User Id, allowing the captured traffic to be more identifiable. When a user joins the network via Cloudpath, the Palo Alto firewall is notified of the user's login. Similarly, when a user is known to have left the network, the firewall is notified of the logout.

Cloudpath also sends Host Information Profile (HIP) data to the firewall, which increases visibility on connections and allows filtering on the type of client (by operating system, etc).

This section describes how to integrate Cloudpath with a Palo Alto firewall.

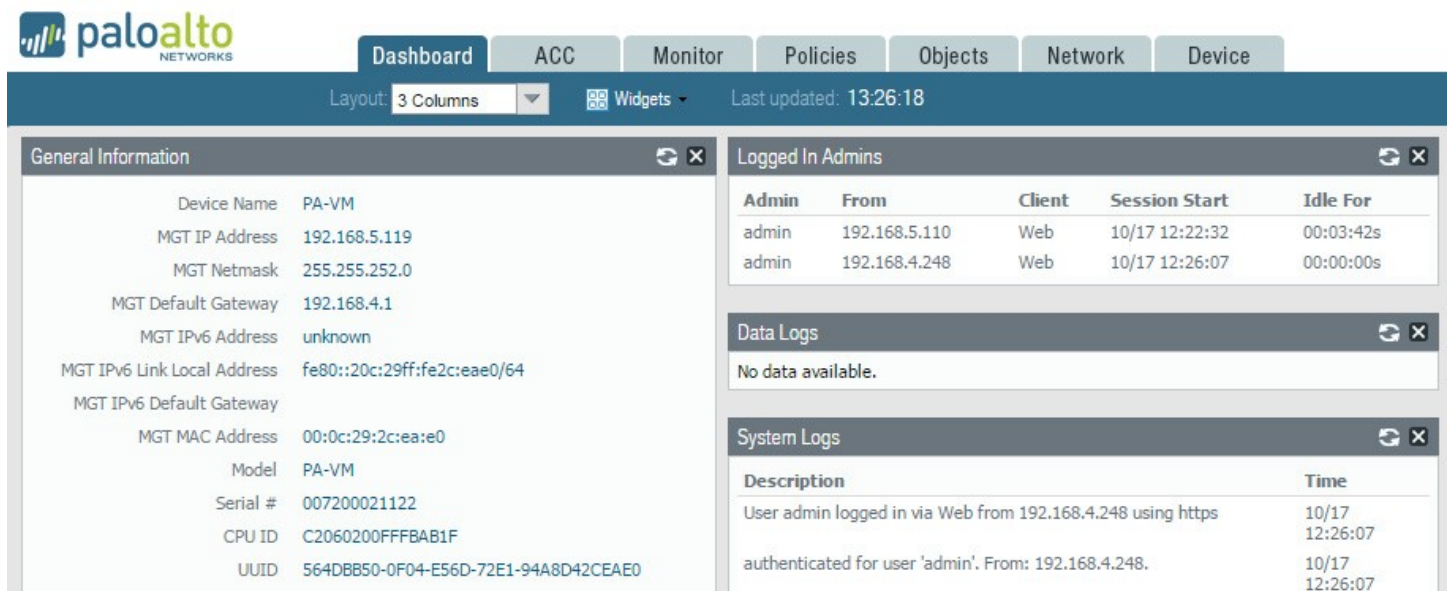
Palo Alto Firewall Prerequisites

Configuring Cloudpath to integrate with a Palo Alto firewall requires:

- Administrator credentials for the Palo Alto system

IP address or hostname of the Palo Alto system

FIGURE 1 Palo Alto Firewall System Information



Wireless Controller Configuration

The examples in this section show Ruckus Wireless controllers. However, Cloudpath supports integration with Palo Alto firewalls using wireless controllers from most vendors.

The wireless controller configuration requirements:

- AAA authentication server and AAA accounting server.
 - RADIUS enabled (RADIUS Accounting for AAA Accounting server)
 - IP address of Cloudpath system
 - Authentication port =1812 (Accounting port=1813)

- Shared must match the shared secret for the Cloudpath onboard RADIUS server (or shared secret for the external RADIUS server).
- WLAN configuration
 - Standard Usage
 - 802.1x EAP Method
 - WPA2 Encryption
 - AES Algorithm
 - Select AAA authentication server previously configured
 - In Advanced Options section, select AAA accounting server previously configured

FIGURE 2 WLAN Configuration with AAA Accounting Server

Editing (eng-Anna40)

General Options

Name/ESSID* ESSID

Description

WLAN Usages

Type

- Standard Usage (For most regular wireless network usages.)
- Guest Access (Guest access policies and access control will be applied.)
- Hotspot Service (WISPr)
- Hotspot 2.0
- Autonomous
- Social Media

Authentication Options

Method Open 802.1x EAP MAC Address 802.1x EAP + MAC Address

Fast BSS Transition Enable 802.11r FT Roaming
(Recommended to enable 802.11k Neighbor-list Report for assistant.)

Encryption Options

Method WPA2 WPA-Mixed WEP-64 (40 bit) WEP-128 (104 bit) None

Algorithm AES Auto (TKIP+AES)

Options

Authentication Server

Wireless Client Isolation

- Isolate wireless client traffic from other clients on the same AP.
- Isolate wireless client traffic from all hosts on the same VLAN/subnet.

(Requires whitelist for gateway and other allowed hosts.)

Zero-IT Activation™

- Enable Zero-IT Activation
(WLAN users are provided with wireless configuration installer after they log in.)

Priority High Low

Advanced Options

Accounting Server Send Interim-Update every minutes

Cloudpath Configuration

1. Navigate to **Configuration > Firewalls & Web Filters**.
2. Select **Palo Alto Firewall**.

FIGURE 3 Firewalls & Web Filters

The screenshot shows the configuration page for Firewalls & Web Filters, specifically the 'Create' step. The breadcrumb navigation at the top reads 'Configuration > Firewalls & Web Filters > Create'. There are 'Cancel' and 'Save' buttons in the top right corner. The main section is titled 'System Type' and contains four radio button options: 'Palo Alto Firewall' (selected), 'Lightspeed Systems Web Filter', 'iBoss Web Security Gateway', and 'Custom via RADIUS Accounting'. The 'Palo Alto Firewall' section is expanded, showing an 'IP Address' field with the placeholder '[ex. 1.1.1.1]' and an 'XML API Key' field with a '<-- Get Key' button. Below this, there is an 'Advanced: Scope' section with an 'SSID Regex' field containing the value '*'. The entire form is enclosed in a light gray border.

3. Enter the management IP address of the Palo Alto system.

- Click **Get Key**.

FIGURE 4 Palo Alto Credentials

Palo Alto Credentials [X]

Enter Hostname or IP Address of a Palo Alto firewall and associated credentials to obtain a Palo Alto XML API key:

Hostname:

Username:

Password:

Cancel **Continue**

- In the Palo Alto Credentials popup, enter:
 - Hostname or IP address of the Palo Alto firewall.
 - Palo Alto administrator username.
 - Palo Alto administrator password.

The API key is generated by the system and displayed. This is the API key the Cloudpath system will use to communicate with the firewall.

- Scope** is optional. If you want only information from a specific SSID to be forwarded to the Palo Alto firewall (or other specified web filters), enter it in the **SSID Regex** field.

Palo Alto Output

The example output below displays the type of information displayed from the Palo Alto firewall **Monitor** tab, and **Host Information Profile (HIP) Match** logs. The **Source address** and **Source User** display the user data from the Cloudpath enrollment record. The **Machine Name** and **Operating System** fields, if known by Cloudpath, display the machine information.

Integration with Palo Alto Firewalls

Palo Alto Output

FIGURE 5 Palo Alto Firewall Displaying Cloudpath Traffic

Receive Time	Source address	Source User	Machine Name	Operating System	HIP	HIP Type	Generate Time	Logtype	Virtual System
10/13 13:48:59	192.168.95.244	jim@byod.cloudpath.net	192.168.95.244	IOS	HIP Test	object	10/13 13:48:59		vsys1
10/13 13:45:46	192.168.95.119	bob@byod.cloudpath.net	192.168.95.119	Mac	HIP Test	object	10/13 13:45:46		vsys1
10/13 13:42:51	192.168.95.244	jim@byod.cloudpath.net	192.168.95.244	IOS	HIP Test	object	10/13 13:42:51		vsys1
10/13 13:32:34	192.168.95.244	jim@byod.cloudpath.net	192.168.95.244	IOS	HIP Test	object	10/13 13:32:34		vsys1
10/13 13:08:16	192.168.95.244	jim@byod.cloudpath.net	192.168.95.244	IOS	HIP Test	object	10/13 13:08:16		vsys1
10/13 13:01:09	192.168.95.224	anna eichel@guest.company.c...	LTP-78	Windows	HIP Test	object	10/13 13:01:09		vsys1
10/13 12:53:35	192.168.95.138	nick@byod.cloudpath.net	192.168.95.138	Android	HIP Test	object	10/13 12:53:35		vsys1
10/13 12:52:59	192.168.95.138	nick@byod.cloudpath.net	192.168.95.138	Android	HIP Test	object	10/13 12:52:59		vsys1
10/13 12:14:27	192.168.95.138	nick@byod.cloudpath.net	192.168.95.138	Android	HIP Test	object	10/13 12:14:27		vsys1
10/13 12:09:02	192.168.95.138	nick@byod.cloudpath.net	192.168.95.138	Android	HIP Test	object	10/13 12:09:02		vsys1
10/13 12:08:46	192.168.95.138	nick@byod.cloudpath.net	192.168.95.138	Android	HIP Test	object	10/13 12:08:46		vsys1
10/13 09:24:09	192.168.95.224	anna eichel@guest.company.c...	LTP-78	Windows	HIP Test	object	10/13 09:24:09		vsys1
10/13 09:17:24	192.168.95.35	anna eichel@guest.company.c...	192.168.95.35	Mac	HIP Test	object	10/13 09:17:24		vsys1
10/13 09:15:49	192.168.95.35	anna eichel@guest.company.c...	192.168.95.35	Mac	HIP Test	object	10/13 09:15:49		vsys1
10/13 08:59:19	192.168.95.35	anna eichel@guest.company.c...	192.168.95.35	Mac	HIP Test	object	10/13 08:59:19		vsys1
10/13 08:49:40	192.168.95.35	anna@byod.company.com	192.168.95.35	Mac	HIP Test	object	10/13 08:49:40		vsys1
10/13 07:52:06	192.168.95.35	anna@byod.company.com	192.168.95.35	Mac	HIP Test	object	10/13 07:52:06		vsys1
10/13 05:17:10	192.168.95.224	anna@byod.company.com	LTP-78	Windows	HIP Test	object	10/13 05:17:10		vsys1
10/13 03:12:12	192.168.95.224	anna@byod.company.com	LTP-78	Windows	HIP Test	object	10/13 03:12:12		vsys1
10/13 03:12:07	192.168.95.224	anna@byod.company.com	LTP-78	Windows	HIP Test	object	10/13 03:12:07		vsys1

The information displayed is obtained from the Cloudpath Enrollment Record.



Copyright © 2006-2017. Ruckus Wireless, Inc.
350 West Java Dr. Sunnyvale, CA 94089. USA
www.ruckuswireless.com