



Checkpoint firewall Quick Integration Guide

for PacketFence version 5.0.0

Checkpoint firewall Quick Integration Guide

by Inverse Inc.

Version 5.0.0 - Mar 2015

Copyright © 2015 Inverse inc.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

The fonts used in this guide are licensed under the SIL Open Font License, Version 1.1. This license is available with a FAQ at: <http://scripts.sil.org/OFL>

Copyright © Łukasz Dziejczak, <http://www.latofonts.com>, with Reserved Font Name: "Lato".

Copyright © Raph Levien, <http://levien.com/>, with Reserved Font Name: "Inconsolata".

9279VnJ

Table of Contents

- About this Guide 1
- Assumptions 2
- Quick installation 3
 - Step 1: Enabling Identity Awareness on the Security Gateway 3
 - Step 2: Enabling RADIUS Accounting on a Security Gateway 3
 - Step 3: Configuring RADIUS Accounting 4
 - Step 4: RADIUS Client Access Permissions 4
 - Step 5: LDAP Groups 5
 - Step 6: SSO Configuration in PacketFence 5
 - Step 7: Verification 6

About this Guide

This guide has been created in order to help sales engineers, product managers, or network specialists demonstrate the PacketFence capabilities on-site with an existing or potential customer. It can also provide guidelines to setup a proof of concept for a potential PacketFence deployment using the **Checkpoint firewall**.

Assumptions

- You have a configured PacketFence environment with working test equipment;
- You have a Checkpoint firewall.

Quick installation

Step 1: Enabling Identity Awareness on the Security Gateway

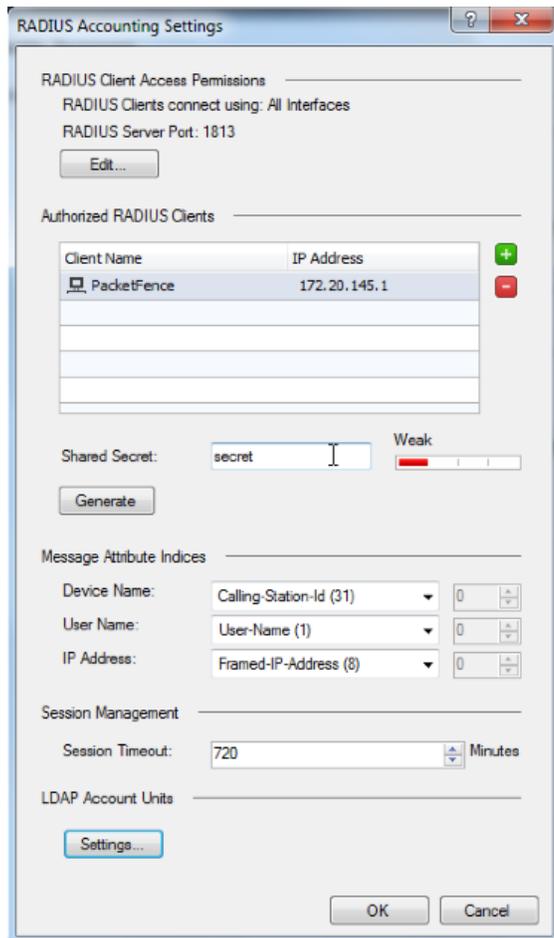
To enable Identity Awareness:

1. Log in to *SmartDashboard*.
2. From the *Network Objects tree*, expand the *Check Point branch*.
3. Double-click the *Security Gateway* on which to enable *Identity Awareness*.
4. In the *Software Blades* section, select *Identity Awareness* on the *Network Security tab*. The *Identity Awareness Configuration wizard* opens.
5. Select *one or more options*. These options set the methods for acquiring identities of managed and unmanaged assets.
6. Select *AD Query - Lets the Security Gateway seamlessly identify Active Directory users and computers* and click *Next*. The *Integration With Active Directory* window opens.
7. Select the *Active Directory* to configure from the list that shows configured LDAP account units or create a new domain. If you have not set up *Active Directory*, you need to enter a domain name, username, password and domain controller credentials.
8. Enter the *Active Directory* credentials and click *Connect* to verify the credentials. (Important - For *AD Query* you must enter domain) administrator credentials.
9. Click *Finish*.

Step 2: Enabling RADIUS Accounting on a Security Gateway

To enable RADIUS Accounting for a Security Gateway: 1. In the *SmartDashboard Network Objects tree*, open the *Security Gateway*. 2. On the *General Properties* page, make sure that the *Identity Awareness Blade* is enabled. 3. On the *Identity Awareness* page, select *RADIUS Accounting*.

Step 3: Configuring RADIUS Accounting



1. In the *Check Point Gateway* window > *Identity Awareness* panel, click *Settings* (to the right of the RADIUS Accounting option).
2. In the *RADIUS Accounting Settings* window, configure the *Message Attribute Indices* like this:
 - **Device Name:** Calling-Station-Id (31) (Mac Address of the device)
 - **User Name:** User-Name (1) (Username put on the PacketFence Portal)
 - **Device Name:** Framed-IP-Address (8) (IP Address of the device in the production network)

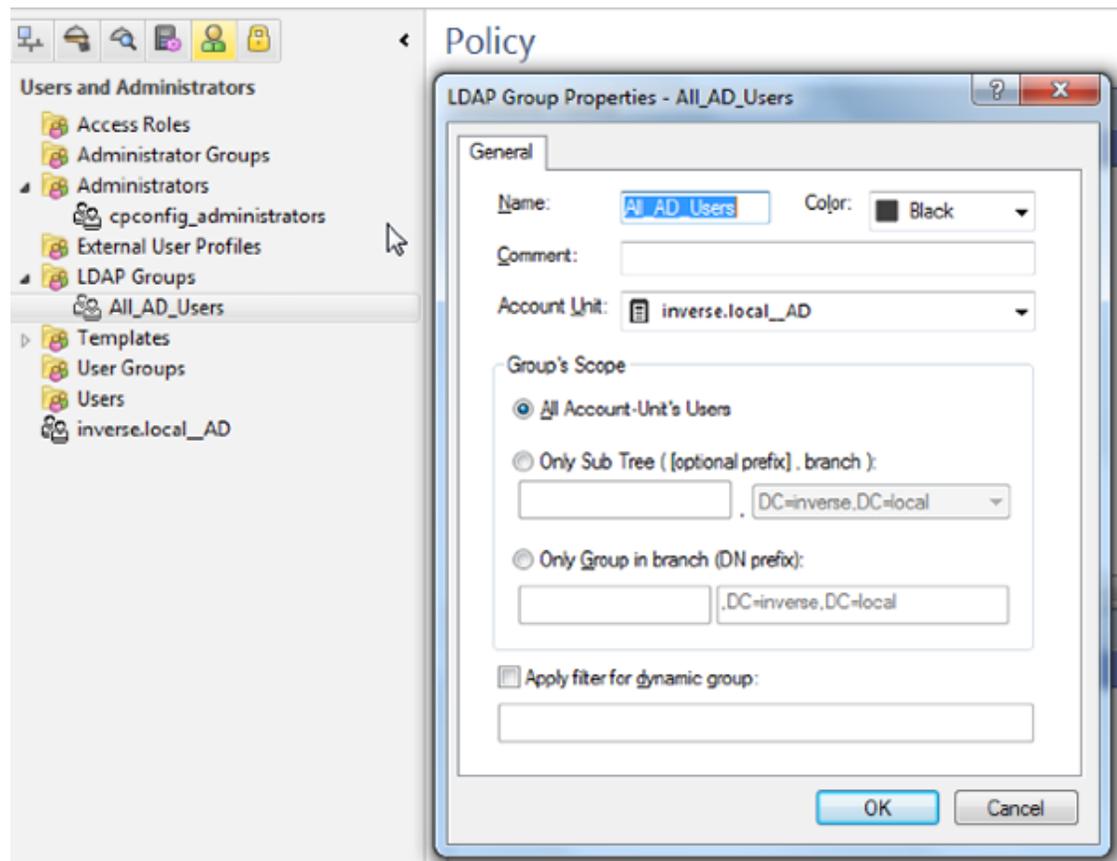
Step 4: RADIUS Client Access Permissions

Gateway interfaces must be authorized to accept connections from PacketFence RADIUS Accounting.

To select gateway interfaces: 1. In the *RADIUS Client Access Permissions* section, click Edit. 2. Select *All Interfaces - All Security Gateway interfaces can accept connections from RADIUS Accounting clients*. 3. Leave the default port to 1813. 4. Click OK on both windows to submit the configuration. 5. Select *Policy > Install* from the SmartDashboard menu.

Step 5: LDAP Groups

Make sure that you have the correct LDAP Objects created on the Checkpoint.



Step 6: SSO Configuration in PacketFence

Go to **Configuration → Firewall SSO → Add Firewall → Checkpoint **.

- **Hostname or IP Address:** IP of your Checkpoint firewall
- **Secret or Key:** secret (radius shared secret)
- **Port:** 1813
- **Roles:** add the roles that you want to do SSO with

The image shows a configuration window titled "Firewall SSO" with a close button in the top right corner. The window contains the following fields and options:

- Hostname or IP Address**: A text input field containing "192.168.100.2".
- Secret**: A text input field containing "*****".
- Port of the service**: A text input field containing "1813" with a help icon to its right.
- UID type**: A dropdown menu with "PID" selected. Above it is the text "If you use an alternative port, please specify".
- Roles**: A text input field containing "staff" with a close icon to its right.

Below the Roles field, the text "Nodes with the selected roles will be affected" is displayed. At the bottom right of the dialog, there are two buttons: "Close" and "Save".

Step 7: Verification

You can check the correct log in with the SmartView Tracker under **Network & Endpoint Queries** → **Predefined** → **Identity Awareness Blade** → **Login Activity**