



Pulse Policy Secure

Admission Control with Check Point Next-Generation
Firewall

Deployment Guide

Pulse Secure, LLC
2700 Zanker Road, Suite 200
San Jose, CA 95134
www.pulsesecure.net

© 2019 by Pulse Secure, LLC. All rights reserved.

Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Pulse Policy Secure: Admission Control with Check Point Next-Generation Firewall

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at www.pulsesecure.net. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.”

Contents

Purpose of this Guide.....	4
Prerequisites.....	4
Overview: Deploying PPS with Check Point Next-Generation Firewall	5
Overview: Deploying PPS with Check Point Next-Generation Firewall in a Large Enterprise	6
Summary of Configuration.....	7
Configuring PPS with Check Point Next-Generation Firewall	7
Configuring Check Point Infranet Enforcer in PPS.....	7
Configuring Auth Table Mapping Policies	9
Configuring Check Point Next-Generation Firewall.....	11
Configuring Identity Awareness using Smart Console	11
Troubleshooting	14
Unsupported Features	14

Purpose of this Guide

This guide describes how to configure *Pulse Policy Secure (PPS)* to provide identity-based admission control using *Check Point Next-Generation Firewall*.

Prerequisites

This guide assumes you are familiar with the use of the following products and their related terminology.

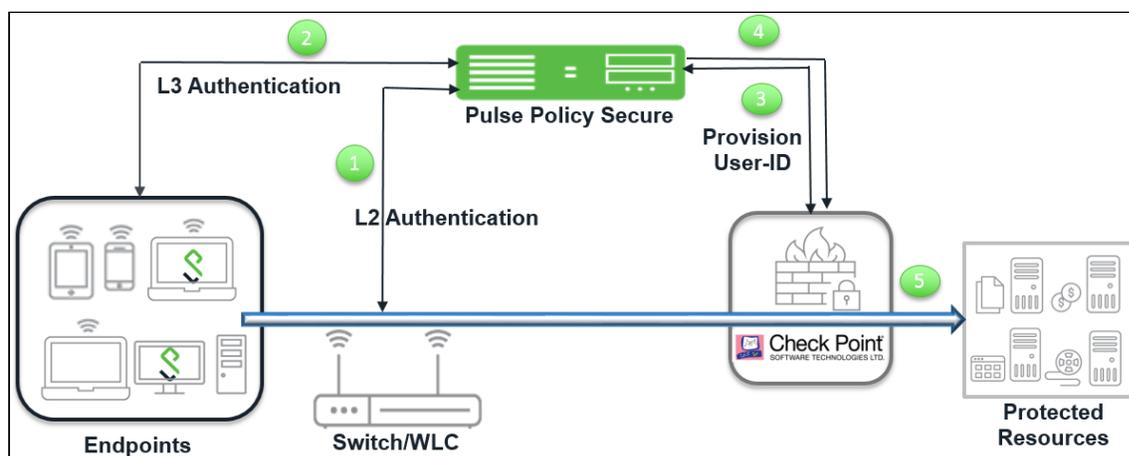
- *Pulse Policy Secure* at version 9.0R3
- *Check Point Next-Generation Firewall* at version R80.10.

Overview: Deploying PPS with Check Point Next-Generation Firewall

This section describes the integration of *PPS* with *Check Point Next-Generation Firewall*. The *Check Point Next-Generation Firewall* controls the access to protected resources (for example, internet, CRM systems, Wikis and so on.) based on policy settings that defines the access. The *Check Point Next-Generation Firewall* enables integration with directory sources (For example, AD or LDAP) to get user and group information. The policies are then defined based on user role information.

PPS serves as the provider of identity information (For example, user-ID, IP address, and roles) for *Check Point Next-Generation Firewall*. The *Check Point Next-Generation Firewall* uses the identity information provided by the *PPS* for deciding the resource access.

Figure 1: Integrating Check Point with PPS



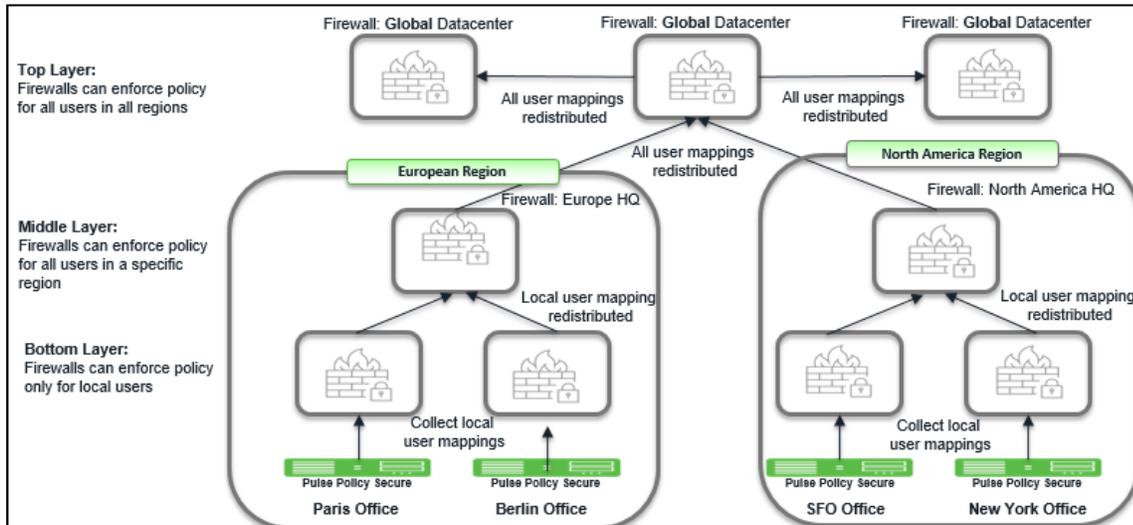
The authentication process is described below:

- 1) The endpoints connect to Switch/WLAN and performs the layer 2 authentication with *PPS*.
- 2) *PPS* performs the layer 3 authentication and performs compliance check on the endpoint and detects for any unauthorized behavior. *PPS* can also learn endpoint IP address using accounting and provision mapping.
- 3) *PPS* provisions the auth table entries (user-ID, IP address, and roles) on the *Check Point Next-Generation Firewall*.
- 4) The user role changes, which includes any unauthorized behavior are dynamically updated on the Next-Generation Firewall. *PPS* provisions the auth table with changes in role information if any on *Check Point Next-Generation Firewall*. The access is based on roles.
- 5) The *Check Point Next-Generation Firewall* applies policies to allow or block user access to protected resources.

Overview: Deploying PPS with Check Point Next-Generation Firewall in a Large Enterprise

For an enterprise with remote branch offices connected to the headquarters with VPN, deploy the Security Gateway at the remote branch offices. When you enable Identity Awareness on the branch office Security Gateway, users are authenticated before they reach internal resources. The identity data on the branch office Security Gateway is shared with other Security Gateways to avoid unnecessary authentication.

Figure 2: Integrating Check Point with PPS for a Large Enterprise



Summary of Configuration

To prepare your network to perform identity-based admission control using Pulse Policy Secure and Check Point Next-Generation Firewall, perform the following tasks:

- [Configuring PPS with Check Point Next-Generation Firewall.](#)
 - [Configuring Check Point Infranet Enforcer in PPS.](#)
 - [Configuring Auth Table Mapping Policies.](#)
- [Configuring Check Point Next-Generation Firewall.](#)
 - [Configuring Identity Awareness.](#)

Configuring PPS with Check Point Next-Generation Firewall

The *PPS* configuration requires adding *Check Point Next-Generation Firewall* as an Infranet Enforcer and creating the auth table mapping policy.

This section covers the following topics:

- [Configuring Check Point Infranet Enforcer in PPS.](#)
- [Configuring Auth Table Mapping Policies.](#)

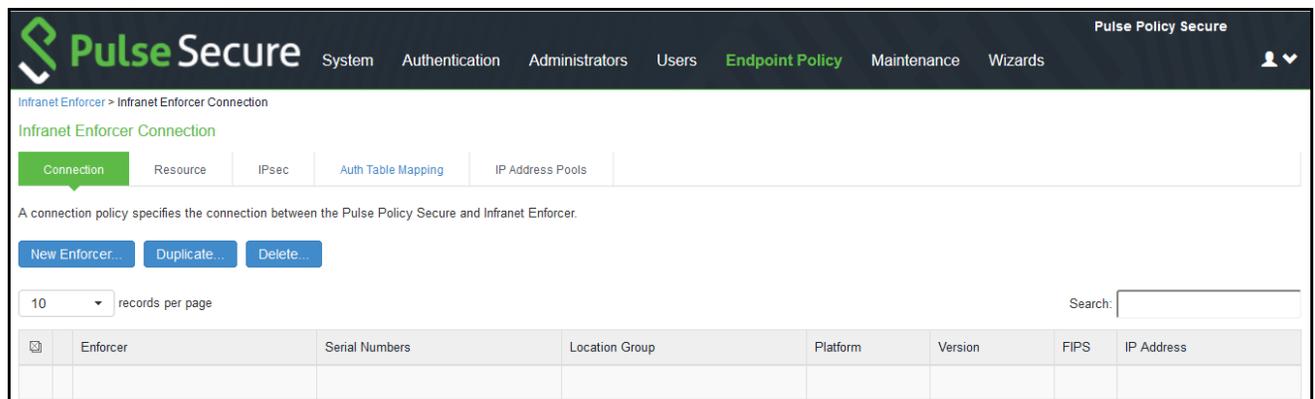
Configuring Check Point Infranet Enforcer in PPS

The *PPS* configuration requires defining a new *Check Point Next-Generation Firewall* Infranet Enforcer instance on *PPS* and then fetching the pre-configured shared secret key from the Next-Generation Firewall. The shared secret key is used to communicate between the *Check Point Next-Generation Firewall* and *PPS*. The standard user authentication / authorization configurations such as Auth Table Mapping Policies should also be created and associated with the required roles.

To configure a *Check Point Next-Generation Firewall* Infranet Enforcer in *PPS*:

- 1) Select **Endpoint Policy > Infranet Enforcer**.

Figure 3: Infranet Enforcer



- 2) Click **New Infranet Enforcer** and select **Check Point Firewall** in the Platform drop down.

- 3) Enter the **Name** and **IP Address** of the *Check Point Next-Generation Firewall* and enter the shared secret between *PPS* and *Check Point Next-Generation Firewall*.

Note: PPS has the default server URL for Check Point R80.10. You can edit/modify the server URL as per your requirement. For Check Point version (R77.30), edit the server URL manually to `https://<IP_Address>/_IA_MU_Agent/idasdk`

Figure 4: Check Point Next-Generation Firewall

The screenshot shows the Pulse Secure web interface. The top navigation bar includes 'System', 'Authentication', 'Administrators', 'Users', 'Endpoint Policy' (highlighted), 'Maintenance', and 'Wizards'. The breadcrumb trail is 'Infranet Enforcer > Connection > CP_1'. The main content area is titled 'CP_1' and has a 'Connection' tab selected. Under 'Infranet Enforcer', the following fields are visible:

- Platform:** Check Point Firewall (dropdown menu)
- * Name:** Check Point
- * IP Address:** 10.20.100.100
- * Shared Secret:** *****
- Server Certificate Validation:**

Below the IP Address field, there is a note: "By default the Server Uri will be "https://<ipAddress>/_IA_API/v1.0". To modify Server Uri click on [edit](#)".

At the bottom left, there is a blue 'Save Changes' button.

- 4) (Optional) Select **Server Certificate Validation** to verify the Next-Generation Firewall certificate.
- 5) Click **Save Changes**.

Configuring Auth Table Mapping Policies

An auth table entry consists of the user's name, a set of roles, and the IP address of the user device. An auth table mapping policy specifies which enforcer device (Next-Generation Firewall) can be used for each user role. These policies prevent the PPS from creating unnecessary auth table entries on all connected enforcer devices.

PPS's default configuration includes only one default auth table mapping policy. When the default auth table mapping policy is enabled, PPS pushes one auth table entry for each authenticated user to the selected Check Point Next-Generation Firewall configured as Infranet Enforcers in PPS.

To configure an auth table mapping policy:

- 1) Select **Endpoint Policy > Infranet Enforcer > Auth Table Mapping** and click **New Policy**.

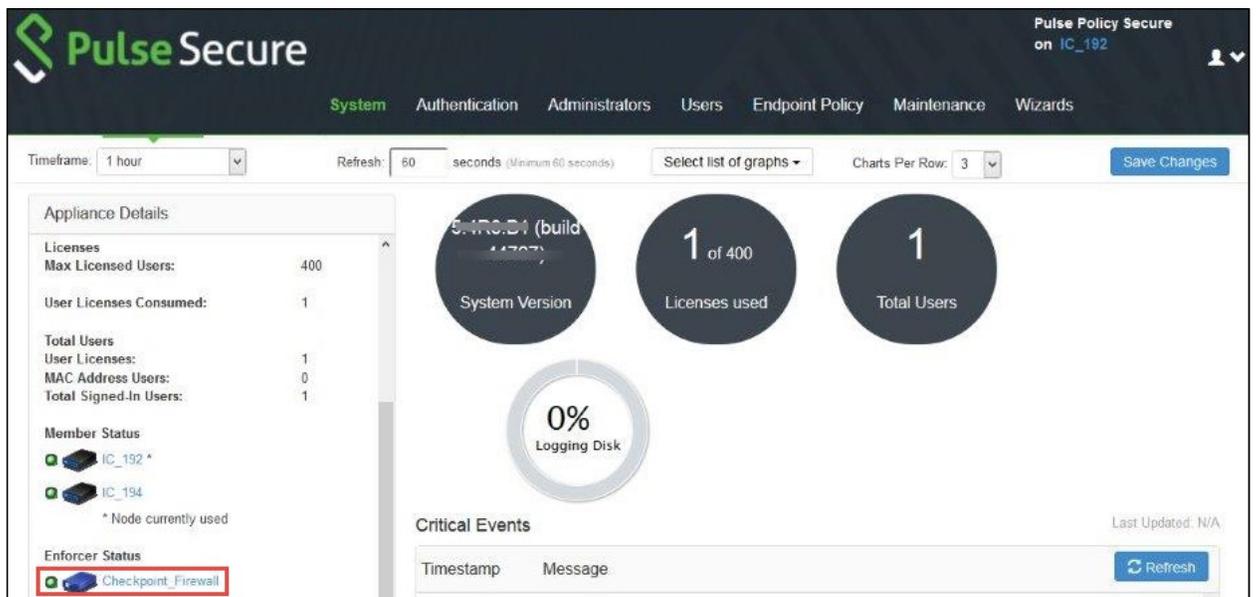
Figure 5: Check Point Next-Generation Firewall Configuration

The screenshot shows the Pulse Secure web interface for configuring an Auth Table Mapping Policy. The breadcrumb trail is: Infranet Enforcer > Infranet Enforcer Auth Table Mapping Policies > Default Policy. The page title is 'Default Policy'. The 'General' section has a required field for 'Name' (CP Policy) and a 'Description' field. The 'Infranet Enforcer' section shows 'Available Enforcers' as '(none)' and 'Selected Enforcers' as 'CP_1'. The 'Roles' section has three radio button options: 'Policy applies to ALL roles', 'Policy applies to SELECTED roles' (selected), and 'Policy applies to all roles OTHER THAN those selected below'. Below these are 'Available roles' (Guest, Guest Admin, Guest Sponsor, Guest Wired Restricted, Users) and 'Selected roles' (Full_Access, Limited_Access). The 'Actions' section has three radio button options: 'Always Provision Auth Table' (selected), 'Provision Auth Table As Needed' (only available for Juniper enforcers), and 'Never Provision Auth Table'. There is a 'VSYS' field and 'Save Changes' and 'Save as Copy' buttons at the bottom. A note at the bottom left says '* indicates required field'.

- 2) On the **New Policy** page:
 - a) For **Name**, enter a name to label the auth table mapping policy.
 - b) (Optional) For **Description**, enter a description.

- c) In the **Enforcer** section, specify the Infranet Enforcer firewall(s) to which you want to apply the auth table mapping policy.
 - d) In the **Roles** section, specify:
 - *Policy applies to ALL roles:* Select this option to apply the auth table mapping policy to all users.
 - *Policy applies to SELECTED roles:* Select this option to apply the auth table mapping policy only to users who are mapped to roles in the **Selected** roles list. You can add roles to this list from the available roles list.
 - *Policy applies to all roles OTHER THAN those selected below:* Select this option to apply the auth table mapping policy to all users except for those who map to the roles in the **Selected** roles list. You can add roles to this list from the available roles list.
 - e) In the **Action** section, specify auth table mapping rules for the specified Infranet Enforcer.
 - *Always Provision Auth Table:* Select this option to automatically provision auth table entries for chosen roles on the specified Infranet Enforcer.
 - *Provision Auth Table as Needed:* Select this option to provision auth table entries only when a user with a chosen role attempts to access a resource behind the specified Infranet Enforcer. This option is greyed out for *Check Point Next-Generation Firewall* Enforcers since it is not supported.
 - *Never Provision Auth Table:* Select this option to prevent chosen roles from accessing resources behind the specified Infranet Enforcer.
- 3) You must delete the default policy if you configure any custom auth table mapping policies. *The* default configuration includes this default auth table mapping policy that allows all source IP endpoints to use all Infranet Enforcers.
 - 4) Click **Save Changes**.

Figure 6: Enforcer Status

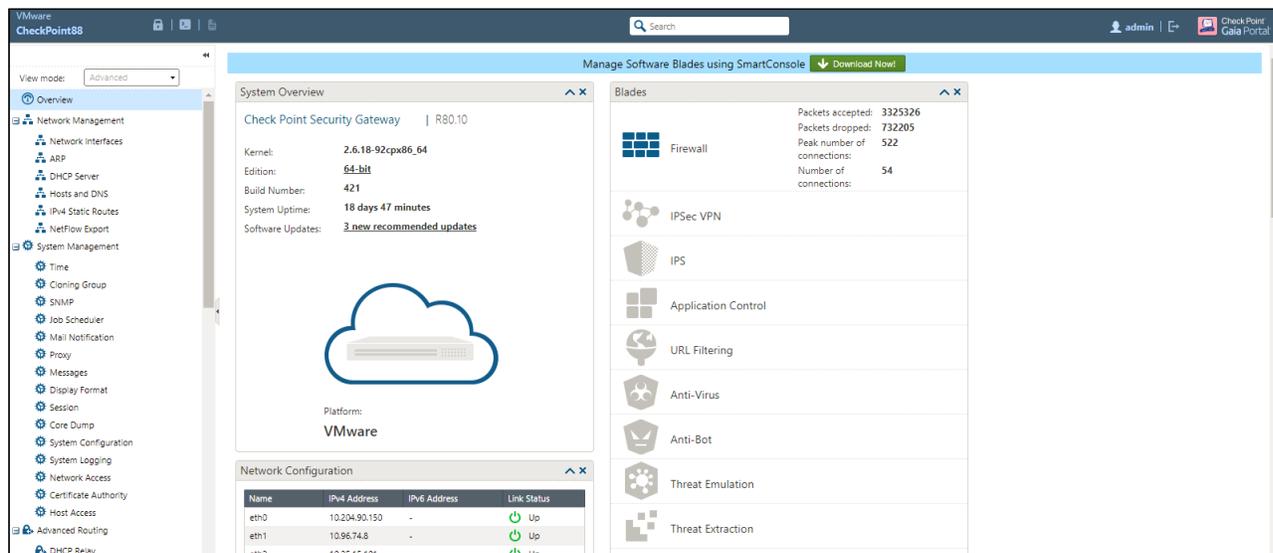


Configuring Check Point Next-Generation Firewall

Check Point Next-Generation Firewall detects traffic from an endpoint that matches a configured security policy using the access roles. It determines the role(s) associated with that user, and allows or denies the traffic based on the actions configured in the security policy.

The network interfaces are configured on the Check Point Next-Generation firewall and the remaining configurations are done on the Check Point Smart Console.

Figure 7: Check Point R80.10



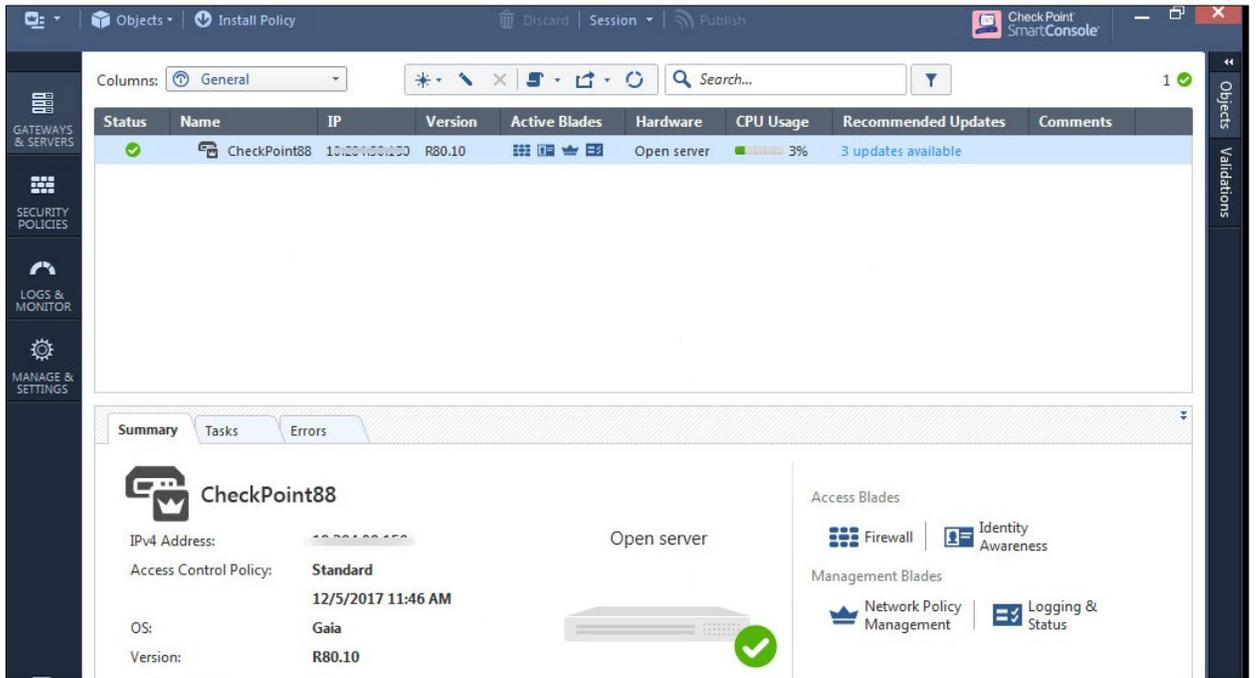
Configuring Identity Awareness using Smart Console

The Identity Awareness lets you easily configure network access and auditing based on network location, identity of user, and identity of the device. When Identity Awareness identifies a source or destination, it shows the IP address of the user or computer with a name. For example, this lets you create firewall rules with any of these properties. You can define a firewall rule for specific users when they send traffic from specific computers or a firewall rule for a specific user regardless of which computer they send traffic from.

To enable Identity awareness:

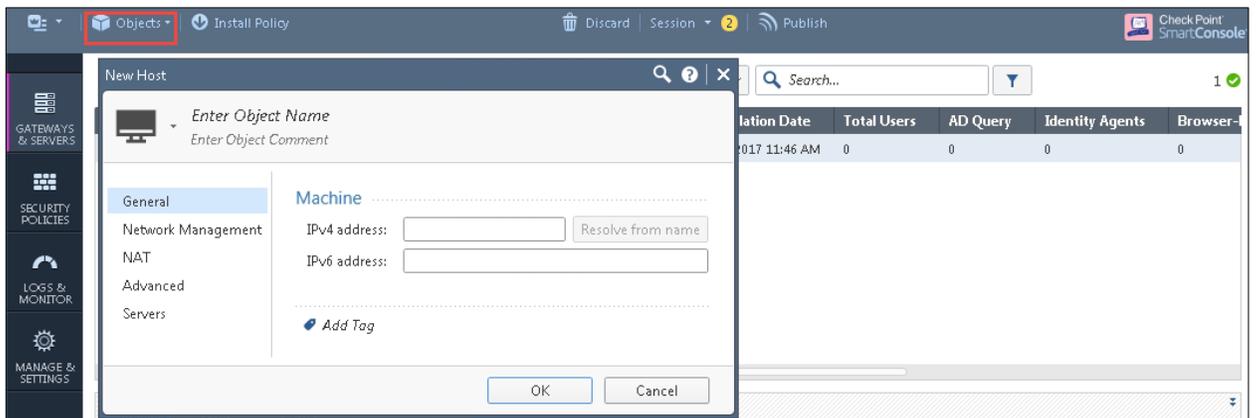
- 1) Login to the Check Point SmartConsole.
- 2) From the **Security & Gateways** view, double-click the Security Gateway on which to enable identity awareness.

Figure 7: SmartConsole



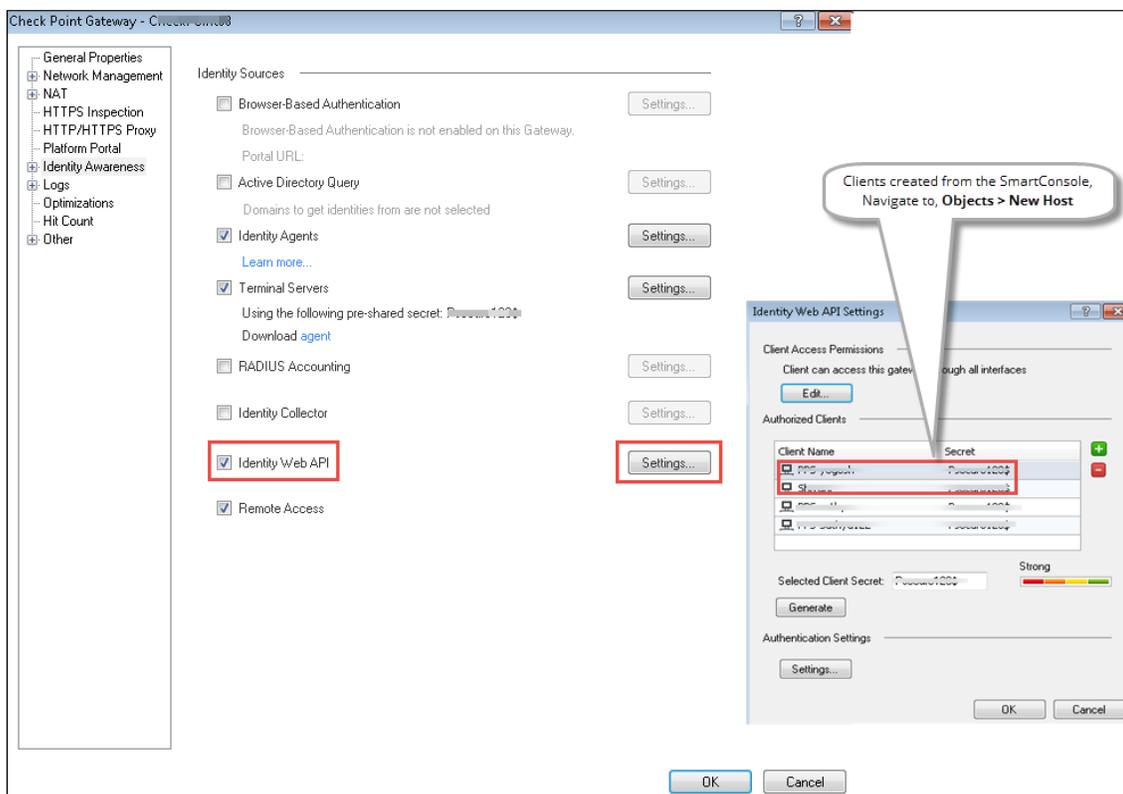
- 3) Create an object for PPS. Select **Objects > New Host** and enter the PPS IP address. Under Servers, enable Web Server and click OK.

Figure 8: Host



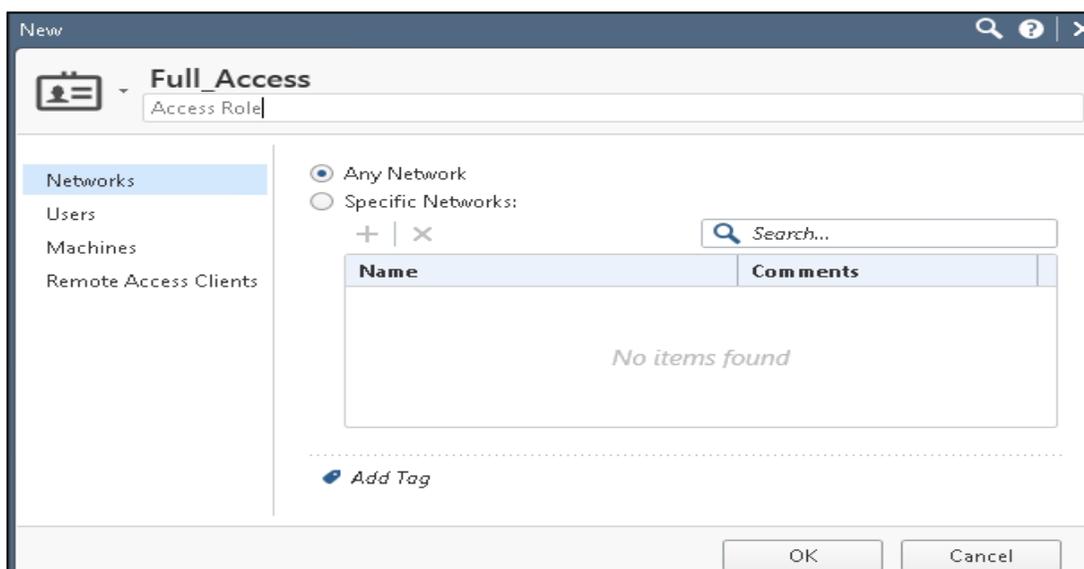
- 4) Select **Gateways & Servers > Identity Awareness** and enable the following options:
 - a) Terminal Servers- Note down the pre-shared secret key.
 - b) Identity Web API- Click **Settings** and add the PPS device as Authorised Clients.

Figure 9: Identity Awareness



- 5) Click **Install Policy**
- 6) From the Object Explorer create an object for Identity matching by creating user roles. Select **Objects > Object Explorer** and Click **New > Users > Access Role**

Figure 10: Creating Access Roles

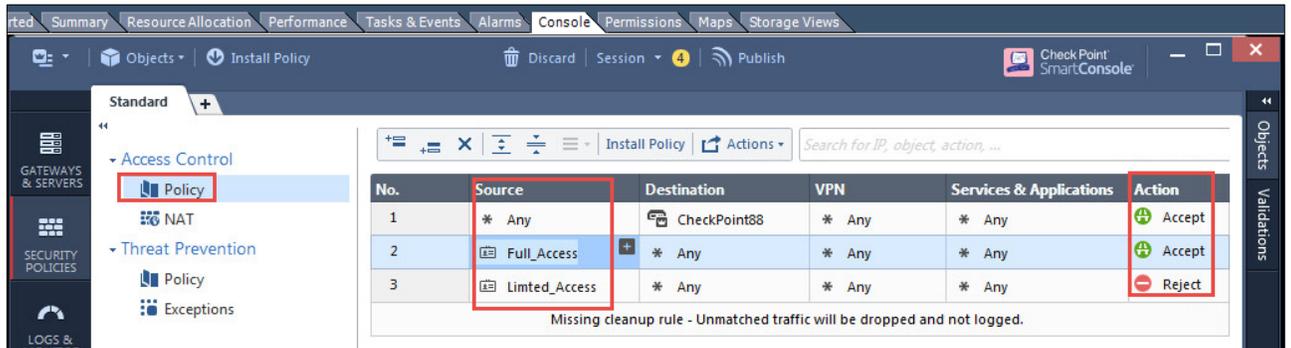


- 7) From the Smart Console create a security policy by keeping the Access Role in Source column. Select **Security Policies > Access Control > Policy** and then configure the required policies. For example:

- *Full_Access* role policy allows traffic from Client with *Full_Access* role
- *Limited_Access* role policy denies traffic from Client with *Limited_Access* role

NOTE: The *Full_Access* role is on the top of the list as it should be considered first. The role names must match with the Role names created on *PPS*.

Figure 11: Security Policy based on Access Roles



8) Click **Install Policy**.

Troubleshooting

You can use the following CLI commands (Expert Mode) on the *Check Point Next-Generation Firewall* for troubleshooting:

```
pdp monitor all
```

This displays the table of user identities mapped to IP addresses.

Unsupported Features

The following features are not supported:

- IP Address Pools.
- IPsec Enforcement.
- IDP Sensors.
- Virtual Systems (VSYS).
- Enforcement for endpoints behind Network Address Translation (NAT).
- Resource access policies. The administrator should configure all firewall policies on the firewall through Check Point *SmartConsole*.