Pulse Secure®

Pulse Policy Secure

Access Control with Check Point Next-Generation Firewall

Deployment Guide

Document 3.0

Published January 2020

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

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

Contents

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 9.1R4
- *Check Point Next-Generation* Firewall at version R80.10.

Identity-Based Access Control with Check Point

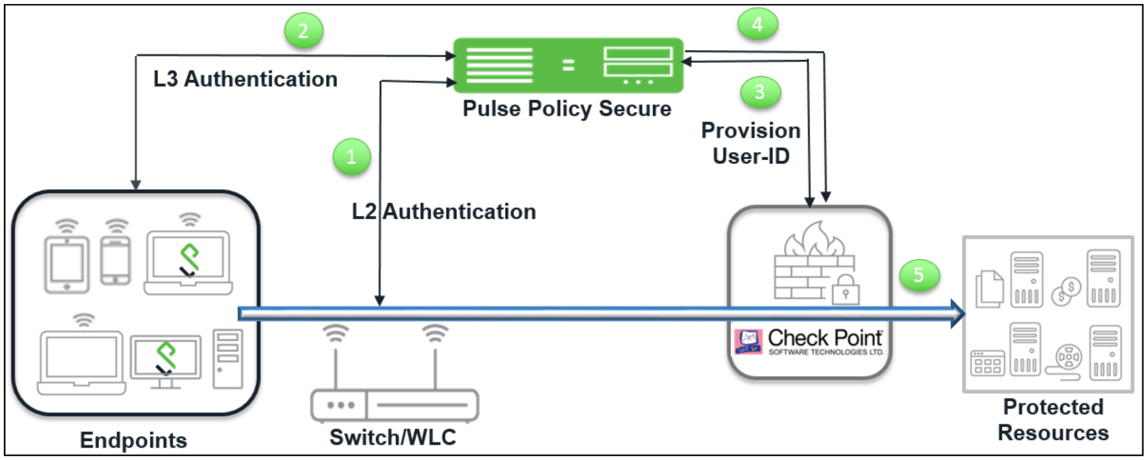
This section describes how to integrate Check Point Next Generation Firewall with PPS to support Identity-based admission control in your network.

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:

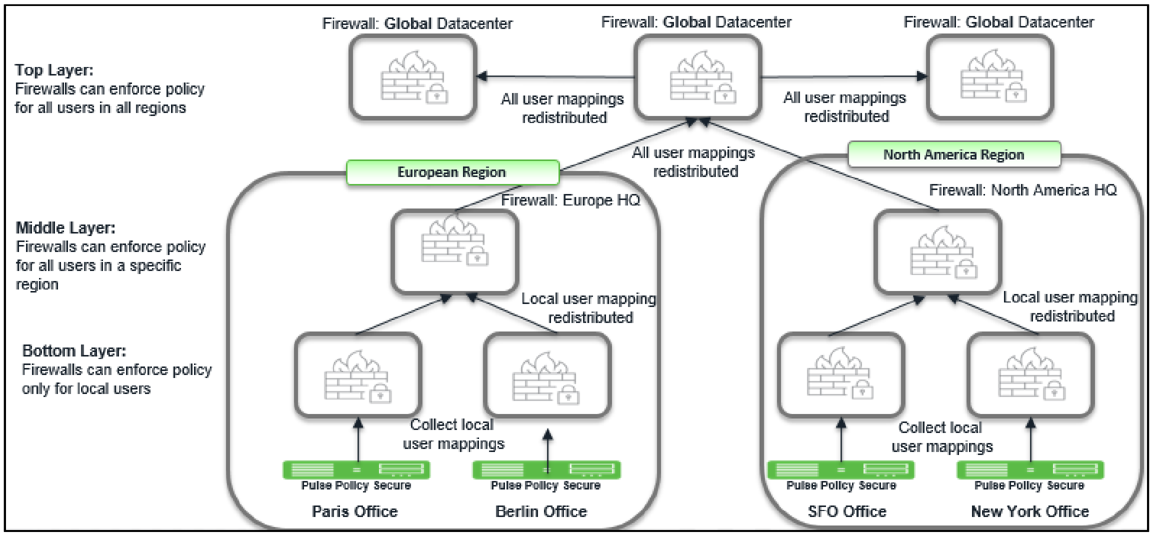
1) The endpoints connect to Switch/WLAN and performs the layer 2 authentication with *PPS*.
2) *PPS* performs the layer 3 authentication and performs compliance check on the endpoint and detects for any unauthorized behavior. *PPS* can also learn endpoint IP address using accounting and provision mapping.
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



Firewall: Global Datacenter
Firewall: Global Datacenter
Firewall: Global Datacenter
Top Layer:
Firewalls can enforce policy for all users in all regions
All user mappings redistributed
All user mappings redistributed
All user mappings redistributed
European Region
North America Region
Firewall: Europe HQ
Firewall: North America HQ
Middle Layer:
Firewalls can enforce policy for all users in a specific region
Local user mapping redistributed
Local user mapping redistributed
Bottom Layer:
Firewalls can enforce policy only for local users
Collect local user mappings
Collect local user mappings
Pulse Policy Secure
Pulse Policy Secure
Pulse Policy Secure
Pulse Policy Secure
Paris Office
Berlin Office
SFO Office
New York Office

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.

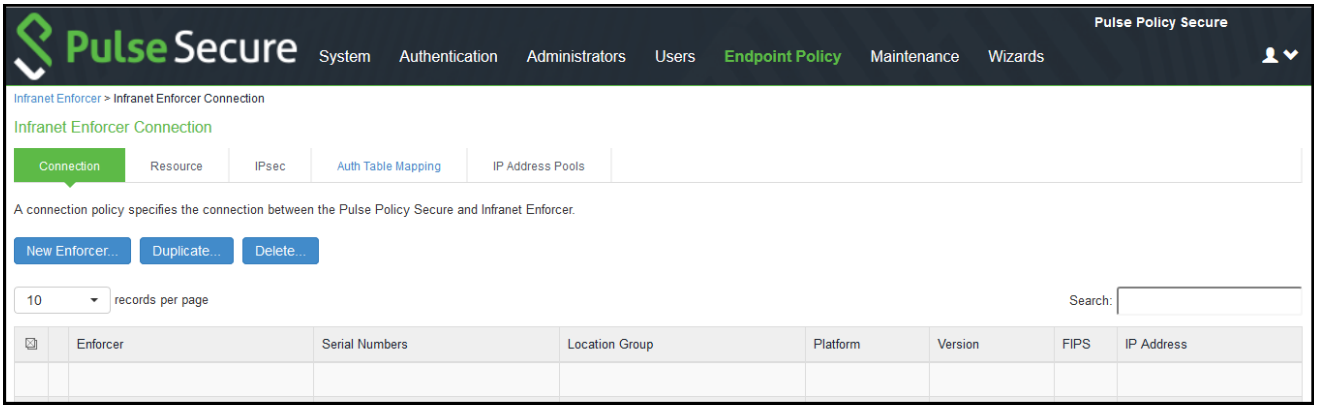
Configuring Check Point Infranet Enforcer in PPS

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



Infranet Enforcer > Infranet Enforcer Connection

Infranet Enforcer Connection

A connection policy specifies the connection between the Pulse Policy Secure and Infranet Enforcer.

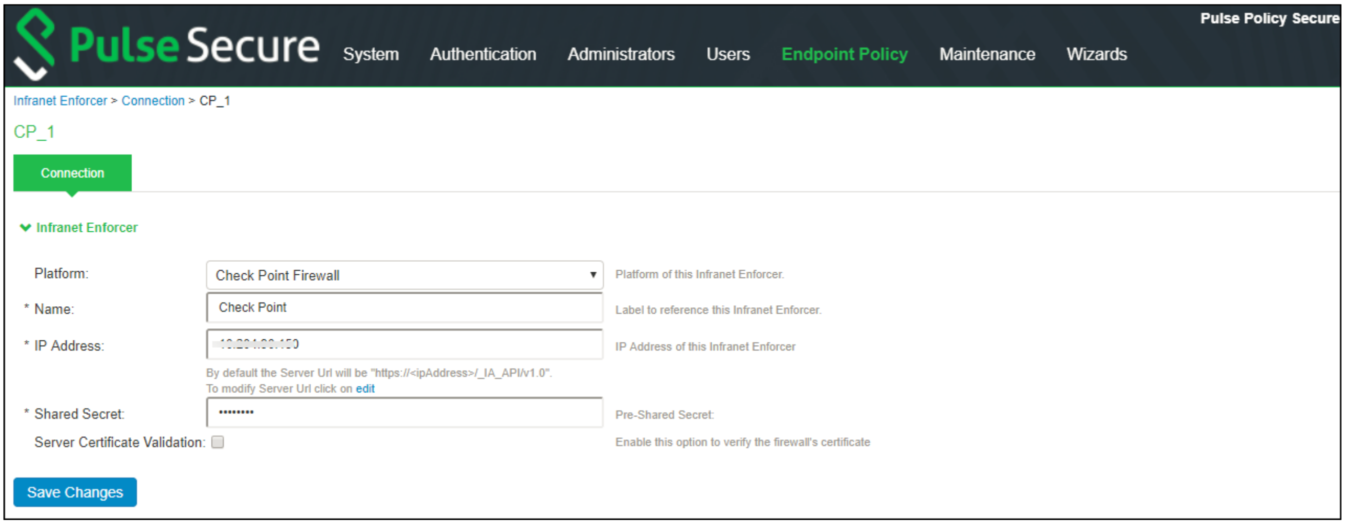
☐	Enforcer	Serial Numbers	Location Group	Platform	Version	FIPS	IP Address

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



Platform: Check Point Firewall ▾ Platform of this Infranet Enforcer.

* Name: Check Point Label to reference this Infranet Enforcer.

* IP Address: [redacted] IP Address of this Infranet Enforcer

By default the Server Url will be "https://<ipAddress>/_IA_API/v1.0".
To modify Server Url click on edit

* Shared Secret: •••••••• Pre-Shared Secret.

Server Certificate Validation: □ Enable this option to verify the firewall's certificate

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

5) Click **Save Changes**.

Configuring Auth Table Mapping Policies

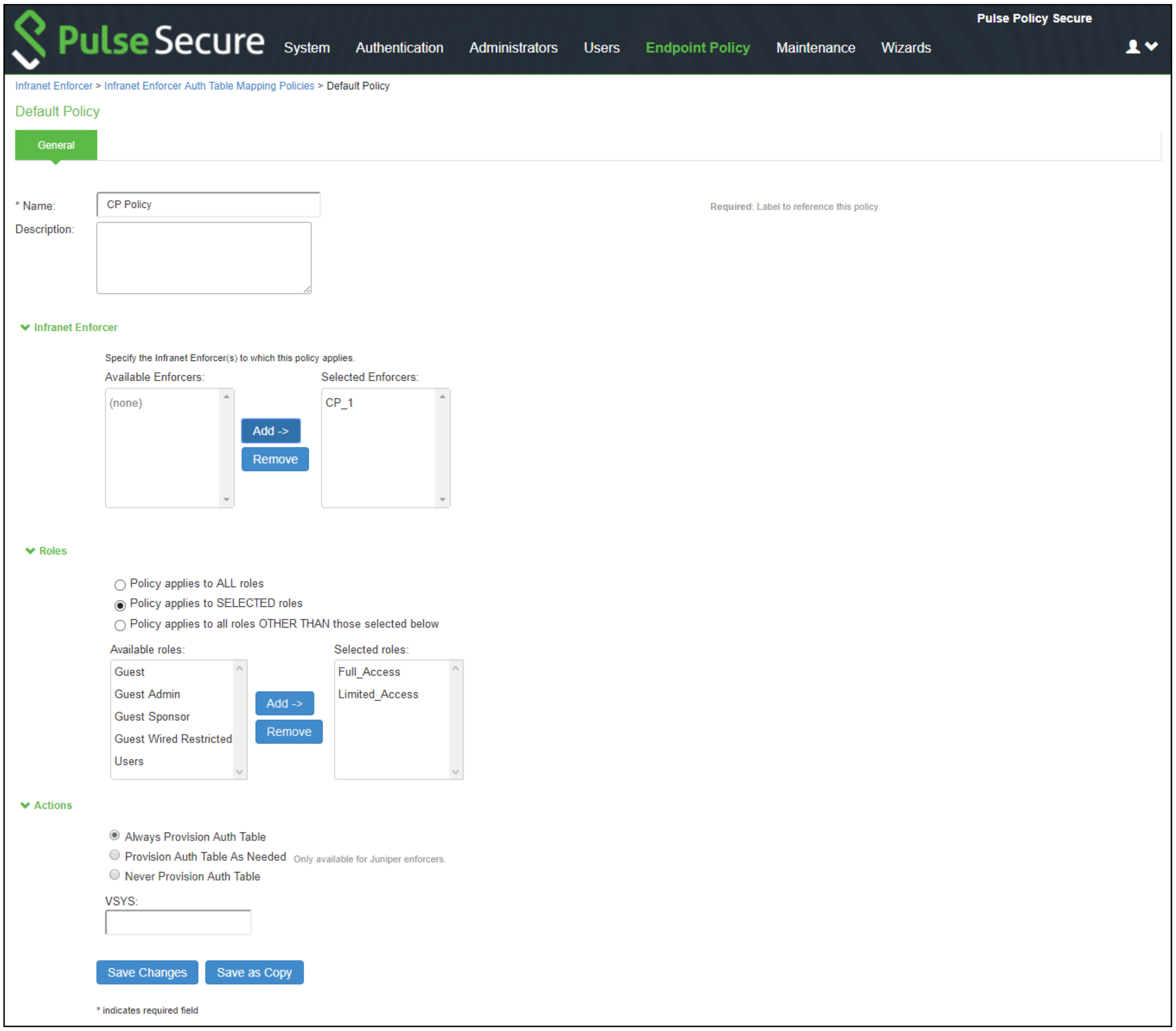
An auth table entry consists of the user's name, a set of roles, and the IP address of the user device. An auth table mapping policy specifies which enforcer device (Next-Generation Firewall) can be used for each user role. These policies prevent the *PPS* from creating unnecessary auth table entries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



Default Policy

* Name: CP Policy

Required: Label to reference this policy.

Description:

Infranet Enforcer

Specify the Infranet Enforcer(s) to which this policy applies.

Available Enforcers: (none)

Selected Enforcers: CP_1

Roles

○ Policy applies to ALL roles

● Policy applies to SELECTED roles

○ Policy applies to all roles OTHER THAN those selected below

Available roles: Guest, Guest Admin, Guest Sponsor, Guest Wired Restricted, Users

Selected roles: Full_Access, Limited_Access

Actions

● Always Provision Auth Table

○ Provision Auth Table As Needed Only available for Juniper enforcers.

○ Never Provision Auth Table

VSYS:

* 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.

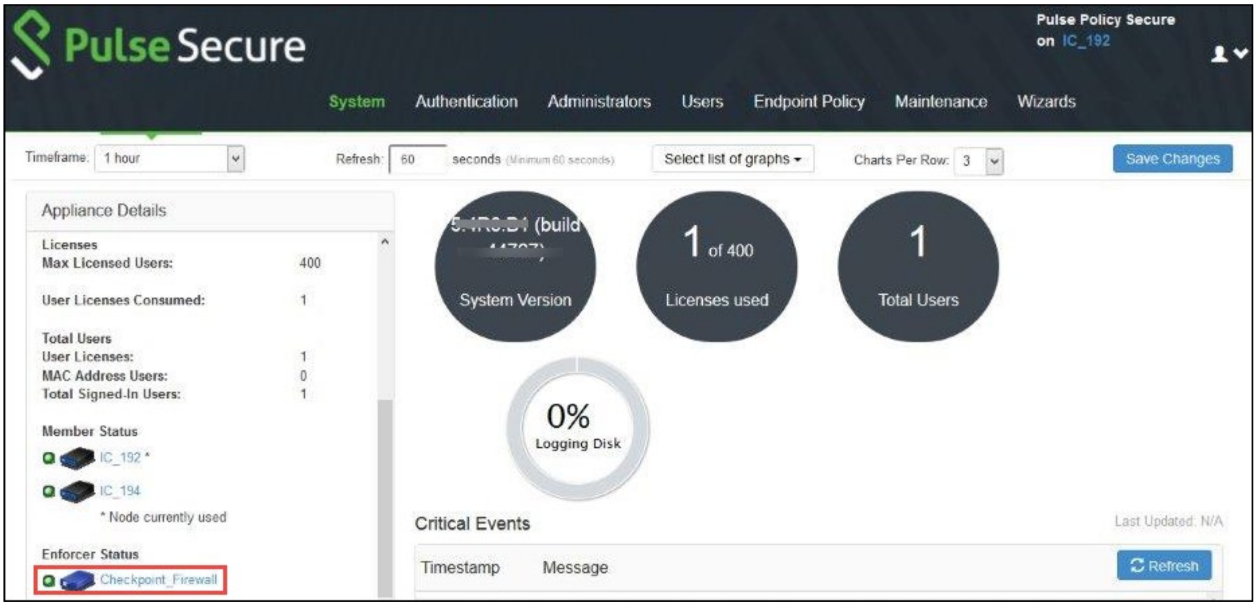
e) In the **Action** section, specify auth table mapping rules for the specified Infranet Enforcer.

- *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



Timeframe: 1 hour

Refresh: 60 seconds (Minimum 60 seconds)

Charts Per Row: 3

Appliance Details

Licenses
Max Licensed Users: 400

User Licenses Consumed: 1

Total Users
User Licenses: 1
MAC Address Users: 0
Total Signed-In Users: 1

Member Status
IC_192 *
IC_194
* Node currently used

Enforcer Status
Checkpoint_Firewall

[redacted] (build [redacted]) System Version

1 of 400 Licenses used

1 Total Users

0% Logging Disk

Critical Events

Last Updated: N/A

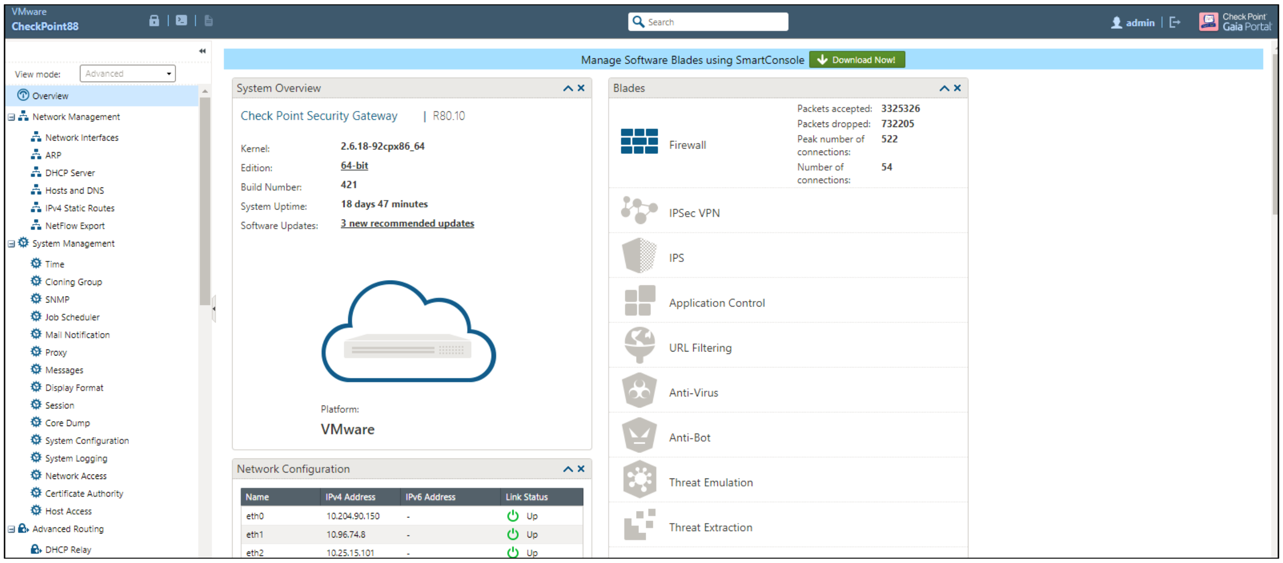
Timestamp	Message

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



Check Point Security Gateway | R80.10

Kernel: 2.6.18-92cpx86_64
Edition: 64-bit
Build Number: 421
System Uptime: 18 days 47 minutes
Software Updates: 3 new recommended updates

Platform:
VMware

Name	IPv4 Address	IPv6 Address	Link Status
eth0	10.204.90.150	-	Up
eth1	10.96.74.8	-	Up
eth2	10.25.15.101	-	Up

Firewall
Packets accepted: 3325326
Packets dropped: 732205
Peak number of connections: 522
Number of connections: 54

IPSec VPN
IPS
Application Control
URL Filtering
Anti-Virus
Anti-Bot
Threat Emulation
Threat Extraction

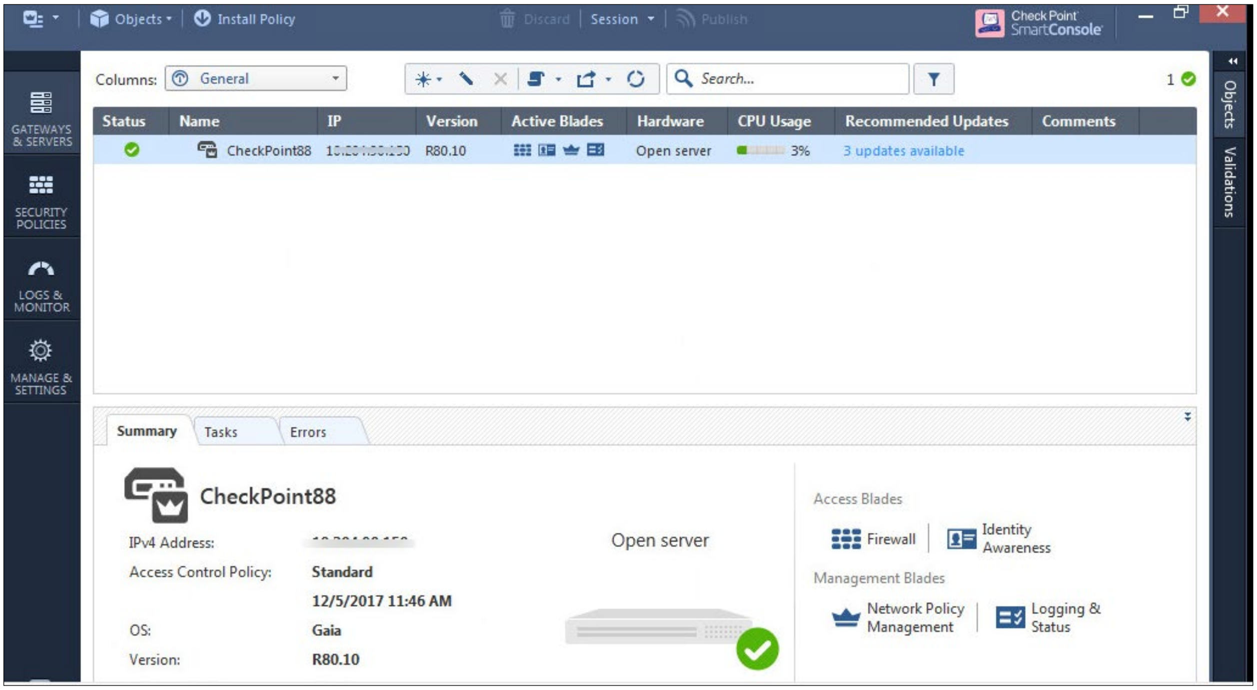
Configuring Identity Awareness using Smart Console

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



Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Recommended Updates	Comments
✓	CheckPoint88	[redacted]	R80.10		Open server	3%	3 updates available	

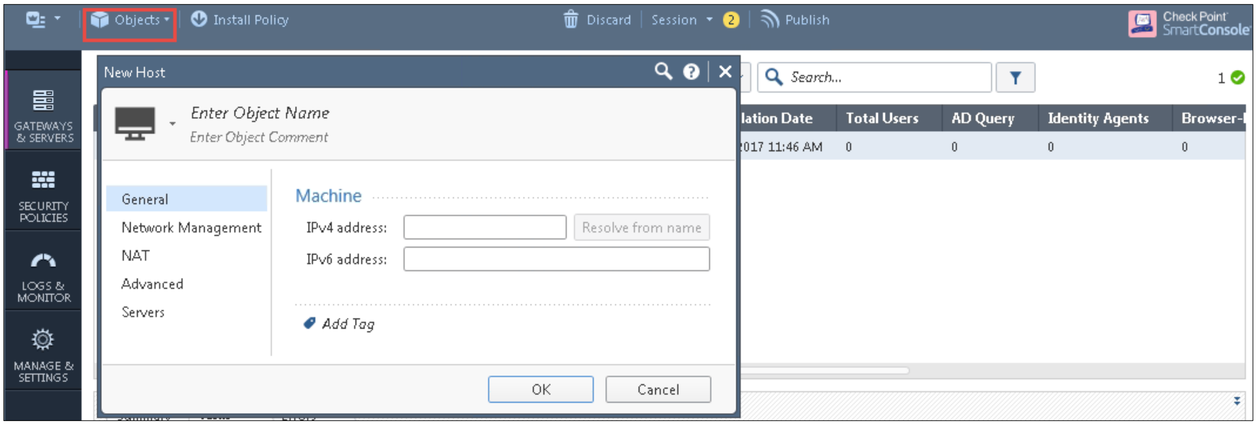
CheckPoint88

Open server

IPv4 Address:	[redacted]
Access Control Policy:	Standard
	12/5/2017 11:46 AM
OS:	Gaia
Version:	R80.10

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

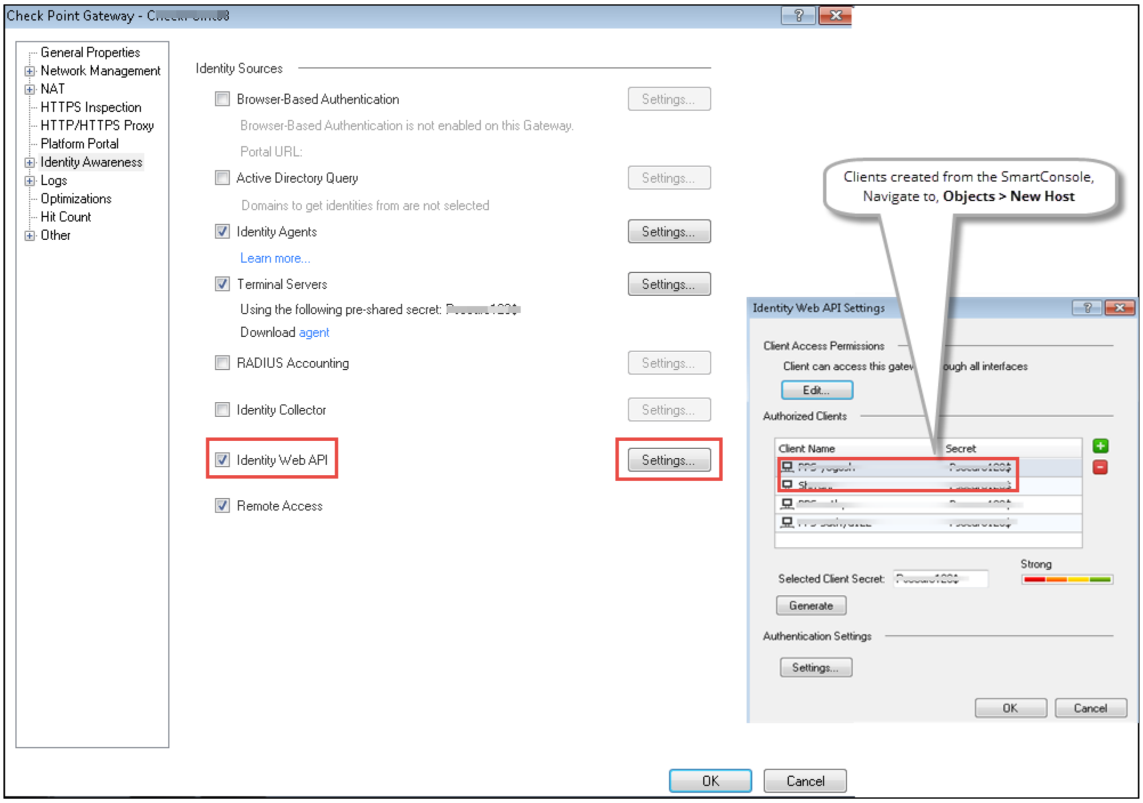


4) Select **Gateways & Servers** > **Identity Awareness** and enable the following options:

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



Check Point Gateway - [redacted]

Identity Sources

□ Browser-Based Authentication — Settings...

Browser-Based Authentication is not enabled on this Gateway.

Portal URL:

□ Active Directory Query — Settings...

Domains to get identities from are not selected

☑ Identity Agents — Settings...

Learn more...

☑ Terminal Servers — Settings...

Using the following pre-shared secret: [redacted]

Download agent

□ RADIUS Accounting — Settings...

□ Identity Collector — Settings...

☑ Identity Web API — Settings...

☑ Remote Access

OK Cancel

Clients created from the SmartConsole, Navigate to, **Objects > New Host**

Identity Web API Settings

Client Access Permissions

Client can access this gatev ough all interfaces

Edit...

Authorized Clients

Client Name	Secret
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Selected Client Secret: [redacted] Strong

Generate

Authentication Settings

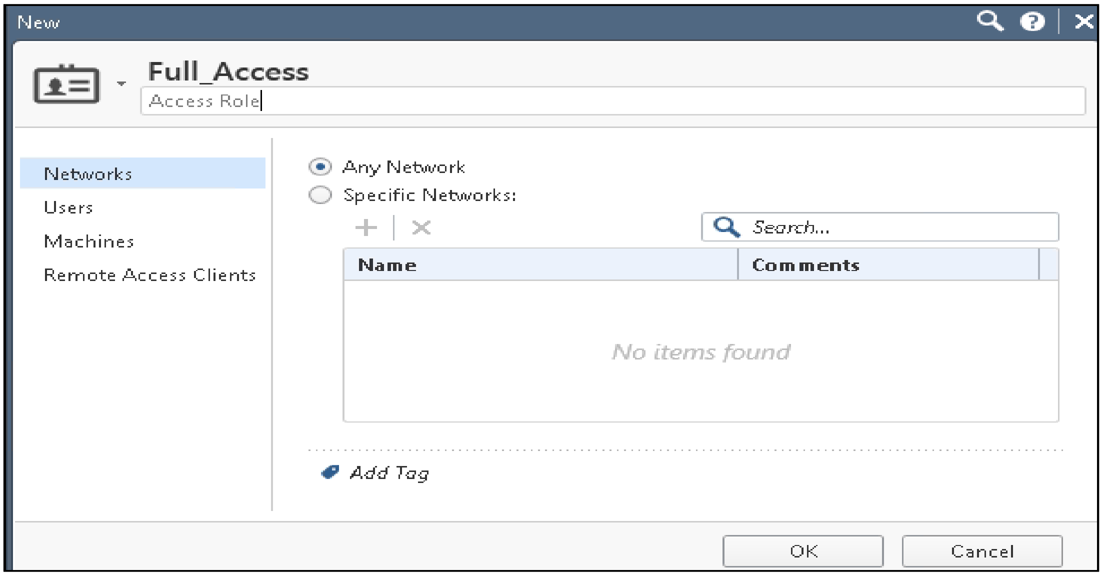
Settings...

OK Cancel

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



New

Full_Access

Access Role

● Any Network

○ Specific Networks:

Search...

Name	Comments
No items found	

Add Tag

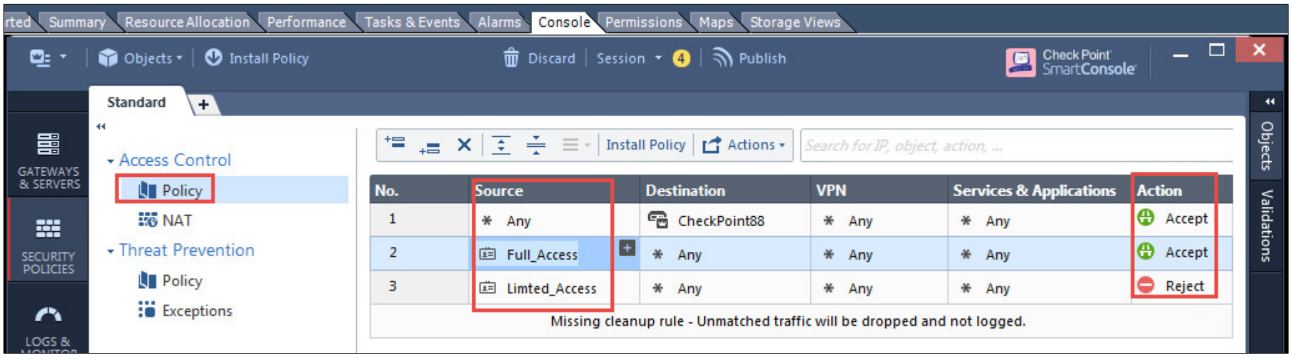
OK Cancel

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



No.	Source	Destination	VPN	Services & Applications	Action
1	Any	CheckPoint88	Any	Any	Accept
2	Full_Access	Any	Any	Any	Accept
3	Limted_Access	Any	Any	Any	Reject

Missing cleanup rule - Unmatched traffic will be dropped and not logged.

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*.

Alert-Based Admission Control with Check Point

This section describes how to integrate Check Point Next Generation Firewall with PPS to support Alert-based admission control in your network.

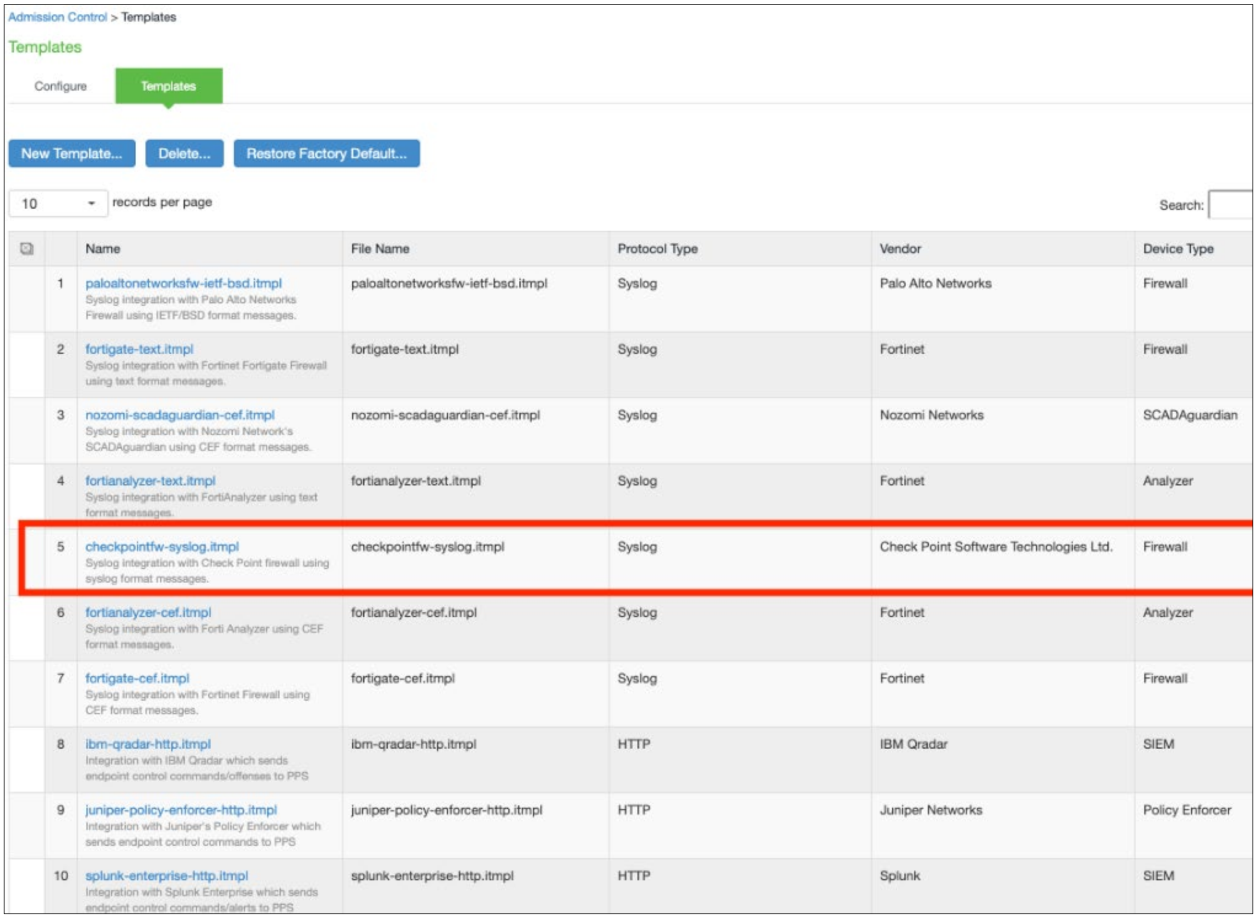
Configuring Pulse Policy Secure

This section describes the integration of PPS with Check Point Next Generation firewall. PPS integrates with Check Point's syslog notification mechanism to receive the threat alert information from Check Point and takes an action based on the admin configured policies.

To view and add the admission control templates:

1) Select **Endpoint Policy > Admission Control > Templates.**

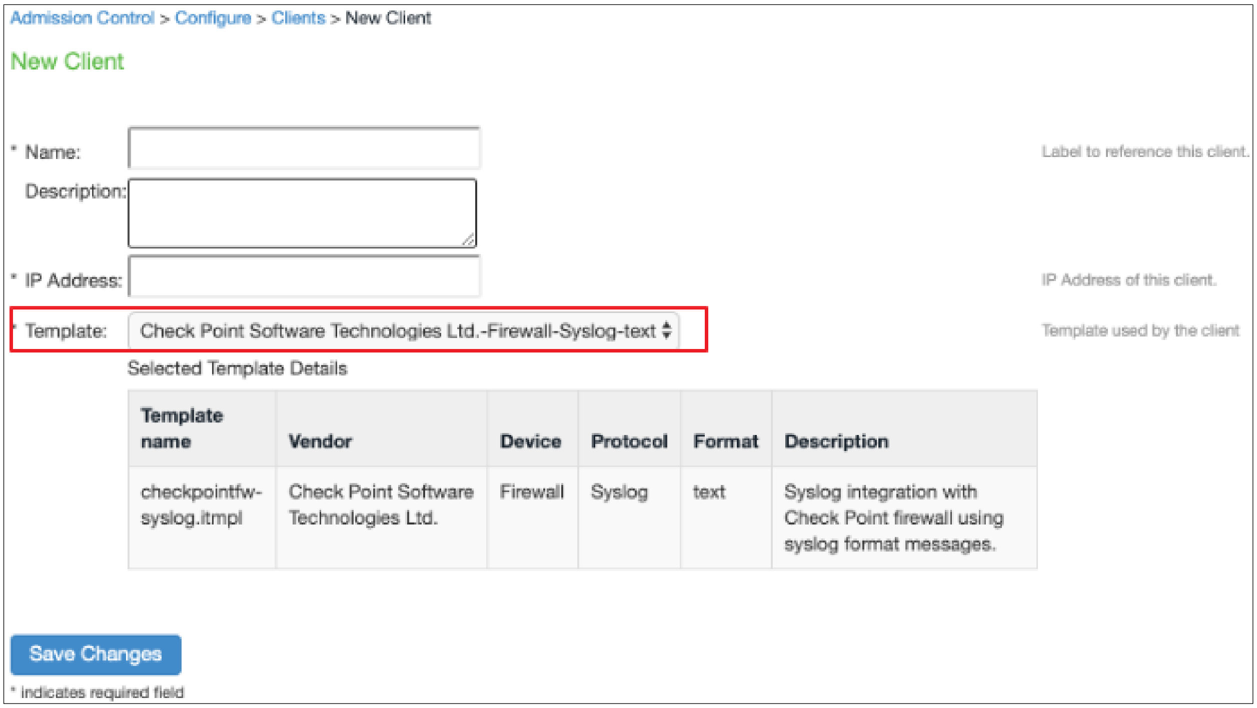
Figure 12: Check Point Template



☐		Name	File Name	Protocol Type	Vendor	Device Type
	1	paloaltonetworksfw-ietf-bsd.itmpl Syslog integration with Palo Alto Networks Firewall using IETF/BSD format messages.	paloaltonetworksfw-ietf-bsd.itmpl	Syslog	Palo Alto Networks	Firewall
	2	fortigate-text.itmpl Syslog integration with Fortinet Fortigate Firewall using text format messages.	fortigate-text.itmpl	Syslog	Fortinet	Firewall
	3	nozomi-scadaguardian-cef.itmpl Syslog integration with Nozomi Network's SCADAguardian using CEF format messages.	nozomi-scadaguardian-cef.itmpl	Syslog	Nozomi Networks	SCADAguardian
	4	fortianalyzer-text.itmpl Syslog integration with FortiAnalyzer using text format messages.	fortianalyzer-text.itmpl	Syslog	Fortinet	Analyzer
	5	checkpointfw-syslog.itmpl Syslog integration with Check Point firewall using syslog format messages.	checkpointfw-syslog.itmpl	Syslog	Check Point Software Technologies Ltd.	Firewall
	6	fortianalyzer-cef.itmpl Syslog integration with Forti Analyzer using CEF format messages.	fortianalyzer-cef.itmpl	Syslog	Fortinet	Analyzer
	7	fortigate-cef.itmpl Syslog integration with Fortinet Firewall using CEF format messages.	fortigate-cef.itmpl	Syslog	Fortinet	Firewall
	8	ibm-qradar-http.itmpl Integration with IBM Qradar which sends endpoint control commands/offenses to PPS	ibm-qradar-http.itmpl	HTTP	IBM Qradar	SIEM
	9	juniper-policy-enforcer-http.itmpl Integration with Juniper's Policy Enforcer which sends endpoint control commands to PPS	juniper-policy-enforcer-http.itmpl	HTTP	Juniper Networks	Policy Enforcer
	10	splunk-enterprise-http.itmpl Integration with Splunk Enterprise which sends endpoint control commands/alerts to PPS	splunk-enterprise-http.itmpl	HTTP	Splunk	SIEM

2) Select **Endpoint Policy > Admission Control > Clients**, choose **Check Point Software Technologies Ltd-Firewall-Syslog-text** as template during the template creation.

Figure 13: Client



Admission Control > Configure > Clients > New Client

New Client

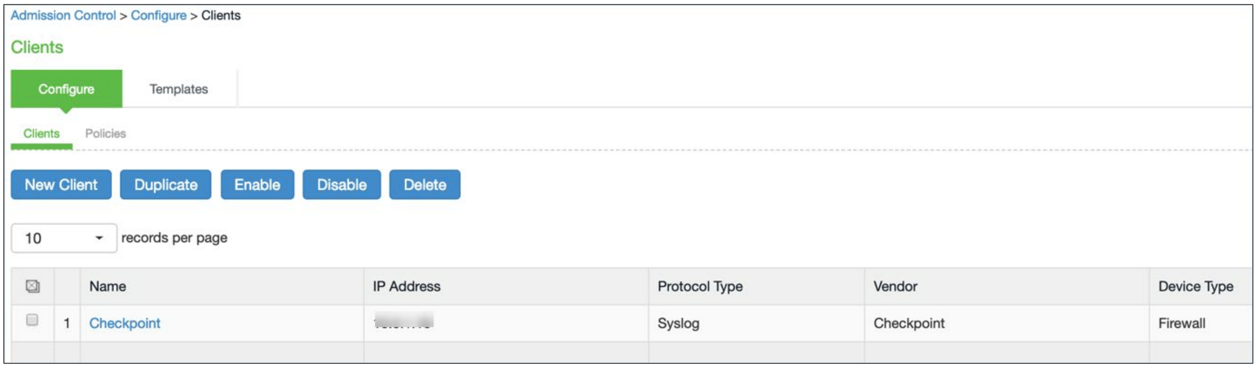
* Name:		Label to reference this client.
Description:		
* IP Address:		IP Address of this client.
* Template:	Check Point Software Technologies Ltd.-Firewall-Syslog-text	Template used by the client

Selected Template Details

Template name	Vendor	Device	Protocol	Format	Description
checkpointfw-syslog.itmpl	Check Point Software Technologies Ltd.	Firewall	Syslog	text	Syslog integration with Check Point firewall using syslog format messages.

* indicates required field

Figure 14: Client Added



Admission Control > Configure > Clients

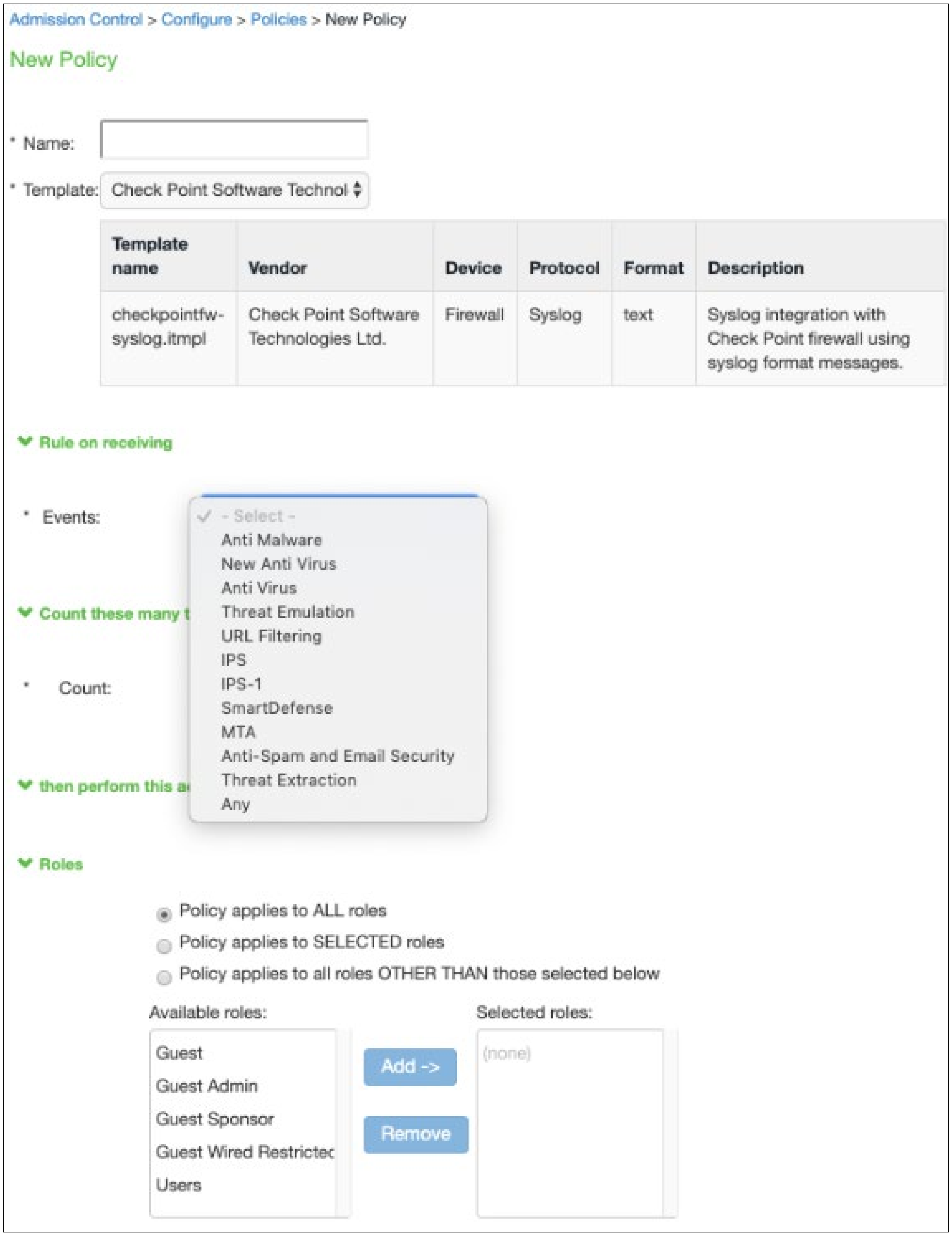
Clients

10 records per page

☐		Name	IP Address	Protocol Type	Vendor	Device Type
☐	1	Checkpoint	[redacted]	Syslog	Checkpoint	Firewall

3) Select the new template during policy creation (Endpoint Policy > Admission Control > Policies). Events and severities are populated based on the template.

Figure 15: Policy



Admission Control > Configure > Policies > New Policy

New Policy

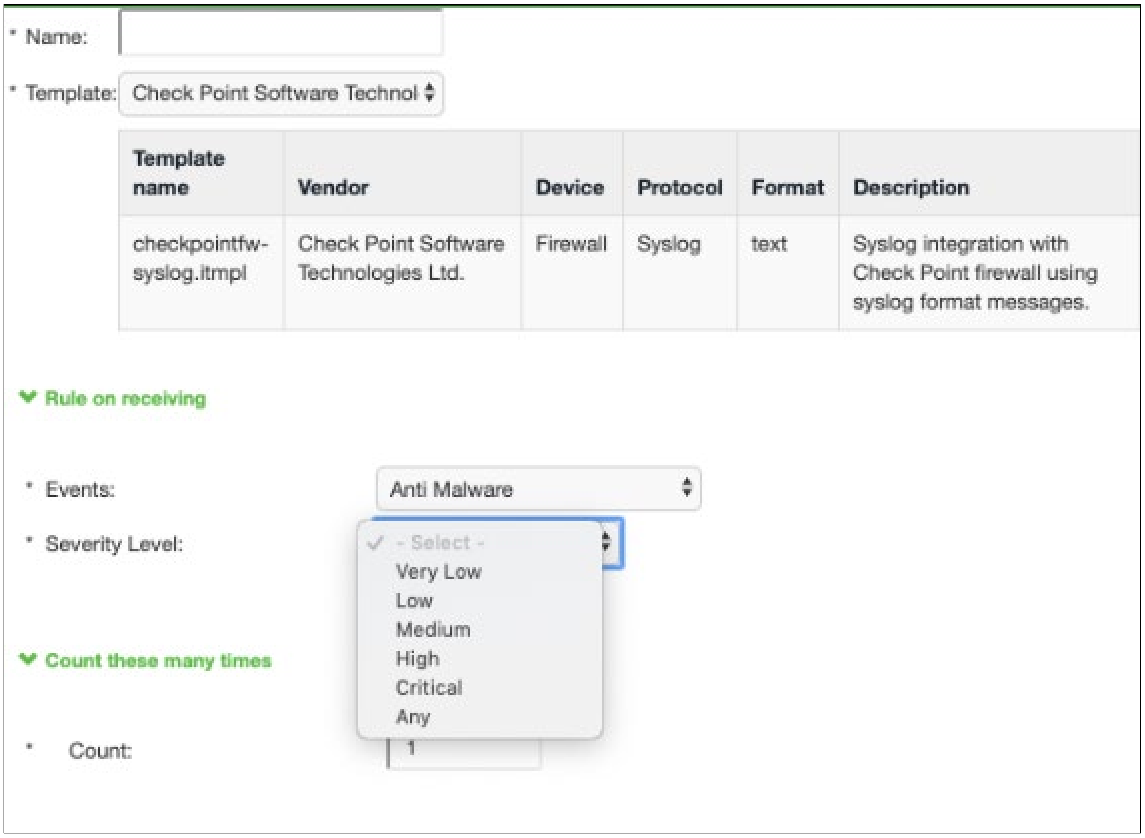
* Name:

* Template: Check Point Software Technol

Template name	Vendor	Device	Protocol	Format	Description
checkpointfw-syslog.itmpl	Check Point Software Technologies Ltd.	Firewall	Syslog	text	Syslog integration with Check Point firewall using syslog format messages.

● Policy applies to ALL roles
○ Policy applies to SELECTED roles
○ Policy applies to all roles OTHER THAN those selected below

Figure 16: Severity



* Name:

* Template: Check Point Software Technol

Template name	Vendor	Device	Protocol	Format	Description
checkpointfw-syslog.itmpl	Check Point Software Technologies Ltd.	Firewall	Syslog	text	Syslog integration with Check Point firewall using syslog format messages.

Rule on receiving

* Events: Anti Malware

* Severity Level: - Select -

Count these many times

* Count: 1

Configuring Check Point Firewall

The PPS device must be added as a syslog server while configuring the Check Point firewall for sending the logging information. You must add Check Point firewall as syslog client on PPS.

```
Sample Syslog:
   cp_log_export add name <name> [domain-server <domain-server>] target-
   server <target-server IP address> target-port <target-port> protocol
   <(udp|tcp)> format <(syslog)|(cef)|(splunk)(generic)> [optional arguments]

Example:
   cp_log_export add name pulse target-server 10.0.1.9 target-port 514
   protocol udp format syslog

   cp_log_export set name <name> filter-blade-in "value2”

   One predefined family for "product" field (filter-blade-in):
   TP for exporting only Threat Prevention logs (Anti-Bot,Anti-Exploit,Anti-
   Malware,Anti-Ransomware,Capsule Docs,Endpoint Compliance,Forensics,Full
   disc encryption,Media Encryption & Port Protection,Secure Client,Threat
   emulation,Threat extraction,Zero Phishing).

Example:
   cp_log_export set name pulse filter-blade-in ”TP”
```

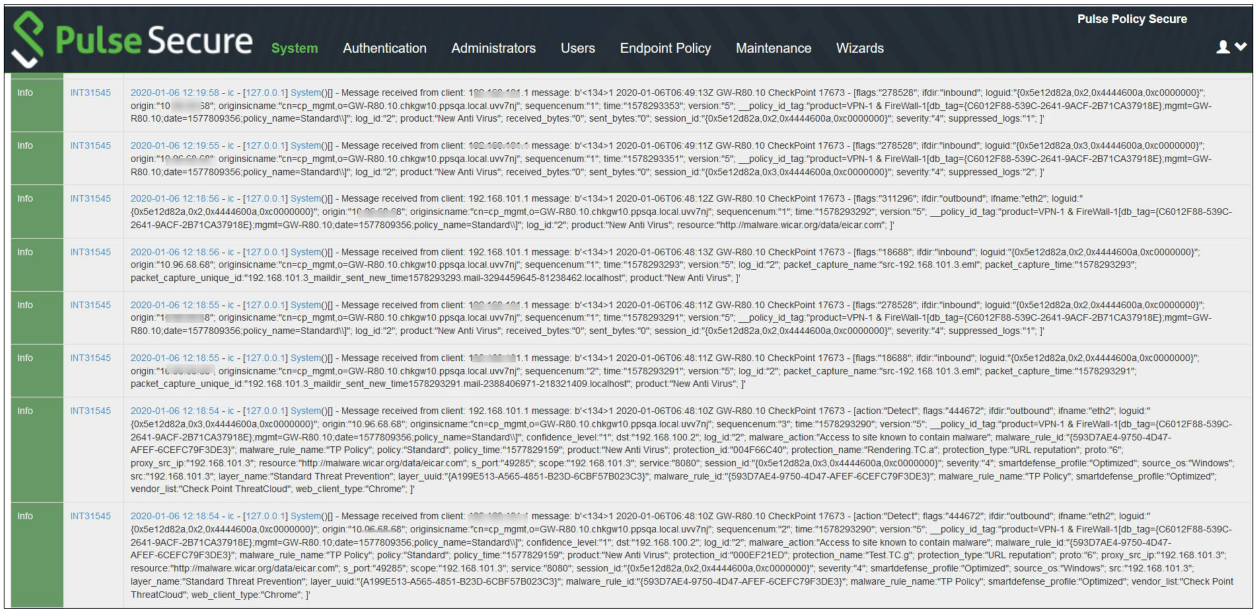
For exporting Check Point logs over syslog, see Log Exporter.

Troubleshooting

To verify the event logs on PPS, select **System > Log/Monitoring > Events**. Ensure Admission control events option is enabled in Event logs settings.

You can verify that the event logs are generated every time when an event is received from Check Point.

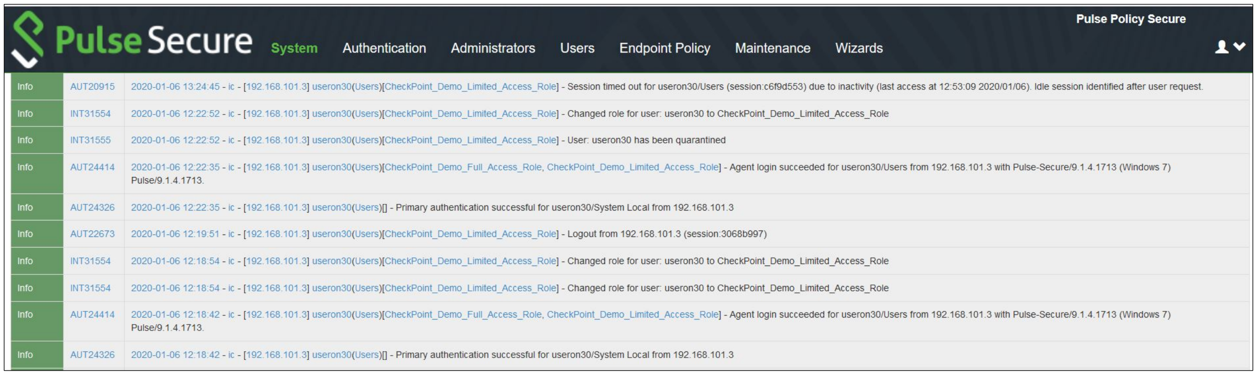
Figure 17: Events



```
Info  INT31545  2020-01-06 12:19:58 - ic - [127.0.0.1] System()[] - Message received from client: 1[redacted].1 message: b'<134>1 2020-01-06T06:49:13Z GW-R80.10 CheckPoint 17673 - [flags:"278528"; ifdir:"inbound"; loguid:"{0x5e12d82a,0x2,0x4444600a,0xc0000000}"; origin:"10[redacted]58"; originsicname:"cn=cp_mgmt,o=GW-R80.10.chkgw10.ppsqa.local.uvv7nj"; sequencenum:"1"; time:"1578293353"; version:"5"; __policy_id_tag:"product=VPN-1 & FireWall-1[db_tag={C6012F88-539C-2641-9ACF-2B71CA37918E};mgmt=GW-R80.10;date=1577809356;policy_name=Standard\\]"; log_id:"2"; product:"New Anti Virus"; received_bytes:"0"; sent_bytes:"0"; session_id:"{0x5e12d82a,0x2,0x4444600a,0xc0000000}"; severity:"4"; suppressed_logs:"1"; ]'

Info  INT31545  2020-01-06 12:19:55 - ic - [127.0.0.1] System()[] - Message received from client: [redacted] message: b'<134>1 2020-01-06T06:49:11Z GW-R80.10 CheckPoint 17673 - [flags:"278528"; ifdir:"inbound"; loguid:"{0x5e12d82a,0x3,0x4444600a,0xc0000000}"; origin:"1[redacted]" originsicname:"cn=cp_mgmt,o=GW-R80.10.chkgw10.ppsqa.local.uvv7nj"; sequencenum:"1"; time:"1578293351"; version:"5"; __policy_id_tag:"product=VPN-1 & FireWall-1[db_tag={C6012F88-539C-2641-9ACF-2B71CA37918E};mgmt=GW-R80.10;date=1577809356;policy_name=Standard\\]"; log_id:"2"; product:"New Anti Virus"; received_bytes:"0"; sent_bytes:"0"; session_id:"{0x5e12d82a,0x3,0x4444600a,0xc0000000}"; severity:"4"; suppressed_logs:"2"; ]'

Info  INT31545  2020-01-06 12:18:56 - ic - [127.0.0.1] System()[] - Message received from client: 192.168.101.1 message: b'<134>1 2020-01-06T06:48:12Z GW-R80.10 CheckPoint 17673 - [flags:"311296"; ifdir:"outbound"; ifname:"eth2"; loguid:"{0x5e12d82a,0x2,0x4444600a,0xc0000000}"; origin:"1[redacted]8"; originsicname:"cn=cp_mgmt,o=GW-R80.10.chkgw10.ppsqa.local.uvv7nj"; sequencenum:"1"; time:"1578293292"; version:"5"; __policy_id_tag:"product=VPN-1 & FireWall-1[db_tag={C6012F88-539C-2641-9ACF-2B71CA37918E};mgmt=GW-R80.10;date=1577809356;policy_name=Standard\\]"; log_id:"2"; product:"New Anti Virus"; resource:"http://malware.wicar.org/data/eicar.com"; ]'

Info  INT31545  2020-01-06 12:18:56 - ic - [127.0.0.1] System()[] - Message received from client: 192.168.101.1 message: b'<134>1 2020-01-06T06:48:13Z GW-R80.10 CheckPoint 17673 - [flags:"18688"; ifdir:"inbound"; loguid:"{0x5e12d82a,0x2,0x4444600a,0xc0000000}"; origin:"10.96.68.68"; originsicname:"cn=cp_mgmt,o=GW-R80.10.chkgw10.ppsqa.local.uvv7nj"; sequencenum:"1"; time:"1578293293"; version:"5"; log_id:"2"; packet_capture_name:"src-192.168.101.3.eml"; packet_capture_time:"1578293293"; packet_capture_unique_id:"192.168.101.3_maildir_sent_new_time1578293293.mail-3294459645-81238462.localhost"; product:"New Anti Virus"; ]'

Info  INT31545  2020-01-06 12:18:55 - ic - [127.0.0.1] System()[] - Message received from client: 1[redacted].1 message: b'<134>1 2020-01-06T06:48:11Z GW-R80.10 CheckPoint 17673 - [flags:"278528"; ifdir:"inbound"; loguid:"{0x5e12d82a,0x2,0x4444600a,0xc0000000}"; origin:"1[redacted]8"; originsicname:"cn=cp_mgmt,o=GW-R80.10.chkgw10.ppsqa.local.uvv7nj"; sequencenum:"1"; time:"1578293291"; version:"5"; __policy_id_tag:"product=VPN-1 & FireWall-1[db_tag={C6012F88-539C-2641-9ACF-2B71CA37918E};mgmt=GW-R80.10;date=1577809356;policy_name=Standard\\]"; log_id:"2"; product:"New Anti Virus"; received_bytes:"0"; sent_bytes:"0"; session_id:"{0x5e12d82a,0x2,0x4444600a,0xc0000000}"; severity:"4"; suppressed_logs:"1"; ]'

Info  INT31545  2020-01-06 12:18:55 - ic - [127.0.0.1] System()[] - Message received from client: 1[redacted]1.1 message: b'<134>1 2020-01-06T06:48:11Z GW-R80.10 CheckPoint 17673 - [flags:"18688"; ifdir:"inbound"; loguid:"{0x5e12d82a,0x2,0x4444600a,0xc0000000}"; origin:"1[redacted], originsicname:"cn=cp_mgmt,o=GW-R80.10.chkgw10.ppsqa.local.uvv7nj"; sequencenum:"2"; time:"1578293291"; version:"5"; log_id:"2"; packet_capture_name:"src-192.168.101.3.eml"; packet_capture_time:"1578293291"; packet_capture_unique_id:"192.168.101.3_maildir_sent_new_time1578293291.mail-2388406971-218321409.localhost"; product:"New Anti Virus"; ]'

Info  INT31545  2020-01-06 12:18:54 - ic - [127.0.0.1] System()[] - Message received from client: 192.168.101.1 message: b'<134>1 2020-01-06T06:48:10Z GW-R80.10 CheckPoint 17673 - [action:"Detect"; flags:"444672"; ifdir:"outbound"; ifname:"eth2"; loguid:"{0x5e12d82a,0x3,0x4444600a,0xc0000000}"; origin:"10.96.68.68"; originsicname:"cn=cp_mgmt,o=GW-R80.10.chkgw10.ppsqa.local.uvv7nj"; sequencenum:"3"; time:"1578293290"; version:"5"; __policy_id_tag:"product=VPN-1 & FireWall-1[db_tag={C6012F88-539C-2641-9ACF-2B71CA37918E};mgmt=GW-R80.10;date=1577809356;policy_name=Standard\\]"; confidence_level:"1"; dst:"192.168.100.2"; log_id:"2"; malware_action:"Access to site known to contain malware"; malware_rule_id:"{593D7AE4-9750-4D47-AFEF-6CEFC79F3DE3}"; malware_rule_name:"TP Policy"; policy:"Standard"; policy_time:"1577829159"; product:"New Anti Virus"; protection_id:"004F66C40"; protection_name:"Rendering.TC.a"; protection_type:"URL reputation"; proto:"6"; proxy_src_ip:"192.168.101.3"; resource:"http://malware.wicar.org/data/eicar.com"; s_port:"49285"; scope:"192.168.101.3"; service:"8080"; session_id:"{0x5e12d82a,0x3,0x4444600a,0xc0000000}"; severity:"4"; smartdefense_profile:"Optimized"; source_os:"Windows"; src:"192.168.101.3"; layer_name:"Standard Threat Prevention"; layer_uuid:"{A199E513-A565-4851-B23D-6CBF57B023C3}"; malware_rule_id:"{593D7AE4-9750-4D47-AFEF-6CEFC79F3DE3}"; malware_rule_name:"TP Policy"; smartdefense_profile:"Optimized"; vendor_list:"Check Point ThreatCloud"; web_client_type:"Chrome"; ]'

Info  INT31545  2020-01-06 12:18:54 - ic - [127.0.0.1] System()[] - Message received from client: [redacted] message: b'<134>1 2020-01-06T06:48:10Z GW-R80.10 CheckPoint 17673 - [action:"Detect"; flags:"444672"; ifdir:"outbound"; ifname:"eth2"; loguid:"{0x5e12d82a,0x2,0x4444600a,0xc0000000}"; origin:"10[redacted]68"; originsicname:"cn=cp_mgmt,o=GW-R80.10.chkgw10.ppsqa.local.uvv7nj"; sequencenum:"2"; time:"1578293290"; version:"5"; __policy_id_tag:"product=VPN-1 & FireWall-1[db_tag={C6012F88-539C-2641-9ACF-2B71CA37918E};mgmt=GW-R80.10;date=1577809356;policy_name=Standard\\]"; confidence_level:"1"; dst:"192.168.100.2"; log_id:"2"; malware_action:"Access to site known to contain malware"; malware_rule_id:"{593D7AE4-9750-4D47-AFEF-6CEFC79F3DE3}"; malware_rule_name:"TP Policy"; policy:"Standard"; policy_time:"1577829159"; product:"New Anti Virus"; protection_id:"000EF21ED"; protection_name:"Test.TC.g"; protection_type:"URL reputation"; proto:"6"; proxy_src_ip:"192.168.101.3"; resource:"http://malware.wicar.org/data/eicar.com"; s_port:"49285"; scope:"192.168.101.3"; service:"8080"; session_id:"{0x5e12d82a,0x2,0x4444600a,0xc0000000}"; severity:"4"; smartdefense_profile:"Optimized"; source_os:"Windows"; src:"192.168.101.3"; layer_name:"Standard Threat Prevention"; layer_uuid:"{A199E513-A565-4851-B23D-6CBF57B023C3}"; malware_rule_id:"{593D7AE4-9750-4D47-AFEF-6CEFC79F3DE3}"; malware_rule_name:"TP Policy"; smartdefense_profile:"Optimized"; vendor_list:"Check Point ThreatCloud"; web_client_type:"Chrome"; ]'
```

To verify the user access logs, select System >Logs & Monitoring > User Access to verify the user login related logs.

Figure 18: User Access Logs



```
Info  AUT20915  2020-01-06 13:24:45 - ic - [192.168.101.3] useron30(Users)[CheckPoint_Demo_Limited_Access_Role] - Session timed out for useron30/Users (session:c6f9d553) due to inactivity (last access at 12:53:09 2020/01/06). Idle session identified after user request.
Info  INT31554  2020-01-06 12:22:52 - ic - [192.168.101.3] useron30(Users)[CheckPoint_Demo_Limited_Access_Role] - Changed role for user: useron30 to CheckPoint_Demo_Limited_Access_Role
Info  INT31555  2020-01-06 12:22:52 - ic - [192.168.101.3] useron30(Users)[CheckPoint_Demo_Limited_Access_Role] - User: useron30 has been quarantined
Info  AUT24414  2020-01-06 12:22:35 - ic - [192.168.101.3] useron30(Users)[CheckPoint_Demo_Full_Access_Role, CheckPoint_Demo_Limited_Access_Role] - Agent login succeeded for useron30/Users from 192.168.101.3 with Pulse-Secure/9.1.4.1713 (Windows 7) Pulse/9.1.4.1713.
Info  AUT24326  2020-01-06 12:22:35 - ic - [192.168.101.3] useron30(Users)[] - Primary authentication successful for useron30/System Local from 192.168.101.3
Info  AUT22673  2020-01-06 12:19:51 - ic - [192.168.101.3] useron30(Users)[CheckPoint_Demo_Limited_Access_Role] - Logout from 192.168.101.3 (session:3068b997)
Info  INT31554  2020-01-06 12:18:54 - ic - [192.168.101.3] useron30(Users)[CheckPoint_Demo_Limited_Access_Role] - Changed role for user: useron30 to CheckPoint_Demo_Limited_Access_Role
Info  INT31554  2020-01-06 12:18:54 - ic - [192.168.101.3] useron30(Users)[CheckPoint_Demo_Limited_Access_Role] - Changed role for user: useron30 to CheckPoint_Demo_Limited_Access_Role
Info  AUT24414  2020-01-06 12:18:42 - ic - [192.168.101.3] useron30(Users)[CheckPoint_Demo_Full_Access_Role, CheckPoint_Demo_Limited_Access_Role] - Agent login succeeded for useron30/Users from 192.168.101.3 with Pulse-Secure/9.1.4.1713 (Windows 7) Pulse/9.1.4.1713.
Info  AUT24326  2020-01-06 12:18:42 - ic - [192.168.101.3] useron30(Users)[] - Primary authentication successful for useron30/System Local from 192.168.101.3
```