



Pulse Policy Secure

Access Control with Fortinet Products

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: Access Control with Fortinet Products

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
Enforcement using FortiGate Firewall.....	5
Overview of Enforcement using FortiGate Firewall	5
Summary of Configuration	6
Configuring PPS with FortiGate Firewall	6
Configuring Auth Table Mapping Policy.....	7
Configuring FortiGate Firewall	7
Reports and Logging	10
Identity-Based Access Control with Fortinet Products.....	12
Overview of Identity-Based Access Control with Fortinet Product	12
Summary of Configuration	13
Configuring PPS with FortiAuthenticator	13
Creating a Custom Filter for User Access Logs.....	13
Editing a Custom Filter	14
Configuring the Syslog Server	15
Configuring FortiAuthenticator	16
Configuring the FortiGate Firewall	20
Reports and Logging	23
Alert-Based Admission Control with Fortinet Products	25
Overview of Alert-Based Admission Control with Fortinet Products.....	25
Summary of Configuration	27
Configuring Network Security Devices with PPS	27
Configuring an Admission Control Template	28
Configuring Admission Control Policies	29
Configuring the Admission Control Client.....	31
Configuring FortiGate Firewall	32
Configuring FortiAnalyzer	35
Confirming Syslog Forwarding.....	37
References.....	37

Purpose of this Guide

This guide describes how to configure *Pulse Policy Secure (PPS)* to provide Identity- and Alert-based protection for your network using Fortinet's products.

Prerequisites

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

- *Pulse Policy Secure* at version 9.1R3
- *FortiGate Firewall* at version v6.0.4 build0231 (GA)
- *FortiAuthenticator* at version v6.0.0, build0010 (GA)
- *FortiAnalyzer* at version v6.0.4-build0292 190109 (GA)

Enforcement using FortiGate Firewall

This chapter provides an overview of enforcement using FortiGate firewall. It includes the following information:

Overview of Enforcement using FortiGate Firewall

This chapter covers the FortiGate firewall integration with PPS using RADIUS accounting messages. FortiGate Firewall "SSO using RADIUS accounting records" feature allows FortiGate to receive user and group information details using RADIUS accounting messages.

FortiGate firewall can authenticate users transparently who have already authenticated on an external RADIUS server. The security policy applies the appropriate profiles based on the user group to which the user belongs. RADIUS SSO is relatively simple because the FortiGate unit does not interact with the RADIUS server, it only monitors RADIUS accounting records that the server forwards (originating from the RADIUS client, i.e Pulse Policy Secure). These records include the user's IP address, user group and user name.

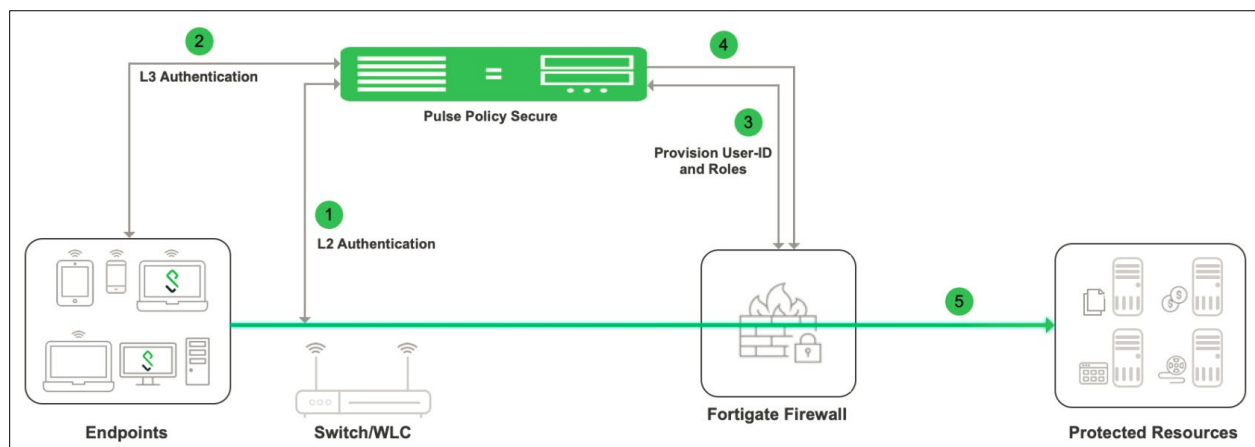
FortiGate needs to know the user's endpoint identifier (usually IP address) and RADIUS user group.

The authentication process is described below:

- 1) The user is authenticated on PPS after validating the host check policy to ensure that the endpoints meets the corporate policy.
- 2) PPS learns the endpoint IP using RADIUS accounting(L2) or L3 connection.
- 3) The User Id, IP address and role(s) are provisioned to the firewall.
- 4) Pulse Policy Secure shares the User Id, IP address and role information with FortiGate firewall in the form of a RADIUS accounting packet.
- 5) The FortiGate firewall maps the user to a specific security policy and then provides the required access.

If multiple firewall devices are configured, then the user's information will be provisioned to all the devices. The user's information will be sent to the firewall only if user's role requires session to be provisioned.

Figure1: Deployment using FortiGate Firewall



Summary of Configuration

To prepare your network to use Enforcement using *FortiGate Firewall*, perform the following tasks:

- Configuring PPS with FortiGate Firewall
 - Configuring Auth Table Mapping Policy
- Configuring FortiGate Firewall
- Reports and Logging

The following sections describe each of these steps in detail.

Configuring PPS with FortiGate Firewall

To configure FortiGate firewall:

- 1) Select **Endpoint Policy > Infranet Enforcer**.
- 2) Click **New Infranet Enforcer** and select **FortiGate Firewall** in the Platform drop down.

Infranet Enforcer > Connection > New Infranet Enforcer

New Infranet Enforcer

▼ Infranet Enforcer

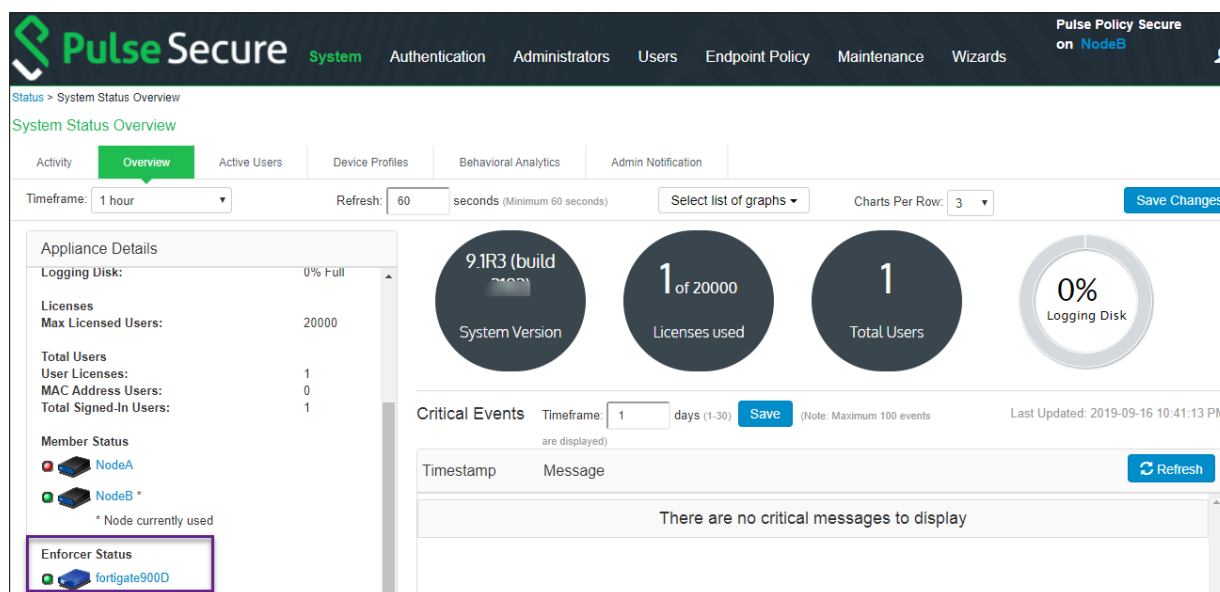
Platform:	FortiGate Firewall	Platform of this Infranet Enforcer.
* Name:	fortigate900D	Label to reference this Infranet Enforcer.
* IP Address:		IP Address of this Infranet Enforcer
* Shared Secret:	*****	Pre-Shared Secret
* Accounting Port:	1813	Port used for RADIUS accounting

[Save Changes](#)

* indicates required field

- 3) Enter the name of the Infranet Enforcer in the Name box.
- 4) Enter the IP address of FortiGate Firewall.
- 5) Enter the shared secret.
- 6) Enter the port number used for RADIUS accounting.
- 7) Click **Save Changes**. You must create security policies on the FortiGate firewall for traffic enforcement.

Check the **Status > Overview** page for checking the status of the connection.



Configuring Auth Table Mapping Policy

To configure auth table mapping policies:

- 1) Select **Endpoint Policy > Infranet Enforcer > Auth Table Mapping**.
- 2) Click **New Policy**.
- 3) Enter a name to label this auth table mapping policy.
- 4) Select FortiGate as an enforcer in the Enforcer section, specify the Infranet Enforcer device(s) to which you want to apply this auth table mapping policy.
- 5) In the Action section, specify auth table mapping rules for the specified Infranet Enforcer.
- 6) Click **Save Changes**.

Configuring FortiGate Firewall

The FortiGate firewall detects traffic from an endpoint that matches a configured security policy using PPS RSSO record. It determines the role(s) associated with that user and allows or denies the traffic based on the actions configured in the security policy.

To configure FortiGate firewall:

- 1) Select **System > Network > Interfaces** [datainterface] and enable **RADIUS Accounting** to allow the interfaces to listen for RADIUS Accounting Messages.

FortiGate 900D FG900D3917800553

Dashboard >
Security Fabric >
FortiView >
Network >
Interfaces ☆
DNS
Packet Capture
SD-WAN
Performance SLA
SD-WAN Rules
Static Routes
Policy Routes
RIP
OSPF
BGP
Multicast
System 1 >
Policy & Objects >

Edit Interface

Interface Name port10 (70:4C:A5:53:69:6C)

Alias

Link Status Up

Type Physical Interface

Tags

Role LAN

Add Tag Category

Address

Addressing mode **Manual** DHCP Dedicated to FortiSwitch

IP/Network Mask

Administrative Access

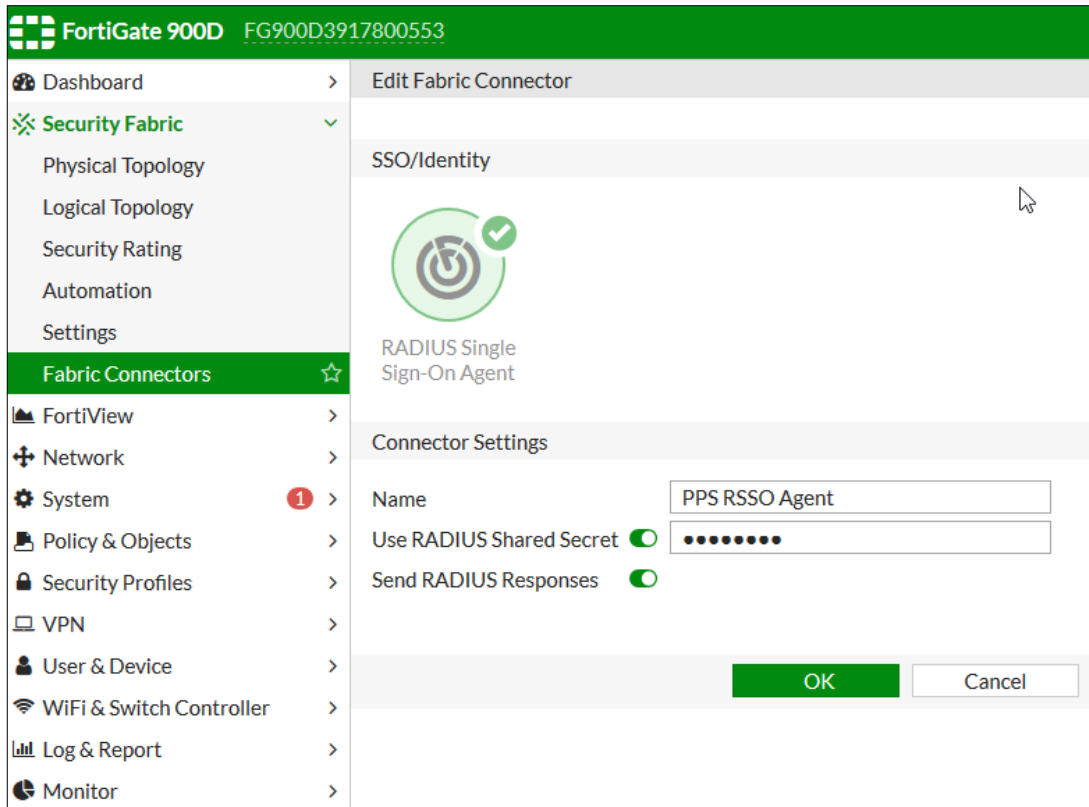
IPv4 ☒ HTTPS ☒ HTTP ☒ PING ☒ FMG-Access

☒ CAPWAP ☒ SSH ☒ SNMP ☒ FTM

☒ RADIUS Accounting ☒ FortiTelemetry

2) Select Fabric Connector > Create New, under SSO/Identity select RADIUS Single Sign-On Agent.

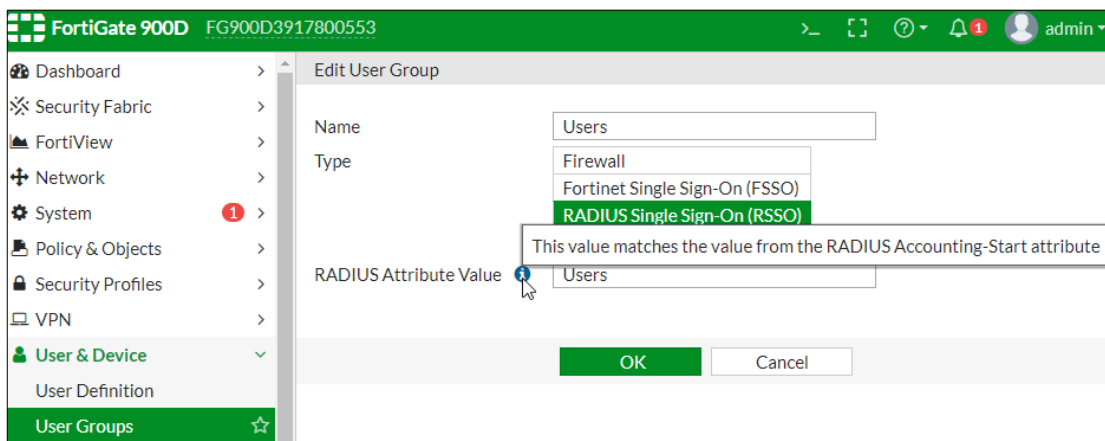
- Name: Enter a name for the entry
- Enter the RADIUS shared secret, which matches with PPS.
- Click **OK**.



3) Create matching User groups. Select **User & Device > User Groups**. Click **create New** and enter the following data:

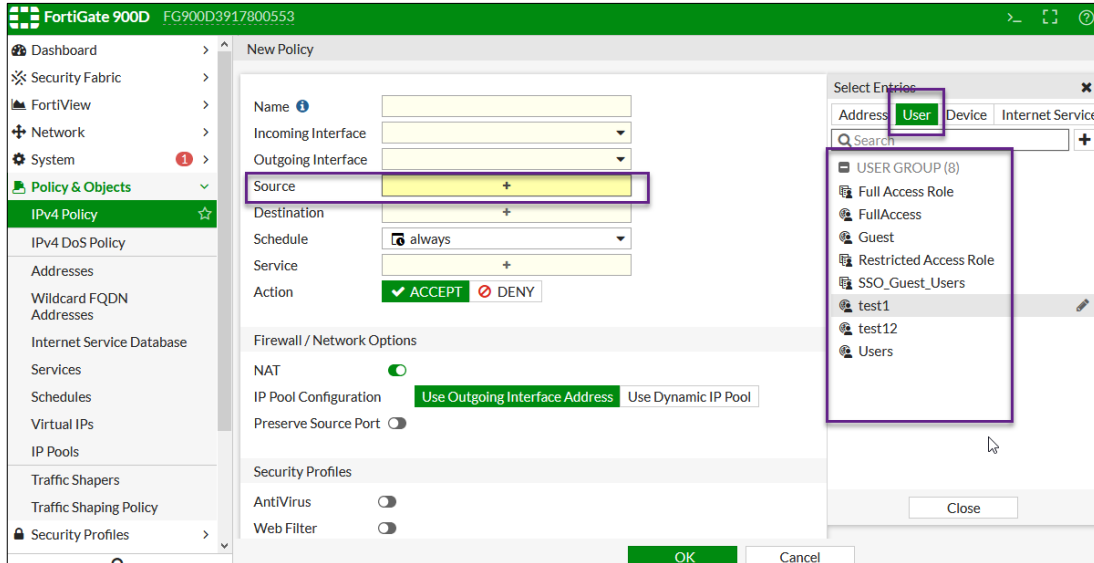
- Name- Enter the name of the group. This name will appear in the firewall policy.
- Type- Select **RADIUS Single Sign-On** as type.
- RADIUS Attribute Value- Enter the User Role created on PPS to match the User Group in FortiGate.
- Click **OK**.

Figure 2: Creating User Groups



- 4) Create a firewall policy to use the PPS enforcement groups just created. Select **Policy & Objects > IPv4 Policy**. Click **Create New** and create the policy based on the resource access restrictions to be enforced.

Figure 3: Creating Firewall policies



- 5) Disable overriding of the roles on FortiGate firewall when the same user logs in with a different device. The default behavior is to override the role information with the latest role received from PPS.

For example, if a same user login's to PPS from different devices (mobile/laptop) with different roles (Employee/Guest). Fortigate firewall overrides the role information with the latest role by default. To disable overriding with the latest roles "set sso-attribute-value-override disable".

```
config user radius
edit <My_Rsso>
set rsso enable
set sso-attribute-value-override enable/disable // Enable/Disable override old attribute value with
new value for the same endpoint.
end
```

Reports and Logging

You can monitor the RSSO Sessions on FortiGate firewall from CLI or GUI:

- 1) Using the FortiGate CLI, type:


```
diag rsso query ip <Ip-Address>
diag rsso query rsso-key
*Queries the RSSO database
```

Figure 4: Monitor the RSSO Sessions on FortiGate firewall from CLI

```
FG900D3917800553 # diag rso query ip 10.96.67.10
Querying IP '10.96.67.10'
Endpoint: qauser10
  RSSO Key: Users
  IP Addresses:
    IP: 10.96.67.10, Time left (hh:mm:ss): 07:59:56 **
```

- 2) Select **Monitor > Firewall user Monitor**. The list shows all the identity records.

Figure 5: Monitor the RSSO Sessions on FortiGate firewall from GUI

FortiGate 900D FG900D3917800553						
<div>Security Profiles ></div> <div>VPN ></div> <div>User & Device ></div> <div>WiFi & Switch Controller ></div> <div>Log & Report ></div> <div>Monitor ✓</div> <div>Routing Monitor</div> <div>DHCP Monitor</div> <div>SD-WAN Monitor</div> <div>IPsec Monitor</div> <div>SSL-VPN Monitor</div> <div>Firewall User Monitor ☆</div>	<div>Refresh Deauthenticate Show all FSSO Logons Search</div>					
	User Name	User Group	Duration	IP Address	Traffic Volume	Method
	employee1	Users	3 second(s)	172.21.9.76	0 B	Radius Single Sign-On
	qauser10	Users	1 minute(s) and 40 second(s)	10.96.67.10	0 B	Radius Single Sign-On
	qauser2	Users	1 minute(s) and 40 second(s)	10.96.67.2	0 B	Radius Single Sign-On
	qauser3	Users	1 minute(s) and 40 second(s)	10.96.67.3	0 B	Radius Single Sign-On
	qauser4	Users	1 minute(s) and 40 second(s)	10.96.67.4	0 B	Radius Single Sign-On
	qauser5	Users	1 minute(s) and 40 second(s)	10.96.67.5	0 B	Radius Single Sign-On
	qauser6	Users	1 minute(s) and 40 second(s)	10.96.67.6	0 B	Radius Single Sign-On
	qauser7	Users	1 minute(s) and 40 second(s)	10.96.67.7	0 B	Radius Single Sign-On
	qauser8	Users	1 minute(s) and 40 second(s)	10.96.67.8	0 B	Radius Single Sign-On

Identity-Based Access Control with Fortinet Products

This section describes how to integrate *FortiAuthenticator* and *FortiGate Firewall* products with *PPS* to support Identity-based admission control in your network.

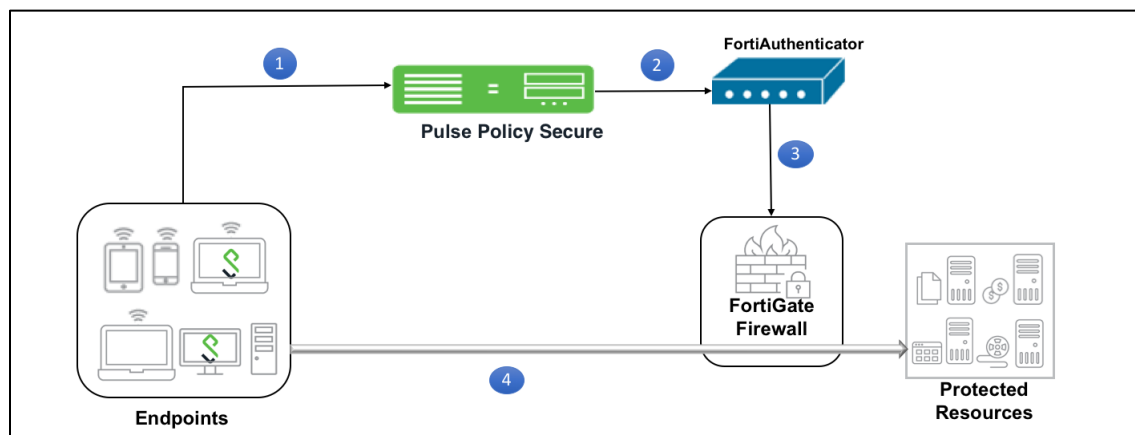
Overview of Identity-Based Access Control with Fortinet Product

Pulse Policy Secure (PPS) integration with the *FortiGate Firewall* provides identity-enabled enforcement with backend authentication and comprehensive compliance checks.

The authentication process is described below:

- 1) The user is authenticated on *PPS* after validating the host check policy to ensure that the endpoints meets the corporate policy.
- 2) The syslog sessions are exported to *FortiAuthenticator*.
- 3) *FortiAuthenticator*, which acts as a syslog server, parses identity information from the syslog message and creates an IP address to username mapping file within *FortiAuthenticator*. This information is shared with *FortiGate Firewall* in the form of a FSSO record.
- 4) The *FortiGate Firewall* maps the user to a specific resource access policy and then provides the required access to protected resources.

Figure 1: Deployment using PPS, FortiAuthenticator and FortiGate Firewall



For example, you can use this to extend NAC/BYOD (Bring Your Own Device) to perimeter defense. This unifies the access policies that extend from NAC/BYOD systems to firewall perimeter defenses to enable end-to-end enforcement across the network.

Summary of Configuration

To prepare your network to perform identity-based access control using *Pulse Policy Secure*, *FortiAuthenticator* and *FortiGate Firewall*, perform the following tasks:

- [Configuring PPS with FortiAuthenticator](#):
 - [Creating a Custom Filter for User Access Logs](#).
 - [Editing a Custom Filter](#).
 - [Configuring the Syslog Server](#).
- [Configuring FortiAuthenticator](#).
- [Configuring the FortiGate Firewall](#).
- (Optional) [Reports and Logging](#).

The following sections describe each of these steps in detail.

Configuring PPS with FortiAuthenticator

The *PPS* configuration requires defining the *FortiAuthenticator* as the syslog server on *PPS*. The Syslog server uses the filter created in the User Access Log Filters for receiving and parsing the logs.

This section covers the following topics:

- [Creating a Custom Filter for User Access Logs](#) with default settings.
- [Editing a Custom Filter](#) to enable communication with *FortiAuthenticator*.
- [Configuring the Syslog Server](#).

Creating a Custom Filter for User Access Logs

To create a custom filter in *PPS*:

- 1) Select **System > Log/Monitoring > User Access > Filters**.
- 2) Click **New Filter**.
- 3) Under **Filter**, enter the required **Filter Name**.
- 4) Under **Export Format**, select **WELF**.

NOTE: This selection populates the text box with all parameters for the selected filter. This ensures that it is simple to edit the filter to enable communication with *FortiAuthenticator*, see [Editing a Custom Filter](#).

- 5) Click **Save** to save the filter.

Figure 2: Creating a Custom Filter

The screenshot shows the Pulse Secure web interface. The top navigation bar includes 'System', 'Authentication', 'Administrators', 'Users', 'Endpoint Policy', 'Maintenance', and 'Wizards'. The breadcrumb trail is 'Log/Monitoring > User Access > Filters > New Log filter'. The 'New Log filter' page has tabs for 'Events', 'User Access', 'Admin Access', 'Sensors', 'Client Logs', 'SNMP', 'Statistics', and 'Advanced Settings'. The 'User Access' tab is active. Below the tabs, there are sections for 'Filter', 'Query', and 'Export Format'. The 'Filter' section has a 'Filter Name' field with 'FSSO' and a checkbox 'Make default for syslog and archiving filter selection'. The 'Export Format' section has radio buttons for 'Standard', 'WELF' (selected), 'W3C', and 'Custom'. The 'Format' field contains a syslog message template: 'id=firewall time=%date% %time%' pri=%syslogcode% fw=%localip% vpn=%node% user=%user% realm=%realm% roles=%role% proto=%protocol% src=%sourceip% dst=%remoteip% dstname=%remotehost% type=vpn'. At the bottom are 'Save' and 'Cancel' buttons.

Editing a Custom Filter

Once you have created a populated custom filter for User Access Logs (see [Creating a Custom Filter for User Access Logs](#)), you must update the ID for the filter to enable communication with *FortiAuthenticator*.

To edit a custom filter:

- 1) Select **System > Log/Monitoring > User Access > Filters**.
- 2) Click on the filter created in the previous procedure, see [Creating a Custom Filter for User Access Logs](#).
- 3) Under **Export Format**, select the **Custom** format.
- 4) In the text box, edit the ID from "*id=firewall*" to "*id=FSSO*".

This ID will be used by *FortiAuthenticator* when parsing the syslog events.

Figure 3: Editing the Filter

This screenshot is identical to Figure 2, showing the 'New Log filter' configuration page in the Pulse Secure web interface. The 'User Access' tab is selected, and the 'Filter Name' is 'FSSO'. The 'Export Format' is set to 'WELF'. The 'Format' field contains a syslog message template: 'id=firewall time=%date% %time%' pri=%syslogcode% fw=%localip% vpn=%node% user=%user% realm=%realm% roles=%role% proto=%protocol% src=%sourceip% dst=%remoteip% dstname=%remotehost% type=vpn'. At the bottom are 'Save' and 'Cancel' buttons.

- 5) Click **Save**.

Configuring the Syslog Server

Once you have prepared a custom filter for User Access Logs (see [Creating a Custom Filter for User Access Logs](#)), you must configure *PPS* to send logs to the *FortiAuthenticator* syslog server.

NOTE: You must add *FortiAuthenticator* as a syslog server in all the nodes in a clustering environment.

To configure the syslog server:

- 1) Select **System > Log/Monitoring > User Access > Settings**.
- 2) Under **Select Events to Log**, retain the default settings.
- 3) Under **Syslog Servers**, create a syslog server with the following details:
 - **Server name/IP:** Enter the fully qualified domain name or the IP address of the syslog server (that is, *FortiAuthenticator*).
 - **Facility:** Select *LOCAL0* as the facility level.
 - **Type:** Select *UDP* as the connection type.
 - Do not change **Client Certificate**.
 - **Filter:** Select the *FSSO Custom* created filter format.

Figure 4: Configuring Syslog Server

▼ Syslog Servers

Events are logged locally. You can also log them to one or more external Syslog servers.

Delete

Server name/IP	Facility	Type	Client Certificate	Filter	
10.204.59.64	LOCAL0	UDP	Select Client Cert	FSSO: Custom	Add

Save Changes Reset

- 4) Click **Add** and then click **Save Changes**.

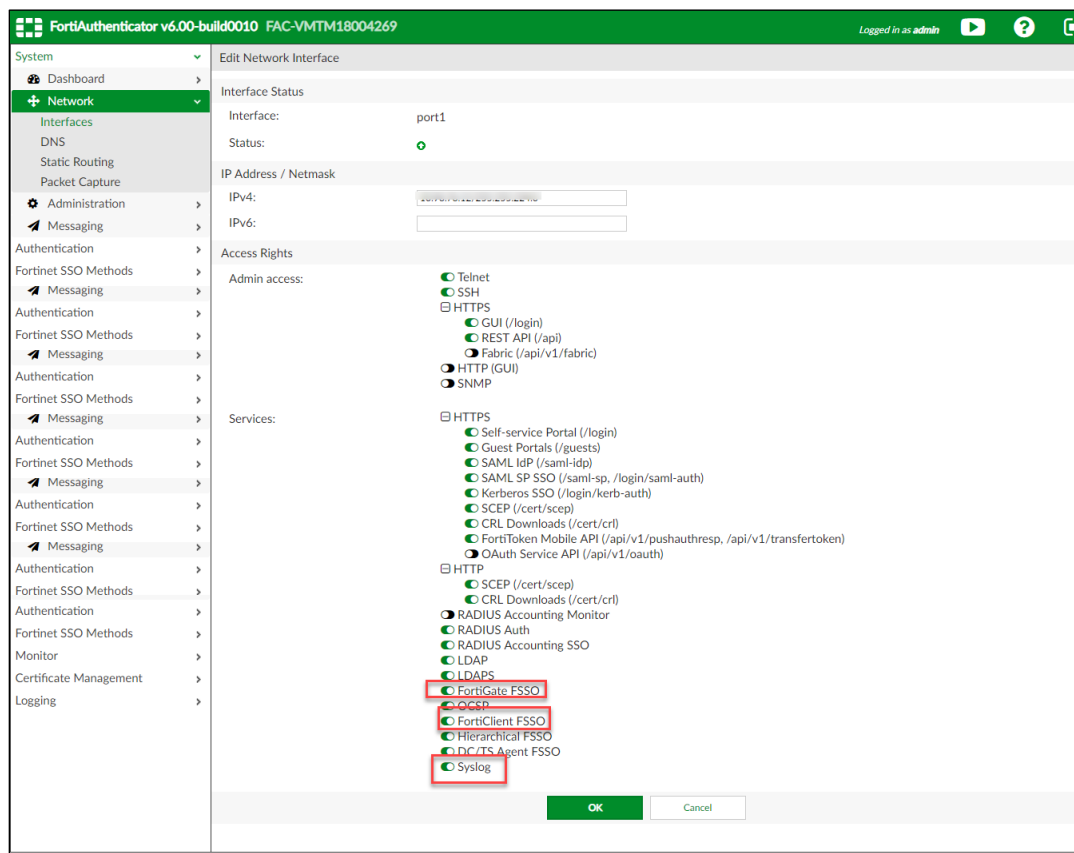
Configuring FortiAuthenticator

You must add PPS as a syslog source in *FortiAuthenticator* to parse the information.

Before you start, ensure you have completed the following tasks:

- Ensure that the *FortiAuthenticator* instance is communicating on the network and is reachable from the *PPS* appliance's management interface.
- Select **System > Network > Interfaces**, then select the required port and enable the *FortiGate FSSO*, *FortiClient FSSO* and *Syslog* services on *FortiAuthenticator* interface, which communicates with *PPS* and the *FortiGate Firewall*.

Figure 5: Enabling Fortinet Interfaces for a Port



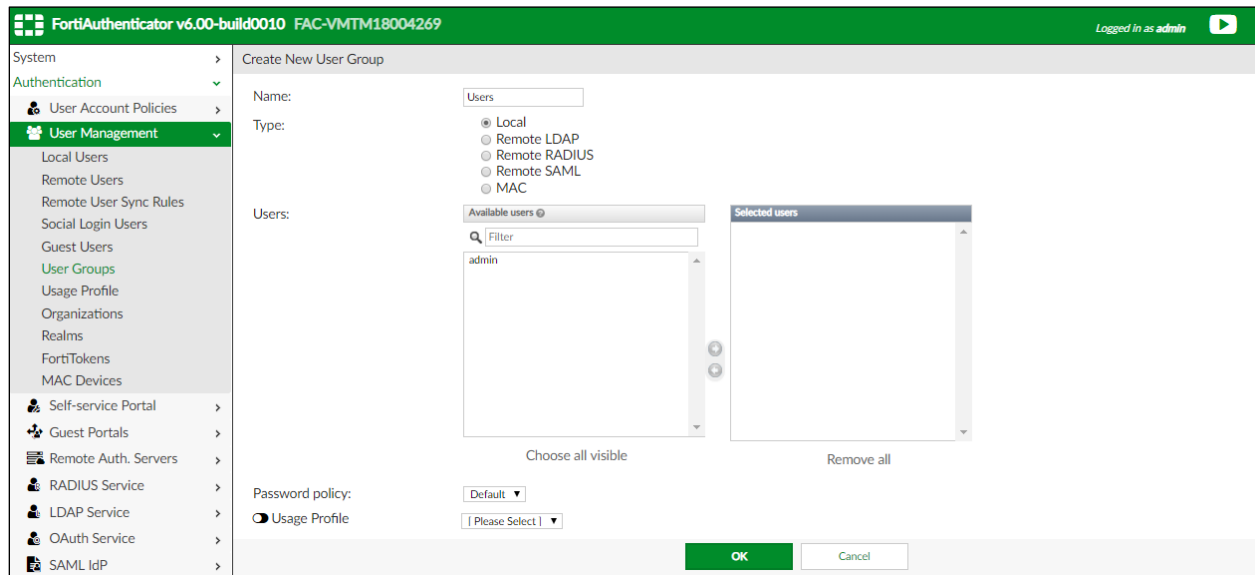
To configure *FortiAuthenticator*:

- 1) Create a Local user group with a name that matches the name that Pulse Policy Secure will send as the 'Group=' value in your Syslog messages.

To do this, select **Authentication > User Management > User Groups** and click **Create New**. Create the group with the following data:

- **Name:** Enter the name that is defined on *PPS*. For example, *Users*.
- **Type:** Select *Local*.
- Click **OK**.

Figure 6: Creating a User Group



2) Create a Syslog matching rule.

To do this, select **Fortinet SSO methods > SSO > Syslog Sources**. In the upper right corner, from the **View** drop down choose matching rules and click **Create New** and give the following data:

- **Name:** Enter the name for the syslog Rule.
- **Trigger:** Enter the filter name created in PPS. For example, id=FSSO.
- **Auth Type Indicators:** Enter strings to differentiate between the types of user activities. For example:
 - **Logon:** AUT24803
 - **Update:** AUT23524
 - **Logoff:** AUT22673
- **Username field:** Define the semantics of the username field. In this field, `{{:username}}` indicates from where the username is extracted. For example: `user= {{:username}}`.
- **Client IP field:** Define the semantics of the client IP address. For example: `src= {{:client_ip}}`
- **Group field:** Define the semantics of the group. For example: `roles= " {{: group}}"`

NOTE: There is a trailing space after **Username field**, **Client IP field**, and **Group field**. The parser requires the trailing space as an end character for each of these fields, and will fail if the trailing space is omitted. Do not remove this space.

- **Group List Separator:** SSO syslog feed can parse multiple groups if the names are separated by a plus (+) symbol or a comma (,). Use the Group list separator to specify the separator.
- **Test Rule:** Enter a sample log message into the text box, then select **Test** to test that the desired fields are correctly extracted.

Figure 7: Create Matching Rule

- 3) Click **OK** to add the new matching rule.

NOTE: For the **Logon** and **Logoff** indicators, the required data will vary, depending on both your installation and your syslog message contents.

In this example, when a user logs in, the message ID created is *AUT24414* and is considered as a **Logon** event on *FortiAuthenticator*. When the role change happens as part of periodic host check updates, the message ID created by *PPS* is *AUT23524*. A sign-out event is considered a **Logoff** event on *FortiAuthenticator*, and the identity is removed from the user group, and thus fails to match policy. This logic can be altered depending on the customer's design and intentions.

- 4) Create a Syslog source.

To do this, select **Fortinet SSO methods > SSO > Syslog Sources**. In the upper right corner, select the **View** drop down, select **Syslog Source** and click **Create New**. Then, specify the following fields:

- **Name:** Enter a name for the Syslog source.
- **IP address:** Enter the IP address of *PPS* server.
- **Matching rule:** Select the matching rule created above.
- **SSO user type:** Select *External* as the user type.

Figure 8: Creating a Syslog Source

FortiAuthenticator v6.00-build0010 FAC-VM18004269

System > Edit Syslog Source

Authentication >

Fortinet SSO Methods >

SSO >

General

Portal Services

SAML Authentication

Windows Event Log Sources

RADIUS Accounting Sources

Syslog Sources

Fine-grained Controls

SSO Users

Name: PPS

IP address: 10.10.10.10

Matching rule: PPS

SSO user type:

☒ External

☐ Local users

☐ Remote users [Please Select]

☒ Strip off prefix or suffix from username if any

OK Cancel

NOTE: You must add all the cluster node IPs (not cluster VIPs) in the *FortiAuthenticator* when using a *PPS* cluster setup.

Configuring the FortiGate Firewall

The *FortiGate Firewall* detects traffic from an endpoint that matches a configured security policy using the *FortiAuthenticator* FSSO record. It determines the role(s) associated with that user, and allows or denies the traffic based on the actions configured in the security policy.

To configure *FortiGate Firewall*:

- 1) (Applies to Release 6.0.*) Create the *FortiAuthenticator* as an FSSO agent in the *FortiGate Firewall*. To do this, select **Fabric Connector > Create New**, under SSO/Identity select **Fortinet Single Sign-On Agent**. Then, specify the following fields:
 - **Name:** Enter a name for the entry.
 - **Primary FSSO Agent:** Enter the IP address of the *FortiAuthenticator* appliance, and the password used to communicate with it. This password is the same as the secret key configured on *FortiAuthenticator* in the **Fortinet SSO Methods > General** section.
 - Click **Apply & Refresh** to test your configuration. If correct, the **Users /Groups** area will populate automatically.

The screenshot shows the FortiGate 900D web interface. The left sidebar contains a navigation menu with options: Dashboard, Security Fabric, Fabric Connectors (selected), FortiView, Network, System, Policy & Objects, Security Profiles, VPN, User & Device, WiFi & Switch Controller, and Log & Report. The main content area is titled 'Edit Fabric Connector' and shows the 'SSO/Identity' section. A 'Fortinet Single Sign-On Agent' is being configured. The 'Connector Settings' section includes: Name (PPS agent), Primary FSSO Agent (10.96.71.2), Collector Agent AD access mode (Standard selected, Advanced available), and Users/Groups (2, with a View button). At the bottom right are buttons for 'Apply & Refresh', 'OK', and 'Cancel'.

- 2) (Applies to Release 5.6.*) Create the *FortiAuthenticator* as an FSSO agent in the *FortiGate Firewall*. To do this, select **User & Device > Single Sign-On** and then click **Create New**. Then, specify the following fields:
 - **Type:** Select *Fortinet Single-Sign-On Agent*.
 - **Name:** Enter a name for the entry.
 - **Primary FSSO Agent:** Enter the IP address of the *FortiAuthenticator* appliance, and the password used to communicate with it. This password is the same as the secret key configured on *FortiAuthenticator* in the **Fortinet SSO Methods > General** section.
 - Click **Apply & Refresh** to test your configuration. If correct, the **Users /Groups** area will populate automatically.

Figure 10: Creating Single Sign on Server

FortiGate VM64 FortiGate-VM64

Dashboard > New Single Sign-On Server

FortiView >

Network >

System >

Policy & Objects >

Security Profiles >

VPN >

User & Device >

User Definition >

User Groups >

Guest Management >

Device Inventory >

Custom Devices & Groups >

Single Sign-On ☆

LDAP Servers

RADIUS Servers

Authentication Settings

FortiTokens

WiFi & Switch Controller >

Log & Report >

Monitor >

Type: Poll Active Directory Server, Fortinet Single-Sign-On Agent, RADIUS Single-Sign-On Agent

Name: [Text Field]

Primary FSSO Agent: Server IP/Name [Text Field] - Password [Text Field] +

Collector Agent AD access mode: Standard, Advanced

LDAP Server: [Text Field]

Apply & Refresh OK Cancel

- 3) Create matching User groups. To do this, select **User & Device > User Groups** and click **Create New**. Then, specify the following fields:
 - **Name:** Enter the name of the group. This name will appear in the firewall policy.
 - **Type:** Select *Fortinet Single Sign-On*.
 - Under **Members**, select the matching user group created on *FortiAuthenticator*, and click **OK**.

Figure 11: Creating User Groups

FortiGate VM64 FGVM020000076196 Release Candidate 1

Dashboard > New User Group

FortiView >

Network >

System >

Policy & Objects >

Security Profiles >

VPN >

User & Device >

User Definition >

User Groups ☆

Name: PulseUserGroups

Type: Firewall, Fortinet Single Sign-On (FSSO), Guest, RADIUS Single Sign-On (RSSO)

Members: [Text Field]

Please Select

ENGG

HC

REMED

REMEDICATION

OK Cancel

- 4) Create a firewall policy to use the *PPS* enforcement groups just created. To do this, select **Policy & Objects > IPv4 Policy** and click **Create New**. Then, create the policy based on the resource access restrictions to be enforced.

Figure 12: Creating a Firewall Policy

The screenshot displays the 'New Policy' configuration window in the FortiGate VM64 web interface. The left sidebar shows the navigation menu with 'Policy & Objects' selected. The main area contains the following configuration fields:

- Name:** full_access
- Incoming Interface:** port2
- Outgoing Interface:** port3
- Source:** all
- Destination:** all
- Schedule:** always
- Service:** ALL
- Action:** ☒ ACCEPT ☐ DENY ☐ LEARN

Below the main fields are two sections:

- Firewall / Network Options:**
 - NAT:** ☐
 - IP Pool Configuration:** ☒ Use Outgoing Interface Address ☐ Use Dynamic IP Pool
- Security Profiles:**
 - Antivirus:** ☐
 - Web Filter:** ☐
 - DNS Filter:** ☐
 - Application Control:** ☐
 - IPS:** ☐

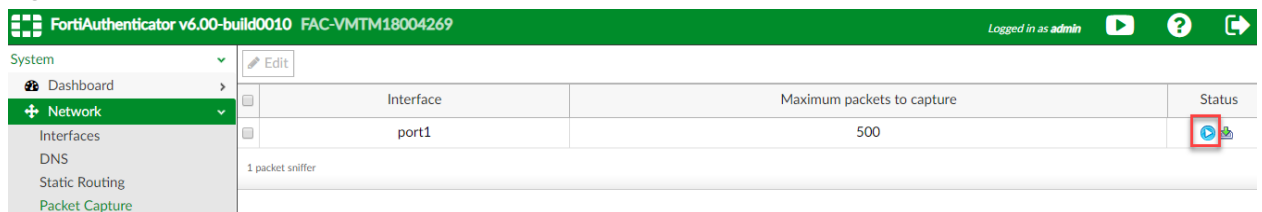
At the bottom of the window are 'OK' and 'Cancel' buttons.

Reports and Logging

You can verify that the syslog messages are reaching the *FortiAuthenticator* by doing a packet capture from the *FortiAuthenticator* user interface.

- 1) Select **System > Network > Packet Capture** and select the interface which is used to communicate with the *PPS* and click **Start Capture**. Once packet capture is complete, stop the capture. Then, download the packets and view them using any tool like *WireShark*.
- 2) To view identity records from the *FortiAuthenticator* user interface, select **Monitor > Sessions**. The list shows the records parsed through syslog.

Figure 13: Monitor SSO Sessions



- 3) You can monitor the FSSO Sessions on a *FortiGate Firewall* from either its graphical user interface (GUI) or its command-line (CLI) user interface.
 - To do this using the *FortiGate Firewall* CLI, type:
diag debug auth fsso list

This command displays identity records received from *FortiAuthenticator*. For example:

Figure 14: Monitor the FSSO Sessions from the FortiGate Firewall CLI

```
FortiGate-VM64 #  
FortiGate-VM64 # diagnose debug authd fsso list  
----FSSO logons----  
IP: 172.21.16.102 User: TEST Groups: USERS Workstation: 172.21.16.102 MemberOf: PulsesecureUserGroup  
Total number of logons listed: 1, filtered: 0  
-----end of FSSO logons-----  
FortiGate-VM64 #
```

- To do this using the *FortiGate Firewall* GUI, select **Monitor > Firewall User Monitor**. The list shows all the identity records.

Figure 15: Monitor the FSSO Sessions on FortiGate Firewall

The screenshot displays the FortiGate VM64 Firewall User Monitor interface. The left sidebar contains a navigation menu with the following items: Dashboard, FortiView, Network, System, Policy & Objects, Security Profiles, VPN, User & Device, WiFi & Switch Controller, Log & Report, Monitor (highlighted), Routing Monitor, DHCP Monitor, SD-WAN Monitor, IPsec Monitor, SSL-VPN Monitor, Firewall User Monitor (highlighted), User Quarantine Monitor, FortiClient Monitor, WiFi Client Monitor, Rogue AP Monitor, and WiFi Health Monitor. The main content area shows a table of FSSO sessions. The table has columns for User Name, User Group, Duration, IP Address, Traffic Volume, and Method. A single session is listed for user TEST, belonging to the PulsesecureUserGroup, with a duration of 0 day(s) 0 hour(s) 0 minute(s), IP address 172.21.16.102, and traffic volume of 0 B. The method is Fortinet Single-Sign-On. The interface also includes a Refresh button, a Deauthenticate button, and a Show all FSSO Logons toggle.

User Name	User Group	Duration	IP Address	Traffic Volume	Method
TEST	PulsesecureUserGroup	0 day(s) 0 hour(s) 0 minute(s)	172.21.16.102	0 B	Fortinet Single-Sign-On

Alert-Based Admission Control with Fortinet Products

This section describes how to integrate *FortiAnalyzer* and *FortiGate Firewall* products with *PPS* to support Alert-based admission control in your network.

Overview of Alert-Based Admission Control with Fortinet Products

Pulse Policy Secure (PPS) integration with network security devices provide user access control based on the threats identified by the network security devices.

The network security device provides detection of threats based on the intrusion prevention system. This helps in detecting unknown threats, and also reduces the number of false alarms.

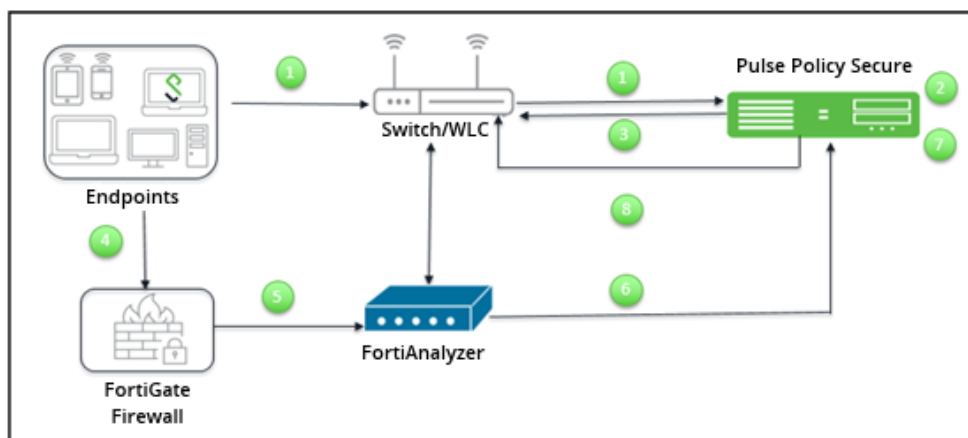
The network security device uses the syslog events mechanism to notify the other devices regarding the network threats. *PPS* also supports dynamically changing the access to the user based on the information received from the network security device.

The admission control user flow is described below:

- 1) The user connects to *PPS* through the Switch (or Wireless LAN Controller).
- 2) The user session is created on the *PPS*.
- 3) The user details are pushed to the Switch for enforcing user access.
- 4) The *FortiGate Firewall* monitors the user traffic.
- 5) The *FortiAnalyzer* generates the syslog messages for the user.
- 6) The syslog message is sent to *PPS* if any suspicious traffic or activity is detected from the user.
- 7) *PPS* processes the received syslog message and, based on the configured policies, actions are taken.
- 8) New/Updated details are pushed to Switch for updating the enforcement of the user.

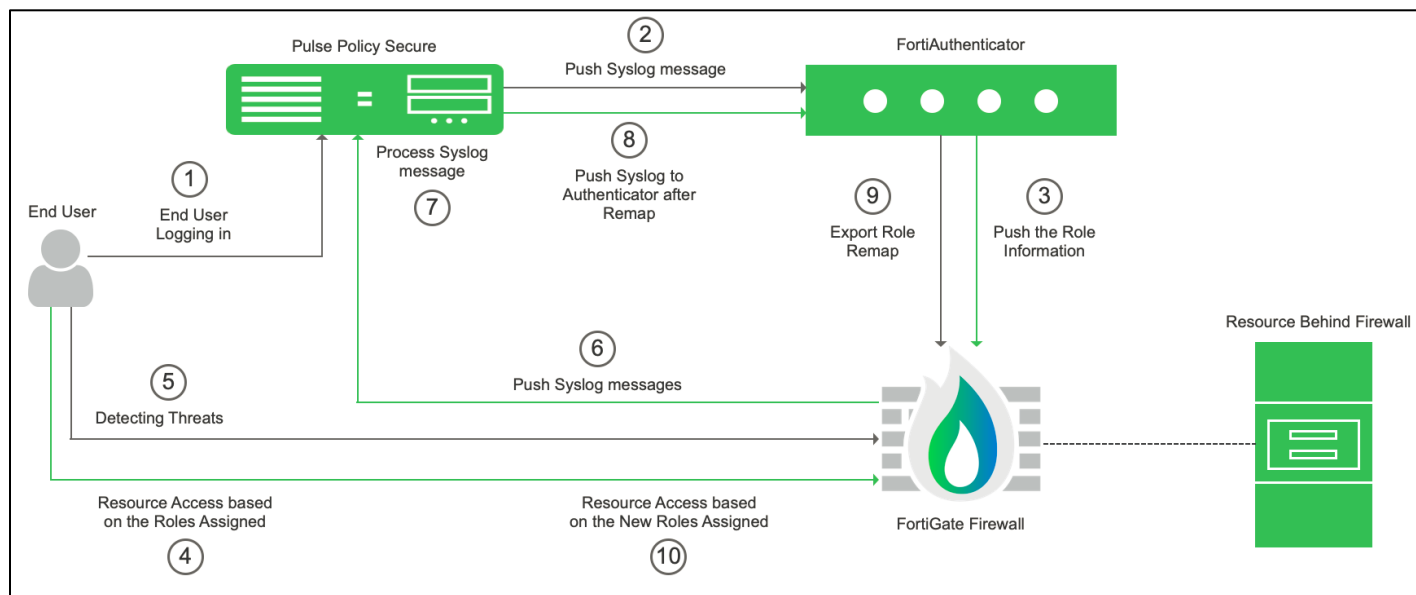
NOTE: The enforcement of the user is also updated on the *FortiGate Firewall*.

Figure 16: Deployment using PPS and Fortinet products



For example, a user is connected to *PPS* and wants to access protected resource which is behind *FortiGate Firewall*. Users get access to the resource, and when the firewall detects a threat from the user, the firewall sends a syslog message and user is removed from the network.

Figure Dynamic Identity Enforcement with Admission Control



The dynamic identity enforcement using admission control user flow is described below:

- 1) The user connects to PPS through the Switch (or Wireless LAN Controller). User is authenticated on PPS after validating the HC policy.
- 2) The syslog sessions are exported to FortiAuthenticator.
- 3) Identity information is parsed from the Syslog message and is used to create an IP to username mapping within FortiAuthenticator. This information is shared with FortiGate firewall in the form of a Fortinet Single Sign-On (FSSO) record.
- 4) The firewall uses this information to either allow or block traffic based on the configured policy
- 5) FortiGate Firewall Monitors the end user flow and activity and detects attacks/malicious activity at the end user session
- 6) FortiGate Firewall/Analyser sends a syslog message to PPS for any suspicious traffic or activity detected from end user.
- 7) PPS process the received syslog message and based on the configured policies, action will be taken for the end user session.
- 8) PPS exports New Roles to the FortiAuthenticator.
- 9) The firewall changes users Role based on the information received from Authenticator.
- 10) User gets access to the protected resources based on the new role assigned.

Summary of Configuration

To prepare your network to use alert-based access control using *Pulse Policy Secure*, *FortiAuthenticator*, *FortiAnalyzer* and *FortiGate Firewall*, perform the following tasks:

- [Configuring Network Security Devices with PPS.](#)
- [Configuring an Admission Control Template](#)
 - [Configuring Admission Control Policies](#)
 - [Configuring the Admission Control Client](#)
- [Configuring FortiGate Firewall](#)
- [Configuring FortiAnalyzer](#)
- [Confirming Syslog Forwarding](#)

The following sections describe each of these steps in detail.

Configuring Network Security Devices with PPS

The network security devices are configured with *PPS* for admission access control. A high-level overview of the configuration steps needed to set up and run the integration is described below:

- The Administrator configures the required syslog clients on the *PPS* Admin UI. Each network security device acts as a syslog client on which syslog forwarding is enabled, and *PPS* receives the forwarded syslog messages.
- The Administrator then configures a set of policies that define what actions are to be taken on user sessions, based on the data in the threat events.
- The user defined templates are used to map the data and the predefined variables. The predefined variables in the template are Rule Name, Source IP Address, Source User, and Severity.
- The templates for parsing the syslog messages from *Fortinet Firewall/Analyzer* are available by default. The administrators can also add customised templates for integrating with other network security devices.

This section covers the following topics:

- [Configuring an Admission Control Template](#)
- [Configuring Admission Control Policies](#)
- [Configuring the Admission Control Client](#)

Configuring an Admission Control Template

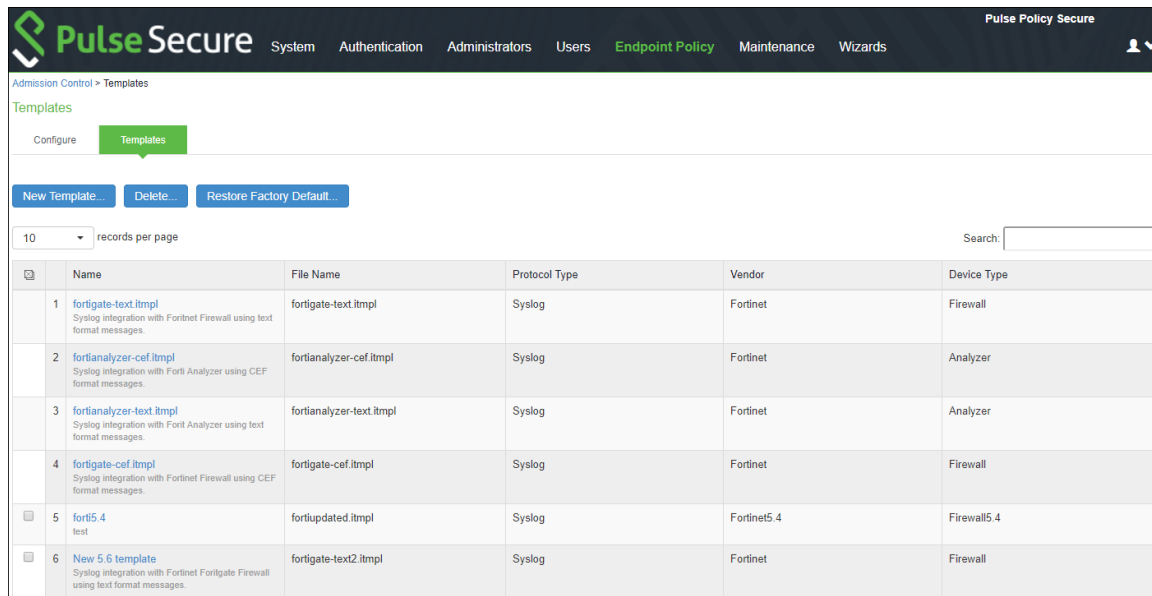
The admission control template provides a list of possible events that can be received from the network security device, along with a regular expression to parse the message. The template also provides possible actions that can be taken for an event.

Only the admission control policy defines the actions to be taken on receipt of an event. The admission control template only provides possible events and possible actions for that event.

To view and add the admission control templates:

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

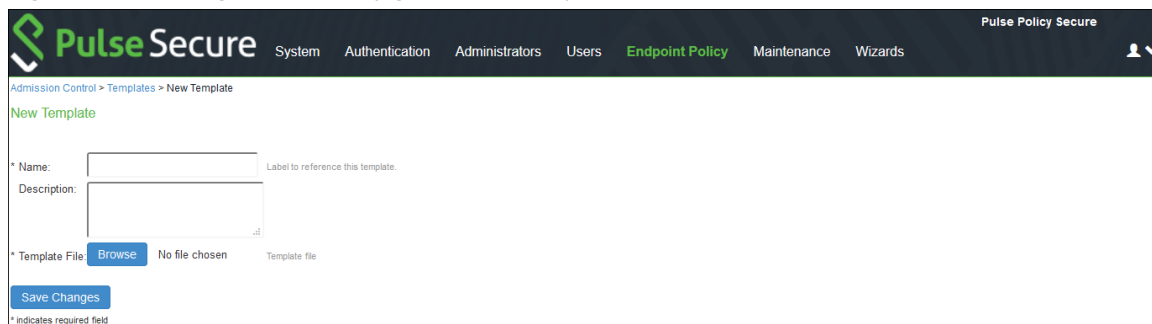
Figure 17: Existing Templates



	Name	File Name	Protocol Type	Vendor	Device Type
1	fortigate-text.itmpl Syslog integration with Fortinet Firewall using text format messages.	fortigate-text.itmpl	Syslog	Fortinet	Firewall
2	fortianalyzer-cef.itmpl Syslog integration with Forti Analyzer using CEF format messages.	fortianalyzer-cef.itmpl	Syslog	Fortinet	Analyzer
3	fortianalyzer-text.itmpl Syslog integration with Forti Analyzer using text format messages.	fortianalyzer-text.itmpl	Syslog	Fortinet	Analyzer
4	fortigate-cef.itmpl Syslog integration with Fortinet Firewall using CEF format messages.	fortigate-cef.itmpl	Syslog	Fortinet	Firewall
5	forti5.4 test	fortiupdated.itmpl	Syslog	Fortinet5.4	Firewall5.4
6	New 5.6 template Syslog integration with Fortinet Fortigate Firewall using text format messages.	fortigate-text2.itmpl	Syslog	Fortinet	Firewall

- 2) Click **New Template**.

Figure 18: Adding a New Configuration Template



New Template

* Name: Label to reference this template.

Description:

* Template File: No file chosen Template file

* indicates required field

- 3) Enter the template **Name**.
- 4) Enter a template **Description**.
- 5) Click **Browse** and select the template file.
- 6) Click **Save Changes**.

Configuring Admission Control Policies

The admission control policies define the actions that are performed on *PPS* for user sessions. The actions are based on the specific threat event information received from the network security device.

To view and add the new integration policy:

- 1) Select **Endpoint Policy > Admission Control > Policies**.

Figure 19: Configuring Policies

	Name	Protocol Type	Vendor	Device Type	Event	Severity	Action	Applies to
1	policy	Syslog	Fortinet	Firewall	utm:app-ctrl	Elevated risk	changeRole	All
2	policy2	Syslog	Fortinet5.4	Firewall5.4	utm:app-ctrl	Elevated risk	changeRole	Full Access Role1 Guest

- 2) Click **New Policy**.
- 3) Enter the policy name.
- 4) Select the template used by the client. The following templates are available by default for Fortinet:
 - *Fortinet-Analyzer-Syslog-CEF*
 - *Fortinet-Analyzer-Syslog-text*
 - *Fortinet-Firewall-Syslog-CEF*
 - *Fortinet-Firewall-Syslog-text*
- 5) Under **Rule on Receiving**, select the event type and the severity level. The event types and the severity level are based on the selected template.
- 6) Under **Count these many times**, enter a number between 1-256.
- 7) Under **Then perform this action**, select the desired action.
 - *Ignore (log the event)*: Received syslog event details are logged on the *PPS* and no specific action is taken.
 - *Terminate user session*: Terminates the user session on the *PPS* for the received messages.
 - *Disable user account*: Terminates the user session and disables the user on the *PPS* for the received messages.
 - *Replace user role with this role*: Changes the roles assigned to the user on *PPS* so that restriction/privileges for the user can be changed.

NOTE: You must specify whether to apply the role assignment permanently or only for the session.

8) Under **Roles**, specify:

- *Policy applies to ALL roles:* Applies the policy to all users.
- *Policy applies to SELECTED roles:* Applies this policy only to users who are mapped to roles in the **Selected** roles list. You must add roles to this list from the **Available** roles list.
- *Policy applies to all roles OTHER THAN those selected below:* Applies this policy to all users except for those who map to the roles in the **Selected** roles list. You must add roles to this list from the **Available** roles list.

9) Click **Save Changes**.

Figure 20: Adding a New Configuration Policy

Pulse Secure System Authentication Administrators Users **Endpoint Policy** Maintenance Wizards

Admission Control > Policies > New Policy

New Policy

* Name: Label to reference this policy.

* Template: Fortinet-Firewall-Syslog-text Template used by the client

Selected Template Details

Template name	Vendor	Device	Protocol	Format	Description
fortigate-text.itmpl	Fortinet	Firewall	Syslog	text	Syslog integration with Fortinet Firewall using text format messages.

▼ Rule on receiving

* Events: anomaly:anomaly Events supported

* Severity Level: Any Severity Levels supported

▼ Count these many times

* Count: 1 (1-256)

▼ then perform this action

☒ Ignore (just log the event)

☐ Terminate user session

☐ Disable user account

☐ Replace user's roles with this one

Make this role assignment

☐ Permanent

☒ For this session only

▼ Roles

☒ Policy applies to ALL roles

☐ Policy applies to SELECTED roles

☐ Policy applies to all roles OTHER THAN those selected below

Available roles: Full Access Role1, Full Access Role2, Full Access Role3, Guest, Guest Admin

Selected roles: (none)

Add > Remove

Save Changes

* indicates required field

Configuring the Admission Control Client

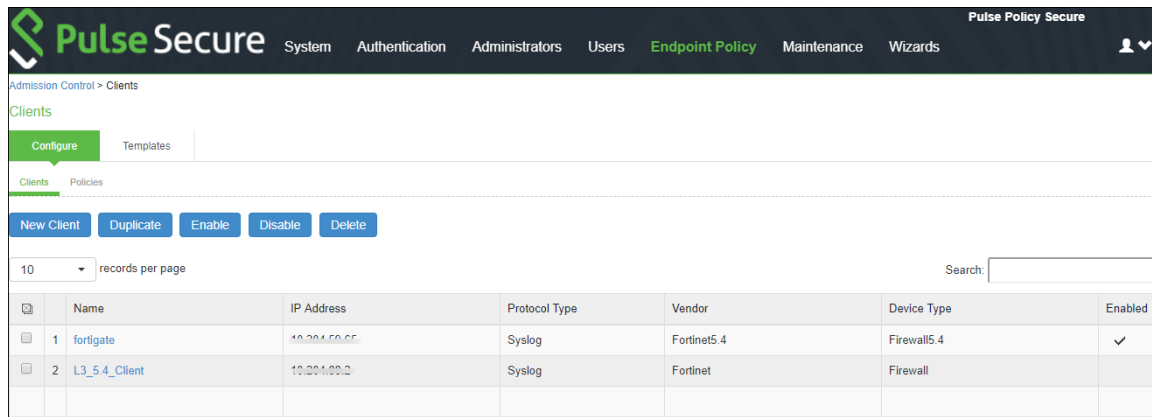
The admission control clients are the network security devices on which the syslog forwarding is enabled. The messages are received by the syslog server module running on *PPS*.

You must add either the *FortiGate Firewall* or the *FortiAnalyzer* as separate clients on *PPS* to enable it to receive the required threat information through syslogs.

To add a client:

- 1) Select **Endpoint Policy > Admission Control > Clients**.

Figure 21: Admission Control Client



	Name	IP Address	Protocol Type	Vendor	Device Type	Enabled
1	fortigate	10.204.50.55	Syslog	Fortinet5.4	Firewall5.4	✓
2	L3_5_4_Client	10.204.00.0	Syslog	Fortinet	Firewall	

- 2) Click **New Client**.
- 3) Enter the **Name** of the client that will be added in the *PPS*.
- 4) Enter a **Description**.
- 5) Enter the **IP Address** of the client.
- 6) Select the **Template** for the client.
 - *Fortinet-Analyzer-Syslog-CEF*
 - *Fortinet-Analyzer-Syslog-text*
 - *Fortinet-Firewall-Syslog-CEF*
 - *Fortinet-Firewall-Syslog-text*

- 7) Click **Save Changes**.

Figure 22: Adding Clients

Pulse Secure System Authentication Administrators Users **Endpoint Policy** Maintenance Wizards

Admission Control > Clients > New Client

New Client

* Name: Label to reference this client.

Description:

* IP Address: IP Address of this client.

* Template: Fortinet-Firewall-Syslog-text Template used by the client

Selected Template Details

Template name	Vendor	Device	Protocol	Format	Description
fortigate-text.ftmpl	Fortinet	Firewall	Syslog	text	Syslog integration with Fortinet Firewall using text format messages.

Save Changes

* indicates required field

Configuring FortiGate Firewall

Once you have added the *FortiGate Firewall* as a syslog client on *PPS* (see [Configuring the Admission Control Client](#)), the *PPS* must be added as a syslog server on the *FortiGate Firewall*.

To configure *FortiGate Firewall*:

- 1) Select **Log & Report > Log Settings**.
- 2) Enable **Send Logs to Syslog**.
- 3) Enter the **IP Address/FQDN** of the *PPS* device and click **Apply**. The *PPS* is added as a syslog server.

Figure 23: Log Settings

FortiGate VM64 FortiGate-VM64

Log Settings

0B Jul 12 Jul 13 Jul 14 Jul 15 Jul 16 Jul 17 Jul 18

Traffic Log Event Log IPS Log Application Control Log

Send Logs to FortiCloud ☐

Send Logs to Syslog ☒

IP Address/FQDN 10.0.0.103

Log Settings

Event Logging All Customize

Local Traffic Log All Customize

☐ Log Allowed Traffic ☐ Log Denied Unicast Traffic

☐ Log Local Out Traffic ☐ Log Denied Broadcast Traffic

GUI Preferences

Display Logs/FortiView From Disk

Resolve Hostnames ☒

Resolve Unknown Applications ☒

Apply

- 4) The default syslog format is text. You must use the following Command-Line user Interface (CLI) to change the format to CEF.

Figure 24: Changing Syslog Format

```
FortiGate-VM64 # config log syslogd setting
FortiGate-VM64 (setting) # show
config log syslogd setting
    set status enable
    set server "10.96.7.68"
    set format cef
end
```

- 5) To access the firewall, you must configure the firewall management interface settings from the CLI.

Figure 25: Changing Management Interface Settings

```
FGVM020000076196 # config system interface
FGVM020000076196 (interface) # edit port6
FGVM020000076196 (port6) # set ip 192.168.0.1 255.255.255.0

FGVM020000076196 (port6) # set allowaccess ping https http ssh fgfm
FGVM020000076196 (port6) # set type physical
FGVM020000076196 (port6) # set status up

FGVM020000076196 (port6) #
FGVM020000076196 (port6) #
FGVM020000076196 (port6) # show
config system interface
    edit "port6"
        set vdom "root"
        set ip 192.168.0.1 255.255.255.0
        set allowaccess ping https ssh http fgfm
        set type physical
        set snmp-index 6
    next
end
```

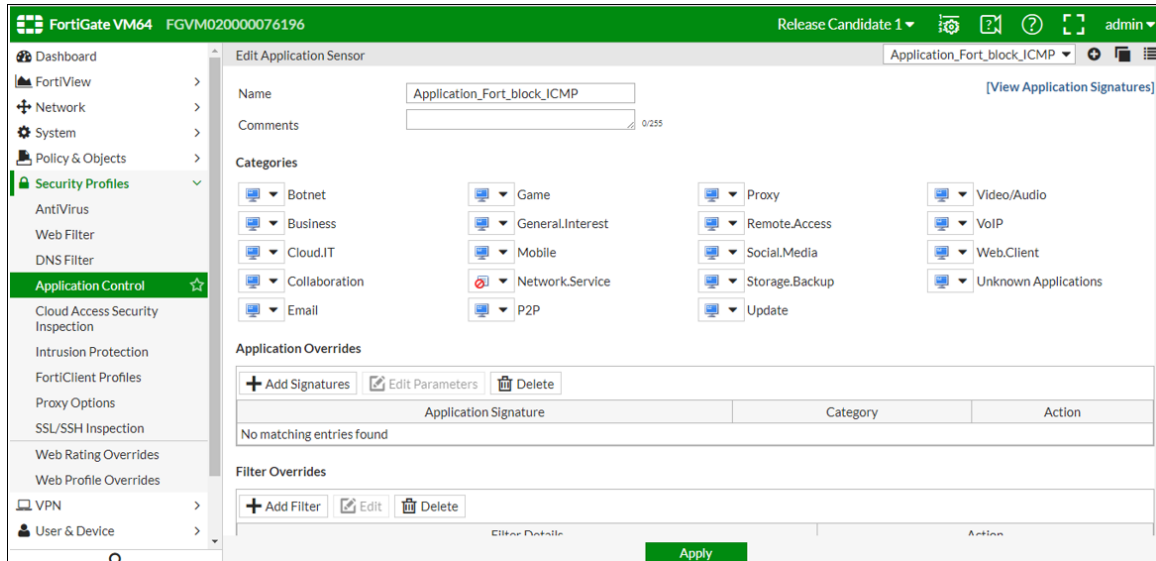
- 6) Under **Interfaces**, configure the trust and untrust zones.

Figure 26: Configuring Trust/Untrust Zones

Status	Name	Members	IP/Netmask	Type	Access	Ref.
+	port1		10.0.1.10 255.255.252.0	Physical Interface	PING HTTPS SSH HTTP	1
+	port2		10.0.1.20 255.255.252.0	Physical Interface	PING HTTPS SSH	3
+	port3		10.0.1.30 255.255.252.0	Physical Interface	PING HTTPS SSH	2
-	port4		0.0.0.0 0.0.0	Physical Interface		0
-	port5		0.0.0.0 0.0.0	Physical Interface		0
-	port6		10.0.1.250 255.255.252.0	Physical Interface	PING HTTPS SSH	0
-	port7		0.0.0.0 0.0.0	Physical Interface		0
-	port8		0.0.0.0 0.0.0	Physical Interface		0
-	port9		0.0.0.0 0.0.0	Physical Interface		0
-	port10		0.0.0.0 0.0.0	Physical Interface		0

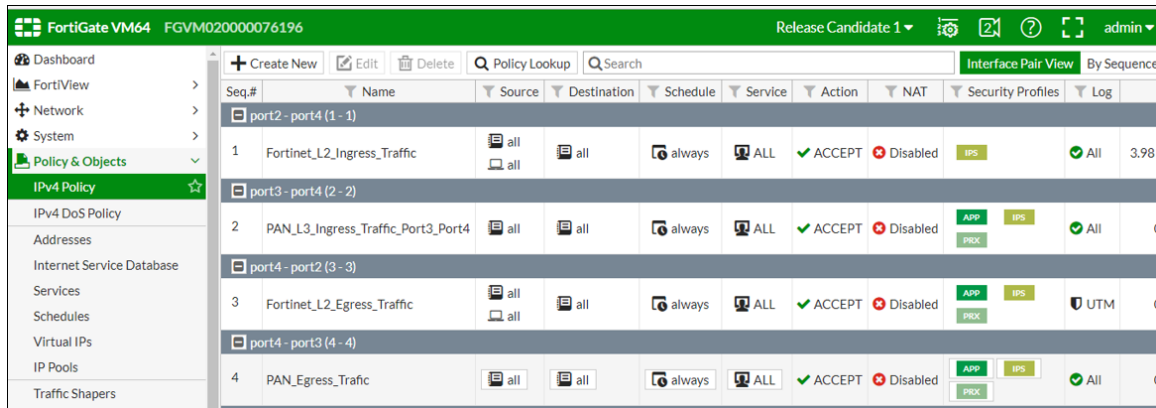
- 7) Under **Security Profiles > Application Control**, create a security profile.

Figure 27: Creating Security Profile



- 8) Under **Policy & Objects**, apply policies to desired port.

Figure 28: Applying Policies



Configuring FortiAnalyzer

Once you have added the *FortiAnalyzer* as a syslog client on *PPS* (see [Configuring the Admission Control Client](#)), the *PPS* must be added as a syslog server on the *FortiAnalyzer*.

- 1) Configure the *FortiAnalyzer* management interface using its Command-Line user Interface (CLI).

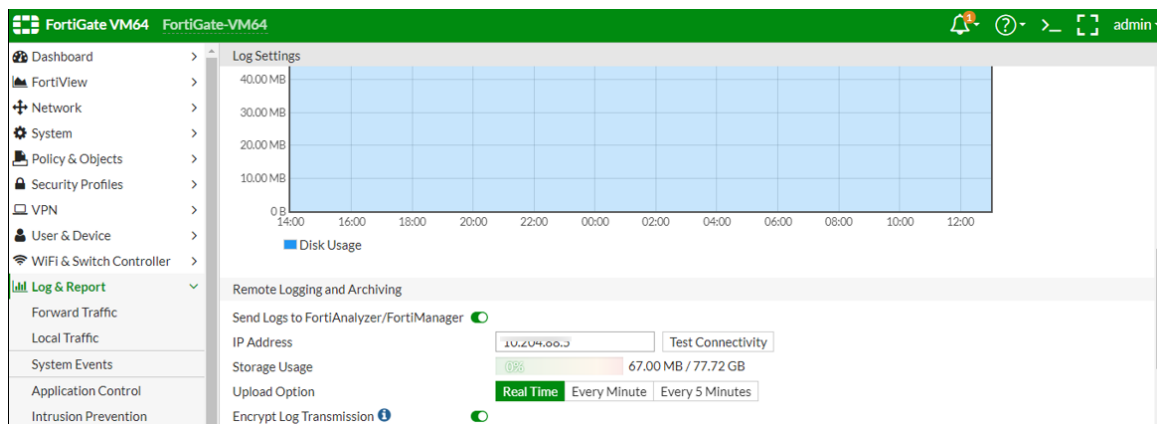
Figure 29: Configuring the FortiAnalyzer Management Interface

```
FAZVM64 # config system interface
(interface)# show
config system interface
  edit "port1"
    set ip 10.204.88.5 255.255.252.0
    set allowaccess ping https ssh telnet http
  next
  edit "port2"
    set ip 10.96.71.6 255.255.224.0
    set allowaccess ping https ssh snmp telnet http fgfm
  next
  edit "port3"
  next
  edit "port4"
  next
end
```

```
FAZVM64 # config system route
(route)# show
config system route
  edit 1
    set device "port1"
    set gateway 10.204.63.254
  next
  edit 2
    set device "port3"
    set gateway 10.96.64.1
  next
end
```

- 2) On the *FortiGate Firewall*, under **Log & Report**, enable **Send Logs to FortiAnalyzer/FortiManager** to forward the syslog message to *FortiAnalyzer*. Enter the IP Address of the *FortiAnalyzer*.

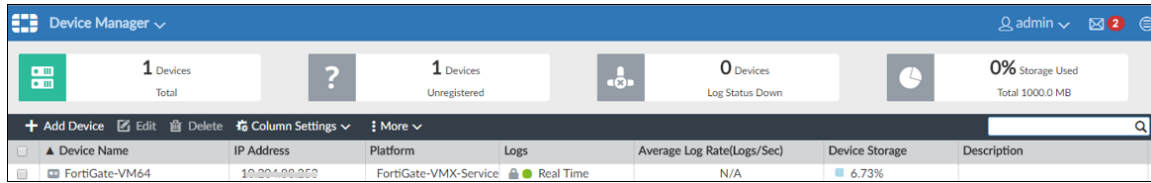
Figure 30: Forwarding Logs



NOTE: On *FortiGate Firewall*, ensure you have configured the security policy's network trust, untrust zone and apply the policy to desired ports.

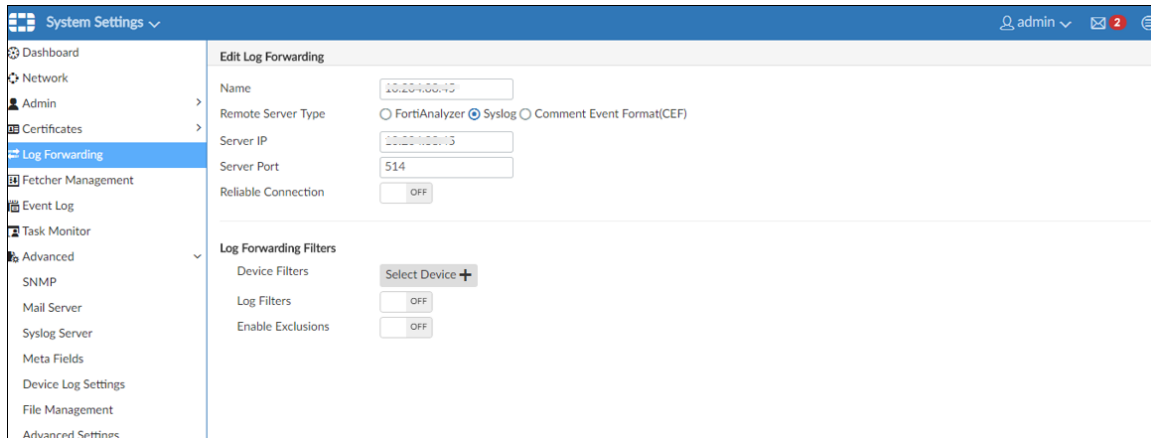
- 3) Under **FortiAnalyzer > Device Manager**, click **Add Device** to add the *FortiGate Firewall*.

Figure 31: Adding Device



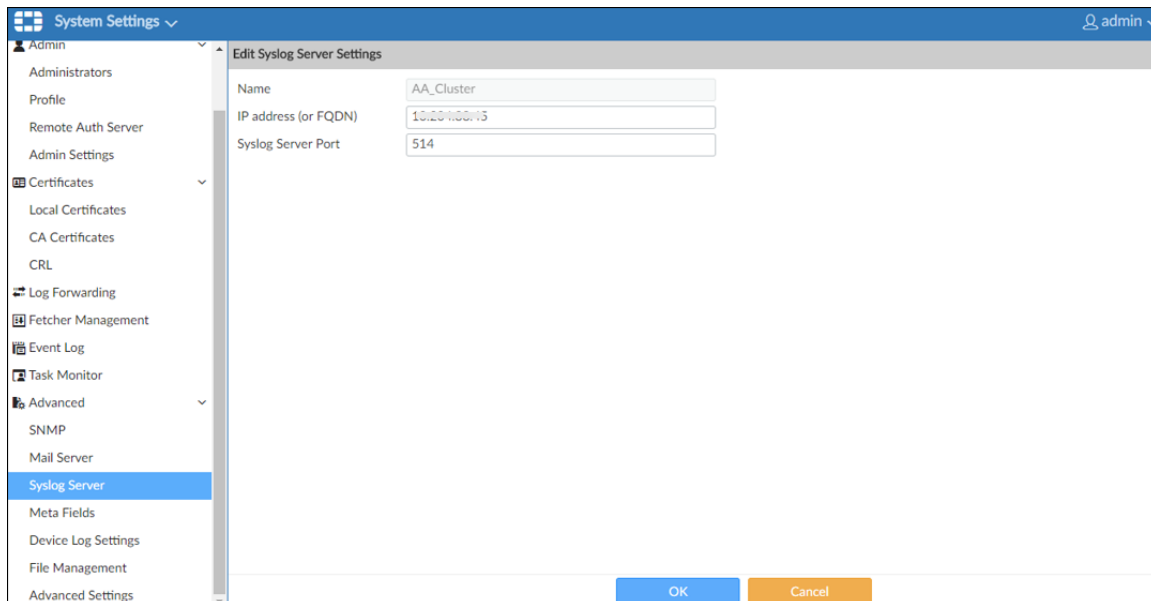
- 4) Under **System Settings > Log Forwarding > Edit Log Forwarding**, enter the IP address of the *PPS* device for log forwarding.

Figure 32: Configuring Log Forwarding



- 5) Under **System Settings > Advanced > Syslog Server**, enter the IP address of *PPS* device.

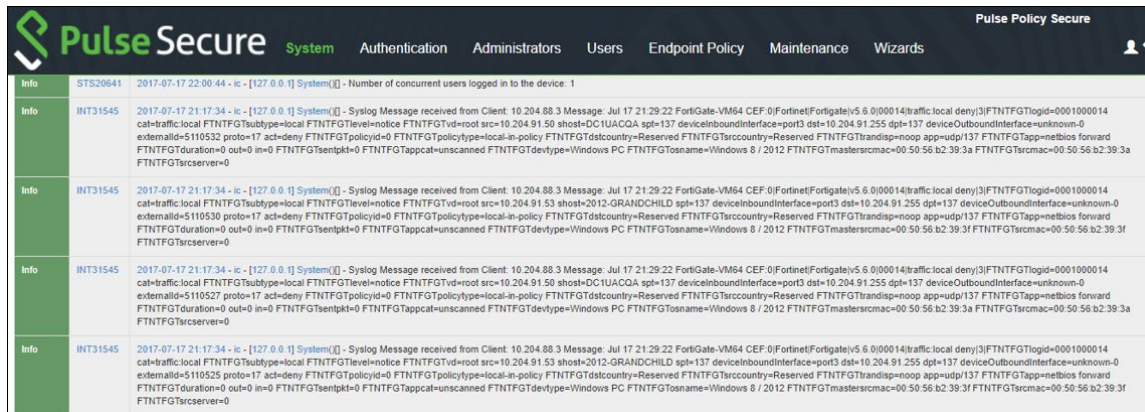
Figure 33: Configuring Syslog Server Settings



Confirming Syslog Forwarding

When the network security device detects a threat, the syslog messages are forwarded to PPS. To verify the event logs have been received on PPS, select **System > Log/Monitoring > Events > Log**.

Figure 34: Viewing Event Logs



The screenshot shows the Pulse Secure web interface. The top navigation bar includes 'Pulse Secure' logo, 'System' (selected), 'Authentication', 'Administrators', 'Users', 'Endpoint Policy', 'Maintenance', and 'Wizards'. Below the navigation bar, there is a table of event logs. The table has columns for 'Info', 'ID', and 'Message'. The first row shows a system message about concurrent users. The subsequent rows show detailed intrusion prevention system (IPS) logs with fields like 'cat=traffic:local', 'FTNTFGTsubtype=local', 'FTNTFGTlevel=notice', 'FTNTFGTvd=root', 'src=10.204.91.50', 'shost=2012-GRANDCHILD', 'spl=137', 'deviceInboundInterface=port3', 'dst=10.204.91.255', 'dpt=137', 'deviceOutboundInterface=unknown-0', 'externalid=5110527', 'proto=17', 'act=deny', 'FTNTFGTpolicyid=0', 'FTNTFGTpolicytype=local-in-policy', 'FTNTFGTdstcountry=Reserved', 'FTNTFGTsrcountry=Reserved', 'FTNTFGTtrandisp=noop', 'app=udp/137', 'FTNTFGTapp=netbios forward', 'FTNTFGTduration=0', 'out=0', 'in=0', 'FTNTFGTsentpkt=0', 'FTNTFGTappcat=unscanned', 'FTNTFGTdevtype=Windows PC', 'FTNTFGTosname=Windows 8 / 2012', 'FTNTFGTmastersrcmac=00:50:56:b2:39:3f', and 'FTNTFGTsrcmac=00:50:56:b2:39:3f'.

Info	ID	Message
Info	STS20641	2017-07-17 22:00:44 - [127.0.0.1] System() - Number of concurrent users logged in to the device: 1
Info	INT31545	2017-07-17 21:17:34 - [127.0.0.1] System() - Syslog Message received from Client: 10.204.88.3 Message: Jul 17 21:29:22 FortiGate-VM64 CEF:0 Fortinet Fortigate v5.6.0 00014 traffic:local deny 3 FTNTFGTlogid=0001000014 cat=traffic:local FTNTFGTsubtype=local FTNTFGTlevel=notice FTNTFGTvd=root src=10.204.91.50 shost=2012-GRANDCHILD spl=137 deviceInboundInterface=port3 dst=10.204.91.255 dpt=137 deviceOutboundInterface=unknown-0 externalid=5110527 proto=17 act=deny FTNTFGTpolicyid=0 FTNTFGTpolicytype=local-in-policy FTNTFGTdstcountry=Reserved FTNTFGTsrcountry=Reserved FTNTFGTtrandisp=noop app=udp/137 FTNTFGTapp=netbios forward FTNTFGTduration=0 out=0 in=0 FTNTFGTsentpkt=0 FTNTFGTappcat=unscanned FTNTFGTdevtype=Windows PC FTNTFGTosname=Windows 8 / 2012 FTNTFGTmastersrcmac=00:50:56:b2:39:3f FTNTFGTsrcmac=00:50:56:b2:39:3f FTNTFGTsrcserver=0
Info	INT31545	2017-07-17 21:17:34 - [127.0.0.1] System() - Syslog Message received from Client: 10.204.88.3 Message: Jul 17 21:29:22 FortiGate-VM64 CEF:0 Fortinet Fortigate v5.6.0 00014 traffic:local deny 3 FTNTFGTlogid=0001000014 cat=traffic:local FTNTFGTsubtype=local FTNTFGTlevel=notice FTNTFGTvd=root src=10.204.91.53 shost=2012-GRANDCHILD spl=137 deviceInboundInterface=port3 dst=10.204.91.255 dpt=137 deviceOutboundInterface=unknown-0 externalid=5110527 proto=17 act=deny FTNTFGTpolicyid=0 FTNTFGTpolicytype=local-in-policy FTNTFGTdstcountry=Reserved FTNTFGTsrcountry=Reserved FTNTFGTtrandisp=noop app=udp/137 FTNTFGTapp=netbios forward FTNTFGTduration=0 out=0 in=0 FTNTFGTsentpkt=0 FTNTFGTappcat=unscanned FTNTFGTdevtype=Windows PC FTNTFGTosname=Windows 8 / 2012 FTNTFGTmastersrcmac=00:50:56:b2:39:3f FTNTFGTsrcmac=00:50:56:b2:39:3f FTNTFGTsrcserver=0
Info	INT31545	2017-07-17 21:17:34 - [127.0.0.1] System() - Syslog Message received from Client: 10.204.88.3 Message: Jul 17 21:29:22 FortiGate-VM64 CEF:0 Fortinet Fortigate v5.6.0 00014 traffic:local deny 3 FTNTFGTlogid=0001000014 cat=traffic:local FTNTFGTsubtype=local FTNTFGTlevel=notice FTNTFGTvd=root src=10.204.91.50 shost=2012-GRANDCHILD spl=137 deviceInboundInterface=port3 dst=10.204.91.255 dpt=137 deviceOutboundInterface=unknown-0 externalid=5110527 proto=17 act=deny FTNTFGTpolicyid=0 FTNTFGTpolicytype=local-in-policy FTNTFGTdstcountry=Reserved FTNTFGTsrcountry=Reserved FTNTFGTtrandisp=noop app=udp/137 FTNTFGTapp=netbios forward FTNTFGTduration=0 out=0 in=0 FTNTFGTsentpkt=0 FTNTFGTappcat=unscanned FTNTFGTdevtype=Windows PC FTNTFGTosname=Windows 8 / 2012 FTNTFGTmastersrcmac=00:50:56:b2:39:3f FTNTFGTsrcmac=00:50:56:b2:39:3f FTNTFGTsrcserver=0
Info	INT31545	2017-07-17 21:17:34 - [127.0.0.1] System() - Syslog Message received from Client: 10.204.88.3 Message: Jul 17 21:29:22 FortiGate-VM64 CEF:0 Fortinet Fortigate v5.6.0 00014 traffic:local deny 3 FTNTFGTlogid=0001000014 cat=traffic:local FTNTFGTsubtype=local FTNTFGTlevel=notice FTNTFGTvd=root src=10.204.91.53 shost=2012-GRANDCHILD spl=137 deviceInboundInterface=port3 dst=10.204.91.255 dpt=137 deviceOutboundInterface=unknown-0 externalid=5110525 proto=17 act=deny FTNTFGTpolicyid=0 FTNTFGTpolicytype=local-in-policy FTNTFGTdstcountry=Reserved FTNTFGTsrcountry=Reserved FTNTFGTtrandisp=noop app=udp/137 FTNTFGTapp=netbios forward FTNTFGTduration=0 out=0 in=0 FTNTFGTsentpkt=0 FTNTFGTappcat=unscanned FTNTFGTdevtype=Windows PC FTNTFGTosname=Windows 8 / 2012 FTNTFGTmastersrcmac=00:50:56:b2:39:3f FTNTFGTsrcmac=00:50:56:b2:39:3f FTNTFGTsrcserver=0

References

- Logging and Reporting Overview:
<http://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-logging-reporting-54/logs.htm?Highlight=Logging%20and%20Reporting>
- Inside FortiOS: Application Control:
<http://help.fortinet.com/fos50hlp/56/Content/FortiOS/fortiOS-HTML5-v2/InsideFOS/ApplicationControl.htm>
- Inside FortiOS: Intrusion Prevention System (IPS):
<http://help.fortinet.com/fos50hlp/56/Content/FortiOS/fortiOS-HTML5-v2/InsideFOS/IPS.htm>