

Configure Palo Alto NGFW

Sending Syslog Messages



STEP 1: Configure PANW Log message Profile

The screenshot shows the Palo Alto Networks GUI with the 'Syslog Server Profile' configuration page. The 'Servers' tab is active, displaying a table of configured servers. A blue box highlights the 'Forescout_VPN' server entry. A large blue arrow points from the text 'Forescout IP Address (Syslog Destination)' to the IP address field in the table.

Name	Location	Name	Syslog Server	Transport	Port	Format
Forescout_VPN		FSct222	192.168.10.222	UDP	514	BSD

Forescout IP Address
(Syslog Destination)

The screenshot shows the 'Syslog Server Profile' configuration page with the 'Custom Log Format' tab selected. A blue box highlights the 'Log Type' and 'Custom Format' columns. The 'Escaping' checkbox is unchecked.

Log Type	Custom Format
Config	Default
System	Default
Threat	Default
Traffic	Default
URL	Default
Data	Default
WildFire	Default
Tunnel	Default
Authentication	Default

☐ Escaping

Escaped Characters:

Escape Character:

OK Cancel



STEP 2: Attach profile to System Log (Informational)

The screenshot shows the Palo Alto Networks configuration interface. On the left, the 'Log Settings' menu item is highlighted. The main panel displays a table of log settings for the 'System' category. The 'SystemLogs2FSCT' profile is selected, and its configuration is shown in a modal window titled 'Log Settings - System'.

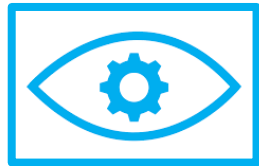
Log Settings - System

- Name:** SystemLogs2FSCT
- Filter:** (severity eq informational)
- Description:**
- Forward Method:**
 - ☐ Panorama
 - ☒ Syslog
 - SNMP:** Add, Delete
 - Email:** Add, Delete
 - Syslog:** Add, Delete
 - HTTP:** Add, Delete
 - Forescout_VPN:** Add, Delete

The background table shows the following data:

Name	Description	Filter	Panorama	SNMP Trap	Email	Syslog
SystemLogs2FSCT		(severity eq informational)	<input type="checkbox"/>			Forescout_VPN

Configure Fore Scout Syslog Sources



STEP 1: Syslog parsing configs -- Connect

Configure with following fstool commands; Ensure that the Connect GP 1.1.0 App is deployed first

```
#Custom Traps Event for GlobalProtect VPN
fstool syslog set_property config.type1.option.gp_vpn_logs "GlobalProtect VPN Events"
fstool syslog set_property config.type2.option.gp_vpn_logs "GlobalProtect VPN Events"
fstool syslog set_property config.type3.option.gp_vpn_logs "GlobalProtect VPN Events"

#GlobalProtect VPN Connect Event

fstool syslog set_property template.gp_vpn_connect.type "gp_vpn_logs"
fstool syslog set_property template.gp_vpn_connect.regexp ".*\\ \\d{1,2}\\:\\d{1,2}\\:\\d{1,2}\\ (\\w-
.]*).*,globalprotectgateway-config-succ,.*Private IP:\\ (\\d{1,3}\\\\.\\d{1,3}\\\\.\\d{1,3}\\\\.\\d{1,3})"
fstool syslog set_property template.gp_vpn_connect.properties "\\$connect_globalprotect_firewall,\\$ip"
fstool syslog set_property template.gp_vpn_connect.set_true "\\$online"

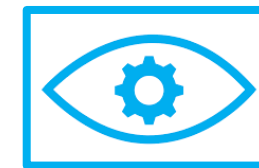
#GlobalProtect VPN Disconnect Event
fstool syslog set_property template.gp_vpn_disconnect.type "gp_vpn_logs"
fstool syslog set_property template.gp_vpn_disconnect.regexp ".*globalprotectgateway-config-release.*Private IP:\\
(\\d{1,3}\\\\.\\d{1,3}\\\\.\\d{1,3}\\\\.\\d{1,3})"
fstool syslog set_property template.gp_vpn_disconnect.properties "\\$ip"
fstool syslog set_property template.gp_vpn_disconnect.set_false "\\$online"
```

STEP 2: Restart Box

```
[root@forescout ~]# fstool service restart
```

STEP 3: Wait for Box

```
[root@forescout ~]# fstool service status
CounterACT Appliance is running
```



STEP 4: Configure Syslog Sources

Options 10.100.1.233

Options

Search

- > CounterACT Devices
- ▼ Modules
 - DNS Query Extension
 - Flow Analyzer
 - Channels
 - Splunk
 - Microsoft SMS/SCCM
 - Advanced Tools
 - IoT Posture Assessment Engine
 - Flow Collector
 - IoT Posture Assessment Engine
 - IOC Scanner
 - Connect
 - Azure
 - AWS
 - Wireless
 - RADIUS
 - MAC Address Repository
 - CEF

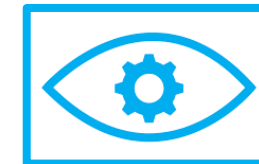
Modules

Modules extend CounterACT's capabilities by enabling integration with other tools, allowing deeper inspection, additional enforcement actions and more. Some modules, such as Base Modules, contain plugins that provide added functionality. New and updated Base Modules, Extended Modules and Content Modules are available from the product downloads portal.

Search

Name	Type	Version
▶ Device Data Publisher	Base	1.0.0
⏸ External Classifier	Base	2.3.0
▶ Flow Analyzer	Base	1.4.1
⏸ Flow Collector	Base	1.1.0
▶ IOC Scanner	Base	2.4.0
⏸ IoT Posture Assessment Engine	Base	1.1.3
▶ NBT Scanner	Base	3.2.0
▶ Packet Engine	Base	8.2.0
▶ Reports	Base	5.2.0
▶ Syslog	Base	3.6.0
▶ Technical Support	Base	1.3.0
▶ Web Client	Base	1.2.0
⏸ Operational Technology	Base	1.2.0

Install
Uninstall
Rollback
Start
Stop
Appliances
Configure
Test
Help
About



STEP 5: Configure Syslog Sources

Options 192.168.10.222

Options

syslog

Modules

Syslog

Modules > Syslog

Send Events To Syslog Triggers Default Action Configuration Receive From

1st Syslog Source

Source Type GlobalProtect VPN Events

IP Address 192.168.0.1

2nd Syslog Source

Source Type <Select Type>

IP Address

3rd Syslog Source

Source Type <Select Type>

IP Address

Ports for Incoming Syslog Messages

UDP Port 514

TCP Port 514

☐ Use TLS

Firewall IP Address
(syslog source)

Add all FWs that have
VPN connections