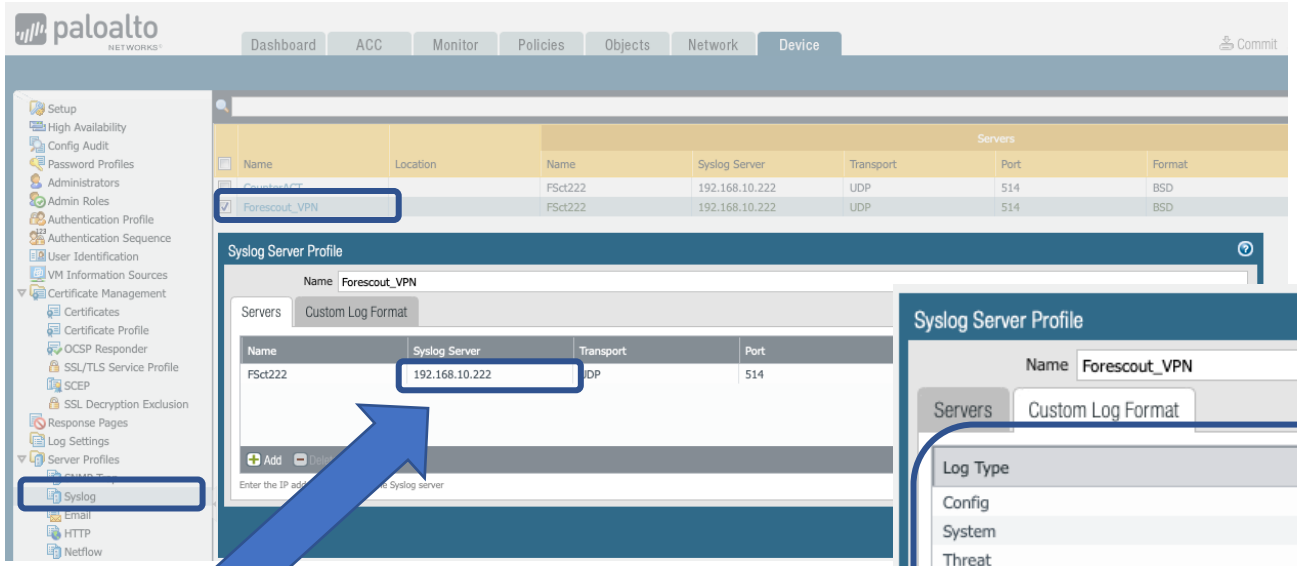
Configure Palo Alto NGFW

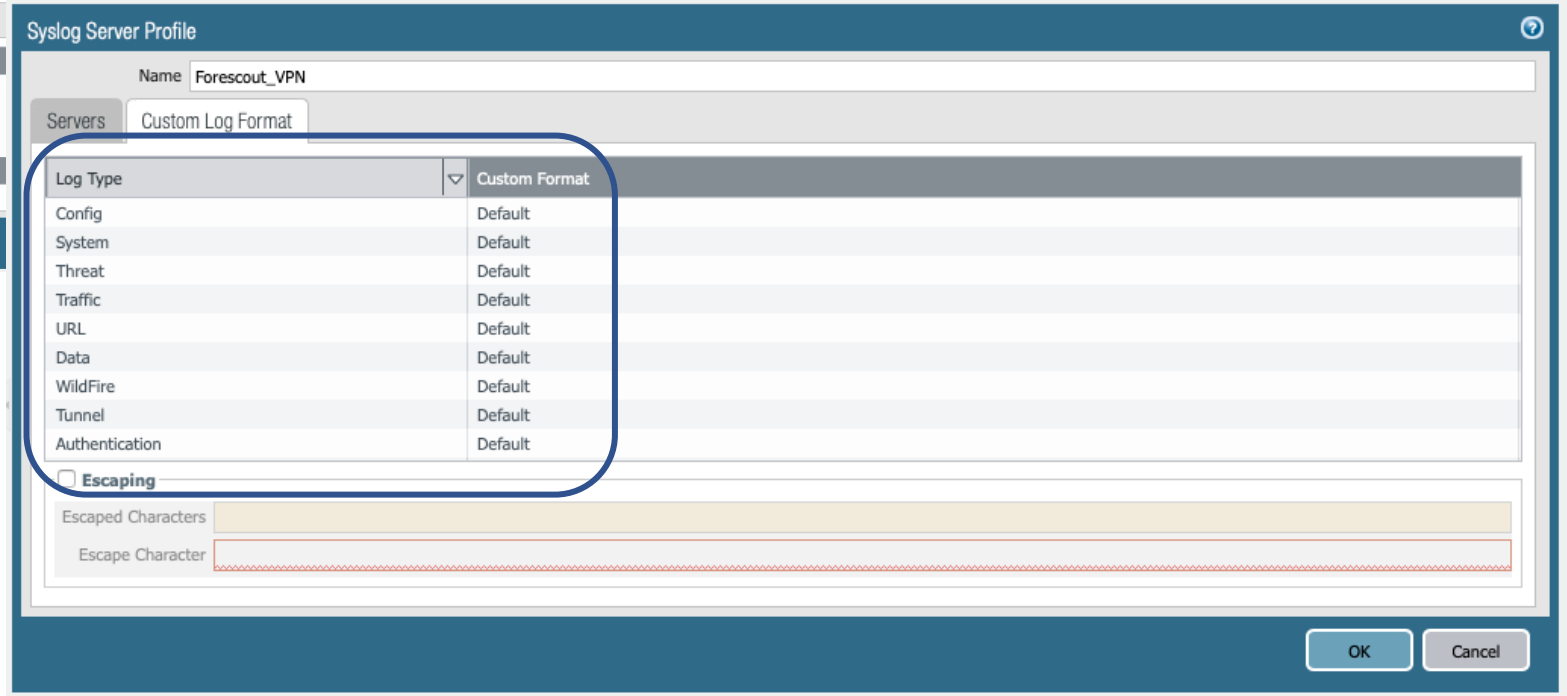
Sending Syslog Messages

STEP 1: Configure PANW Log message Profile

Palo Alto Next Generation Firewall

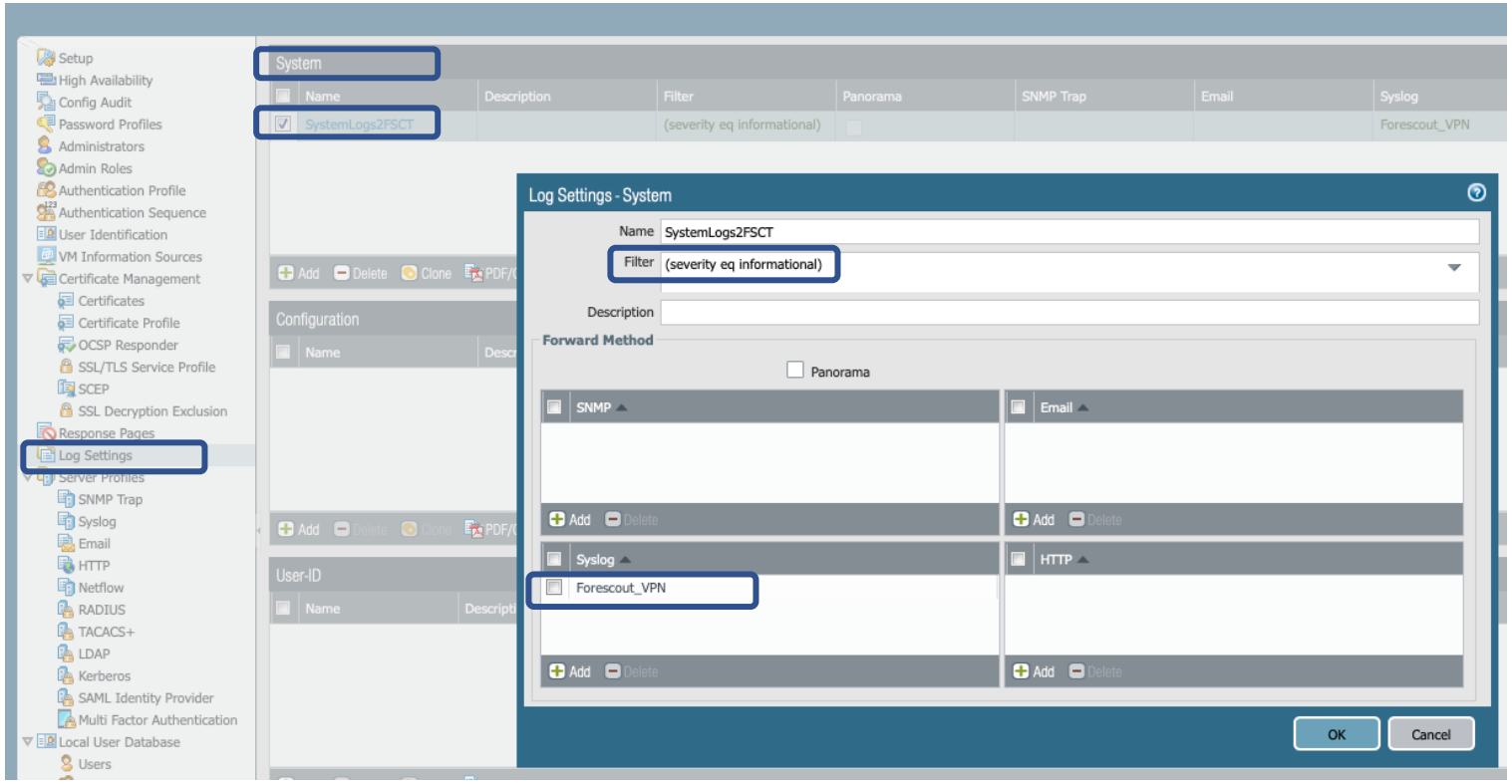


Forescout IP Address
(Syslog Destination)



STEP 2: Attach profile to System Log (Informational)

Palo Alto Next Generation Firewall



Configure Forescout 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"
```

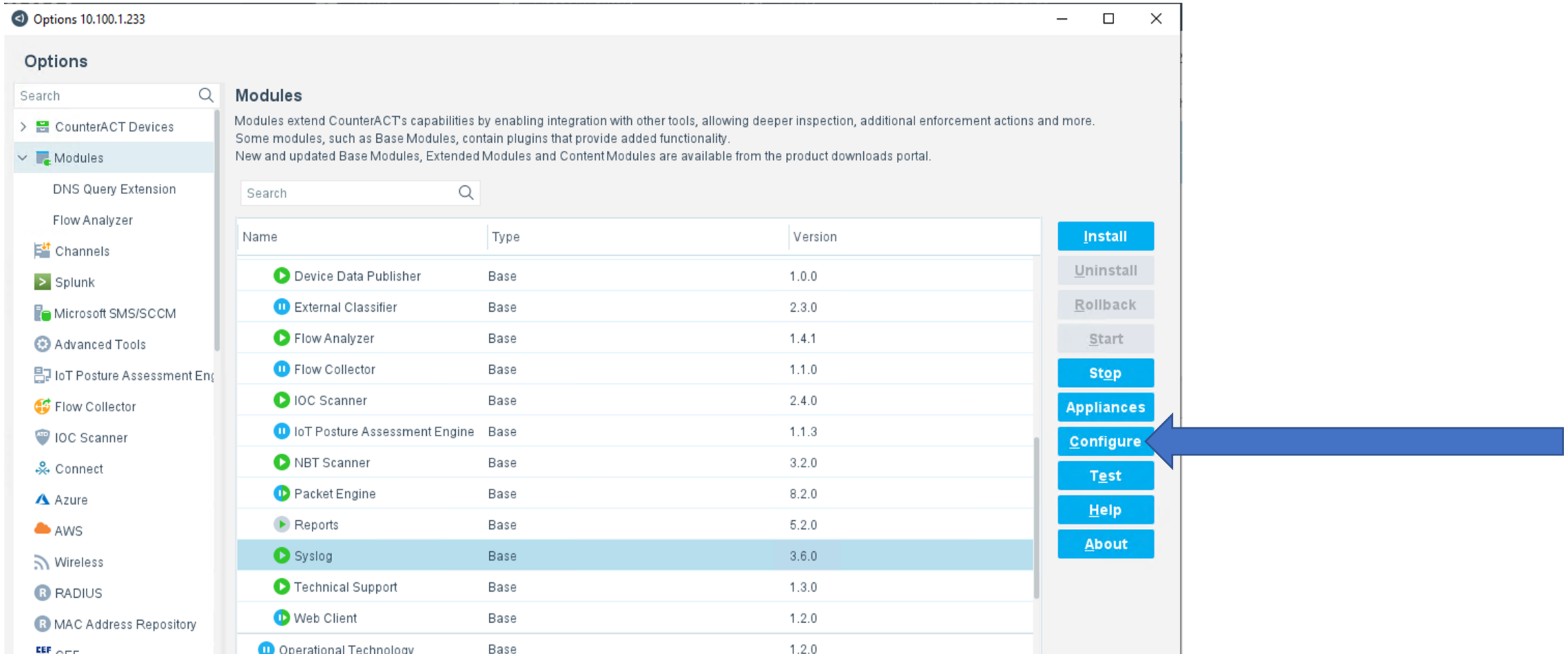
STEP 2: Restart Box

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

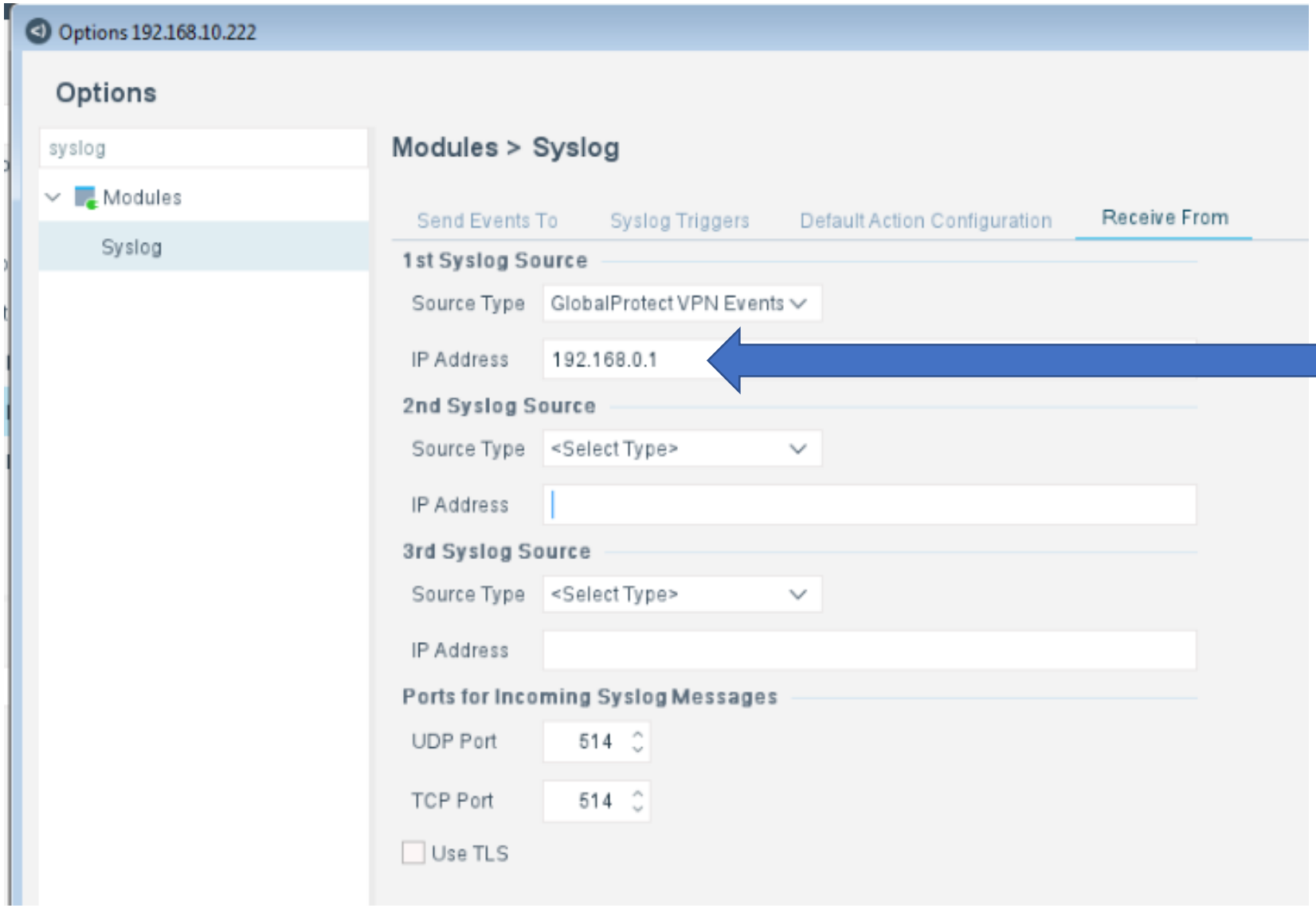
STEP 3: Wait for Box

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

STEP 4: Configure Syslog Sources



STEP 5: Configure Syslog Sources



Firewall IP Address (syslog source)

Add all FWs that have VPN connections