

AQUILA - Zyxel USG Flex 200 SIEM Integration

AQUILA - Zyxel USG Flex 200 Integration

The Zyxel USG Flex 200 is a unified security gateway that provides comprehensive network security and management capabilities. It generates syslog events that can be collected, analyzed, and monitored for security insights and network performance monitoring. This integration enables centralized log collection from Zyxel USG devices for visualization and analysis.

Integration Overview

This integration supports event collection through:

- Syslog messages via UDP from Zyxel USG Flex 200 devices
- File-based log collection from configured syslog servers

Events can be searched, observed, and visualized for security monitoring and network analysis.

Compatibility

- Supports syslog event collection from Zyxel USG Flex 200 devices via UDP on port 514
 - Requires syslog-ng service for log collection and filtering
 - Compatible with Linux-based log collection servers
-

Syslog Server Configuration

Installing Syslog-ng:

Install the syslog-ng package on your log collection server:

```
sudo apt-get install syslog-ng
```

```
cytarb@cytarb-international:~$ sudo apt-get install syslog-ng
```

Configuring Syslog-ng:

Edit the syslog-ng configuration file:

```
sudo nano /etc/syslog-ng/syslog-ng.conf
```

```
cytarb@cytarb-international:~$ sudo nano /etc/syslog-ng/syslog-ng.conf
[sudo] password for cytarb: 
```

Add the following configuration blocks:

Define the syslog source to listen for UDP traffic on IP address **<IP_Address_of_Log_Source_Server>** and port 514:

Replace **<IP_Address_of_Log_Source_Server>** to the actual IP Address of Syslog-ng Server:

```
source s_net { udp(ip(<IP_Address_of_Log_Source_Server>) port(514)); };
```

Create a filter to match traffic from the Zyxel device (this filter catches all syslog messages from the Zyxel Firewall):

replace **<IP_Address_of_Zyxel_Firewall>** to the actual IP Address of Zyxel Firewall:

```
filter f_zyxel { host( "<IP_Address_of_Zyxel_Firewall>" ); };
```

Define a destination file for the syslog messages:

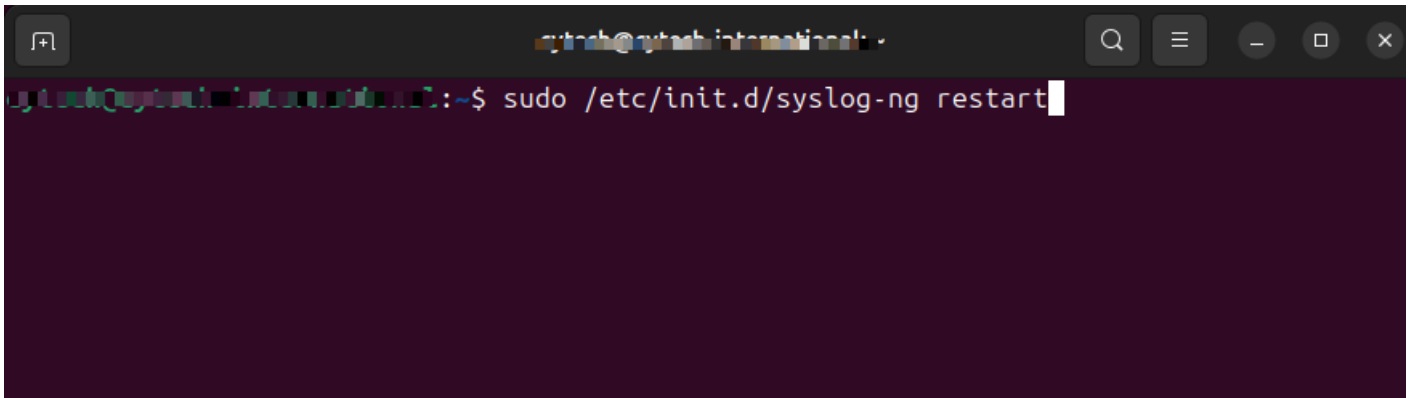
```
destination df_zyxel { file("/var/log/zyxel.log"); };
```

Bundle the source, filter, and destination rules together with a logging rule:

```
log { source ( s_net ); filter( f_zyxel ); destination ( df_zyxel ); };
```

Restart the syslog-ng service to apply changes:

```
sudo /etc/init.d/syslog-ng restart
```

A terminal window with a dark background. The prompt is 'zyxel@zyxel-international: ~'. The command 'sudo /etc/init.d/syslog-ng restart' has been entered and is followed by a cursor. The window title bar shows search, menu, and window control icons.

Full code snippet:

```
source s_net { udp(ip(<IP_Address_of_Log_Source_Server>) port(514)); };  
filter f_zyxel { host( "<IP_Address_of_Zyxel_Firewall>" ); };  
destination df_zyxel { file("/var/log/zyxel.log"); };  
log { source ( s_net ); filter( f_zyxel ); destination ( df_zyxel ); };
```

```
GNU nano 7.2 /etc/syslog-ng/syslog-ng.conf *
log { source(s_src); filter(f_debug); destination(d_debug); };
log { source(s_src); filter(f_error); destination(d_error); };
log { source(s_src); filter(f_messages); destination(d_messages); };

log { source(s_src); filter(f_console); destination(d_console_all); destination(d_xcon
log { source(s_src); filter(f_crit); destination(d_console); };

source s_net { udp(ip(102.160.20.75) port(514)); };
filter f_zyxel { host( "102.160.20.1" ); };
destination df_zyxel { file("/var/log/zyxel.log"); };
log { source ( s_net ); filter( f_zyxel ); destination ( df_zyxel ); };

# All messages send to a remote site
#
#log { source(s_src); destination(d_net); };

###
# Include all config files in /etc/syslog-ng/conf.d/
###

^G Help      ^O Write Out  ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File  ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

Zyxel USG Flex 200 Device Configuration

Follow these steps to configure the Zyxel USG Flex 200 to send syslog messages to your log collection server:

Step 1: Log in to the Zyxel USG Flex 200 Firewall web interface.

Step 2: Navigate to **Configuration > Log & Report > Log Settings > Remote Server 4**.

Step 3: Click **Edit** to configure the remote log server settings.

Log Settings

Log Settings

Edit
 Activate
 Inactivate

#	Status	Name	Log Format
1	<input type="checkbox"/>	System Log	Internal
2	<input type="checkbox"/>	System Log	Internal
3	<input type="checkbox"/>	USB Storage	Internal
4	<input type="checkbox"/>	Remote Server 1	Syslog
5	<input type="checkbox"/>	Remote Server 2	Syslog
6	<input type="checkbox"/>	Remote Server 3	Syslog
7	<input checked="" type="checkbox"/>	Remote Server 4	CEF/Syslog

Step 4: Configure the following log settings for Remote Server:

- **Active:** Check the box to enable remote logging
- **Log Format:** Select **CEF/Syslog** from the dropdown menu
- **Server Address:** Enter the IP address of your syslog-ng server
- **Server Port:** Enter **514**
- **Log Facility:** Select any available facility from the dropdown menu

Edit log Category Setting - Remote Server 4 ?

Log Settings for Remote Server

Active

Log Format: (Server Name or IP Address)

Server Address:

Server Port:

Log Facility:

Active Log

Log Category +	Selection		
	disable	normal	debug
<input checked="" type="checkbox"/> Authenticate	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> BWM	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> File Manager	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> Hotspot	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> License	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> Log & Report	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> Network	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> Security	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> System	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

OK **Cancel**

Step 5: Click **Apply** or **Save** to apply the configuration changes.

Step 6: Verify that syslog messages are being sent to the remote server by checking the log file on your Syslog server:

```
sudo tail -f /var/log/zyxel.log
```

```
root@zyxel-internal:~$ sudo tail -f /var/log/zyxel.log
[sudo] password for root:
Jan 24 01:26:14 10.0.0.1 CEF:0|ZyXEL|USG FLEX 200|5.39(ABUI.1)|0|Traffic Log|4|devI
D=d0c0c57ed010 src=10.100.100.10 dst=50.50.50.102 spt=50001 dpt=100 dvchost=usgflex20
0 msg=Traffic Log cat=Traffic Log sourceTranslatedAddress=10.100.100.102 sourceTranslat
edPort=10001 suser=unknown ZYduration=5 out=2927 in=988 proto=6 app=https ZYnote=Traffi
c Log ZYdir=RND:EASTERN-2 deviceInboundInterface=RND deviceOutboundInterface=EASTERN-2
ZYmac=10.00.00.07.07.00
Jan 24 01:26:14 10.0.0.1 CEF:0|ZyXEL|USG FLEX 200|5.39(ABUI.1)|0|Traffic Log|4|devI
D=d0c0c57ed010 src=10.100.100.10 dst=10.100.100.10 spt=10013 dpt=1000 dvchost=usgflex
200 msg=Traffic Log cat=Traffic Log destinationTranslatedAddress=10.100.100.102 destina
tionTranslatedPort=10001 suser=unknown ZYduration=10 out=752 in=10271 proto=6 app=others
ZYnote=Traffic Log ZYdir=EASTERN-2:RND deviceInboundInterface=EASTERN-2 deviceOutbound
Interface=RND ZYmac=10.00.00.07.07.00
Jan 24 01:26:14 10.0.0.1 CEF:0|ZyXEL|USG FLEX 200|5.39(ABUI.1)|0|Traffic Log|4|devI
D=d0c0c57ed010 src=10.100.100.10 dst=10.100.100.10 spt=10013 dpt=1000 dvchost=usgflex200
msg=Traffic Log cat=Traffic Log sourceTranslatedAddress=10.100.100.102 sourceTranslated
Port=10001 suser=unknown ZYduration=14 out=3730 in=6960 proto=6 app=https ZYnote=Traffi
c Log ZYdir=RND:EASTERN-2 deviceInboundInterface=RND deviceOutboundInterface=EASTERN-2
ZYmac=10.00.00.07.07.00
```

Log Rotation Configuration

To manage log file sizes and prevent disk space issues, configure log rotation for Zyxel logs.

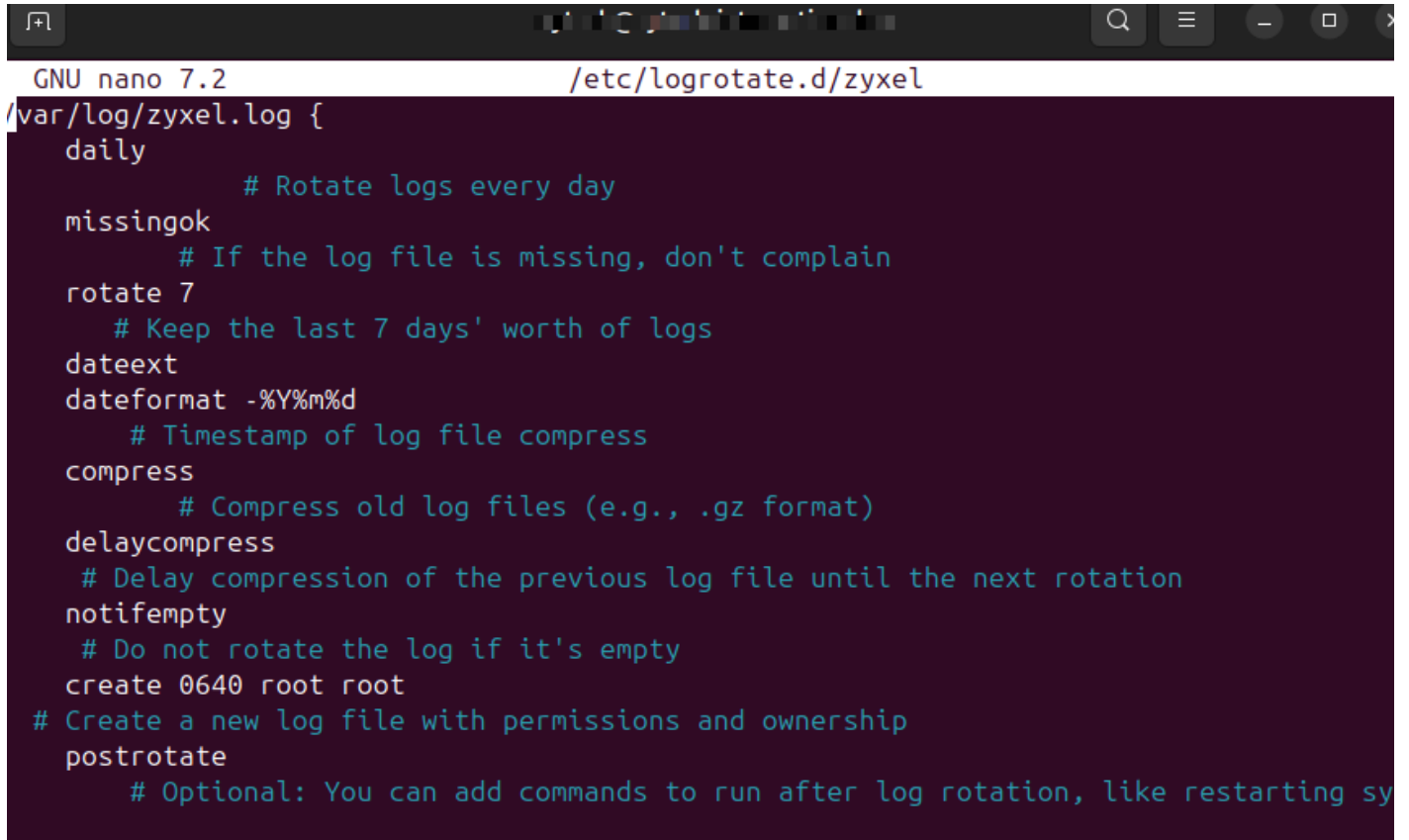
Create a logrotate configuration file:

```
sudo nano /etc/logrotate.d/zyxel
```

Paste the following configuration to the file:

```
/var/log/zyxel.log {
    daily                # Rotate logs every day
    missingok            # If the log file is missing, don't complain
    rotate 7             # Keep the last 7 days' worth of logs
    compress              # Compress old log files (e.g., .gz format)
    delaycompress        # Delay compression of the previous log file until the next rotation
    notifempty           # Do not rotate the log if it's empty
    create 0640 root root # Create a new log file with permissions and ownership
    postrotate
        # Optional: You can add commands to run after log rotation, like restarting syslog
        # For example, to reload syslog:
        # /etc/init.d/syslog-ng reload
        # Or for rsyslog:
```

```
# systemctl reload rsyslog
endscript
}
```



```
GNU nano 7.2 /etc/logrotate.d/zyxel
/var/log/zyxel.log {
    daily
        # Rotate logs every day
    missingok
        # If the log file is missing, don't complain
    rotate 7
        # Keep the last 7 days' worth of logs
    dateext
    dateformat -%Y%m%d
        # Timestamp of log file compress
    compress
        # Compress old log files (e.g., .gz format)
    delaycompress
        # Delay compression of the previous log file until the next rotation
    notifempty
        # Do not rotate the log if it's empty
    create 0640 root root
# Create a new log file with permissions and ownership
    postrotate
        # Optional: You can add commands to run after log rotation, like restarting sy
```

Testing Log Rotation:

To verify the log rotation configuration is working correctly:

```
sudo logrotate --debug /etc/logrotate.d/zyxel
```

```
root@zyxel:~$ sudo logrotate --debug /etc/logrotate.d/zyxel
warning: logrotate in debug mode does nothing except printing debug messages! Consider
using verbose mode (-v) instead if this is not what you want.

reading config file /etc/logrotate.d/zyxel
error: /etc/logrotate.d/zyxel:9 lines must begin with a keyword or a filename (possibly
in double quotes)
error: found error in /var/log/zyxel.log , skipping
removing last 1 log configs
Reading state from file: /var/lib/logrotate/status
Allocating hash table for state file, size 64 entries
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
```

Log Events

Here are the types of events you might find in the event log of a Zyxel UFG Flex 200, categorized by their typical nature:

- **System Events:**
 - **Boot Events:** Records when the device starts up, restarts, or shuts down.
 - Example: "Device started successfully" or "Reboot initiated."
 - **Configuration Changes:** Logs any changes to the system configuration, such as updates to firmware or network settings.
 - Example: "Configuration changed by user admin" or "Firmware updated."
 - **Service Events:** Events related to system services starting or stopping, like the DHCP service, VPN service, etc.
 - Example: "VPN service started" or "DHCP service stopped unexpectedly."
- **Network Events:**
 - **Connection Events:** Logs events related to device connections, such as establishing or dropping a connection with other network devices.
 - Example: "WAN interface up" or "LAN interface down."
 - **Traffic Logs:** Logs traffic-related information, such as the amount of data sent or received.
 - Example: "Incoming traffic exceeded threshold" or "Traffic dropped due to policy."

- **Security Events:**
 - **Authentication and Authorization Events:** Logs successful or failed login attempts, user authentications, or permissions changes.
 - Example: "User login from IP address 192.168.1.5" or "Failed login attempt from IP 10.0.0.1."
 - **Firewall or Intrusion Detection Logs:** Captures security-related incidents like firewall rule violations, intrusion attempts, or malware alerts.
 - Example: "Firewall rule blocked access from external IP" or "Intrusion detection alert triggered."
 - **VPN Events:** Logs VPN connections, including successful connections, disconnections, or errors.
 - Example: "VPN tunnel established" or "VPN authentication failure."
- **Error Events:**
 - **Hardware or Software Failures:** Captures any critical failures of the system's hardware or software components.
 - Example: "Memory allocation failure" or "Disk error on storage device."
 - **Network Failures:** Logs when the network encounters issues, such as a dropped connection or misconfiguration.
 - Example: "Lost connection to ISP" or "Network interface error."
- **Warning Events:**
 - **Thresholds and Limits:** Logs warnings when system performance reaches a threshold or limit.
 - Example: "CPU usage exceeded 80%" or "Disk space running low."
 - **Potential Security Risks:** Alerts about actions that might pose a security risk.
 - Example: "Multiple failed login attempts detected" or "Suspicious packet detected."
- **Informational Events:**
 - **Status Updates:** Logs general information about the device's operational status.
 - Example: "Device configuration completed" or "Service started successfully."
 - **Routine Operations:** Logs that provide context to everyday network activity.
 - Example: "DHCP lease granted to 192.168.1.10" or "Client connected via wireless."

Logs Dataset

The zyxel.log dataset contains events collected from the configured syslog-ng server. All Zyxel USG Flex 200 specific syslog fields are available under the /var/log/zyxel.log file for detailed analysis and security monitoring.

sample data logs:

```
Jan 19 18:45:26 192.168.20.1 CEF:0|ZyXEL|USG FLEX 200|5.39(ABUI.1)|0|Traffic
Log|4|devID=d8xxxxx40 src=1xx.1xx.xx.xx dst=4xx.xxx.2xxx.xxx spt=62126 dpt=123
dvchost=usgflex200 msg=Traffic Log cat=Traffic Log sourceTranslatedAddress=1xx.xx.xxxx.xxxx
sourceTranslatedPort=6xxxxx6 suser=unknown ZYduration=300 out=76 in=76 proto=17 app=others
```

ZYnote=Traffic Log ZYdir=RND:EASTERN-2 deviceInboundInterface=RND
deviceOutboundInterface=EASTERN-2 ZYmac=xx:xx:xx:xx:xx:24

If you need further assistance, kindly contact our support at support@cytechint.com for prompt assistance and guidance.

Revision #4

Created 20 January 2026 08:43:39 by Benjie Janlay Jr.

Updated 17 March 2026 22:28:46 by Benjie Janlay Jr.