FortiGate Firewall - Syslog Configuration for Log Integration & Security Configuration Recommendations Introduction

Introduction

The FortiGate integration enables to monitor your Fortinet FortiGate firewall for security threats, traffic analysis, and compliance reporting. Currently, we are not receiving logs from your firewall. This guide will help you configure syslog to send logs to our monitoring system.

Step 1: Log in to your Fortinet FortiGate Admin Portal and Navigate to CLI Console

Log in to your FortiGate web interface and access the CLI Console. Please refer to the images below.

1. Open your web browser and go to: `https://[your-firewall-ip-address]`
2. Click on your **username** in the top-right corner
3. Select **CLI Console** from the dropdown menu

Step 2: Required Information for Integration

To configure FortiGate to send logs to your syslog server, we need the following information from you:

Provide:

```
FortiGate Source IP (Management IP): _____________________________
Log Collector IP (Where FortiGate sends logs to): _____________________________
FortiGate Model: _____________________________
Firmware Version: _____________________________
```

To get the FortiGate information, run these commands in CLI:

```
get system status
get system interface physical
```

Step 3: Execute Configuration Commands

Execute these commands on the CLI Console:

For Syslog Setting:

```
config log syslogd setting
    set status enable
    set server <Address of remote syslog server>
    set facility user
    set source-ip <Source IP address of syslog>
    set port 10514
    set mode tcp
    set format default
end
```

What each setting does:

- `set status enable` = Turns on syslog functionality
- `set server` = IP address of your log collector (where FortiGate sends logs to)
- `set facility user` = Categories logs as "user" type
- `set source-ip` = FortiGate's management IP address
- `set port 10514` = Destination port for log transmission
- `set mode tcp` = Uses TCP protocol (reliable delivery, no packet loss)
- `set format default` = Uses standard syslog format (compatible with Elastic integration)

Example with actual values:

```
config log syslogd setting
    set status enable
    set server 192.168.10.50
    set facility user
    set source-ip 192.168.1.99
    set port 10514
    set mode tcp
    set format default
end
```

Note:

- Use own log collector IP for `set server`
- Use FortiGate management IP for `set source-ip`
- We recommend using port **10514** if port **514** is already in use

For Syslog Filter:

```
config log syslogd filter
    set anomaly enable
    set forward-traffic enable
    set local-traffic enable
    set multicast-traffic disable
    set netscan-discovery enable
    set netscan-vulnerability enable
    set severity warning
    set sniffer-traffic enable
    set voip disable
    set ztna-traffic enable
end
```

This configuration enables logging for:

- **Anomaly events** – Unusual network behavior
- **Forward traffic** – Traffic passing through the firewall
- **Local traffic** – Traffic to/from the firewall itself
- **Network scanning** – Port scans and vulnerability scans
- **Sniffer traffic** – Packet capture events
- **ZTNA traffic** – Zero Trust Network Access events

Step 4: Network Firewall Configuration Requirements

IMPORTANT: Please ensure the following network connectivity is allowed:

On your FortiGate device:

- Allow **OUTBOUND** traffic from FortiGate to your log collector
- **Port:** 10514
- **Protocol:** TCP

On your Log Collector server:

- Allow **INBOUND** traffic from FortiGate
- **Port:** 10514
- **Protocol:** TCP

Network Path:

- Ensure no firewall or network device between your FortiGate is blocking TCP port 10514
- Verify your FortiGate can reach the log collector IP address

Step 5: Verify Configuration

After executing the commands, verify the configuration by running:

To verify Syslog Setting:

```
show log syslogd setting
```

Expected output should show:

```
status: enable
server: <Your log collector IP>
port: 10514
mode: tcp
format: default
```

To verify Syslog Filter:

```
show log syslogd filter
```

Step 6: Test Connectivity and Log Transmission

Test 1: Verify network connectivity to your log collector

```
execute ping <Log_Collector_IP>
```

This should return successful ping responses.

Test 2: Send a test log message

```
execute log test
```

This command sends a test syslog message to your log collector to verify the configuration is working.

Step 7: Enable Logging on Firewall Policies

For us to receive traffic logs, logging must be enabled on your firewall policies.

GUI Method:

1. Navigate to: **Policy & Objects** → **Firewall Policy**
2. For each policy, click to edit
3. Scroll to **Logging Options**
4. Set **Log Allowed Traffic** to: **All Sessions**

5. Click **OK**

CLI Method (to check current status):

```
show firewall policy | grep logtraffic
```

CLI Method (to enable logging on a specific policy):

```
config firewall policy
    edit <policy-id>
        set logtraffic all
    next
end
```

Verification and Information Needed

To help us verify the integration is working correctly, we would appreciate if you could provide the following:

Configuration Verification (Screenshots would be helpful):

1. ☐ Output of: `show log syslogd setting`
2. ☐ Output of: `show log syslogd filter`
3. ☐ Output of: `get system status`

Network Connectivity Test:

Please test connectivity to your log collector by running:

```
execute ping <Your_Log_Collector_IP>
```

This helps us confirm there are no network issues between your firewall and log collector.

Information for Our Integration Setup:

To complete the integration on our end, please provide:

```
FortiGate Source IP: _____________________________
Log Collector IP: _____________________________
FortiGate Model: _____________________________
Firmware Version: _____________________________
Port Number: 10514
Protocol: TCP
```

Optional (but helpful for troubleshooting):

- Is there any firewall or network device between your FortiGate and log collector? Yes / No
- Did the ping test succeed? Yes / No

What Needs for Integration

After completing the configuration and provide the screenshots above, kindly provide us:

Network Information:

- **FortiGate Source IP** (Your FortiGate management IP): _____
- **Log Collector IP** (Your log collector server IP): _____
- **Port Number**: 10514
- **Protocol**: TCP

Troubleshooting Common Issues

Issue 1: Cannot ping log collector

Possible causes:

- Network firewall blocking traffic
- Incorrect routing
- Log collector server is down

Solution:

```
# Check your default route
get router info routing-table all

# Verify interface is up
get system interface physical
```

Issue 2: Test log command shows no output

Solution:

```
# Verify syslog is enabled
show log syslogd setting | grep status

# Check if server IP is correct
show log syslogd setting | grep server
```

Issue 3: Configuration not saving

Solution:

- Ensure you typed `end` after each config block
- Verify no syntax errors in commands
- Check you have admin permissions

Reference Documentation Links

Source Link for Full Documentation Manual:
https://docs.cytechint.io/books/system-integrations/page/fortinet-fortigate-syslog-setting-and-syslog-filter

Source Link Documentation for Syslog Setting:
https://docs.fortinet.com/document/fortigate/6.4.4/cli-reference/444620/config-log-syslogd-setting

Source Link Documentation for Syslog Filter:
https://docs.fortinet.com/document/fortigate/7.0.9/cli-reference/456620/config-log-syslogd-filter
https://help.fortinet.com/fgt/handbook/cli52_html/index.html#page/FortiOS%205.2%20CLI/config_log.16.17.html

Source Link to Better Understand Log Priority Level:
https://help.fortinet.com/fweb/551/log/Content/FortiWeb/fortiweb-log/Priority_level.htm

---

FortiGate Firewall - Security Configuration Recommendations

Introduction

This document provides security recommendations for your Fortinet FortiGate firewall to strengthen network security, improve policy management, and optimize firewall configuration based on industry standards.

1. Enable Security Profiles on Firewall Policies

Risk: Without security profiles, viruses, malware, exploits, and malicious websites can pass through your firewall undetected.

Required Profiles for Internet-Bound Policies (LAN → WAN):

```
☑ Antivirus (AV) - Blocks viruses, malware, ransomware
☑ Web Filter - Blocks malicious and phishing websites
☑ Application Control - Controls which applications can be used
☑ IPS (Intrusion Prevention) - Blocks hacking attempts and exploits
```

Configuration Steps:

1. Navigate to **Policy & Objects → Firewall Policy**
2. Click on policy allowing internet access
3. Scroll to **Security Profiles** section
4. Enable profiles:
   - Antivirus: `default`
   - Web Filter: `default`
   - Application Control: `default`
   - IPS: `protect_client`
5. Click **OK**

2. Review and Optimize Firewall Policies

A) Remove Unused Policies

1. Navigate to **Policy & Objects → Firewall Policy**
2. Check **Hit Count** column (0 hits for 30+ days = unused)
3. Verify with department owners before deleting
4. Delete unused policies

B) Eliminate "Any-Any" Policies

Dangerous policies have:

- Source: `all`
- Destination: `all`
- Service: `ALL`

Action: Replace with specific rules defining exact sources, destinations, and services.

C) Implement Naming Convention

Format: `[SOURCE]-[DESTINATION]-[SERVICE]-[DESCRIPTION]`

Examples:

```
LAN-WAN-HTTPS-Employee_Internet_Access
LAN-DMZ-HTTP-Access_to_WebServer
Branch1-HQ-ALL-Site_to_Site_VPN
```

3. Configure Address Objects

A) Create Named Objects for Servers

Naming Format: `[TYPE]_[LOCATION]_[PURPOSE]`

Examples:

```
SVR_DMZ_WebServer01
SVR_HQ_DatabaseServer
NET_Branch1_LAN
HOST_Finance_Workstation
```

Steps:

1. Navigate to **Policy & Objects → Addresses**
2. Click **Create New → Address**
3. Configure:
   - Name: `SVR_DMZ_WebServer01`
   - Type: IP/Netmask
   - Subnet/IP: `10.10.10.50/32`
   - Comment: "Production web server"
4. Click **OK**

B) Create Address Groups

Example:

```
Group: GRP_Web_Servers
Members:
- SVR_DMZ_WebServer01
- SVR_DMZ_WebServer02
- SVR_DMZ_WebServer03
```

Benefit: One policy can manage multiple servers.

C) Geographic Blocking (Optional)

Block traffic from high-risk countries:

1. Navigate to **Policy & Objects → Addresses**
2. Create New → Address
3. Type: Geography
4. Select countries to block
5. Create deny policy using this object

4. Optimize Service Objects

A) Create Custom Services

Naming Format: `[PROTOCOL]_[PURPOSE]_[PORT]`

Examples:

```
TCP_Custom_App_8080
TCP_Database_MySQL_3306
TCP_Web_Application_8443
```

B) Create Service Groups

Example: Web Services

```
GRP_Web_Services:
- HTTP (80)
- HTTPS (443)
- HTTP-ALT (8080)
```

Example: Email Services

```
GRP_Email_Services:
- SMTP (25)
- SMTPS (465)
- IMAPS (993)
- POP3S (995)
```

C) Phase Out Insecure Protocols

Replace:

- Telnet → SSH
- FTP → SFTP/FTPS
- HTTP → HTTPS
- SNMPv1/v2 → SNMPv3

5. Configure NAT Policies

Source NAT (Outbound Internet)

Verify NAT is enabled on internet access policies:

1. Go to **Policy & Objects → Firewall Policy**
2. Click internet access policy (LAN → WAN)
3. NAT section:

```
☑ NAT: Enable☑ Use Outgoing Interface Address
```

Destination NAT (Inbound Services)

For published services (web, email servers):

```
Name: VIP_External_WebServerExternal IP: <Public IP>Mapped IP: <Internal Server IP>Port Forwarding: EnableProtocol: TCP
```

1. Navigate to **Policy & Objects → Virtual IPs**
2. Create New → Virtual IP
3. Configure:
4. Always enable security profiles (AV, IPS) on VIP policies

6. Secure VPN Configuration

SSL VPN (Remote Access)

Navigate to: VPN → SSL-VPN Settings

Security Settings:

```
☑ Two-Factor Authentication: Enable
Method: FortiToken, Email, or SMS

Login Attempt Limit: 5
Lockout Duration: 30 minutes

Session Timeout: 12 hours
Idle Timeout: 30 minutes

□ Split Tunneling: Disable (force all traffic through VPN)
```

IPsec VPN (Site-to-Site)

Navigate to: VPN → IPsec Tunnels

Strong Encryption:

```
Phase 1 (IKE):
- Encryption: AES256-GCM
- Authentication: SHA256
- DH Group: 14 or higher

Phase 2 (IPsec):
- Encryption: AES256-GCM
```

```
- Authentication: SHA256
- PFS: Enable (Group 14)

☑ Dead Peer Detection: Enable
Interval: 10 seconds
```

7. Administrator Security

A) Enable Two-Factor Authentication

1. Navigate to **System → Administrators**
2. Click administrator account
3. Enable Two-Factor Authentication:
   ```
   ☑ Enable Two-Factor AuthenticationMethod: FortiToken (recommended) or Email
   ```
4. Click **OK**

B) Restrict Trusted Hosts

Only allow admin login from specific IPs:

```
Trusted Host 1: 10.10.10.0/24 (IT subnet)
Trusted Host 2: 172.16.5.100/32 (VPN gateway)
```

C) Disable WAN Management

Navigate to **System → Settings**

```
WAN Interface:
□ HTTPS: Disable
□ HTTP: Disable
□ SSH: Disable
```

8. Configure Regular Backups

Manual Backup

1. Click **username** (top-right)
2. Configuration → Backup
3. Choose Local PC
4. Save as: `FortiGate_[Model]_[Date].conf`

Backup Schedule

```
Daily: Automated
Before changes: Always
Weekly: Manual verification
Monthly: Offsite storage

Retention:
- Daily: 7 days
- Weekly: 30 days
- Monthly: 1 year
```

Storage Locations

```
Primary: Local computer
Secondary: Network file server
Tertiary: Cloud storage (encrypted)
Emergency: USB drive (offsite)
```

9. Enable FortiGuard Services

Check License Status

1. Navigate to **System → FortiGuard**
2. Verify active licenses:

   ```
   ☑ Antivirus☑ IPS (Intrusion Prevention)☑ Web Filtering☑ Application Control
   ```

3. Check expiration dates (renew 30 days before)

Configure Auto-Updates

```
☑ Automatic Updates: Enable
Update Schedule: Daily
Push Update: Enable
```

10. Configure NTP (Time Synchronization)

Why Critical

Accurate timestamps required for:

- Log correlation
- Certificate validation
- Compliance

Configuration

1. Navigate to **System → Settings**
2. System Time section:

```
☑ Enable NTPSync with: FortiGuard NTP ServersTime Zone: <Your timezone>
```

Verify NTP

CLI command:

```
diagnose sys ntp status
```

Expected: `synchronized: yes`

Summary Checklist

```
Security Profiles:
□ AV, Web Filter, App Control, IPS enabled

Policy Management:
□ Unused policies removed
□ "Any-any" policies replaced
□ Naming convention implemented

Objects:
□ Address objects for servers
□ Address groups created
□ Service objects organized

NAT:
□ Source NAT configured
□ Destination NAT secured

VPN:
□ 2FA enabled
□ Strong encryption
□ Session timeouts set

Admin Security:
□ 2FA for admins
□ Trusted hosts configured
```

```
□ WAN management disabled

Maintenance:
□ Backup procedure
□ FortiGuard licenses valid
□ NTP working
```

Reference Links

FortiGate Best Practices:
https://docs.fortinet.com/document/fortigate/7.4.0/best-practices

Administration Guide:
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/

FortiGuard Services:
https://www.fortiguard.com/

Revision #1
Created 8 December 2025 23:28:02
Updated 8 December 2025 23:41:35