Create a Remote Log Source - Fortinet Security Gateway.mobile.phone

Armor Knowledge Base

Armor Knowledge Base / Armor Management Portal / Log Management

Create a Remote Log Source (Fortinet Security Gateway)

Topics Discussed

⚠ To obtain Log Relay and to configure your account for remote log collection, you must have the following AMP permissions added to your account:

- Write Virtual Machine
- Delete Log Management
- Read Log Endpoints
- Read Log Relays
- Write Log Relays
- Delete Log Relays

You can use this document to send Fortinet Security Gateway logs to Armor's Security Information & Event Management (SIEM).

Pre-Deployment Considerations

Before you begin, review the following requirements:

Log Relay

To create a remote **Log Relay**, you must already have:

- Added **Log Relay** to your account
  - To learn how to add Log Relay to your account, see Obtain Log Relay for Remote Log Collection.
- Configured the system clock

Log Relay IP Address

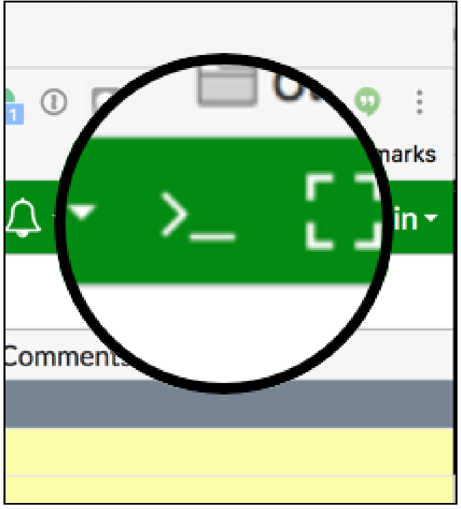
You must be able to retrieve the log relay IP address from your AMP account:

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Log & Data Management**.
3. Click **Agent Sources**.
4. Locate and select the desired log relay.
5. Click **Overview**.
6. Locate and copy the **Public IP**.

Update your Fortinet Security Gateway

1. Log into your Fortinet Security Gateway.

2. In the upper, right corner, select CLI Console.



3. Run the following commands to configure the device to send syslogs to Log Relay, which will then forward the logs to Armor.

```
fgvm1 # config log syslogd setting
fgvm1 (setting) # set status enable
fgvm1 (setting) # set format default
fgvm1 (setting) # set server <LOG_RELAY_IP_ADDRESS>
fgvm1 (setting) # set port 10073
fgvm1 (setting) # end
```

   a. To validate your current configuration, run the following command, either before or after the [fgvm1 (setting) # end] command.

```
fgvm1 # show log syslogd setting
```

> If the format was set to something other than **default**, when the [fgvm1#show log syslogd setting] command is run, the current format will be returned (e.g. cef).
>
> Within the command line, update the format command to **default** [fgvm1 (setting)#set format default].

4. Verify that logs are formatted correctly, similar to either of the following examples:

> Fortigate can send messages in multiple formats.

Example 1

```
Jul  9 14:26:58 13.47.22.124 date=2019-07-09 time=14:26:58 devname=XXX-FW1 devid=YYY logid=0000000013
type=traffic subtype=forward level=notice vd=root srcip=89.28.174.28 srcport=46796 srcintf="port9"
dstip=13.47.22.175 dstport=1639 dstintf="port11" sessionid=2232272452 proto=6 action=deny policyid=0
policytype=policy
```

Example 2

```
date=2019-07-09 time=14:26:58 devname=XXX-FW1 devid=YYY logid=0000000013 type=traffic subtype=forward
level=notice vd=root srcip=89.28.174.28 srcport=46796 srcintf="port9" dstip=13.47.22.175 dstport=1639
dstintf="port11" sessionid=2232272452 proto=6 action=deny policyid=0 policytype=policy
```

Verify Logs in AMP

In the Armor Management Portal (AMP), you can view the actual logs to confirm that the configuration was successful.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Log & Data Management**, and then select **Search**.
3. In the search field, enter the IP address or the device name.
   - For example, you can enter ***13.47.22.124* or *XXX-FW1***
   - This action will display collected FortiGate logs for that particular device.

Troubleshooting

Command Help

Within the CLI Console, you can use the question mark (?) key to display command help.

1. To display a list of available commands, press the question mark (?) key.
   - A list of the available commands will display, along with a description of each command.
2. To display a list of the options available for that command, type a command, followed by a space, then press the question mark (?) key.
   - A list of the options available for that command will display, along with a description of each option.
3. To display a list of additional options available for that command option combination, type a command, followed by an option, then press the question mark (?).
   - A list of additional options available for that command option combination will display, along with a description of each option.

Example Output

```
show system interface ?
```

Additional Documentation

For more information on using CLI, click here.

Was this helpful?

Your Rating:

☆☆☆☆☆

Results:

★★★☆☆

1 rates