Configure Fortigate SIEM Integration

Section 1: Create a Firewall Rule on your Utility Agent

1. From the Utility Host – open the Run command and enter the following command **wf.msc** or open the control panel and navigate to the firewall settings page
   mceclip1.png
   Image not found or type unknown

   Linux can be used as a utility agent, Ubunut 20.04 and 22.04 are the currently supported versions.
2. Select **Inbound Rules** on the right side
3. Right-click and select **New Rule**
   mceclip2.png
   Image not found or type unknown

4. Select **Custom**
5. Click **Next**
   mceclip3.png
   Image not found or type unknown

6. Select **All Programs**
7. Click **Next**
   mceclip4.png
   Image not found or type unknown

8. Use the following settings:
   - Protocol Type: UDP
   - Local Port: 514
9. Click **Next**
   mceclip0.png
   Image not found or type unknown

10. Under the "Which remote IP addresses does this rule apply to?" section, select **These IP Addresses**

11. Click **Add**
    mceclip6.png
    Image not found or type unknown

12. If the utility agent resides on the same LAN as the Firewall, enter the **LAN IP of the Fortinet device**. If the utility agent is on a different subnet than the Firewall, enter the **Public IP of the Fortinet device** that is sending logs under the **This IP address or subnet** field.
    mceclip1.png
    Image not found or type unknown

13. You'll be brought back to the Scope screen, click **Next**
14. On the Action screen, select **Allow the connection**, then click **Next**
    mceclip8.png
    Image not found or type unknown

15. On the Profile screen, ensure **Domain**, **Private**, and **Guest** are selected, then click **Next**
    mceclip9.png
    Image not found or type unknown

16. Give the Firewall rule a **name** and **description**, then click **Finish**
    mceclip10.png
    Image not found or type unknown

Section 2a (Legacy): Configure Fortinet to Forward Logs

1. Log in to the Fortinet console
2. Select **Log & Report** Menu Option on the left
3. Select **Log Settings**
   mceclip2.png
   Image not found or type unknown

4. Enable **Send logs to syslog**
5. Enter the **LAN IP of the Utility Agent**
   mceclip3.png
   Image not found or type unknown

6. **Save** your configuration

Section 2b (FortiOS v5.x+): Configure Fortinet to Forward Logs

1. Open the CLI
2. Find a syslogd setting that is not in use:

   ```
   config log {syslogd | syslogd2 | syslogd3 | syslogd4} setting
   show
   end
   ```

   Note: One of the options within the brackets should be selected and entered without the brackets.

3. Configure the desired syslogd setting:

   ```
   config log syslogd setting
   ```

   Note: Change syslogd to the one you determined to use in step 2.

4. ```
   set mode udp
   set server "LAN IP of Utility Agent"
   set port 514
   set facility user
   set source-ip "LAN IP of FW"
   set format default
   set priority default
   set max-log-rate 0
   set interface-select-method auto
   ```

5. use command `config log syslogd filter` and then `set severity <severity level>` to change the severity level of the logs being ingested. Setting to level Warning and above is probably best. Fortinet article that shows the logging levels.
6. Confirm settings:

   ```
   show full
   end
   ```

Section 3: Todyl Portal

Configure the integration within the Todyl Portal with the following settings:

- **UDP Host:** 0.0.0.0
- **UDP Port:** 514

fortinet_last_photo.jpg

Revision #1
Created 18 October 2024 19:27:44 by ColtM
Updated 18 October 2024 19:34:01 by ColtM
   ```