FORTINET FORTIGATE AND FIREMON
FORTINET FORTIGATE AND FIREMON

Overview .................................................. 3
Deployment Prerequisites ............................... 3
Architecture Overview ................................... 3
FireMon Configuration .................................... 4
Fortinet Configuration ................................. 8
Summary .................................................... 13
OVERVIEW

The FireMon Security Manager Core Platform provides detailed, customizable IT risk analytics that allow network and security management to respond quickly to changing business demands and ensure protection, with real-time assessment of policy enforcement spanning from the specific rules and configurations of every individual device to the combined effectiveness of all defenses.

Fortinet (NASDAQ:FTNT) is a global provider of high-performance network security and specialized security solutions that provide our customers with the power to protect and control their IT infrastructure. Our purpose-built, integrated security technologies, combined with our FortiGuard security intelligence services, provide the high performance and complete content protection our customers need to stay abreast of a constantly evolving threat landscape.

The Fortinet Security Fabric brings together all components in your network. It is Broad, Powerful and Automated. In addition to Fortinet products, the Security Fabric also integrates with 3rd Party partners to extend the power of the Security Fabric to other parts of an organization. For more information regarding our Security Fabric Partners, please refer our Technology Alliances here: https://www.fortinet.com/partners/partnerships/alliance-partners.html

DEPLOYMENT PREREQUISITES

1. Fortinet FortiGate version 4.x or newer
2. FireMon FMOS version 8.15.x or newer

ARCHITECTURE OVERVIEW
**FIREMON CONFIGURATION**

From the Administration Screen click Device

![Device Configuration Diagram](image)

From the Devices Screen click Create > Fortinet

Choose Fortigate Firewall or Fortigate Firewall VDOM if your deployment has VDOMs

For VDOMs be sure to input the correct VDOM name in the device property section
Under General Properties give the device a name and enter the IP Address

Under Device Settings enter the password for the Admin user then re-enter the password

Click Save when done

Please note the Admin user will need to be configured with the super_admin profile on the FortiGate
The next screen should look like this

If you plan on using Policy Optimizer make sure to check the box to enable the License

Then go to Workflow

Under Policy Planner click Create > Access Request
Give it a Name then click Save

The Workflow screen should now look like the image below

Do the same for the Policy Optimizer configuration

**Note**: if adding FortiGate Firewalls via FortiManager do this from Devices > Management Stations.

The Admin user will need access to all VDOMs enabled
FORTINET CONFIGURATION

Ensure all Firewall rules are set to Log All Sessions

If not, enable this for each rule under Logging Options

Configure FortiGate to send Syslog to the FireMon IP address

Under Log & Report click Log Settings
Enable Send Logs to Syslog
Enter the IP Address or FQDN of the FireMon server
Select the desired Log Settings
Click Save

**Note:** If the primary Syslog is already configured you can use the CLI to configure additional Syslog servers

```
FortiGate-ESX2 # config log syslogd2 setting
FortiGate-ESX2 (setting) # set status enable
FortiGate-ESX2 (setting) # set server 1.2.3.4
FortiGate-ESX2 (setting) # end
```

The configuration is now complete

Go back to the Devices screen in the FireMon interface

It should look like the image below once logs are received and the configuration has been retrieved

You can initiate a manual retrieval of the configuration by clicking the box on the far right
Security Manager Dashboard views
Security Manager Policy views
Security Manager Security & Compliance views
SUMMARY

FireMon helps keep Fortinet firewalls running smoothly with a complete configuration management solution, including full support for the Fortigate line of network security platforms and appliances. FireMon monitors each appliance, capturing event and traffic logs in real time. All change events trigger a full configuration capture including detailed change history and a full audit trail of operations. Fortinet devices can be monitored directly or indirectly if another event collection system is in place.

Solution Guide: [https://www.fortinet.com/content/dam/fortinet/assets/alliances/firemon-integration-brief-for-fortinet.pdf](https://www.fortinet.com/content/dam/fortinet/assets/alliances/firemon-integration-brief-for-fortinet.pdf)