

## Fortinet Security Fabric:

### Physical Topology:

The full Security Fabric topology can be viewed on the root FortiGate. Downstream FortiGate devices' topology views do not include upstream devices. The Physical Topology shows the physical structure of your network, including all connected devices and the connections between them.

### Logical Topology:

The Logical Topology shows information about the interfaces that connect devices to the Security Fabric. It shows the network interfaces, logical or physical, that are used to connect devices in the Security Fabric. The size of the bubbles in the topology vary based on traffic volume.

### Security Rating:

The security rating uses real-time monitoring to analyze your Security Fabric deployment, identify potential vulnerabilities, highlight best practices that can be used to improve the security and performance of your network, and calculate Security Fabric scores.









The Security Rating page is separated into three major scorecards: **Security Posture**, **Fabric Coverage**, and **Optimization**, which provide an executive summary of the three largest areas of security focus in the Security Fabric.

### Security Fabric Score:

The Security Fabric score is calculated when a security rating check is run, based on the severity level of the checks that are passed or failed. A higher scores represents a more secure network. Points are added for passed checks and removed for failed checks.

### Asset Identity Center:

The Asset Identity Center page unifies information from detected addresses, devices, and users into a single page, while building a data structure to store the user and device information in the backend. Asset view groups information by Device, while Identity view groups information by User. Hover over a device or a user in the GUI to perform different actions relevant to the object, such as adding a firewall device address, adding an IP address, banning the IP, quarantining the host, and more.

Device	Software OS	Hardware	Status
 <u>50:00:00:08:00:01</u>	FortiManager OS	Fortinet / FortiManager / VM	 Online
 FortiGate-VM64-KVM	FortiOS	Fortinet / FortiGate / VM64-KVM	 Online
 <u>50:00:00:0d:00:01</u>	Other identified device	Other identified device	 Offline
 <u>DESKTOP-W10</u>	Windows	Other identified device	 Offline