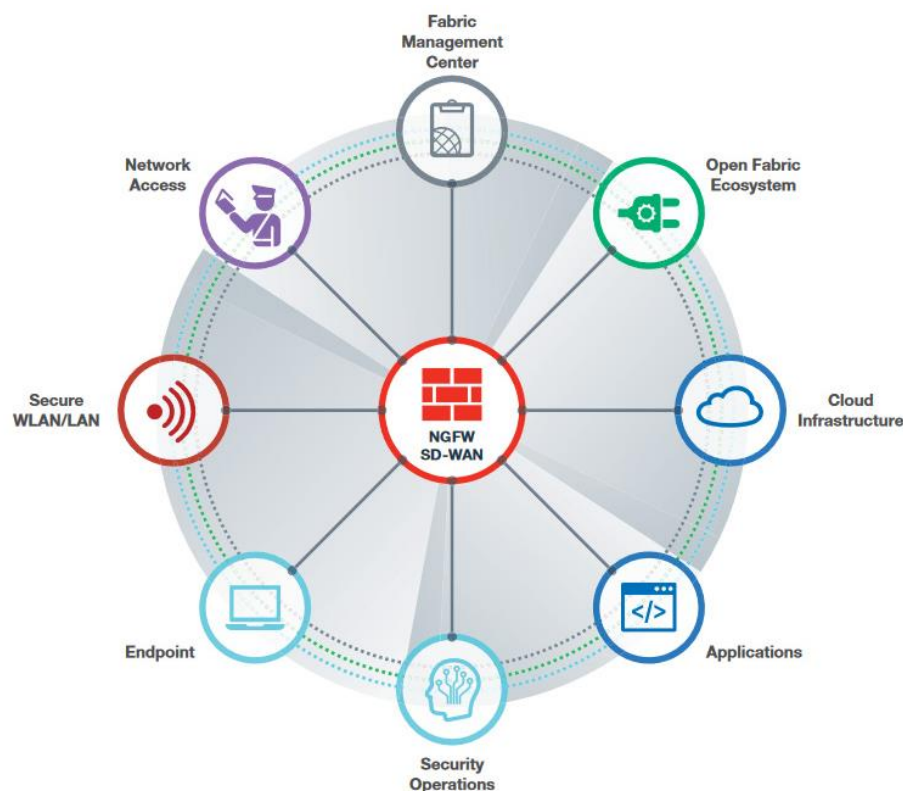


Fortinet Security Fabric:

It's an integrated solution allowing you to see, manage, and secure your network products in one place. Fortinet's Security Fabric protects the entire infrastructure end-to-end without compromising performance to deliver a broad, integrated, and automated security solution. It delivers broad protection and visibility into every network segment and device, be they hardware, virtual, or cloud based. The physical topology view shows all connected devices, including access layer devices. The logical topology view shows information about the interfaces that each device is connected to. Security rating checks analyze the Security Fabric deployment to identify potential vulnerabilities and highlight best practices to improve the network configuration, deploy new hardware and software, and increase visibility and control of the network. The FortiGates must be operating in NAT mode. The Fortinet Security Fabric, built on the FortiOS network operating system, enables multiple security technologies to work seamlessly together, across all environments and is supported by a single source of threat intelligence. This eliminates security gaps in the network and hastens responses to attacks and breaches.



Topology Views, Security Rating, External Connections, Centralized Updated, Centralized Objects creation, one place Synchronization and many more.

Fortinet Security Fabric:

Fortinet Security Fabric is made up of different security tools that work together to defend your network. These tools include things like firewalls, antivirus programs, and other security features. They talk to each other and share information, like a team communicating to stop attacks. Fortinet Security Fabric collaborate to detect and stop the threat. They work as a team, making it harder for the bad guys to get through.

The Fortinet Security Fabric spans across an entire network linking different security sensors and tools together to collect, coordinate, and respond to malicious behavior in real time. Security Fabric can be used to coordinate the behavior of different Fortinet products in your network, including FortiGate, FortiAnalyzer, FortiClient, FortiSandbox, FortiAP, FortiSwitch, and FortiClient Enterprise Management Server (EMS).

Root:

the Root FortiGate in the Security Fabric. This FortiGate is named “Edge” because it’s the only FortiGate that directly connects to the Internet. This role is also known as the gateway FortiGate. In the Security Fabric, Edge is the root FortiGate. This FortiGate receives information from the other FortiGates in the Security Fabric. Set Administrative Access to allow FortiTelemetry, which is required so that FortiGate devices in the Security Fabric can communicate with each other. From the root FortiGate, you can see information about the entire Security Fabric on the Physical and Logical Topology pages in the GUI.

Downstream:

After a root FortiGate is installed, all other FortiGate devices in the Security Fabric act as Internal Segmentation Firewalls (ISFWs), located at strategic points in your internal network, rather than on the network edge. ISFW FortiGate devices create network visibility by sending traffic and information about the devices that are connected to them to the root FortiGate.

FortiAnalyzer:

Configure a Fortinet Security Fabric that consists of FortiGate devices and a FortiAnalyzer. FortiAnalyzer gives you increased visibility into your network, centralized monitoring, and awareness of threats, events, and network activity by collecting and correlating logs from all Security Fabric devices. This gives you a deeper and more comprehensive view across the entire Security Fabric.

FortiManager:

Add FortiManager to simplify the network management of devices in the Security Fabric by centralizing management access in a single device. This allows you to easily control deployment of security policies, FortiGuard content security updates, firmware revisions, and individual configurations for devices in the Security Fabric.

In our topology HQ-FW will play the role of Root FortiGate, while FW1, BR-FW and DC-FW will play role of Downstream devices. Also, we FortiManager and FortiAnalyzer as well for centralize management and monitoring.

