

Fortinet Enterprise Firewall:

Whether you need to deploy a **High Performance Data Center Firewall**, an Enterprise **Next Generation Firewall** or a smaller **UTM device** for your Distributed Enterprise site or small business, there is a FortiGate physical or virtual appliance to fit your unique Network Security requirements.

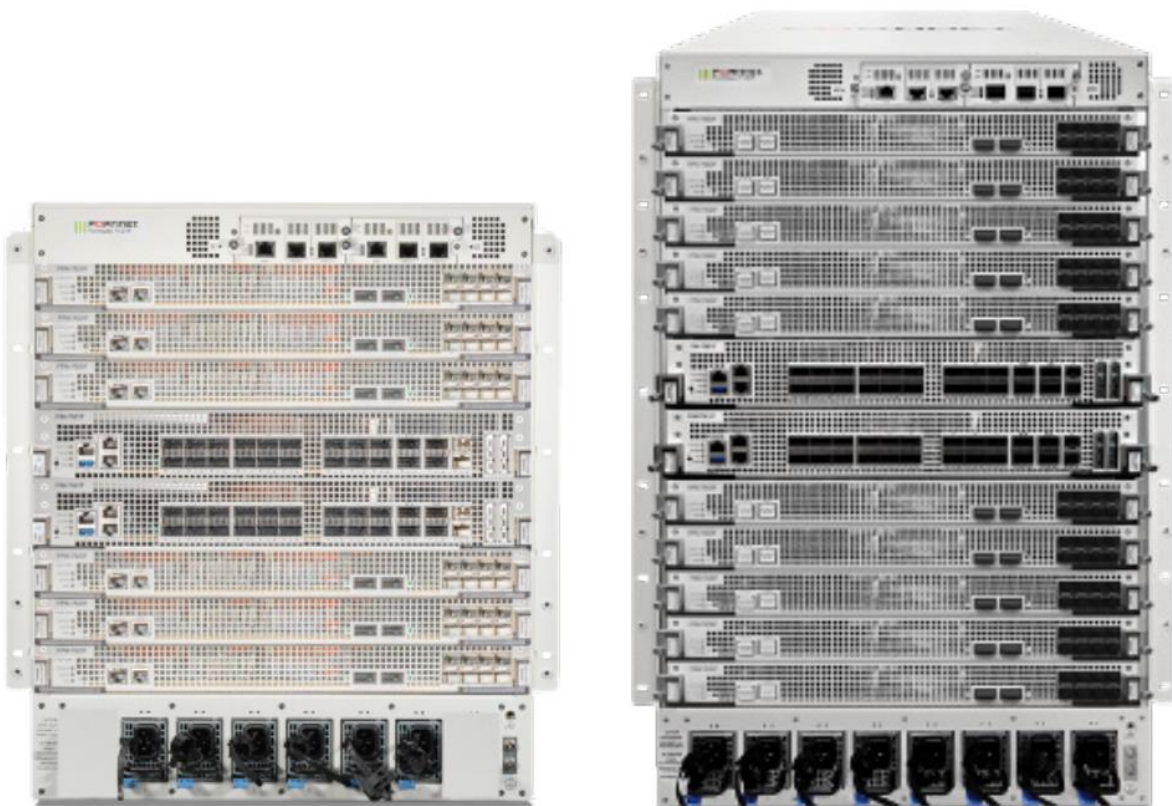
Fortinet's award-winning FortiGate enterprise firewall platform provides end-to-end security across your entire network. FortiGate next-generation firewalls are optimized for internal segmentation, perimeter, cloud, data center, distributed, and small business deployments. Simplify your security posture with one security solution across your physical, virtual, and cloud deployments.

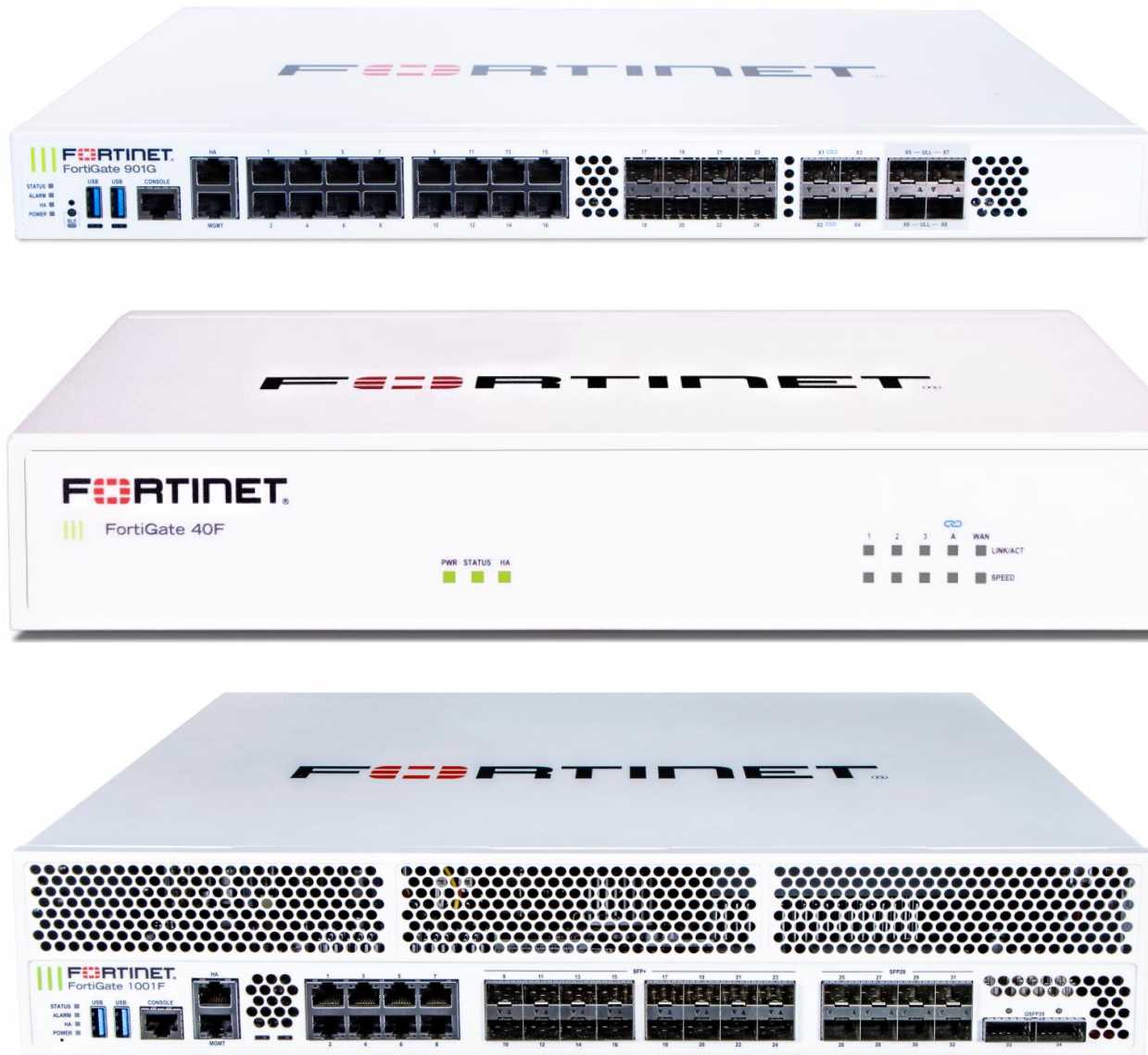
FortiGate Enterprise Firewalls offer flexible deployments from the **network edge** to the **core**, **data center**, **internal segment**, and the **Cloud**.

Fortinet's FortiGate enterprise firewall platform provides end-to-end security across your entire network. FortiGate next-generation firewalls are optimized for internal segmentation, perimeter, cloud, data center, distributed, and small business deployments.

Fortinet offers a variety of firewall series, ranging from home office firewalls to business firewalls. The FortiGate family of network security appliances represents the industry's broadest range of firewall platforms.

Enterprise firewalls are deployed based on their specific locations and focus in the enterprise, but the network security fabric that connects them stretches across the entire infrastructure.





The Fortinet Enterprise firewall solution answers networking and security challenges. It offers effective and fast end-to-end security. The core of the solution is the Security Fabric, which enables the communication of all the security devices in an enterprise network.

The Fortinet Enterprise firewall solution offers guidelines about where to install your network security devices and what roles they will have in each part of the enterprise network. You can deliver Single-Pan-of-Glass management and reporting for all the deployment across the enterprise using FortiManager and FortiAnalyzer.

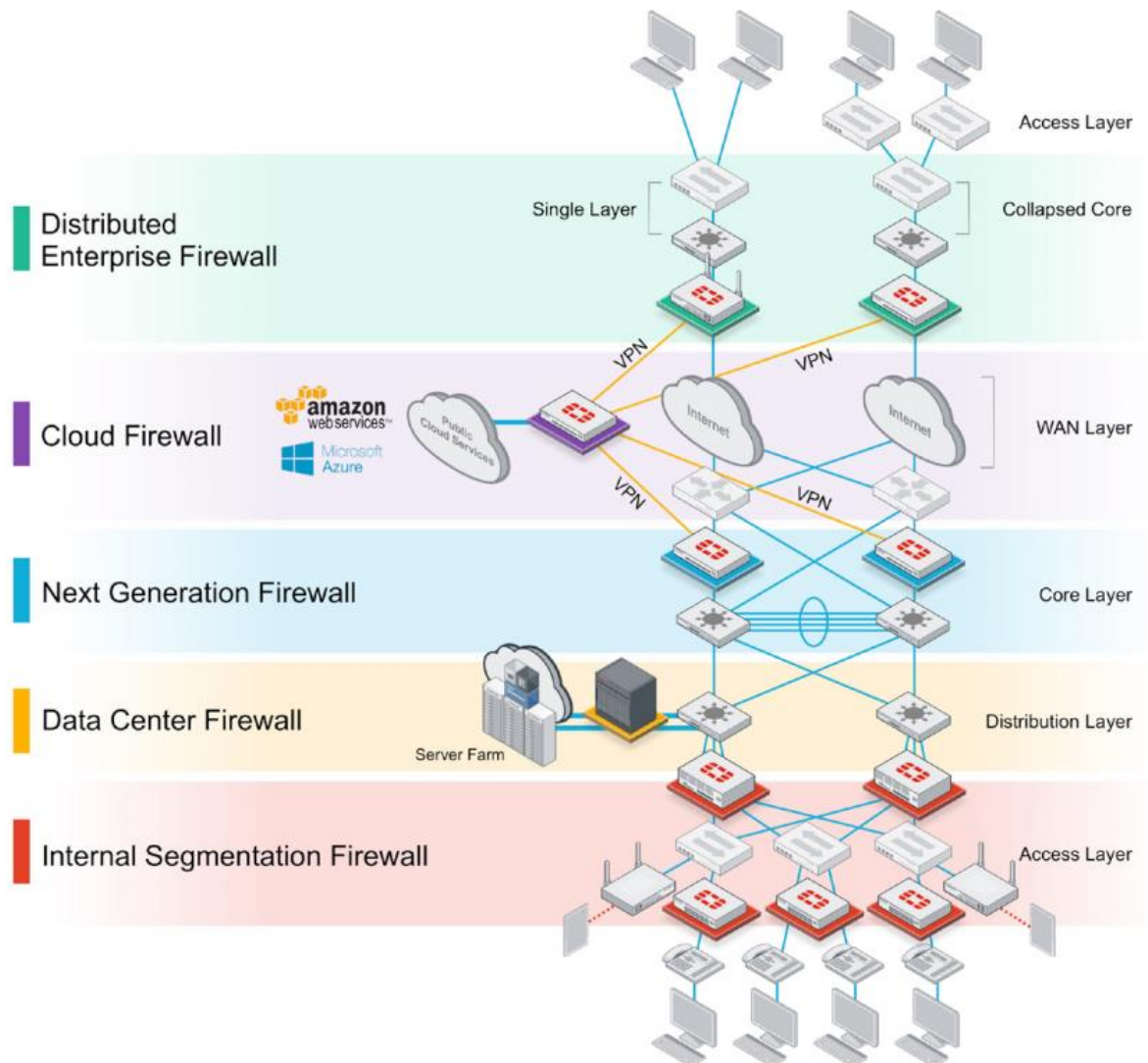
The key functional domains of Fortinet Enterprise Firewall Solution work as one to remove complexity and increase security.

Firewall Roles in Enterprise Firewall Solution:

In the Enterprise Firewall solution, each FortiGate device has a specific role, depending on where it is installed and what assets it is protecting.

When planning on deployment, it is important to consider not only where the perimeter is (WAN /LAN points), but also how malware could get to the data and most sensitive systems.

The location of the firewall in the network environment is the key to selecting the deployment mode. For example, will it be located at a data center, where servers need to be protected at very fast rates, or is this firewall meant to protect a few hundred users at a corporate office:



Distributed Enterprise Firewall (DEFW):

Distributed Enterprise Firewall (DEFW) are usually smaller devices installed in branch offices and remote sites. Distributed enterprises usually don't follow a standardized enterprise network design, and therefore multiple layers are collapsed into one or two layers. They are connected to the corporate headquarters using a VPN. DEFWs are all-in-one security devices, doing firewall, application control, IPS, web filtering, and antivirus inspection. Target Throughput is up to 1 Gbps.

Next-Generation Firewall (NGFW):

Next-Generation Firewall (NGFW) are usually deployed for firewall, application visibility, intrusion prevention, malware detection, and VPNs. NGFWs can play the traditional role of the entry-point firewall or, depending on the network infrastructure, can be deployed in the core or edge. Target Throughput is up to 1 to 40 Gbps.

Data Center Firewall (DCFW):

Data Center Firewall (DCFW) protect corporate services. They focus on inspecting incoming traffic and are usually installed at the distribution layer. Because of the high-performance requirements, in most cases the security functions are kept to a minimum: firewall, application control, and IPS. Target Throughput is up to 10 Gbps to 1 Tbps.

Internal Segmentation Firewall (ISFW):

Internal Segmentation Firewall (ISFW) split your network into multiple security segments. They serve as breach containers for attacks that come from inside. Firewall, application control, web filtering, and IPS are the features that are commonly enabled in these firewalls. Target Throughput is up to 1 to 100 Gbps. Usually Deploy on Access Layer.