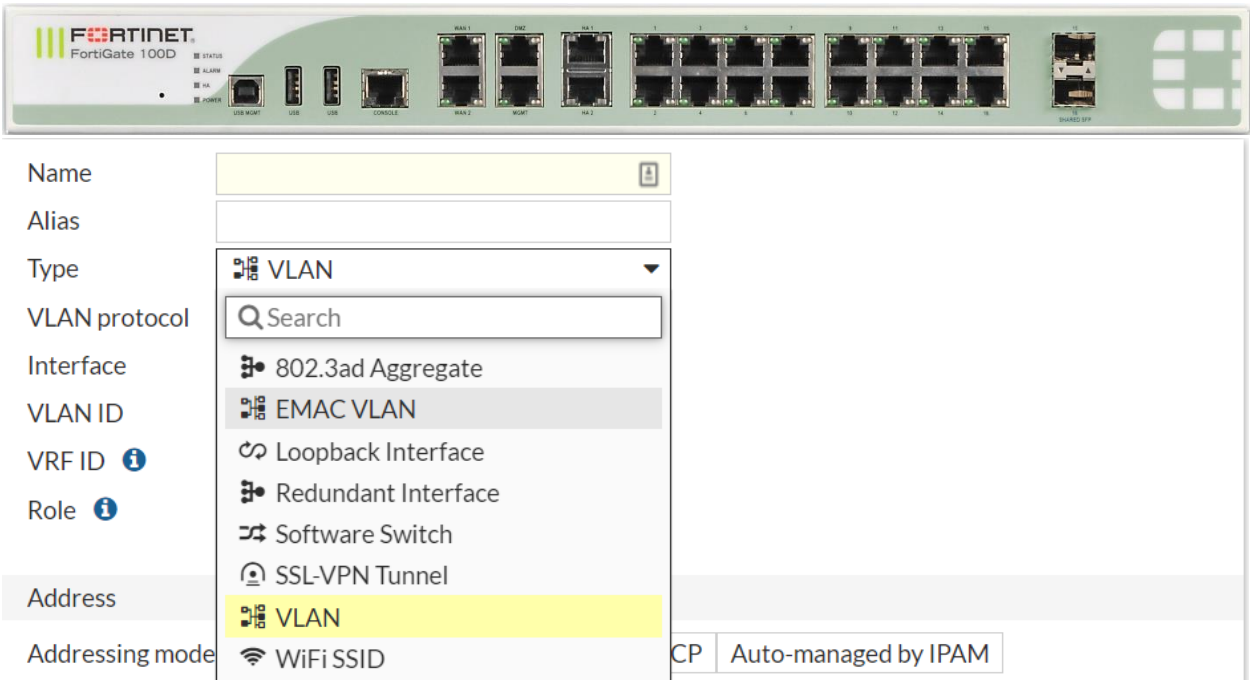
FortiGate Firewall Interfaces:

- Interfaces, both physical & virtual, enable traffic to flow to & from internal network.
- Interfaces, both physical & virtual to flow traffic Internet & between internal networks.
- FortiGate has number of options for setting up interfaces and groupings of subnetworks.
- This interfaces and groupings of subnetwork can scale company's growing requirements.
- FortiGate have a number of physical ports where you connect ethernet or optical cables.
- Depending on the Firewall model, they can have anywhere from four to 40 physical ports.
- Some have grouping of ports labelled as internal, providing built-in switch functionality.
- They appear when you want to configure the interfaces, by going to Network > Interface.
- There are also virtual interfaces such as VLANs, loopback and VPN tunnels are another.
- You can create and edit fortigate VLAN, EMAC-VLAN, switch interface, zones, and so on.



VLANs:

- Virtual Local Area Networks (VLANs) multiply the capabilities of your FortiGate Firewall.
- VLANs use ID tags to logically separate devices on network into smaller broadcast domains.
- These smaller domains forward packets only to devices that are part of that VLAN domain.
- This Virtual Local Area Networks (VLAN) reduces traffic and increases network security.
- FortiGate unit can also forward untagged packets to other networks such as the Internet.
- In NAT mode, FortiGate unit supports VLAN trunk links with IEEE 802.1Q-compliant switch.
- The trunk link transports VLAN-tagged packets between physical subnets or networks.
- You can define the VLAN subinterfaces on all FortiGate Firewalls physical interfaces.

Loopback Interfaces:

- Loopback interface is a logical interface that is always up (no physical link dependency).
- The loopback interface attached subnet is always present in the routing table of FortiGate.
- The FortiGate's firewall loopback IP address does not depend on one specific external port.
- And is therefore possible to access it through several physical or VLAN interfaces of firewall.
- Multiple loopback interfaces can be configured in either non-VDOM mode or VDOM mode.
- Loopback interfaces still require appropriate firewall policies to allow traffic to and from.
- A loopback interface can be used with Management access, BGP (TCP) peering or PIM RP.
- Loopback interfaces are good practice for OSPF easier & remembering the management IP.

Redundant Interfaces:

- Some models can combine two or more physical interfaces to provide link redundancy.
- This feature enables you to connect to two or more switches to ensure the connectivity.
- In the event one physical interface or the equipment on that interface fails other work.
- In FG Firewall a redundant interface, traffic is only going over one interface at any time.
- This differs from an aggregated interface where the traffic is going over all interfaces.
- This interfaces have more robust configurations with fewer possible points of failure.
- Redundant interface is important in a fully-meshed High Availability (HA) configuration.
- An interface has to be in redundant interface if it is physical interface, not VLAN interface.
- It is not already part of an aggregated or redundant interface and in the same VDOM.
- It has no defined Internet Protocol IP address & it is not configured for DHCP or PPPoE.
- It has no DHCP server or relay configured on it & t does not have any VLAN subinterfaces.
- It is not referenced in any security policy, VIP, or multicast policy & not monitored by HA.

Aggregate Interfaces:

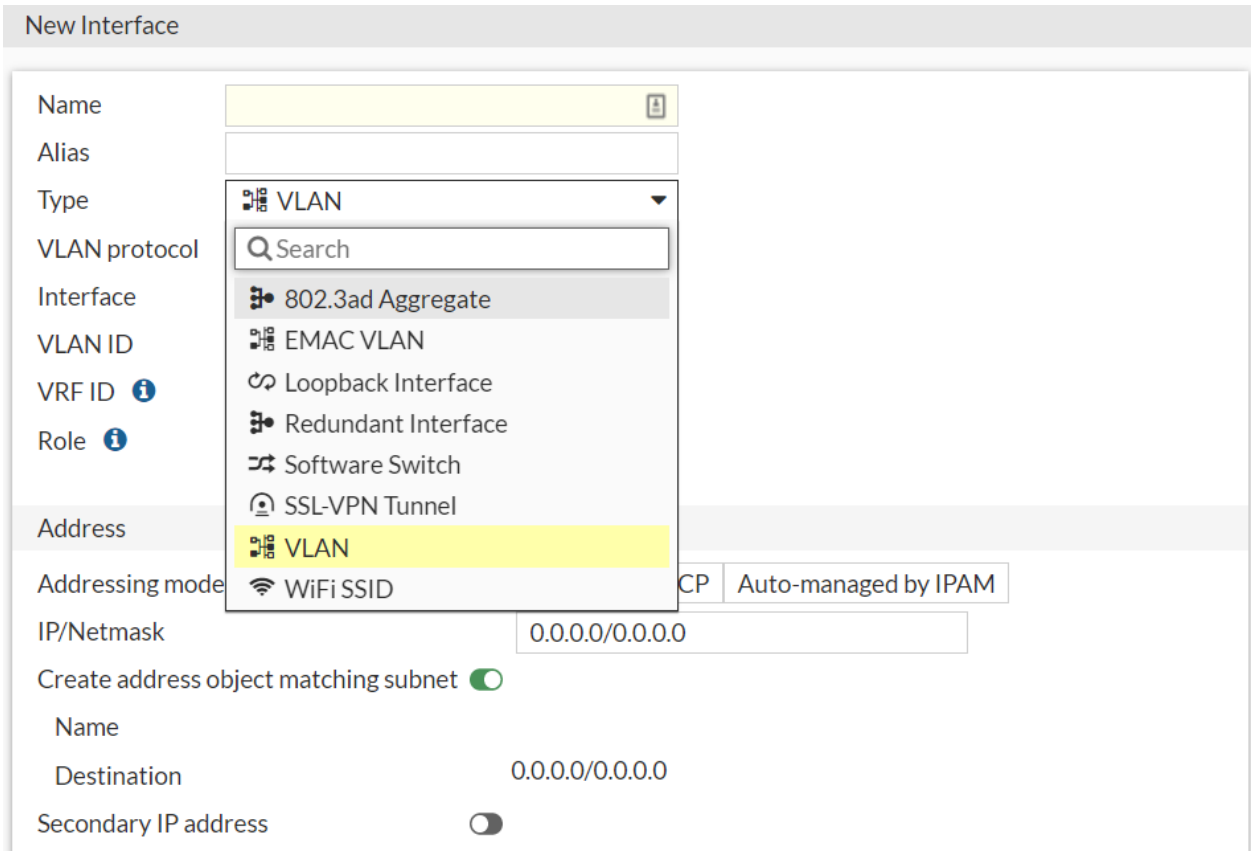
- Link aggregation (IEEE 802.3ad) enables to bind two or more physical interfaces together.
- Link aggregation bind two or more interfaces to form an aggregated (combined) link.
- The link aggregation(IEEE 802.3ad) new link has the bandwidth of all the links combined.
- If a link in the group fails, traffic is transferred automatically to the remaining interfaces.
- Major difference being that a redundant interface group only uses one link at a time.
- Where an aggregate link group uses the total bandwidth of the functioning links in group.
- Support of the IEEE standard 802.3ad for link aggregation is available on some models.
- An interface is available to be an aggregate interface if it is physical interface, not VLAN.
- It is not a Subinterface and it is not already part of an aggregate or redundant interface.
- it is in same VDOM as aggregated interface & Aggregate ports cannot span multiple VDOMs.
- it does not have an Internet Protocol IP address and is not configured for DHCP or PPPoE.
- it is not referenced in security policy, VIP, IP Pool or multicast policy & not HA heartbeat.

One-Armed Sniffer:

- Used to configure physical interface on FortiGate as one-arm intrusion detection system.
- Traffic sent to the interface is examined for matches to the configured IPS sensor.
- Traffic send to interface is examined for matches to configured application control list.
- Matches are logged & then all received traffic is dropped, Sniffing only reports on attacks.
- One-Armed Sniffer interface does not deny (Block) or otherwise influence the traffic.
- Using one-arm sniffer, you can configure a FortiGate unit to operate as an IDS appliance.
- It us use to sniff the network traffic for attacks without actually processing the packets.
- To configure one-arm IDS, you enable sniffer mode on a FortiGate Firewall interface.
- Connect interface to hub or to the SPAN port of a switch that is processing network traffic.

Interface Settings:

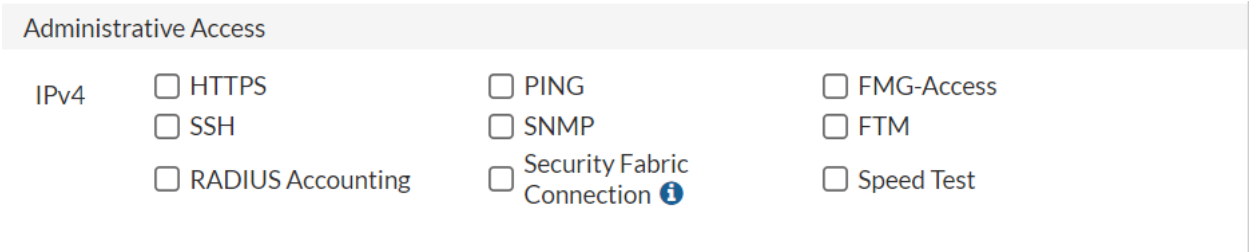
- In Network > Interface, can configure interfaces, physical and virtual, for FortiGate FW.
- There are different options for configuring interfaces when FortiGate FW is in NAT mode.
- There are different options for configuring interface when firewall is in transparent mode.
- Can configure Interface name, Alias, type, Interface, VLAN ID, VRF ID, Role & Address etc.



Interface Name	Physical interface names cannot be changed.
Alias	Enter an alternate name for a physical interface on the FortiGate unit.
Type	Configuration type for the interface, such as VLAN or Software Switch.
Interface	Select name of physical interface that want to add a VLAN interface to.
VLAN ID	Enter the VLAN ID. The VLAN ID can be any number between 1 and 4094 and must match the VLAN ID added by the IEEE 802.1Q-compliant router or switch that is connected to the VLAN Subinterface.
Role	Set the role setting for the interface. LAN: Used to connected to a local network of endpoints. WAN: Used to connected to the internet. DMZ: Used to connected to the DMZ. Undefined: The interface has no specific role.
Addressing mode	Select the addressing mode for the interface. Manual: Add an IP address and netmask for the interface. DHCP: Get the interface IP address & other network settings from DHCP.
IP/Netmask	If Addressing Mode is set to Manual, enter an IPv4 address & subnet mask.
Create address object matching subnet	This option is available when Role is set to LAN or DMZ. Enable this option to automatically create address object that matches the interface subnet.
Secondary IP Address	Add additional IPv4 addresses to this interface.

Administrative Access to Interfaces:

Configure protocols that administrators can use to access interfaces on the FortiGate.
This helps secure access to FortiGate by restricting access to limited number of protocols.
It helps to prevent users from accessing interfaces that you do not want them to access.
You should configure administrative access when you're setting the IP address for a port.
Go to Network > Interfaces Create or edit an interface. In the Administrative Access section, select which protocols to enable for IPv4 and IPv6 Administrative Access.



HTTPS	Allow secure HTTPS connections to the FortiGate GUI through this interface. If configured, this option is enabled automatically.
HTTP	Allow HTTP connections to the FortiGate GUI through this interface. This option can only be enabled if HTTPS is already enabled.
PING	Interface responds to pings. Use to verify installation and for testing.
FMG-Access	Allow FortiManager authorization automatically during the communication exchanges between FortiManager and FortiGate devices.
CAPWAP	Allow FortiGate wireless controller to manage wireless access point such as FortiAP device. Control & Provisioning of Wireless AP protocol.
SSH	Allow SSH connections to the CLI through this interface.
SNMP	Allow a remote SNMP manager to request SNMP information by connecting to this interface.
FTM	FortiToken Mobile Push (FTM) access.
RADIUS Accounting	Allow RADIUS accounting information on this interface.
FortiTelemetry	Communicates info between FortiClient & FortiGate, sending status info to FortiGate & receiving network-access rules from FortiGate.
Security Fabric Connection	Allow Security Fabric access. This enables FortiTelemetry and CAPWAP.

FortiManager:

FortiManager is a central management device that can be used to access and configure FortiGate devices in your network. It also allows you to deploy FortiGuard across your network.

FortiToken Mobile Push (FTM):

VPN connections to FortiGate might require network authentication that uses a token from FortiToken Mobile, which is an application that runs on Android or iOS devices. When configured, you can push the token by clicking the FTM Push button in FortiClient console.

FortiClient Telemetry:

FortiClient Telemetry communicates information between FortiClient and FortiGate, sending status information to FortiGate and receiving network-access rules from FortiGate.

Zone:

- Zones are a group of one or more physical or virtual FortiGate firewall interfaces.
- To simplify the policy configuration, you can group interfaces into logical zones.
- That you can apply the security policies to control inbound and outbound traffic.
- Grouping interfaces, VLAN subinterfaces into zones simplifies creation security policies.
- Where number of network segments can use same policy settings & protection profiles.
- When add zone, select names of interfaces and VLAN subinterfaces to add to the zone.
- Each interface still has its own address and routing is still done between the interfaces.
- You can use FortiGate Firewall security policies to control the flow of intra-zone traffic.
- Admin making separate security policies make simpler by adding interfaces to a zone.
- However, you should note that an interface in a zone cannot be referenced individually.
- Only configure policies for connections to & from zone but not between interfaces zone.
- You can create a security policy in FortiGate Firewall to go between zone 1 and zone 3.
- but you cannot create security policy between WAN2 and WAN1, or WAN1 and DMZ1.
- In zone configuration set intrazone deny prohibiting different interfaces in same zone.
- Enable Block intra-zone traffic, block different interfaces in same zone to talk each other.