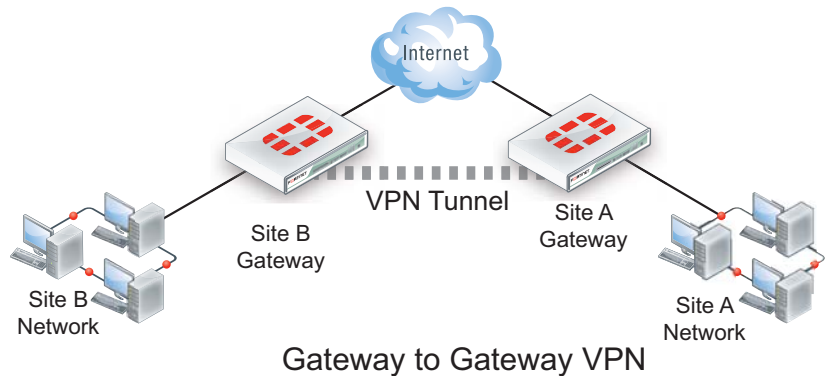




# Virtual Private Networking (VPN)

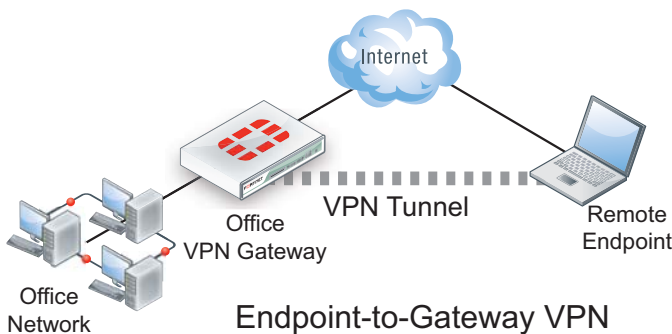
FortiOS supports IPsec and SSL VPNs that are compatible with industry standards, provide a high level of flexibility, and are accelerated by FortiASIC hardware.

Fortinet VPN technology provides secure communications across the Internet between multiple networks and endpoints, through both secure socket layer (SSL) and IPsec VPN technologies, leveraging FortiASIC hardware acceleration to provide high-performance communications and data privacy. Benefits include enforcing complete FortiOS UTM content inspection and multi-threat security for VPN communications, including antivirus, application control, IPS, Web filtering, Email filtering, and Data Leak Protection (DLP). SSL and IPsec VPN tunnels may operate simultaneously on the same FortiGate unit.



FortiOS IPsec and SSL VPN support a full range of authentication options to identify users and control access to resources. VPNs can authenticate individual users against the internal FortiOS user database or with external LDAP, RADIUS, or TACACS+ servers. Authentication can also use PKI or Windows directory service resources. FortiOS VPNs are also compatible with FortiOS traffic optimization, traffic shaping, high availability, and Endpoint NAC.

## Why use a VPN?



Virtual Private Network (VPN) technology enables users to transparently cross the Internet between private networks in a secure way. Any organization with off-site employees, more than one location connected to the Internet, or that communicates with other organizations over the Internet can benefit from employing VPN solutions to ensure privacy of communication across the Internet.

Employees traveling or working from home can use endpoint-to-gateway VPNs to securely access the office network through the Internet. Employees in a

branch office can use gateway-to-gateway VPNs to securely access main office resources. These VPNs ensure that unauthorized parties cannot intercept any of the protected information that is exchanged across the VPNs.

## FortiOS IPsec VPN feature set

FortiOS IPsec VPN supports all of the common industry standard IPsec features, including IKE v1 and v2, manual keys, static and dynamic gateway IP addresses, aggressive and main mode negotiation, preshared keys, X.509 security certificates, extended authentication (XAUTH), Diffie Hellman (DH) groups 1, 2, 5, and 14, dead peer detection, replay detection, perfect forward secrecy, and autokey keep alive.

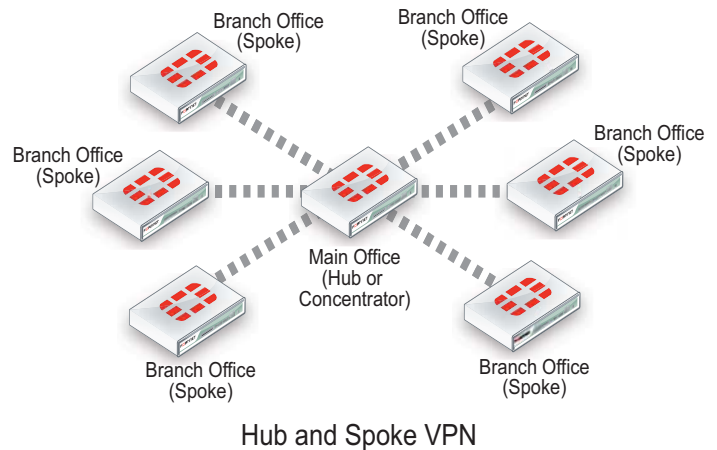
Fortinet IPsec VPNs employ industry standard features to ensure the best security and inter-operability with industry standard VPN solutions provided by other vendors. FortiOS IPsec VPN encryption methods include DES, 3DES, AES128, 192, and 256. Authentication methods include MD5, SHA1, SHA256, SHA384, SHA512. Simple authentication can optionally be offloaded to

FortiOS also supports policy-based and route-based IPsec VPNs. A route-based VPN creates a virtual IPsec network interface that applies encryption or decryption as needed to any traffic that interface carries. Route-based VPNs are also known as interface-based VPNs. A policy-based VPN is implemented through a special IPsec VPN firewall policy that applies the encryption you specified in the phase 1 and phase 2 settings to traffic accepted by the policy.

FortiOS Endpoint NAC is compatible with route-based VPNs if the VPN user's Windows PCs have the FortiClient Endpoint Security application running on them. This includes PCs on a private network communicating over the IPsec VPN as well as PCs that are operating as an IPsec VPN client using FortiClient Endpoint Security IPsec VPN to connect to the VPN. Network Access Control (NAC) ensures that computers (endpoints) meet security requirements, or they are not permitted access.

Other FortiOS IPsec VPN features include:

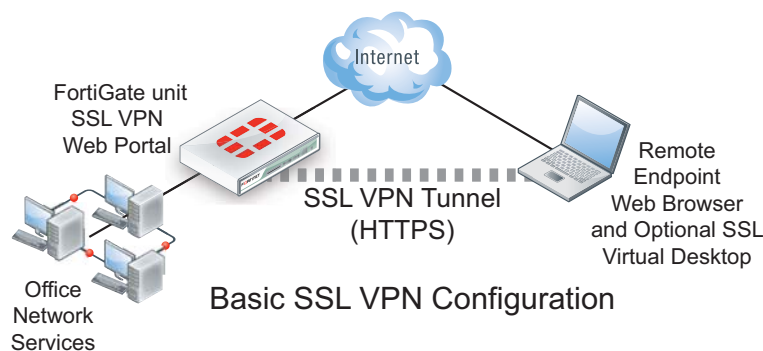
- Hub-and-spoke VPN enables a head office to securely connect to all of its branch offices while enabling any branch office to communicate with any other branch office through the VPN concentrator. This provides the same connectivity as a full-mesh topology but uses a less complex configuration that provides central control of the VPN configuration from the hub or concentrator.
- Redundant tunnels between VPN gateways ensure that if the first tunnel goes down, the second tunnel is immediately available to carry traffic and seamlessly maintain service.
- Hardware offloading allows FortiASIC NP2 network processors to provide accelerated processing for IPsec VPN traffic that would otherwise be processed by the FortiGate unit main processor. This encrypting and decrypting packets, and HMAC checking improves IPsec tunnel performance.
- Dynamic routing over IPsec VPN tunnels allows communication between complex multi-subnet networks over VPN so that complex private networks can be built on public (Internet) infrastructure. IPsec VPNs protect all traffic, including traffic routed by dynamic routing protocols—RIP, OSPF, BGP, and ISIS.
- Compatibility with most third-party IPsec VPN gateway and client solutions. FortiOS IPsec VPN is also compatible with the VPN capabilities of Microsoft Windows (L2TP-IPsec) and Cisco routers (GRE over IPsec).
- Automatic IPsec VPN configuration parameters for endpoints running FortiClient Endpoint Security ensures FortiClient users need only know their security credentials and the FortiGate VPN server IP address. FortiOS can also support auto-configuration of third-party clients that conform to the IKE Mode Config protocol.



## FortiOS SSL VPN Feature Set

IPsec VPN tunneling is performed at Layer 3 (Network Layer) or lower. To enable remote access, encrypted network connectivity is established between a remote node and the internal network, thereby making the remoteness of the connection invisible to the IPsec VPN user. However, IPsec VPNs require potentially complex IPsec gateway and endpoint PC configurations.

SSL VPN gateway configurations are simpler than IPsec VPNs because they don't require specialized network configurations. SSL VPNs establish connectivity using SSL, which functions at OSI Levels 4 - 5 (Transport and Session). Information is encapsulated at Levels 6 - 7 (Presentation and Application) and SSL VPNs communicate at the highest levels in the OSI model and independent of the network architecture.



Also, since SSL is built into most web browsers (as HTTPS) in most cases no additional configuration of SSL VPN endpoints is required. Instead users can connect to a FortiOS SSL VPN from an endpoint by opening any web browser and browsing to and logging into the FortiOS SSL VPN web portal. From the web portal users can securely access resources on the protected network. The portal can also automatically install and invoke extended SSL VPN features such as tunneling and virtual desktop protection without user intervention or the need to configure SSL VPN settings on the endpoint.

## SSL VPN Web Portal Mode

The SSL VPN web portal is a clientless method of providing secure remote access through a captive portal. The portal can be customized according to the user's authentication group and can include a custom look. As well, groups can have pre-configured bookmarks to specific network resources, access to file servers, remote desktops, and SSH, telnet, file sharing, Citrix, and RDP applications. Users can also add their own bookmarks, which are not visible to other users. For resources that require authentication, bookmarks can include user credentials, making the SSL VPN web portal a single sign-on (SSO) solution for remote users.

## SSL VPN Tunnel Mode

SSL VPN tunnel mode is similar to IPsec VPN because it allows users to use their own applications to access protected network resources, instead of those provided in the web portal. Tunnel mode assigns a virtual IP address to the endpoint and communication from the endpoint to the private network is sent through the tunnel. Tunnel mode communication can be split so that only communication with the private network uses the tunnel or an Internet browsing configuration can send all of the SSL VPN user's traffic through the tunnel. The SSL VPN user's Internet traffic is sent to the Internet from the FortiGate unit operating as the SSL VPN gateway and replies are sent back over the SSL VPN tunnel to the endpoint. FortiOS supports tunnel mode for MS Windows, Mac OS X, Linux and selected mobile devices.

SSL VPN port forwarding listens on local ports on the user's computer, enabling a user to access applications, such as POP3 for email access. When it receives data from a client application, the port forward module encrypts and sends the data to the FortiGate unit, which then forwards the traffic to the application server. The port forward module is implemented with a Java applet, which is downloaded and runs on the user's computer.

## Virtual Desktop

On a Microsoft Windows endpoint, SSL VPN sessions can be protected by the SSL VPN virtual desktop application that replaces the user's normal Windows desktop. Virtual desktop information is encrypted so that no information from it remains available after the session ends. This is particularly useful if users are working with sensitive information. Depending on how the virtual desktop is configured, the user may be able to switch between the virtual desktop and the regular desktop. When the virtual desktop session ends, the regular desktop is restored.

The virtual desktop application control list specifies the applications that users can access from the virtual desktop. The application control list and other virtual desktop options are configured on the FortiGate unit and no manual configuration of endpoint virtual desktops is required.

## Endpoint security checks

As part of the SSL VPN configuration, administrators can configure endpoint security checks for Microsoft Windows endpoints. Endpoint security checks operating system version and service pack level, the existence of antivirus and firewall software can be checked, and browser cache cleaning can be enabled.

## Choosing between IPsec or SSL VPN

Even though IPsec and SSL VPNs use different technologies, both provide similar levels of security and both are accelerated by FortiASIC technology. The most important factors for choosing one or the other VPN technology are the requirements of the VPN itself. In general, because IPsec VPN operates at the network layer its configuration is more complex and requires greater understanding of potentially complex networking configurations and encryption and authentication. However, IPsec VPN is the best solution for gateway to gateway VPNs connecting two or more private networks together over the Internet. Users can communicate transparently with resources on remote networks as long as they know the addresses of the remote network resources. Firewall policies can control the networks that users can communicate with and the protocols that can be used for this communication. UTM features can also be applied to IPsec VPN sessions. IPsec VPN is also the only solution for hub and spoke and redundant solutions where a single VPN must connect multiple networks through a single gateway or concentrator.

Since SSL VPNs operate at higher levels in the OSI model and use technology found in most web browsers, SSL VPN configurations are usually simpler than IPsec VPN configurations. All the complex networking is handled by the network infrastructure and the SSL VPN configuration can focus on high-level communication requirements, access control, UTM, and endpoint control.

Some networks available in public spaces such as hotels, airports, and internet cafes may block IPsec protocols, preventing travelling IPsec endpoints from accessing their IPsec VPN gateways. An SSL VPN is the only workaround in this situation since the HTTPS protocol used for SSL VPNs is a standard Internet protocol required for many applications and is virtually never blocked.

SSL VPN is the best solution for endpoint-to-gateway VPNs. Remote users can securely log into the SSL VPN web portal from any endpoint that can run a web browser that supports HTTPS. Endpoints can include PCs, tablets, and mobile devices. No special software or configuration is required for the endpoint. When users log into the SSL VPN web portal their login credentials assign them appropriate levels of UTM protection and select the SSL VPN Web portal that they see. Thus it is possible to customize the network resources that individual user groups have access to and the level of UTM protection applied to their communication sessions.

## Other options

IPsec VPN can be used for endpoint-to-gateway communication by installing IPsec VPN clients on the endpoints. This is a popular option used by many organizations, but SSL VPN is usually easier to configure and manage and also provides better access control and UTM granularity.

SSL VPN can be used for communication between remote networks (similar to a gateway-to-gateway configuration). Users on one network could connect to a remote network by browsing to and logging into the remote network's SSL VPN portal. However in most cases an IPsec VPN gateway-to-gateway configuration would make it easier for users on remote networks to transparently connect to resources on other networks.

## Conclusion

FortiOS supports both SSL and IPsec VPN technologies. Each combines encryption and VPN gateway functions to create private communication channels over the Internet. Both define and deploy network access and firewall policies using a single management tool. In addition, both support a simple client/user authentication process. You have the freedom to use both technologies; however, one may be better suited to the requirements of your situation.

In general, IPsec VPNs are a good choice for site-to-site connections where appliance based firewalls or routers are used to provide network protection, and company-sanctioned client computers are issued to users. SSL VPNs are a good choice for roaming users who depend on a wide variety of thin-client computers to access enterprise applications and/or company resources from a remote location.