



Inside FortiOS Internet Protocol version 6

FortiOS is in its 5th year of IPv6 support. The IPv6 feature set has been extended over this time to support all FortiOS features, including UTM protection for IPv6 traffic

Mixed IPv4 and IPv6 networks

A major transition period from IPv4 to IPv6 is under way. For a lengthy period networks will have to support both IPv4 and IPv6. The transition will not happen over night simply because of the time required to convert equipment and applications to IPv6. In addition, some legacy equipment and applications may never support IPv6, and will have to either be replaced or will require ongoing support as IT budgets permit.

During this transition period, it will not be possible to operate an IPv6 network without also supporting IPv4. Most networks will become mixed networks that have to understand and route both IPv6 addresses and IPv4 addresses.

To be able to support both IPv4 and IPv6, FortiOS implements a dual stack architecture that recognizes and separately routes both IPv4 and IPv6. In addition to routing, most vital FortiOS network and content protection security features now fully support for IPv6.

FortiOS (4.0 MR3) supports the following FortiOS IPv6 features (all configurable from the Web UI or CLI):

- Static routing and dynamic routing
- DNS
- Network interface addressing
- Routing access lists and prefix lists
- IPv6 tunnel over IPv4, IPv4 tunnel over IPv6
- Firewall policies
- Authentication
- IPv6 over SCTP
- Packet and network sniffing
- IPsec VPNs
- SSL VPN
- UTM protection (see below)
- NAT/Route and Transparent mode
- Logging and reporting
- SNMP
- IPv6 specific troubleshooting such as ping6

UTM protection for IPv6 networks

Maintaining security for both types of traffic will be crucial to the success of IPv6 and mixed networks. Malware and network threats are independent of IPv4 or IPv6. FortiOS uses IPv6 firewall policies to provide UTM protection for IPv6 traffic. Antivirus, web filtering, FortiGuard Web Filtering, email filtering, FortiGuard Email Filtering, data leak prevention (DLP), and VoIP protection features can be enabled in IPv6 firewall policies using normal FortiOS UTM profiles for each UTM feature. This protection is transparent to IPv6 Users.

UTM support for IPv6 makes the transitional mixed network phase easier, because the level of security of transitional networks is extended to both IP protocols. Future releases of FortiOS will extend IPv6 support even further.

FortiOS is Future-proof

The core IPv6 protocol implementation in FortiOS has been evaluated against the stringent requirements of the IPv6 Ready Logo Phase 2 program. Compliance with the program ensures that the FortiOS IPv6 implementation is compliant with relevant RFCs and is ready to be deployed in existing IPv6 networks or in existing IPv4 networks being prepared for an upcoming transition to the next generation of Internet addressing. For more on the IPv6 Ready Logo program, see <http://ipv6ready.org>.

As FortiOS continues to introduce new platforms and new functionality, it will continue to be evaluated by external programs and third-party labs to ensure FortiGate devices and FortiOS adhere to evolving standards. Customers can be assured that FortiGate solutions running FortiOS will allow customers to adapt to evolving security requirements and that Fortinet's Unified Threat Management solutions will continue to provide the means to be prepared

for new technological requirements. For enquiries about FortiGate certifications, contact your local Sales group or visit http://www.fortinet.com/aboutus/fortinet_advantages/certifications.html.

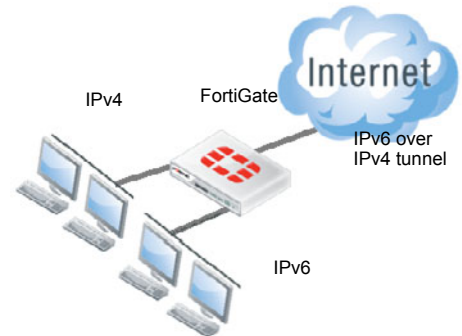
FortiOS enables IPv6 solutions

Solution 1 - Mixed internal network with both IPv4 and IPv6 traffic

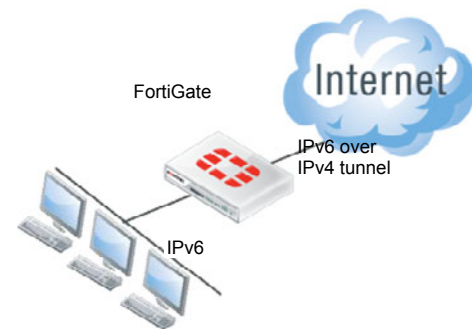
During the transition to IPv6, many organizations will continue to operate mixed internal networks that include both IPv4 and IPv6 devices. The FortiOS dual stack architecture supports both IPv4 and IPv6 traffic and routes the appropriate traffic as required to any device on the network. Administrators can update network components and applications to IPv6 on their own schedule, even maintaining some IPv4 support indefinitely if necessary.

Devices on a mixed network that connect to the Internet can query Internet DNS servers for IPv4 and IPv6 addresses. If the Internet site supports IPv6, the device can connect using the IPv6 address. If the Internet site does not support IPv6, then the device can connect using the IPv4 address. The dual stack architecture of FortiOS provides routing, firewall policies, and UTM security for all traffic on mixed networks.

If an organization with a mixed network uses an Internet service provider that does not support IPv6, they can use an IPv6 tunnel broker to connect to IPv6 addresses on the Internet. FortiOS supports IPv6 tunnelling over service provider IPv4 networks to tunnel brokers. The tunnel broker extracts the IPv6 packets from the tunnel and routes them to their IPv6 destination.



Solution 2 - IPv6 internal network connecting to the Internet



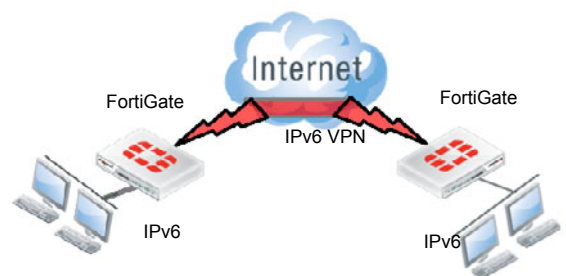
In this scenario, an organization has completed the transition to IPv6. All devices on the organization's networks support IPv6 and traffic among devices on the network uses IPv6 for all communications. FortiGate units can be assigned IPv6 addresses, deployed on IPv6 networks, include IPv6 static and dynamic routing, authentication, and IPv6 firewall policies with UTM functionality.

However, since many Internet services do not support IPv6, even internal networks that completely support IPv6 require the dual stack architecture of FortiOS to connect to IPv4 addresses on the Internet. Networks that have completed the transition to IPv6 may also still require tunneling IPv6 over IPv4 to reach IPv6 addresses on the Internet.

Solution 3 - IPv6 network connecting to a remote IPv6 network over the internet

Similar to the IPv6 over IPv4 tunnelling, FortiOS supports IPv6 tunnelling over IPv4 across the Internet between two IPv6 networks protected by FortiGate units. All traffic between the IPv6 networks can be tunnelled over IPv4. Each FortiGate extracts the IPv6 traffic from the IPv4 tunnel and Traffic on the internal networks uses IPv6.

FortiOS also supports tunnelling IPv6 traffic over an IPsec VPN between two IPv6 networks protected by FortiGate units. The VPN provides higher security for the data transmitted between the networks. Configuration of this topology involves configuring an interface-based IPsec VPN between IPv6 interfaces on each FortiGate unit.



Why use IPv6?

IPv6 handles issues that weren't around decades ago when IPv4 was created—running out of IP addresses, fair distribution of IP addresses, built-in quality of service features (QoS), better multimedia support, and improved handling of fragmentation. The bigger address space, bigger default packet size, and more optional header extensions of IPv6 provide these features with flexibility to customize them to any needs.

IPv6 has 128-bit addresses compared to the 32-bit addresses of IPv4, effectively eliminating address exhaustion. This new very large address space will likely make network address translation (NAT) a thing of the past, since IPv6 provides more than a billion IP addresses for each person on Earth.

Conclusion

All hardware and software network components must support this new address size—an upgrade that may take a while to complete and will force IPv6 and IPv4 to work side-by-side during the transition period. During that time FortiOS and its equal support IPv4 and IPv6 will ensure a smooth transition for networks. FortiOS enables network administrators to easily provide an IPv4-to-IPv6 transition scenario, with minimal or no impact to the users of the network. FortiOS also protects IPv4-to-IPv6 transitional networks from malware arriving through IPv4 or IPv6 as full UTM protection can be applied to both protocols.