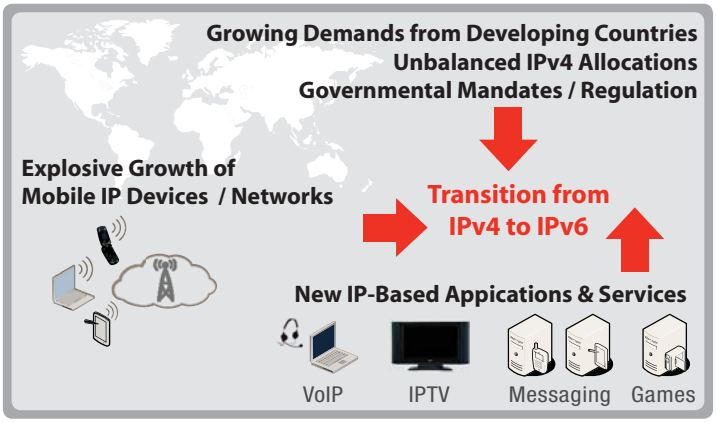
Securing IPv6 Networks

High Performance Next-Generation Security Solutions

The Business Imperative

The transition to IPv6 networks is being driven by the rapid consumption of the IPv4 address space due to the increasing number of users and the imbalance in access to new IP addresses within developing countries. At the same time new mobile IP devices/networks and emerging applications such IPTV, voice-over-IP (VoIP), intelligent appliances, RFID-enabled services, and gaming will require billions of new addresses. Corporations, governments and universities are responding and beginning the transition to IPv6, however this will take many years to realize. Security will be critical during this transition and even more complex in pure IPv6 networks given the new addressing/routing capabilities, devices and applications. A solution is required today that secures IPv4 networks, enables secure IPv4 to IPv6 transition networks and is fully ready and easily evolves to support pure IPv6 networks.



A Quick Look at IPv4 vs. IPv6 Packets

In addition to dramatically increasing the number of IP addresses, IPv6 also implements many enhancements including simplifying the packet header for efficiency, adding Flow Labeling capabilities, expanded Extensions / Options, improved Mobile IP and enhanced unicast / multicast support.

IPv4 32-bit addressing:
$2^{32} = 4{,}294{,}967{,}296$

Version	IHL	Type of Service	Total Length
Identification		Flags	Fragmentation
Time to Live	Protocol	Header Checksum	
Source Address			
Destination Address			
Options			Padding

IPv6 128-bit addressing:
$2^{128} = 340{,}282{,}366{,}920{,}938{,}000{,}000{,}000{,}000{,}000{,}000{,}000$

Version	Traffic Class	Flow Label
Payload Length	Next Header	Hop Limit
Source Address		
Destination Address		

Streamlined in IPv6
- Total Length & Header Checksum removed
- IHL, Identification, Flags, Fragmentation,Options and Padding fields removed

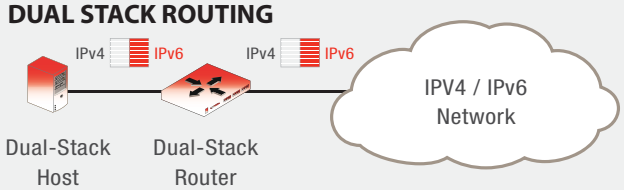
Enhanced in IPv6
- Time to Live becomes Hop Limit
- Protocol becomes Next Header
- Type of Service becomes Traffic Class

New in IPv6
- 128 bit addressing
- 64 bit alignment
- New Flow Label field

Network Transition to IPv6 Addressing

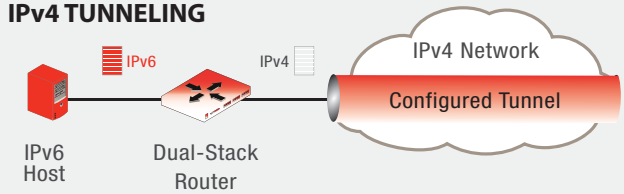
The transition from IPv4 to IPv6 addressing requires that IPv6 hosts and routers maintain interoperability with the existing IPv4 infrastructure. The most common methods for making this transition are to use "Dual Stack Routing" and "IPv4 Tunnels". Both methods require network security systems flexibly capable of supporting both IPv4 and IPv6 addressing and capable of IPv6 over IPv4 tunneling – without impacting network performance.

DUAL STACK ROUTING



Method
Implementing dual IP layers, in Hosts and Routers, to support both IPv6 and IPv4

IPv4 TUNNELING



Method
Encapsulating IPv6 packets within IPv4 headers to carry them over IPv4 tunnels

U.S. Goverment Mandates IPv6

The United States goverment has set a mandate for all federal agencies to implement IPv6 networks by 2008. Migrating from an IPv4 to an IPv6 network can be complex and ensuring consistent security is paramount to a successful migration to IPv6.

Fortinet FortiGate™ Unified Threat Management (UTM) Solutions Secure IPv6 Networks

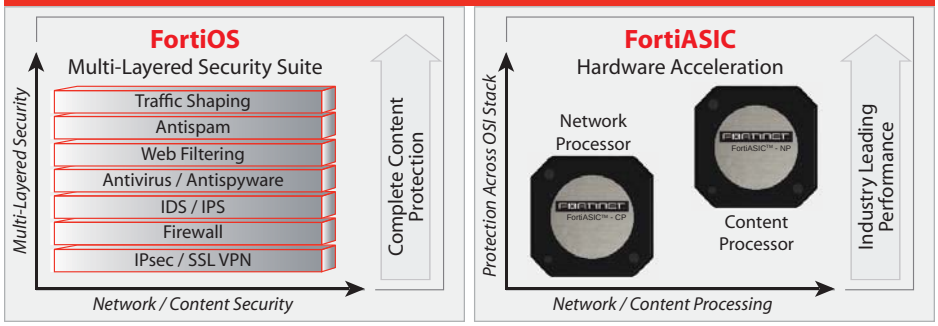
Fortinet's family of FortiGate security platforms are IPv6 ready today and have proven interoperability in North America's largest real world demonstration of next-generation Internet Protocol Version 6 (IPv6) and in many customer deployments. Fortinet's FortiOS™ security operating system and FortiASIC™ hardware acceleration processors are fully IPv6 compatible and support both "dual-stack" and "IPv4 tunneling" implementations with routing between physical and virtual interfaces. FortiGate's industry-leading protection and performance secures the transition to IPv6.

FortiGate
Network Security Platforms

SOHO / ROBO
SMALL / MEDIUM ENTERPRISE
LARGE ENTERPRISE
CARRIER / MSSP

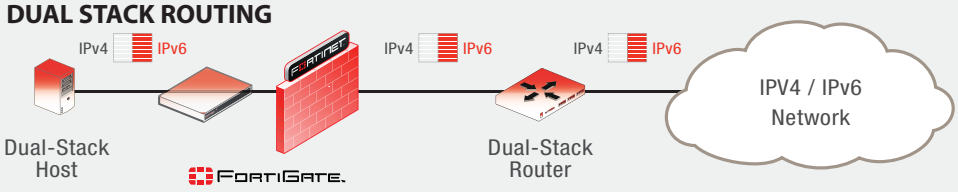
Successfully completed interoperability testing with the DoD IPv6 Generic Test Plan

Fortinet Antispam and Multi-Layered Security Solutions

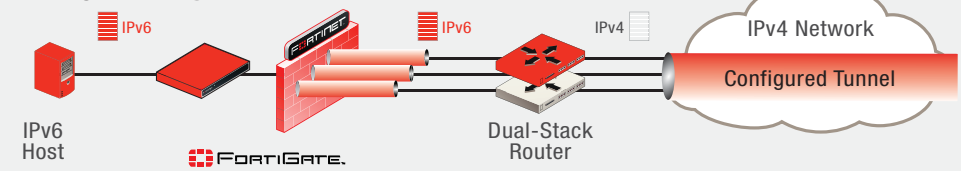


FortiGate IPv6 Deployments

DUAL STACK ROUTING



IPv4 TUNNELING



Key Features

- ✔ Assign both IPv4 and an IPv6 address to any interface
- ✔ Configure static routes and the router advertisements per interface
- ✔ Create virtual tunnels and routes
- ✔ Define IPv4/6 firewall traffic policies
- ✔ Supports interface-based IPv6 IPSec

Fortinet Secures North America's Largest Third-Party IPv6 Network

Fortinet successfully completed interoperability testing in North America's largest real world demonstration of next generation Internet Protocol Version 6 (IPv6).

- ✔ U.S. Department of Defense (DoD)-mandates transition to IPv6 by 2008 for all inter- and intra-networking
- ✔ Fortinet successfully completed interoperability testing in accordance with the DoD IPv6 Generic Test Plan
- ✔ Testing occurred as part of the "Moonv6" project (http://moonv6.sr.unh.edu/) – global effort led by the North American IPv6 Task Force

"Fortinet's FortiGate-3600 security appliance was verified to be IPv6-compliant using Agilent's Network Tester. The system demonstrated seamless operation and deployment in a secure IPv6 environment."

Philip Kazakoff, Agilent Technologies

Fortinet
Governmental / Industry Certifications and Awards

Since 2001, Fortinet has Received more than 80 Awards

GLOBAL HEADQUARTERS
Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1-408-235-7700
Fax +1-408-235-7737
www.fortinet.com/sales

S0L119-0807-R1