IPv6 Security

Rainer Baeder
Manager Solution Consultant - Fortinet

Drivers for IPv6

Car-2-Car

- Basic Demand Drivers
  - More network appliances but lack of IPv4 addresses to support
  - Control OpEx for network and IT
  - Elimination of complex NAT networks
  - Strong intrinsic security
  - Better support for mobility applications
  - Greater flexibility and simplicity

2^{128}=340.282.366.920.938.463.463.374.607.431.768.211.456

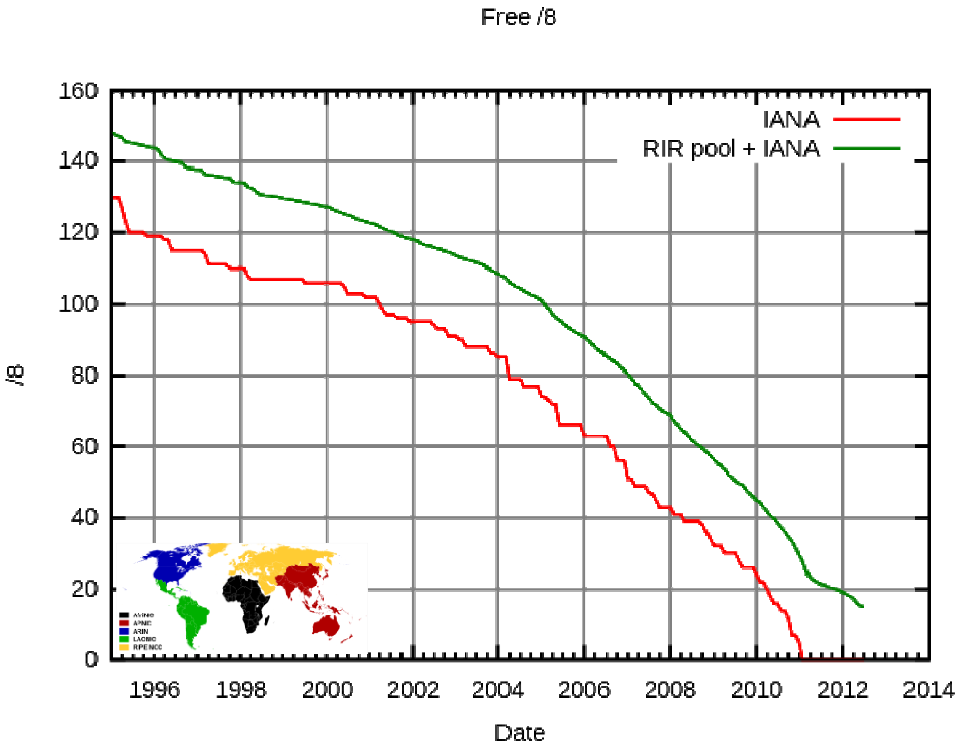
- New Opportunities to Improve Business Performance Business process improvements
  - New business opportunities
  - More addresses for objects – enhanced automation and productivity
  - Machine-to-Machine (M2M) telematics
  - IPv6 connection to anything

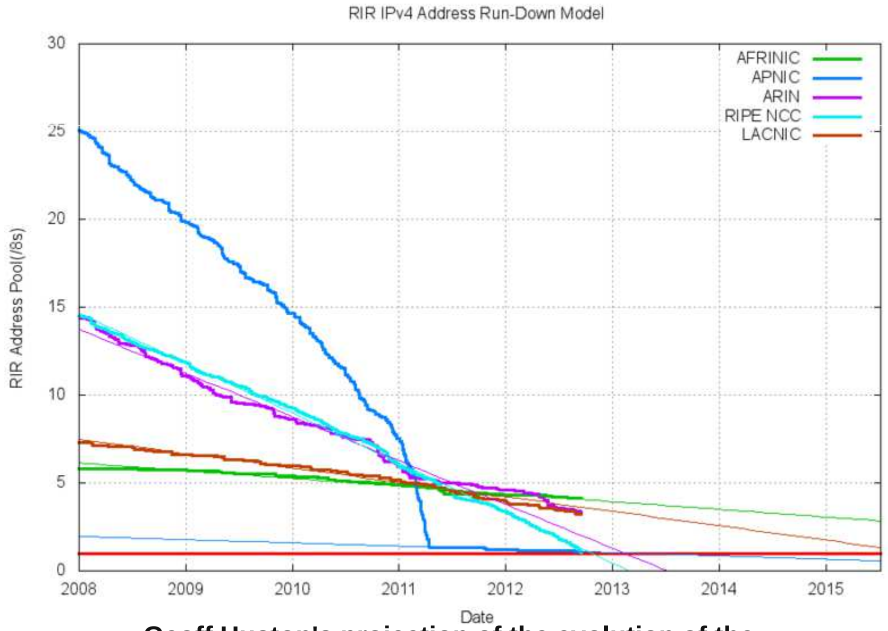
RFID

Internet of Things

IPv4 address trading sites begin to emerge

As reported in *The Register*, German Phython developer Martin von Loewis has launched a site called **www.Tradeipv4.com** . The site is offering IPv4 addresses for **$3 for v4 addresses located in ARIN** (American Registry for Internet Numbers) and **$4 for those in the APNIC** (Asia Pacific Network Information Center) region.





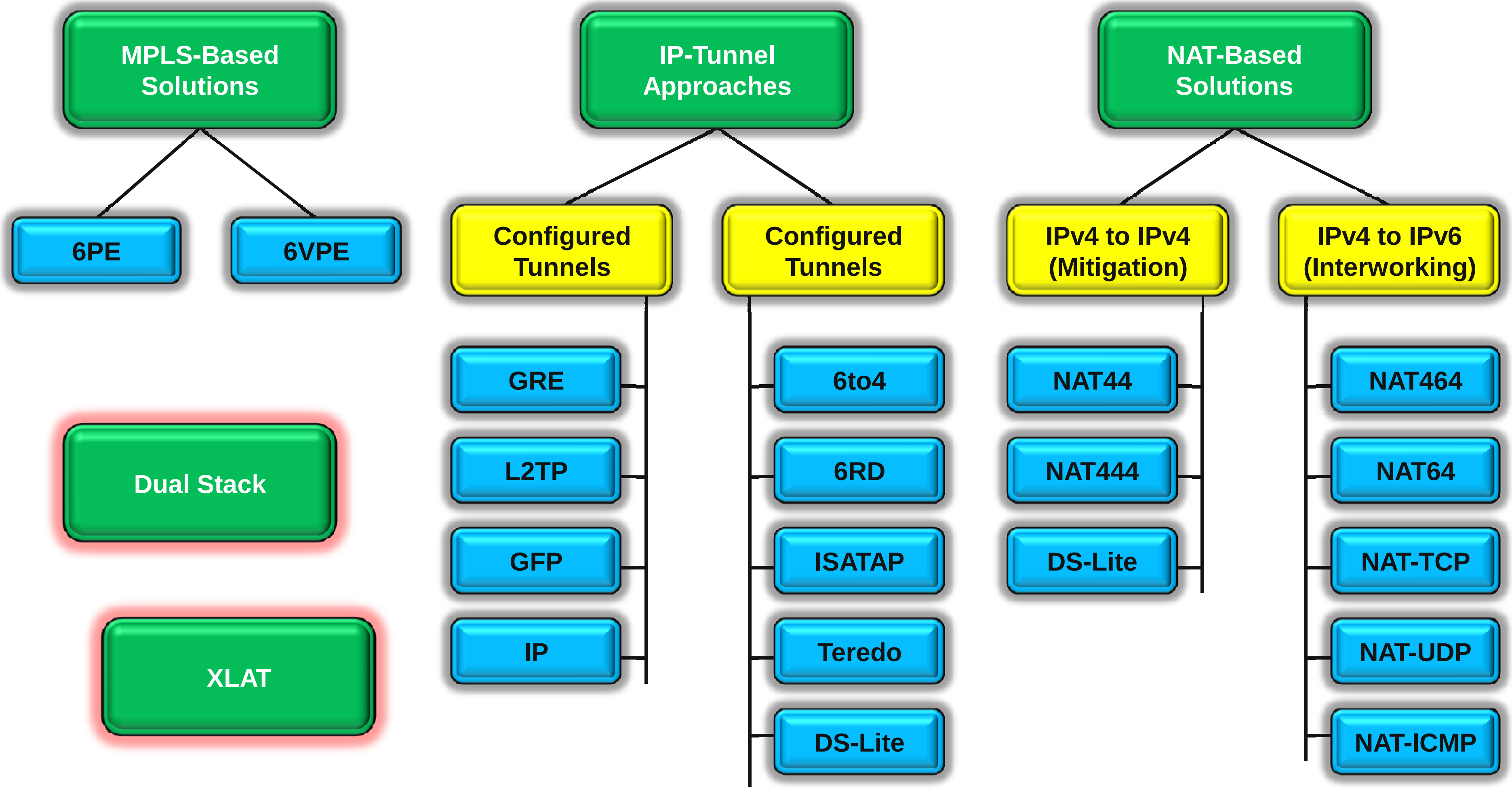
Geoff Huston's projection of the evolution of the IP pool for each RIR

Migration Complexities
Deployment Considerations

- Compatibility issues between IPv4 and IPv6
- Vendor interoperability issues with IPv6
- Potential networking security issues
- Network management considerations
- Existing hardware may not handle IPv6 traffic efficiently
- Router memory and CPU limitations may preclude IPv6 deployment
- Technology refresh cycles can be exploited to deploy IPv6 capabilities
- Global public routing practices continue to evolve

Resulting in
Security Issues !!

IPv6 Transition Methodologies



Threat Types

- Reconnaissance
  - Provide the adversary with information enabling other attacks
- Unauthorized Access
  - Exploit the open transport policy inherent in the IPv4 protocol
- Header Manipulation and Fragmentation
  - Evade or overwhelm network devices with carefully crafted packets
- Layer 3 –Layer 4 Spoofing
  - Modify the IP address and port information to mask the intent or origin of the traffic
- ARP and DHCP Attacks
  - Subvert the host initialization process or a device the host accesses for transit
- Broadcast Amplification Attacks (smurf)
  - Amplify the effect of an ICMP flood by bouncing traffic off of a network which inappropriately processes directed ICMP echo traffic
- Routing Attacks
  - Disrupt or redirect traffic flows in a network
- Viruses and Worms
  - Attacks which infect hosts and optionally automate propagation of the malicious payload to other systems
- Sniffing
  - Capturing data in transit over a network
- Application Layer Attacks
  - Broad category of attacks executed at Layer 7
- Rogue Devices
  - unauthorized devices connected to a network
- Man-in-the-Middle Attacks
  - Attacks which involve interposing an adversary between two communicating parties
- Flooding
  - Sending bogus traffic to a host or network designed to consume enough resources to delay processing of valid traffic

Some will disappear, Some will change !!

But....in the beginning we will see many new one

IPv6 Protocol Vulnerability

- IPv6 Header
  - Header Manipulation
  - Protocol Fuzzing
- ICMPv6
  - ICMPv6 Filtering
  - ICMPv6 Attacks
- Node Survey
  - Scanning
  - Improved/Smart Scanning
  - Multicast techiques
  - Sniffing
- Extension Header
  - EHeader Filtering
  - EHeader Fuzzing
  - Router Header Attacks
  - Fragmentation Header
  - Unknown Header
  - Protocol Layer Header
- Higher Layer Spoofing
- Flooding
- Multicast

You need to be prepared for the unexpected !!

IPv6 Firewalling

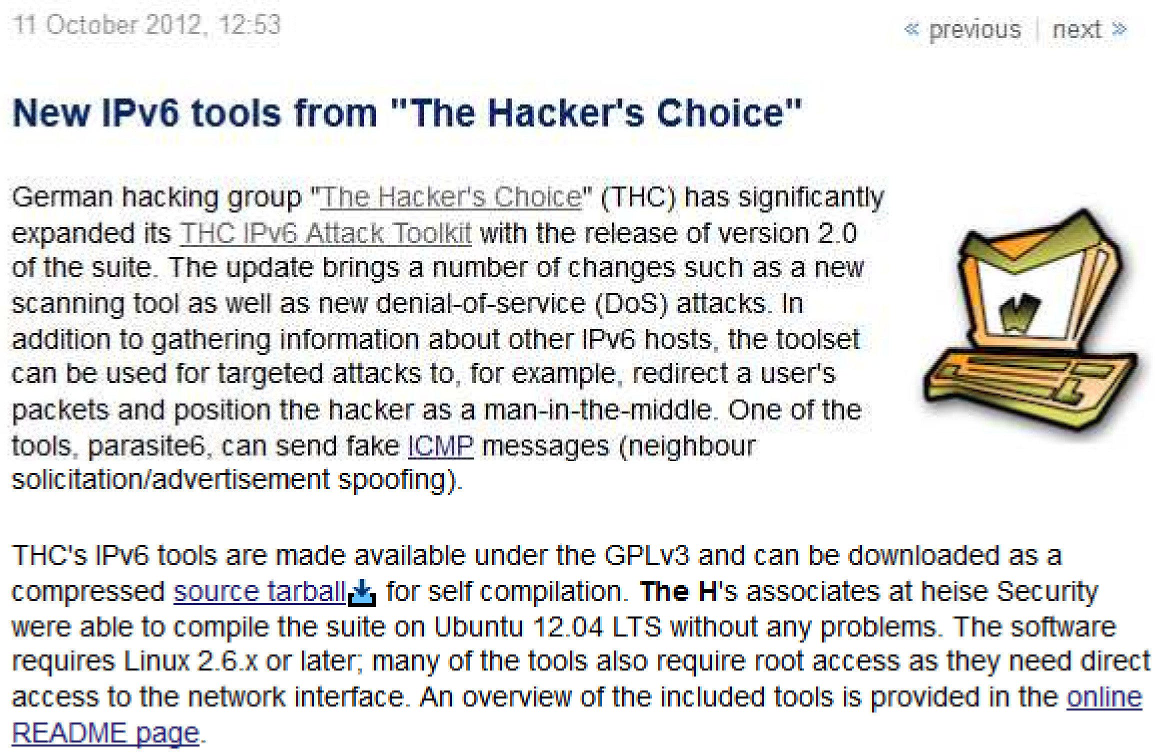
- IPv6 Addressing
  - Unallocated Addresses
- IPv6 Headers Consideration
- L2 FW
- IPv6 and NAT
- Neigbor Discovery Consideration (NDP)
  - Duplicate Address Detection Issue
  - Redirect Issue
- SEcure Neigbor Discovery (SEND)
- DHCP Filtering
- DHCPv6 Threats
- Endpoint Security
- IPv6, IPSec and Firewalls
- Management
- Routing Security
  - RIPng, OSPFv3
- QoS Threats
- Tunneled Traffic Inspection
- Unwanted Tunnels
- Mobile IPv6 (MIPv6)

More to come –

expect a lot more which is unknow today

Hacker are pretty smart

IPv6Hacking



11 October 2012, 12:53

« previous | next »

New IPv6 tools from "The Hacker's Choice"

German hacking group "The Hacker's Choice" (THC) has significantly expanded its THC IPv6 Attack Toolkit with the release of version 2.0 of the suite. The update brings a number of changes such as a new scanning tool as well as new denial-of-service (DoS) attacks. In addition to gathering information about other IPv6 hosts, the toolset can be used for targeted attacks to, for example, redirect a user's packets and position the hacker as a man-in-the-middle. One of the tools, parasite6, can send fake ICMP messages (neighbour solicitation/advertisement spoofing).

THC's IPv6 tools are made available under the GPLv3 and can be downloaded as a compressed source tarball for self compilation. **The H**'s associates at heise Security were able to compile the suite on Ubuntu 12.04 LTS without any problems. The software requires Linux 2.6.x or later; many of the tools also require root access as they need direct access to the network interface. An overview of the included tools is provided in the online README page.

http://www.thc.org/home.php

IPv6 Adress Firewalling

- Ingress
- Accept all ICMPv6 packets for Neighbor Discovery and Path MTU Discovery that is a function necessary for the communication with IPv6
- Reject the packets which contain relevant special-use prefix in the ***source address field***

::1/128	loop back address
::/128unspecified address	
::/96	IETF reserved address;IPv4-compatible IPv6 address
::ffff:0:0/96	IPv4-mapped IPv6 address
::/8	reserved
fc00::/7	unique-local address
ff00::/8	multicast address
2001:db8::/3	documentation addresses

- Egress
- Permit sending all ICMPv6 packets for Neighbor Discovery and Path MTU Discovery that is a function necessary for the communication with IPv6
- Deny sending the packets which contain special-use prefix in the source address field
  - ::1/128 : loop back address
  - ::/128 : unspecified address
  - ::/96 : IETF reserved address;IPv4-compatible IPv6 address
  - ::ffff:0:0/96 : IPv4-mapped IPv6 address
  - ::/8 : reserved
  - fc00::/7 : unique-local address
  - ff00::/8 : multicast address
  - 2001:db8::/32 : documentation address

Architecture Considerations

- Addressing / Naming
  - What subnet boundaries make sense
    - your own network infrastructure
    - filtering considerations
  - Endpoint Identifier management
    - address automation vs obscurity vs auditability
  - DNS and DHCPv6 Considerations
- Native Routing vs Tunnels
- Management
- Security

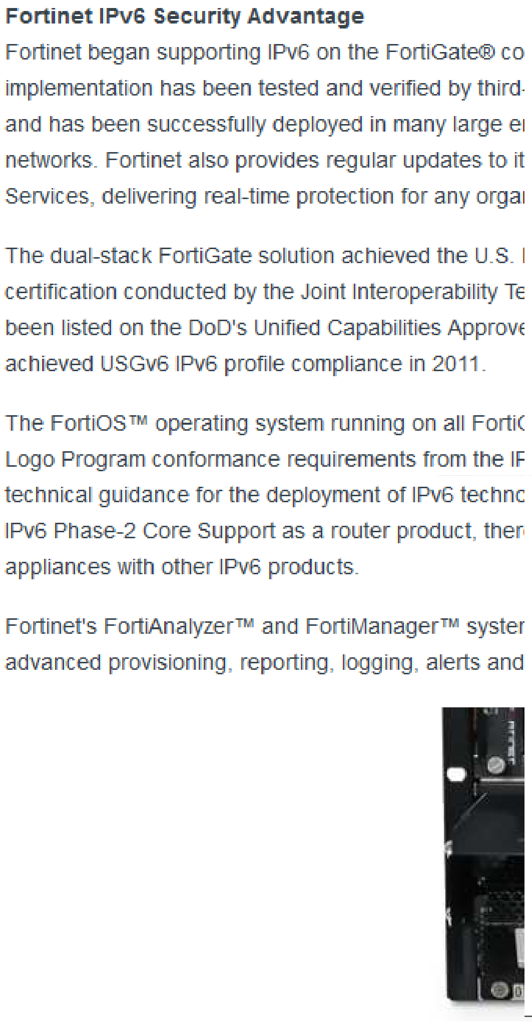
The Architecture is a key element

Forehand Planning is the key

- Hackers might be better skilled about IPv6 than admin team / security team / network team
- Vision for the business or the adoption driver
- IPv6 Training
- IP architecture that supports the vision -> IPv6 addressing scheme + design
- Evaluate infrastructure readiness to support the IPv6 implementation of the architecture
- Drive requirements and define purchasing strategy
- Align with other initiatives to accelerate readiness
- Define timeline

Overnight Adoption is Limiting and Expensive

Fastest IPv6 Firewall



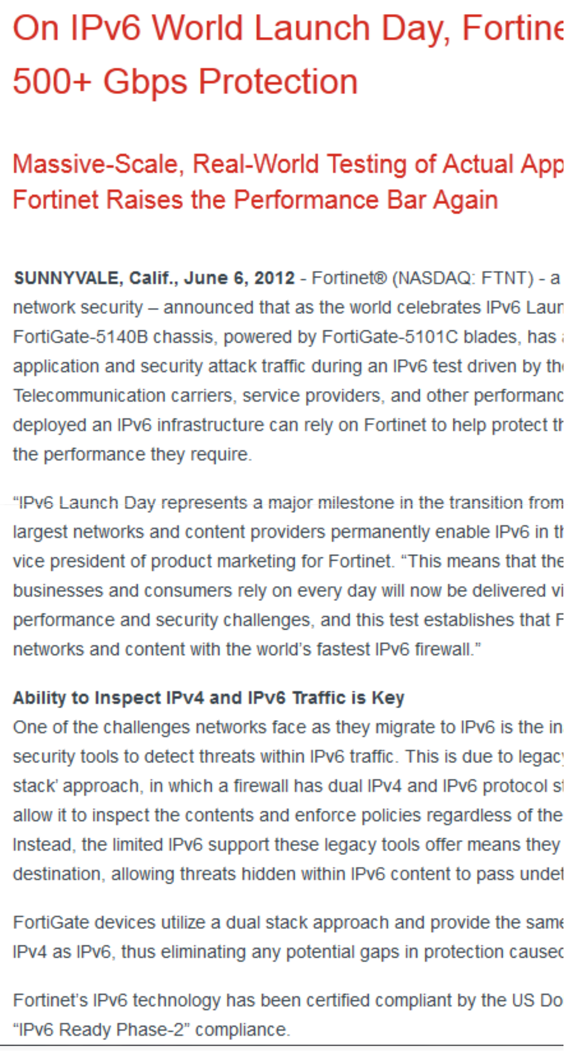
Fortinet IPv6 Security Advantage

Fortinet began supporting IPv6 on the FortiGate® co implementation has been tested and verified by third- and has been successfully deployed in many large e networks. Fortinet also provides regular updates to it Services, delivering real-time protection for any orga

The dual-stack FortiGate solution achieved the U.S. certification conducted by the Joint Interoperability Te been listed on the DoD's Unified Capabilities Approve achieved USGv6 IPv6 profile compliance in 2011.

The FortiOS™ operating system running on all Forti Logo Program conformance requirements from the IP technical guidance for the deployment of IPv6 techno IPv6 Phase-2 Core Support as a router product, ther appliances with other IPv6 products.

Fortinet's FortiAnalyzer™ and FortiManager™ syster advanced provisioning, reporting, logging, alerts and



On IPv6 World Launch Day, Fortine 500+ Gbps Protection

Massive-Scale, Real-World Testing of Actual App Fortinet Raises the Performance Bar Again

SUNNYVALE, Calif., June 6, 2012 - Fortinet® (NASDAQ: FTNT) - a network security – announced that as the world celebrates IPv6 Laur FortiGate-5140B chassis, powered by FortiGate-5101C blades, has application and security attack traffic during an IPv6 test driven by th Telecommunication carriers, service providers, and other performanc deployed an IPv6 infrastructure can rely on Fortinet to help protect th the performance they require.

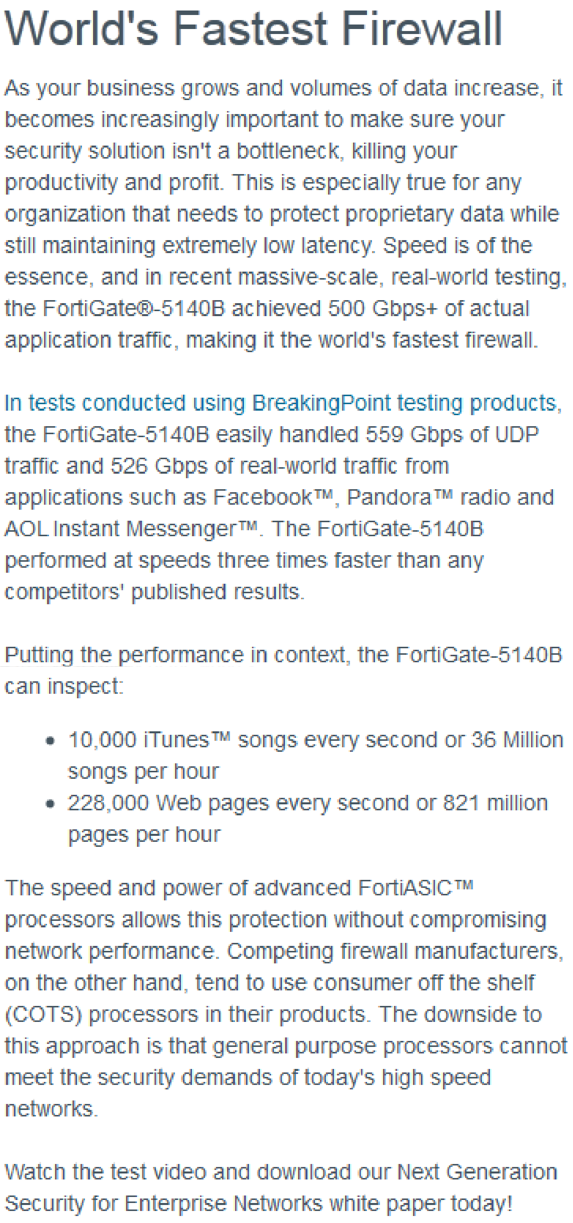
"IPv6 Launch Day represents a major milestone in the transition from largest networks and content providers permanently enable IPv6 in t vice president of product marketing for Fortinet. "This means that the businesses and consumers rely on every day will now be delivered vi performance and security challenges, and this test establishes that F networks and content with the world's fastest IPv6 firewall."

Ability to Inspect IPv4 and IPv6 Traffic is Key

One of the challenges networks face as they migrate to IPv6 is the in security tools to detect threats within IPv6 traffic. This is due to legac stack' approach, in which a firewall has dual IPv4 and IPv6 protocol s allow it to inspect the contents and enforce policies regardless of the Instead, the limited IPv6 support these legacy tools offer means they destination, allowing threats hidden within IPv6 content to pass unde

FortiGate devices utilize a dual stack approach and provide the same IPv4 as IPv6, thus eliminating any potential gaps in protection cause

Fortinet's IPv6 technology has been certified compliant by the US Do "IPv6 Ready Phase-2" compliance.



World's Fastest Firewall

As your business grows and volumes of data increase, it becomes increasingly important to make sure your security solution isn't a bottleneck, killing your productivity and profit. This is especially true for any organization that needs to protect proprietary data while still maintaining extremely low latency. Speed is of the essence, and in recent massive-scale, real-world testing, the FortiGate®-5140B achieved 500 Gbps+ of actual application traffic, making it the world's fastest firewall.

In tests conducted using BreakingPoint testing products, the FortiGate-5140B easily handled 559 Gbps of UDP traffic and 526 Gbps of real-world traffic from applications such as Facebook™, Pandora™ radio and AOL Instant Messenger™. The FortiGate-5140B performed at speeds three times faster than any competitors' published results.

Putting the performance in context, the FortiGate-5140B can inspect:

- 10,000 iTunes™ songs every second or 36 Million songs per hour
- 228,000 Web pages every second or 821 million pages per hour

The speed and power of advanced FortiASIC™ processors allows this protection without compromising network performance. Competing firewall manufacturers, on the other hand, tend to use consumer off the shelf (COTS) processors in their products. The downside to this approach is that general purpose processors cannot meet the security demands of today's high speed networks.

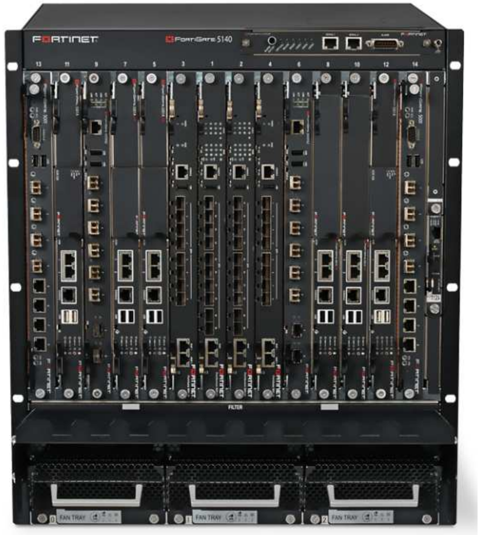
Watch the test video and download our Next Generation Security for Enterprise Networks white paper today!

Fortinet´s IPv6 Firewall

Core Backbone

Stateful Inspection

Virtualization



Transition Techniques

Unified Threat Management

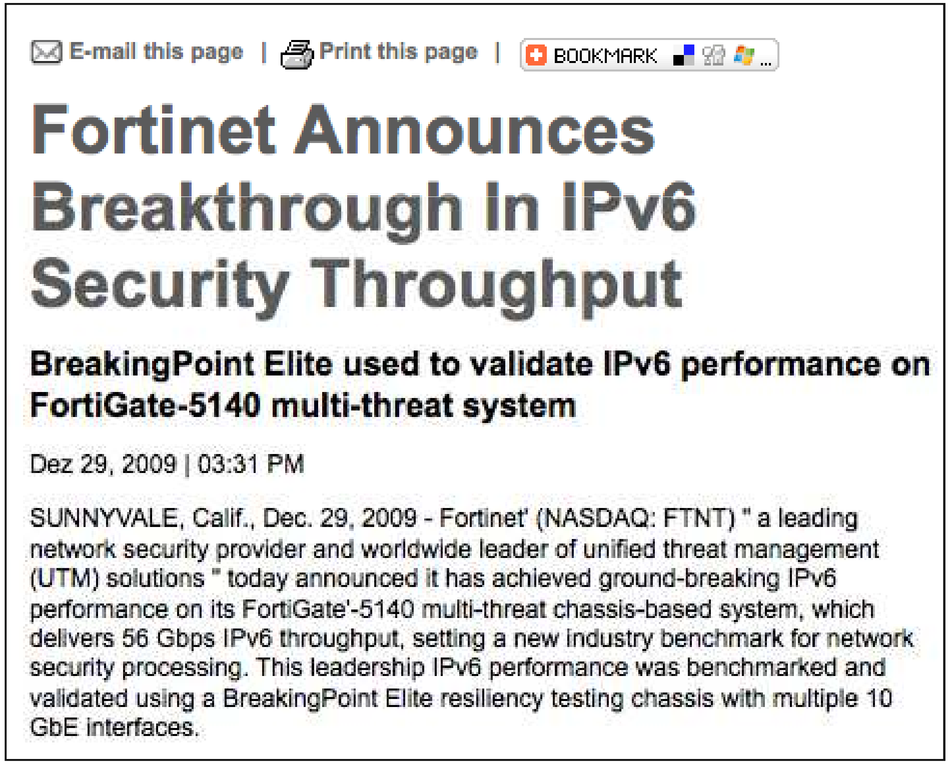
Performance

GTP, SCTP Diameter, SIP

Management

Fortinet IPv6 Strategy

- Feature Parity on all function with IPv4 and IPv6 on higher layers
  - Application unaware weather it runs on IPv4 or IPv6
- IPv6 Firewalling 3+ years integrated
- Stepwise extension to a complete functionality on IPv6



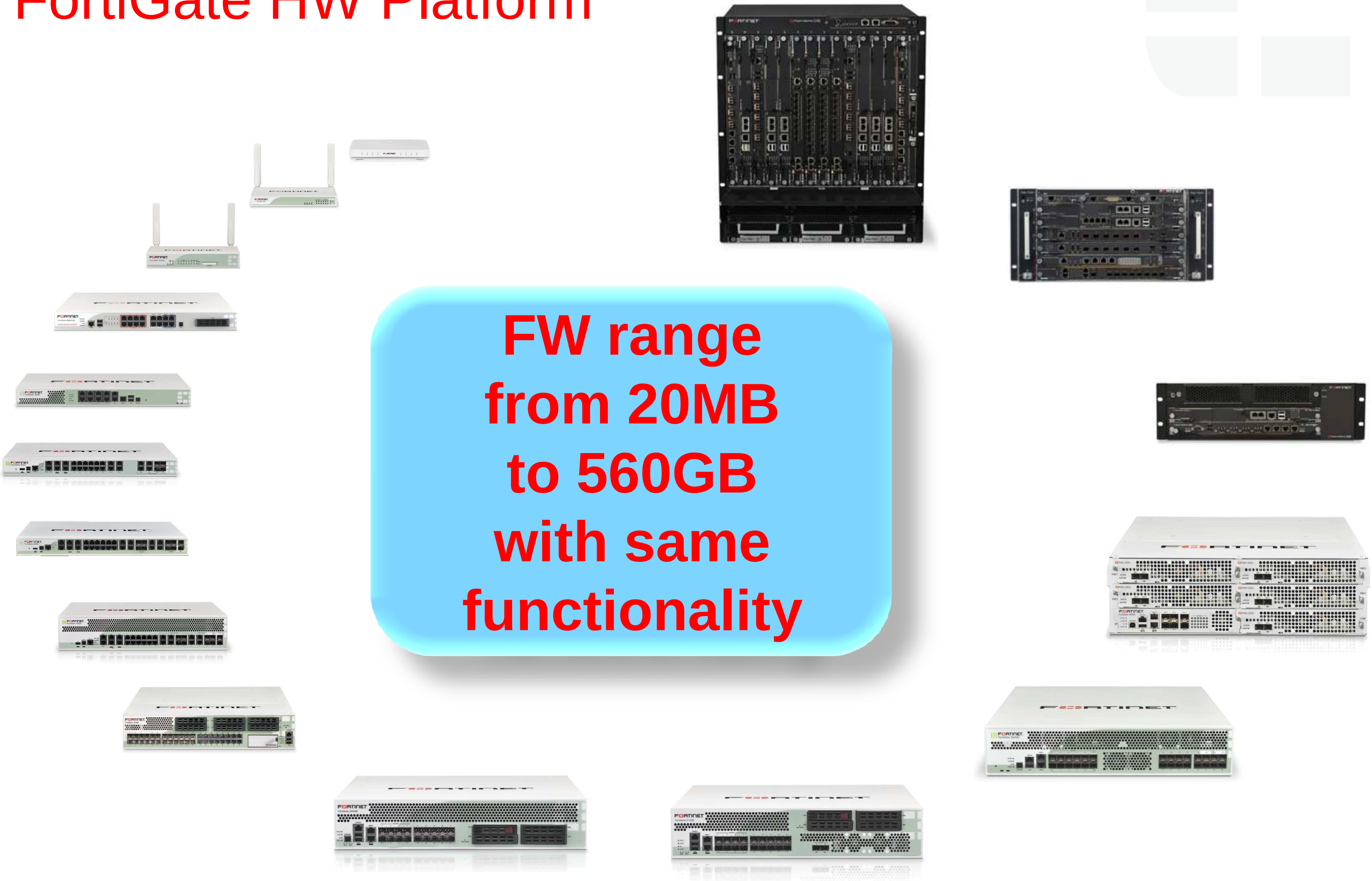
Fortinet Announces Breakthrough In IPv6 Security Throughput

BreakingPoint Elite used to validate IPv6 performance on FortiGate-5140 multi-threat system

Dez 29, 2009 | 03:31 PM

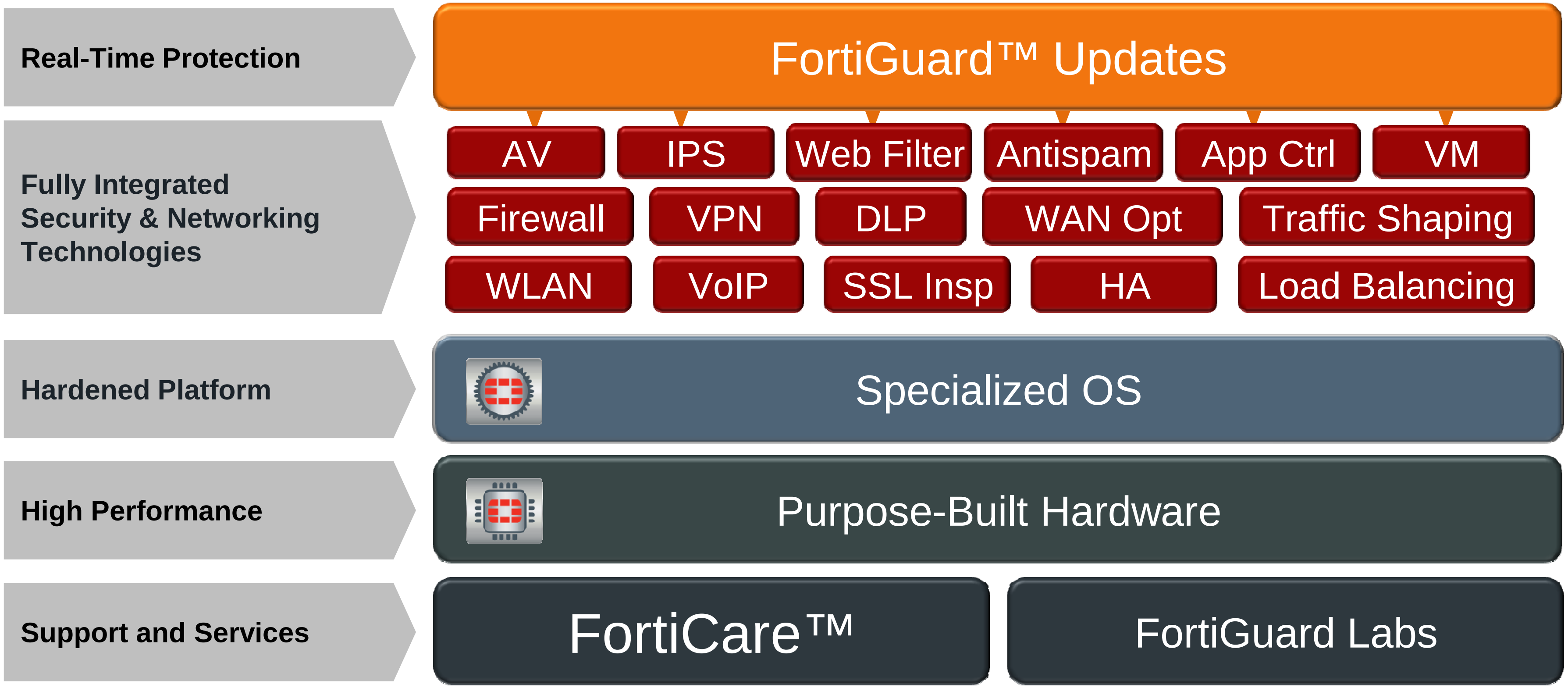
SUNNYVALE, Calif., Dec. 29, 2009 - Fortinet' (NASDAQ: FTNT) " a leading network security provider and worldwide leader of unified threat management (UTM) solutions " today announced it has achieved ground-breaking IPv6 performance on its FortiGate'-5140 multi-threat chassis-based system, which delivers 56 Gbps IPv6 throughput, setting a new industry benchmark for network security processing. This leadership IPv6 performance was benchmarked and validated using a BreakingPoint Elite resiliency testing chassis with multiple 10 GbE interfaces.

FortiGate HW Platform



FW range from 20MB to 560GB with same functionality

FortiGate: Integrated Architecture



Real-Time Protection

FortiGuard™ Updates

Fully Integrated Security & Networking Technologies

AV | IPS | Web Filter | Antispam | App Ctrl | VM

Firewall | VPN | DLP | WAN Opt | Traffic Shaping

WLAN | VoIP | SSL Insp | HA | Load Balancing

Hardened Platform

Specialized OS

High Performance

Purpose-Built Hardware

Support and Services

FortiCare™

FortiGuard Labs

- Purpose-built to deliver overlapping, complementary security
- Provides both flexibility & defense-in-depth capabilities

Today implemented for IPv4 & IPv6

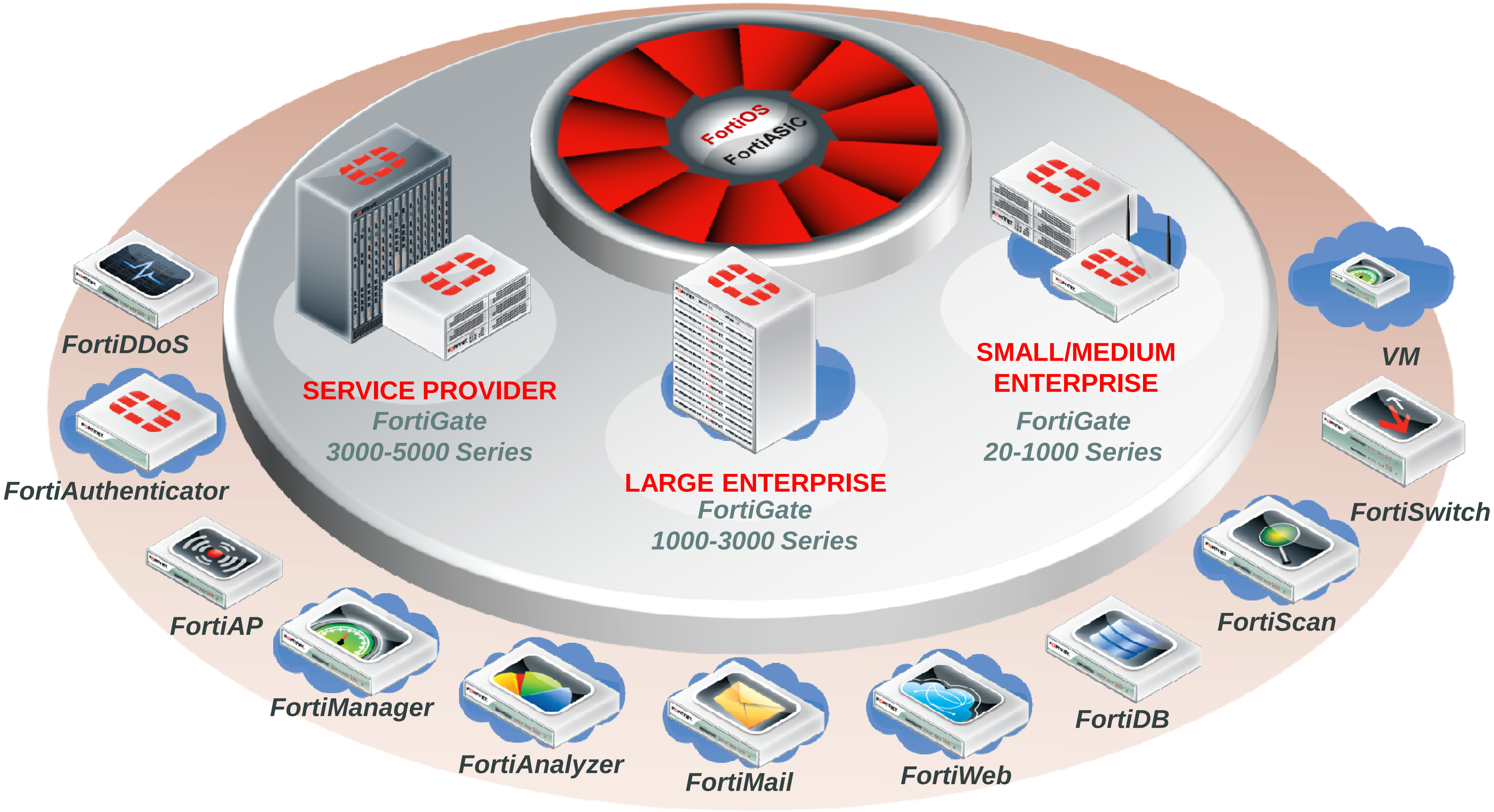
- Stateful Firewalling and Routing
  - Serviceobjects (eg ICMPv6), IPv6 Addressobjects
- Dynamic Routing, OSPF / RIP / BGP
- AntiVirus Scanning
  - http(s), ftp, smtp(s), imap(s), pop3(s), Instant-Messaging, nntp
- Intrusion Prevention
  - Signature based IPS/IDS and DoS-Protection
- URL Filtering
- Data Leak Prevention
- Management of the device via IPv6
  - eg SSH or https via IPv6 for devicemanagement

Today implemented for IPv4 & IPv6

- Bandwidth Management
  - Shaping, QoS
- IPSec (IKEv1 & IKEv2)
- DNS (AAAA Record)
- IPv4 over IPv6 Tunneling
- IPv6 over IPv4 Tunneling (eg Tunnelbroker like SixXS)
- SIP ALG (Application Gateway)
  - Carrier-grade SIP-ALG. SIP-Fuzzing Protection, Pinholing, Rate-Control etc.
- Application Control
- Logging and Reporting of Datatraffic, Reporting on FortiAnalyzer

and much more

Broad Product Portfolio



Questions