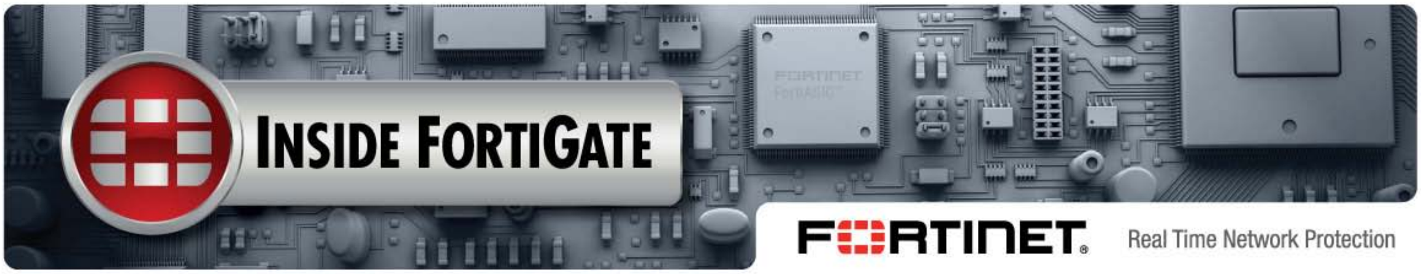
FORTINET

TECHNOLOGY BRIEF

Integrated Switch Fabric

A uniquely scalable approach to forwarding and security processing



Introduction

When designing the next generation of high-end FortiGate appliances the design team at Fortinet wanted to achieve that often referenced modular and scalable architecture, but to deliver it within an appliance utilizing the power of the new FortiASIC-NP4 and FortiASIC-SP2 designs. Initially introduced in the FortiGate 1240B appliance, the integrated switch fabric design provides for an any-to-any approach to traffic forwarding powered by the FortiASIC-NP4 with additional security processing offload capabilities being delivered by the FortiASIC-SP2

Integrated Switch Fabric

The integrated switch fabric (ISF) design of today's high-end FortiGate appliances provides three significant advantages when designing security solutions

- ISF allows the FortiASIC-NP4 to provide increased port density where multiple 1-Gbps ports are required.
- ISF provides line rate firewall processing across the entire appliance, any port to any port.
- ISF enables security processing resources to be shared across physical ports

FortiASIC-NP4

The FortiASIC-NP4 belongs to a family of purpose built high performance ASICs designed to accelerate security services at the interface level hence the term Network Processor. The FortiASIC-NP4 design provides

- Packet size independent wirespeed low latency performance for millions of sessions with dynamic address translation
- IPSec ESP encryption and decryption processing
- Anomaly based intrusion prevention, checksum offload, and packet defragmentation
- Traffic Shaping and Priority Queuing

The FortiASIC-NP4 itself comprises two 10-Gbps interfaces that connect in to the ISF to provide flexible port configurations without sacrificing performance.

Figure 1 illustrates a single NP4 connecting via an ISF to provide twenty 1-Gbps wirespeed ports – each port represents a separate firewall interface.

Multiple NP4s can be provided with various physical port combinations to build out a range of appliance designs.

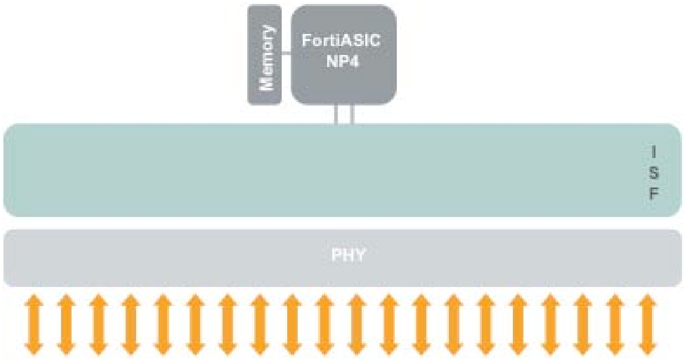


Figure 1. FortiASIC-NP4 and Integrated Switch Fabric

FortiASIC-SP2

The FortiASIC-SP2 represents the second generation of Fortinet Security Processor technology building on the runaway success of the ADM-XE2, ADM-FE8, and ASM-CE4 SP1 modules. The FortiASIC-SP2 provides, in addition to hardware based acceleration, a multi-core multi-threaded security processing complex which builds on the capabilities of the FortiASIC-NP4 to provide additional services, including, but not limited to IPS signature analysis, application control, DOS protection, and locally encrypted multicast acceleration.

The FortiASIC-SP2 is also able to connect directly to the ISF where it can be accessed by all physical ports.

Fortinet Mezzanine Cards

As a part of the next generation design goal for a modular architecture it was natural to include a separately available module to be installed in to the high-end platforms as performance requirements demanded. Since the physical size of current series of AMC cards presented some constraints to the performance goals of the new design, it was decided to opt for a larger form factor providing more space for future designs and thermal demands.

The Fortinet Mezzanine Card (FMC) has been designed to provide a combined physical port and processing resource – initially for the FortiGate 3950 series. The FMC based physical ports connect directly to the integrated switch fabric (ISF) with the processing resource, whether FortiASIC-NP4, or FortiASIC-SP2, having their own direct connections. In this way the additional processing power can be distributed across the entire appliance via the ISF.

Figure 2 illustrates a fully populated FortiGate 3950 showing both the onboard FortiASIC-NP4 and optional FMC hosted NP4 and SP2 modules. Meaning each FMC module has four 10-Gbps connections.

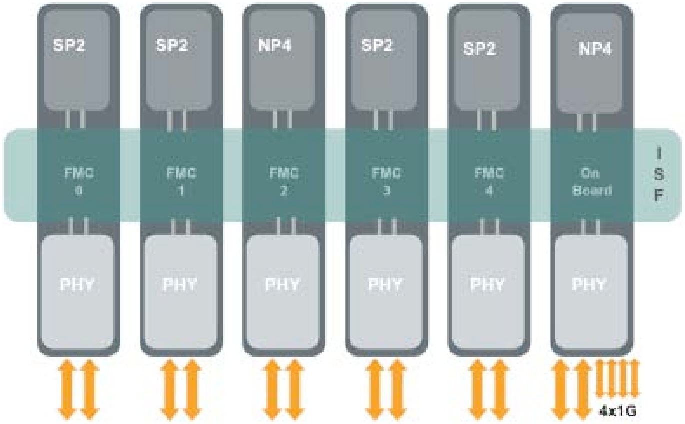


Figure 2. FMC and ISF Connectivity in a FortiGate 3950 Series System

At the heart of the FortiGate 3950 is a 24 port 10-Gbps integrated switch fabric. The ISF enables fully meshed connectivity between all the FMC slots and associated processing modules.

The FortiGate 3950 series has five slots, a *sixth slot* represents the on board physical port module and its FortiASIC-NP4 resources. Meaning that even with no modules installed, the FortiGate 3950 series can provide 20-Gbps of firewall performance.

Planned FMC Modules

The FMC-XD2 and FMC-XG2 represent the FortiASIC-NP4 and FortiASIC-SP2 powered modules respectively, in addition to these, multiple 1-Gbps SFP and RJ45 modules are also planned.

Packet Flow

All ISF enabled FortiGate units share the same capability of flexibly mapping resources and physical ports, however this is perhaps most evident with the FortiGate 3950 where multiple FMC modules will deliver different port and processing configurations over time.

As has been already stated, the ISF allows each port of the FortiGate 3950 series to utilize the resources from any of the FMC processing modules.

There is no requirement to use the processing resource (NP or SP) on the ingress FMC.

Figure 3 illustrates both these local FMC and cross-ISF flows. The cross-ISF flows are set up within the ISF and are created according to the egress port requirements.

Notice that only one NP or SP is used whether we have local FMC or cross-ISF forwarding.

Load Balancing

A future software enhancement will make it possible to use an NP4 as a load balancing module for multiple SP2 units to further assist in those topologies that require high capacity security processing.

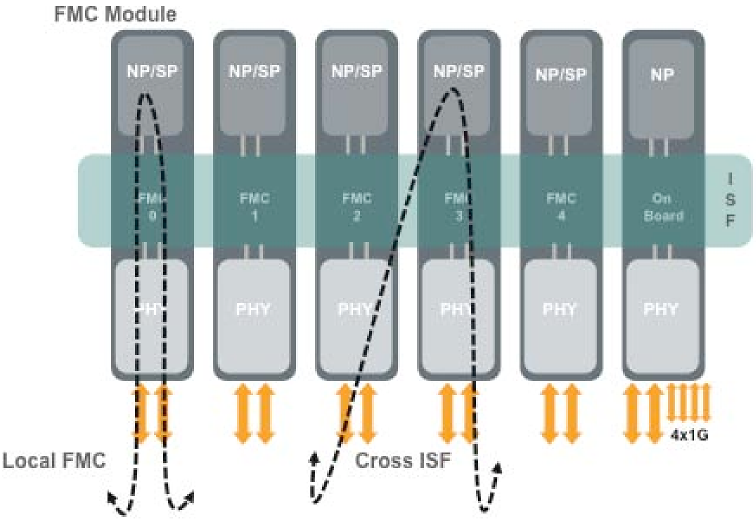


Figure 3. Example Packet Flow within a FortiGate 3950 Series System

Control Plane

Although not directly linked to the ISF implementation the control plane separation apparent with FortiASIC-NP4 powered platforms has been designed from their inception.

This separation includes prioritization of specific network control ingress traffic, a high priority CPU queue, and the ability to distribute control plane processing across multiple CPU cores. This process distribution ensures the CPU block is able to scale both the session set up and network control plane.

In addition, at egress control traffic is a dispatched to the priority output queue with a dedicated egress queue from the network or security processor minimizing any forwarding delays.

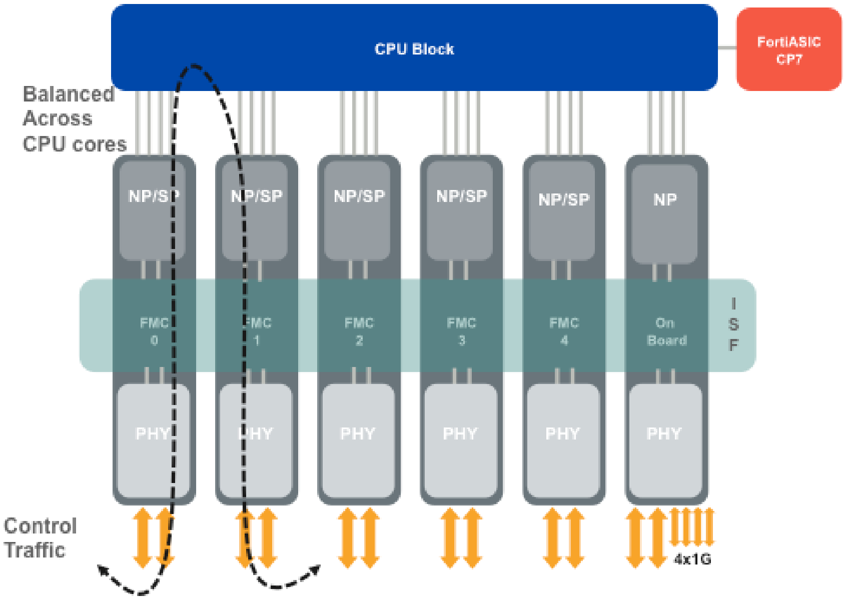


Figure 4. Control Plane Distribution

FortiGate 5000 Series Chassis-Based Systems

The flagship of the Fortinet product line also shares this integrated switch fabric approach, however it provides additional levels of sophistication, scalability, and redundancy not available from a standalone appliance.

The FortiGate 5000 series chassis-based systems allow FortiGate blades to be added to a common backplane, it is to this backplane that the interconnecting switch fabric blades are connecting. This Advanced Switch Fabric (ASF) can be programmed depending on the specific application of the chassis.

The ASF allows scalability not only in the NP4 and SP2 area but also for the control and so called slow path traffic that requires access to a host CPU. This linear scalability of control plane traffic allows for planned 1M plus connections per second.

The ASF can be provided in a dual redundant mode either within a chassis, or between chassis depending on the resilience demanded at the blade level.

FortiGate blade level resilience and redundancy can exist within or between chassis and this will form the subject of a separate paper.

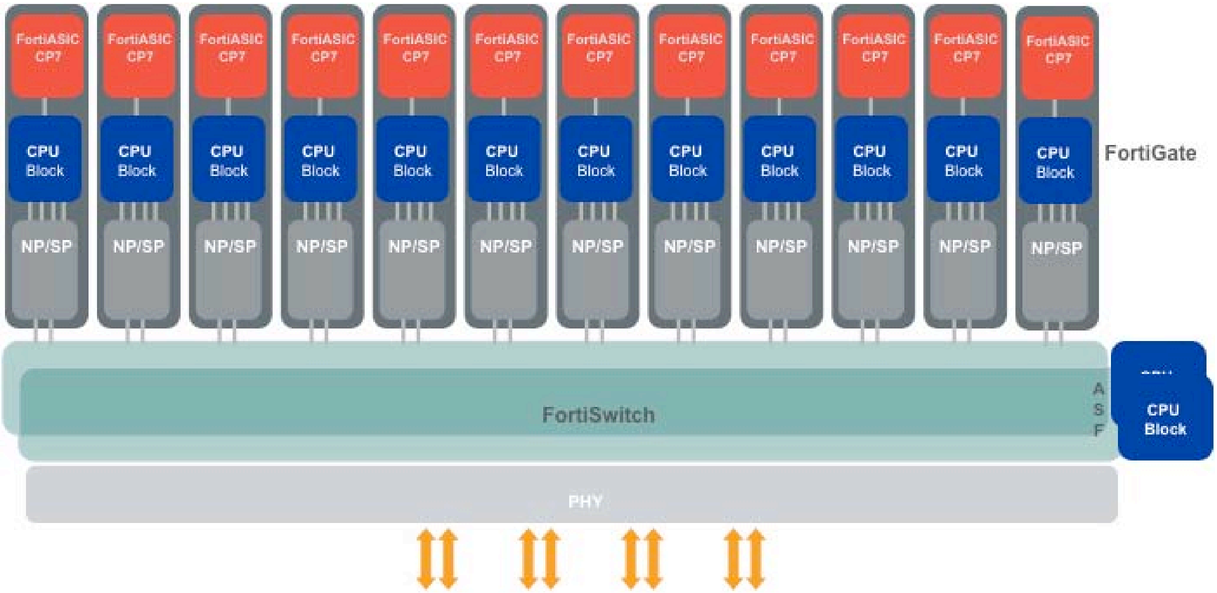


Figure 5. FortiGate 5000 Series Advanced Switch Fabric

Fortinet (NASDAQ: FTNT) is a worldwide provider of network secur.ity appliances and the market leader in unified threat management (UTM). Our products and subscription services provide broad, integrated and high-performance protection against dynamic security threats while simplifying the IT security infrastructure. Our customers include enterprises, service providers and government entities worldwide, including the majority of the 2009 Fortune Global 100. Fortinet's flagship FortiGate product delivers ASIC-accelerated performance and integrates multiple layers of security designed to help protect against application and network threats. Fortinet's broad product line goes beyond UTM to help secure the extended enterprise – from endpoints, to the perimeter and the core, including databases and applications. Fortinet is headquartered in Sunnyvale, Calif., with offices around the world.

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

EMEA SALES OFFICE – FRANCE
Fortinet Incorporated
120 rue Albert Caquot
06560, Sophia Antipolis, France
Tel +33.4.8987.0510
Fax +33.4.8987.0501

APAC SALES OFFICE – SINGAPORE
Fortinet Incorporated
61 Robinson Road, #09-04 Robinson Centre
Singapore 068893
Tel +65-6513-3730
Fax +65-6223-6784