Your Time Is Now

Cisco Next Generation Firewall and IPS

Dragan Novakovic
Security Consulting Systems Engineer

Cisco Connect

Portorož, 15. in 16. marec 2017
Cisco ASA with Firepower services

- World’s most widely deployed, enterprise-class ASA stateful firewall
- Granular Cisco® Application Visibility and Control (AVC)
- Industry-leading FirePOWER next-generation IPS (NGIPS)
- Reputation- and category-based URL filtering
- Advanced malware protection
Next Generation Firewall and IPS

- ASA 5506-X
- ASA 5512/15-X
- ASA 5508-X
- ASA 5506
- ASA 5516-X
- ASA 5545-X
- ASA 5525-X
- ASA 5555-X
- ASA 5585-X
- SSP10
- SSP20
- SSP40
- SSP60
- ISA3000
- FirePOWER 7000/8000
- NGIPS
- NGIPSv

- SMB/Teleworker
- Branch Office
- Internet Edge
- Campus
- Data Center
# Performance Highlights ASA 5500-X Model

<table>
<thead>
<tr>
<th></th>
<th>5506-X</th>
<th>5508-X</th>
<th>5516-X</th>
<th>5525-X</th>
<th>5545-X</th>
<th>5555-X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Throughput (ASA)</td>
<td>750 Mbps</td>
<td>1 Gbps</td>
<td>1.8 Gbps</td>
<td>2 Gbps</td>
<td>3 Gbps</td>
<td>4 Gbps</td>
</tr>
<tr>
<td>Throughput: FW + AVC 1</td>
<td>250 Mbps</td>
<td>450 Mbps</td>
<td>850 Mbps</td>
<td>1100 Mbps</td>
<td>1500 Mbps</td>
<td>1750 Mbps</td>
</tr>
<tr>
<td>Throughput: FW + AVC + NGIPS1</td>
<td>125 Mbps</td>
<td>250 Mbps</td>
<td>450 Mbps</td>
<td>650 Mbps</td>
<td>1000 Mbps</td>
<td>1250 Mbps</td>
</tr>
</tbody>
</table>

1 HTTP sessions with an average packet size of 1024 bytes.
Security Software Convergence

- Two Appliances
  - Two Management Consoles
    - ASA FW
    - Firepower NGIPS

- One Appliance – Two Images
  - ASA with Firepower Services
    - Firepower NGIPS
    - ASA FW

- One Appliance – One Image
  - One Management Console
    - Firepower Threat Defense (FTD)
Firepower Threat Defense

Granular Cisco® Application Visibility and Control (AVC)

Industry-leading FirePOWER next-generation IPS (NGIPS)

Reputation- and category-based URL filtering

Advanced malware protection
Security Software Convergence

ASA
- L2-L4 Stateful Firewall
- Scalable CGNAT, ACL, routing
- Application inspection

FirePOWER
- Threat-centric NGIPS
- AVC, URL Filtering for NGFW
- Advanced Malware Protection

Firepower Threat Defense (FTD)
- New converged NGFW/NGIPS image
- Full FirePOWER functionality for NGFW/NGIPS deployments
- ASA Datapath with TCP Normalizer, NAT, ACL, dynamic routing, failover functions
Firepower 9300 – High-end Platform

Supervisor
- Application deployment and orchestration
- Network attachment and traffic distribution
- Clustering base layer for ASA/FTD

Network Modules
- 10GE, 40GE, and 100GE
- Hardware bypass for inline NGIPS

Security Modules
- Embedded Smart NIC and crypto hardware
- Cisco (ASA, FTD) and third-party (Radware DDoS) applications
- Standalone or clustered within and across chassis
Supervisor Simplified Hardware Diagram

Internal Switch Fabric
(up to 24x40GE)

Security Module 1

Security Module 2

Security Module 3

On-board 8x10GE interfaces

NM Slot 1

NM Slot 2

RAM

x86 CPU

System Bus

Ethernet

2x40Gbps

2x40Gbps

2x40Gbps

5x40Gbps

5x40Gbps

2x40Gbps

5x40Gbps
Firepower 9300 Security Modules

- Same modules must be installed across entire chassis or cluster
  - **SM-44**: 88 x86 CPU cores (10-15% higher performance than SM-36)
  - **SM-36**: 72 x86 CPU cores
  - **SM-24**: 48 x86 CPU cores

- x86 Turbo Mode for all security modules
  - Triggered when 25% of ASA cores reach 80% load
  - Disabled when all ASA cores drop below 60% load
  - Increases performance by 10-20%
Security Module Simplified Diagram

- **RAM**: 256GB
- **x86 CPU 1**
  - SM24: 24 cores
  - SM36: 36 cores
  - SM44: 44 cores
- **x86 CPU 2**
  - SM24: 24 cores
  - SM36: 36 cores
  - SM44: 44 cores
- **Smart NIC and Crypto Accelerator**
- **System Bus**
- **Ethernet**: 2x100 Gbps
- **Backplane Supervisor Connection**: 2x40 Gbps
# Performance Highlights Cisco Firepower Model

<table>
<thead>
<tr>
<th></th>
<th>9300 with 1 SM-24</th>
<th>9300 with 1 SM-36</th>
<th>9300 with 1 SM-44</th>
<th>9300 with 3 SM-44</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Throughput (ASA)</td>
<td>75 Gbps</td>
<td>80 Gbps</td>
<td>80 Gbps</td>
<td>234 Gbps</td>
</tr>
<tr>
<td>Throughput: FW + AVC (FTD)¹</td>
<td>30 Gbps</td>
<td>42 Gbps</td>
<td>54 Gbps</td>
<td>135 Gbps</td>
</tr>
<tr>
<td>Throughput: FW + AVC + NGIPS (FTD)¹</td>
<td>24 Gbps</td>
<td>34 Gbps</td>
<td>53 Gbps</td>
<td>133 Gbps</td>
</tr>
</tbody>
</table>

¹ HTTP sessions with an average packet size of 1024 bytes.
Next Generation Firewall and IPS

ASA 5508-X
ASA 5506-X
ISA3000
ASA 5512/15-X
ASA 5516-X
ASA 5545-X
ASA 5525-X
ASA 5555-X
ASA 5585-X
SSP10/20/40/60
ASA 5512/15-X
ASA 5506
ASA 5508
ASA 5516
ASA 5525
ASA 5545
ASA 5555
ASA 5585

SMB/Teleworker
Branch Office
Internet Edge
Campus Data Center

FirePOWER 7000/8000 NGIPS

NGIPSv
FTDv
Firepower 9300

© 2017 Cisco and/or its affiliates. All rights reserved.
Firepower 4100 Overview

Built-in Supervisor and Security Module
• Same hardware and software architecture as 9300
• Fixed configurations (4110, 4120, 4140, 4150)

Solid State Drives
• Independent operation (no RAID)
• Slot 1 today provides limited AMP storage
• Slot 2 provides optional AMP storage

Onboard Connectivity
• 8 x 10G SFP

Network Modules
• 10GE/40GE interchangeable with 9300
• Partially overlapping fail-to-wire controller options
Firepower 4100 Logical Diagram

- **RAM**
  - 4110: 64Gb
  - 4120: 128Gb
  - 4140: 256Gb
  - 4150: 256Gb

- **x86 CPU 1**
  - 4110: 12 cores
  - 4120: 12 cores
  - 4140: 36 cores
  - 4150: 44 cores

- **x86 CPU 2**
  - 4110: N/A
  - 4120: 12 cores
  - 4140: 36 cores
  - 4150: 44 cores

- **Smart NIC and Crypto Accelerator**
  - 4110: 1x100Gbps
  - 4120-4150: 2x100Gbps

- **Internal Switch Fabric**
  (up to 18x40GE)
  - 2x40Gbps
  - 5x40Gbps

- **On-board 8x10GE interfaces**

- **NM Slot 1**

- **NM Slot 2**

- **System Bus**

- **Ethernet**

- **x86 CPU**
  - 4110: N/A
  - 4120: 12 cores
  - 4140: 36 cores
  - 4150: 44 cores

- **RAM**
  - 4110: 64Gb
  - 4120: 128Gb
  - 4140: 256Gb
  - 4150: 256Gb

- **NM Slot 1**

- **NM Slot 2**
Firepower 9300 and 4100 series performance

<table>
<thead>
<tr>
<th>Firewall Throughput (ASA)</th>
<th>4110</th>
<th>4120</th>
<th>4140</th>
<th>4150</th>
<th>1 SM-24</th>
<th>1 SM-36</th>
<th>1 SM-44</th>
<th>3 SM-44</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Throughput: FW + AVC (FTD)</td>
<td>35 Gbps</td>
<td>60 Gbps</td>
<td>70 Gbps</td>
<td>75 Gbps</td>
<td>75 Gbps</td>
<td>80 Gbps</td>
<td>80 Gbps</td>
<td>234 Gbps</td>
</tr>
<tr>
<td>Throughput: FW + AVC + NGIPS (FTD)</td>
<td>12 Gbps</td>
<td>20 Gbps</td>
<td>25 Gbps</td>
<td>30 Gbps</td>
<td>30 Gbps</td>
<td>42 Gbps</td>
<td>54 Gbps</td>
<td>135 Gbps</td>
</tr>
<tr>
<td>Throughput: FW + AVC + NGIPS (FTD)</td>
<td>10 Gbps</td>
<td>15 Gbps</td>
<td>20 Gbps</td>
<td>24 Gbps</td>
<td>24 Gbps</td>
<td>34 Gbps</td>
<td>53 Gbps</td>
<td>133 Gbps</td>
</tr>
</tbody>
</table>

1 HTTP sessions with an average packet size of 1024 bytes.
FPR 2100 with Firepower Threat Defense
Cisco Firepower 2100

Purpose Build Hardware for Cisco NGFW
- Fixed configurations (2110, 2120, 2130, 2140)
- Dual Power Supplies 2130-2140

Solid State Drives
- Independent operation (no RAID)
- Slot 1 provides default storage
- Slot 2 provides optional AMP storage

Onboard Connectivity
- 12 x 1G RJ45
- 4 x 1G SFP
- Management and Console Port

Network Modules (2130 and 2140 Only)
- 8 x 10GE SFP module
- Fail-to-wire options (future)
Firepower 2100 Logical Diagram

- RAM
- x86 CPU
- Octeon NPU
- Internal Switch Fabric
  - On-board 12x1GE interfaces
  - On-board 4x1GE SPF interfaces
  - NM Slot 2130-2140

System Bus

Ethernet
## Firepower 2100, 4100, 9300 Snapshot

<table>
<thead>
<tr>
<th>Features</th>
<th>FPR 2100</th>
<th>FPR 4100</th>
<th>FPR 9300</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throughput range Firewall + AVC</td>
<td>2 to 8 Gbps</td>
<td>12 to 30 Gbps</td>
<td>30 to 54 Gbps</td>
</tr>
<tr>
<td>Throughput range Firewall + AVC+IPS</td>
<td>2 to 8 Gbps</td>
<td>10 to 24 Gbps</td>
<td>24 to 53 Gbps</td>
</tr>
<tr>
<td>Interface Speed</td>
<td>1/10 Gbps</td>
<td>1/10/40 Gbps</td>
<td>1/10/ 40/100 Gbps</td>
</tr>
<tr>
<td>Rack Unit size</td>
<td>1 RU</td>
<td>1 RU</td>
<td>3 RU</td>
</tr>
<tr>
<td>Clustering</td>
<td>Roadmap</td>
<td>Yes (6.2)</td>
<td>Yes (6.2)</td>
</tr>
<tr>
<td>Other Apps</td>
<td>No</td>
<td>Yes (Radware DDoS)</td>
<td>Yes (Radware DDoS)</td>
</tr>
<tr>
<td>Chassis Manager</td>
<td>Unified With FMC / FDM</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
# Software Support by Platform

<table>
<thead>
<tr>
<th>Platform</th>
<th>Firepower Threat Defense</th>
<th>Firepower NGIPS</th>
<th>ASA Firewall</th>
<th>Firepower Services on ASA</th>
</tr>
</thead>
<tbody>
<tr>
<td>FirePOWER 7000 Series</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>FirePOWER 8000 Series</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>ASA Low-end (5506/08/16)</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ASA Mid-Range (5512/15/25/45/55)</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ASA High-end (5585 SSP-10/20/40/60)</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Firepower 2100</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Firepower 4100, 9300 (SSP 3RU - SM-24/36)</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>VMware</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>AWS</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
</tr>
</tbody>
</table>
Firewall Design: Modes of Operation

- **Routed Mode** is the traditional mode of the firewall. Two or more interfaces that separate L3 domains – Firewall is the Router and Gateway for local hosts.
Firewall Design: Modes of Operation

- **Routed Mode** is the traditional mode of the firewall. Two or more interfaces that separate L3 domains – Firewall is the Router and Gateway for local hosts.

- **Transparent Mode** is where the firewall acts as a bridge functioning at L2
  - Transparent mode firewall offers some unique benefits in the DC
  - Transparent deployment is tightly integrated with our ‘best practice’ data center designs

- **Note:**
  - No multiple context mode and RA VPN available on FTD today
  - Routed or transparent mode configured with setup dialog
    - Changing between these modes requires re-registering with FMC
    - Policies will be re-deployed
FTD - Mix and Match Interface Modes

Routed/Transparent

Policy Tables

Inline Pair 1

Inline Pair 2

Inline Tap

Passive

Interfaces

Inline Set
Integrated Routing and Bridging

- Allows configuration of bridges in routed firewall mode
- Regular routed interfaces can now co-exist with BVI interfaces and interfaces that are members of bridge groups.
- Available with FTD 6.2 release
Flow Offload – Use Cases

• Trusted flow processing with **limited security visibility**
• Maximize single-flow throughput and packet rate, minimize latency
• High performance compute, frequency trading, demanding data center applications
Flow Offload Operation

**Full Inspection**
- Dynamically program offload engine after flow establishment
- Bring flows out of and back to full inspection on demand

**Flow Offload**
- Limited pseudo-stateful inspection in x86 or NPU
- Bidirectional byte count and TCP state tracking

**Application Instance**
- New and fully inspected flows
- Offload instructions
- Established trusted and jumbo flows
- Full Cisco® ASA, NGFW, or NGIPS Engine
- Lightweight Data Path
- Flow updates
Reduce complexity with simplified, consistent management

Unified
- Network-to-endpoint visibility
- Manages firewall, applications, threats, and files
- Track, contain, and recover remediation tools

Scalable
- Central, role-based management
- Multitenancy
- Policy inheritance

Automated
- Impact assessment
- Rule recommendations
- Remediation APIs

Cisco Firepower™ Management Center
Why Recommended rules are important

- Context enabled the detections that are relevant to your specific network
- Firepower Recommendations makes sure your system has the right detections enabled
Impact Assessment

How Relevant is the Attack?

- Prevents information overload

<table>
<thead>
<tr>
<th>IMPACT FLAG</th>
<th>ADMINISTRATOR ACTION</th>
<th>WHY</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Act Immediately, Host vulnerable or Compromised</td>
<td>Event corresponds to vulnerability mapped to host</td>
</tr>
<tr>
<td>2</td>
<td>Investigate, Potentially Vulnerable</td>
<td>Relevant port open or protocol in use, but no vulnerability mapped</td>
</tr>
<tr>
<td>3</td>
<td>Good to Know, Currently Not Vulnerable</td>
<td>Relevant port not open or protocol not in use</td>
</tr>
<tr>
<td>4</td>
<td>Good to Know, Unknown Target</td>
<td>Monitored network, but unknown host</td>
</tr>
<tr>
<td>0</td>
<td>Good to Know, Unknown Network</td>
<td>Unmonitored network Event outside profiled networks If you have a fully profiled network this may be a critical event!</td>
</tr>
</tbody>
</table>
Correlation Rules / Correlation Policy

Respond in real time to threats and network traffic deviates from its normal profile

Correlation Policy

Correlation Rule → Correlation Event

Correlation Rule → Action

Email
Syslog
SNMP
Remediation Module
Network traffic deviates from its normal

Correlation Rule to:

• Ensure only HTTPS traffic is used on port 443
• Ensure traffic is initiated by a Host with a defined Location (host Attribute) is POS
• Ensure the HTTPS traffic from the POS host is received on hosts in the PCI network.
• Any traffic outside this profile will generate an event.
Production Network Change

As new IP addresses appear on the network, Firepower Correlation Polices can trigger Nmap to perform an active scan of the new hosts.
Correlation Rule example
Ensure compliance before granting access

Identity Services Engine (ISE)

- **ISE**
  - BYOD
  - Guest Access
  - Segmentation

- **pxGrid**
  - Propagate
    - User Context
    - Device context
    - Access policies

- **TrustSec**
  - Employee Tag
  - Guest Tag
  - Supplier Tag
  - Quarantine Tag
  - Server Tag
  - Suspicious Tag

- **Firepower Management Center**

- **Set access control policies**
- **Propagate rules and context**
- **Establish a secure network**
- **Remediate breaches automatically**

Policy automation