Cisco Next Generation Firewalls and IPS

Dragan Novakovic
Security Consulting Systems Engineer
dnovakov@cisco.com
Today’s Agenda

• Firepower System Architecture Overview
• Platforms & Capabilities
• Management Options
• Firepower 6.1 New Capabilities
Systems Architecture Overview
How did we get here from there?

- Adaptive Security Appliance (ASA)
- FirePOWER NGIPS
- ASA with FirePOWER Services?
- Firepower NGFW?
ASA “Adaptive Security Appliance”

- HA and Clustering
- VPN
- Protocol Inspection
- Data Center Security
- Network Firewall (Routing | Switching)
- Mix Multi Context Mode
- Identity Based Policy Control
- Service Provider Security

ASDM (OnBox) / Command Line
Cisco Security Manager / RESTful API for Management
Firepower NGIPS Platforms

- Firepower Next Generation IPS
  - Best of breed IPS
  - Based on open source Snort
  - Integrated Advanced Malware Protection

- Acquired by Cisco in 2013
Next Generation IPS platform - FirePower 8300

Single-pass, high-performance, low-latency

Flexible in Software
- Firepower NGIPS & AMP

Flexible in Hardware
- Modular for options in Interfaces, including 10GE and 40GE
- High-Performance:
  - 15-60Gbps (with 8350-8390)

Cost Effective
- Best in class for IPS by NSS Labs
- Best in class for NGFW by NSS Labs
- Best in class for Breach Detection by NSS Labs
## Cisco FirePOWER Platform Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Virtual</th>
<th>7000</th>
<th>7100</th>
<th>8100</th>
<th>8200/8300</th>
</tr>
</thead>
<tbody>
<tr>
<td>1GE Interfaces</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>1GE Interfaces YES</td>
<td>YES</td>
</tr>
<tr>
<td>10GE Interfaces</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>40GE Interfaces</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>SFP Ports</td>
<td>NO</td>
<td>YES *</td>
<td>YES **</td>
<td>YES **</td>
<td>YES **</td>
</tr>
<tr>
<td>Hardware Bypass</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Software Bypass</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Hardware Fast Pass</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>L3 Mode</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
</tbody>
</table>

* 7115, 7125, and 7150 models only  
** Fiber-to-SFP Tranceiver
ASA with FirePOWER Services

- Cisco ASA is world’s most widely deployed, enterprise-class 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

Cisco Collective Security Intelligence Enabled

- Clustering & High Availability
- Intrusion Prevention (Subscription)
- Network Firewall Routing | Switching
- Application Visibility & Control
- FireSIGHT Analytics & Automation
- Advanced Malware Protection (Subscription)
- Built-in Network Profiling
- WWW URL Filtering (Subscription)
- Identity-Policy Control & VPN
- WWW
- Cisco Collective Security Intelligence Enabled

Better together

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public 9
Firepower Threat Defense

Integrated Software - Single Management
Platforms & Capabilities
Cisco Firepower NGFW Product Family
Running Firepower Threat Defense (FTD)

Performance and Scalability

SMB & Distributed Enterprise
- ASA 5506H-X
- ASA 5506W-X
- ASA 5506-X

Commercial & Enterprise
- ASA 5508-X / ASA 5512-X
- ASA 5516-X / ASA 5515-X
- ASA 5525-X
- ASA 5545-X
- ASA 5555-X

Data Center, High Performance Computing, Service Provider
- Firepower 9300 (SM-24, SM-36, SM-44)
- Firepower 4140 / Firepower 4150
- Firepower 4110 / Firepower 4120
- FTDv
Cisco NGFW Platforms

Firepower Threat Defense for ASA 5500-X

Firepower 4100 Series and Firepower 9300

Firepower Services on ASA 5500-X and 5585-X

250 Mb -> 1.75 Gb (Max AVC throughput)

41xx = 12 Gb -> 25 Gb
93xx = 25 Gb -> 100Gb

4.5 Gb -> 15 Gb (Max AVC throughput)

NGFW capabilities all managed by Firepower Management Center
Firepower 4100 Series

Introducing four new high-performance models

Performance and Density Optimization
- 10-Gbps and 40-Gbps interfaces
- Up to 80-Gbps throughput
- 1-rack-unit (RU) form factor
- Low latency

Multiservice Security
- Integrated inspection engines for FW, NGIPS, Application Visibility and Control (AVC), URL, Cisco Advanced Malware Protection (AMP)
- Radware DefensePro DDoS
- ASA and other future third party

Unified Management
- Single management interface with Firepower Threat Defense
- Unified policy with inheritance
- Choice of management deployment options
Cisco Firepower 9300 Platform
High-speed, scalable security

Benefits
• Standards and interoperability
• Flexible architecture

Features
• Template-driven security
• Secure containerization for customer apps
• RESTful/JSON API
• Third-party orchestration and management

Benefits
• Integration of best-in-class security
• Dynamic service stitching

Features*
• Cisco® ASA container
• Cisco Firepower™ Threat Defense containers:
  • NGIPS, AMP, URL, AVC
• Third-party containers:
  • Radware DDoS
  • Other ecosystem partners

Benefits
• Industry-leading performance:
  • 600% higher performance
  • 30% higher port density

Features
• Compact, 3RU form factor
• 10-Gbps/40-Gbps I/O; 100-Gbps ready
• Terabit backplane
• Low latency, intelligent fast path
• Network Equipment-Building System (NEBS) ready
Firepower NGFW Software
Cisco Firepower NGFW

Stop more threats
Gain more insight
Detect earlier, act faster
Reduce complexity
Get more from your network

Threat Focused  Fully Integrated
Offering extensive contextual visibility

The more you see, the better you can protect

Typical IPS
Typical NGFW
Cisco Firepower NGFW

Malware
Client applications
Operating systems
Mobile Devices
Routers & switches
Printers
VOIP phones

Users
Application protocols
Web applications
File transfers
C & C Servers
Network Servers

Typical IPS
Typical NGFW
Cisco Firepower NGFW

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Provide next-generation visibility into app usage

Application Visibility & Control

Cisco database
- 4,000+ apps
- 180,000+ Micro-apps

Prioritize traffic

See and understand risks
Enforce granular access control
Prioritize traffic and limit rates
Create detectors for custom apps

OpenAppID

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Understand threat details and quickly respond
Next-Generation Intrusion Prevention System (NGIPS)

Data packets

App & Device Data

010111010010
10 010001101
010010 10 10

Communications

Blended threats
- Network profiling
- Phishing attacks
- Innocuous payloads
- Infrequent callouts

Prioritize response

Automate policies

ISE

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Scan network traffic
Correlate data
Detect stealthy threats
Respond based on priority
Pick from many deployment modes

Firewall deployment modes

Inline or Passive
- Inline
- Inline Tap
- Passive

Fail-to-wire NetMods
- Route
- Transparent
- Virtual or Physical

Additional options

Pick from many deployment modes
Uncover hidden threats in the environment
Advanced Malware Protection (AMP)

File Reputation
- Known Signatures
- Fuzzy Fingerprinting
- Indications of compromise

File & Device Trajectory

Threat Grid Sandboxing
- Advanced Analytics
- Dynamic analysis
- Threat intelligence

Threat Disposition
- Uncertain
- Safe
- Risky

Block known malware
Investigate files safely
Detect new threats
Respond to alerts

AMP for Endpoint Log
AMP for Network Log

Enforcement across all endpoints
Uncover hidden threats at the edge
SSL decryption engine

Decrypt **3.5 Gbps** traffic over **five million** simultaneous flows

- Inspect deciphered packets
- Track and log all SSL sessions

---

**Encrypted Traffic**

- http://www.%$&^*#$@#$@$.com
- http://www.%$&^*#$@#$@$.com

**SSL decryption engine**

**NGIPS**

**AVC**

**Enforcement decisions**

- Log

---

- http://www.%$&^*#$@#$@$.com
- http://www.%$&^*#$@#$@$.com
- http://www.%$&^*#$@#$@$.com
- http://www.%$&^*#$@#$@$.com
- http://www.%$&^*#$@#$@$.com
- http://www.%$&^*#$@#$@$.com
- http://www.%$&^*#$@#$@$.com
- http://www.%$&^*#$@#$@$.com
- http://www.%$&^*#$@#$@$.com
- http://www.%$&^*#$@#$@$.com
Block or allow access to URLs and domains

Web controls

- Classify 280M+ URLs
- Filter sites using 80+ categories
- Manage “allow/block” lists easily
- Block latest malicious URLs

NGFW

Filtering

Allow
Block

Safe Search

gambling

Policy Creation

Admin
Stop known threats from getting in

Security Intelligence

<table>
<thead>
<tr>
<th>URL Based</th>
<th>IP Based</th>
<th>DNS Based</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block risky sites using a classified database of</td>
<td>Filter out bad IPs using a blacklist of</td>
<td>Get real-time threat intelligence based on</td>
</tr>
<tr>
<td>270 million+ known URLs</td>
<td>70,000+ known IPs</td>
<td>80 billion+ daily DNS requests</td>
</tr>
</tbody>
</table>

Understand risks using reputation scoring
See more through industry-leading research

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Get real-time protection against global threats

Talos

**Threat Intelligence**

- **1.5 million** daily malware samples
- **600 billion** daily email messages
- **16 billion** daily web requests

**Security Coverage**

- Endpoints
- Web
- Networks
- NGIPS
- Devices

**Research Response**

- **250+ Researchers**
- **24 x 7 x 365 Operations**

**Identify advanced threats**

**Get specific intelligence**

**Catch stealthy threats**

**Stay protected with updates**
URL-Based Security Intelligence

- Extension of IP-based SI
- TALOS dynamic feed, 3rd party feeds and lists
- Multiple categories: Malware, Phishing, CnC,…
- Multiple Actions: Allow, Monitor, Block, Interactive Block,…
- Policy configured via Access Rules or black-list
- IoC tags for CnC and Malware URLs
- New Dashboard widget for UR SI
- Black/White-list URL with one click
DNS Inspection

- Security Intelligence support for domains
- Addresses challenges with fast-flux domains
- Cisco provided and user defined DNS lists: CnC, Spam, Malware, Phishing
- Multiple Actions: Block, Domain Not Found, Sinkhole, Monitor
- Indications of Compromise extended with DNS Security Intelligence
- New Dashboard widget for DNS SI
TrustSec
Identity Services Engine (ISE)

Ensure compliance before granting access

Set access control policies
Propagate rules and context
Establishe a secure network
Remediate breaches automatically

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

Policy automation
FTD Flow Offload

• 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

• Static hardware-based offload in Smart NIC for FTD
  • Automatically enabled when rule in Prefilter Policy uses the Fastpath action

  • Targeting 30Gbps+ per single flow (TCP/UDP) and 2.9us of 64-byte UDP latency
  • Unicast IPv4 TCP/UDP/GRE and VLAN encapsulation only, no CMD/SGT

• Conditional offloading and selective inspection in the future
Management Platform Options
Easily manage NGFWs across multiple sites

Firepower Management Center

Centralized management for multi-site deployments

- Multi-domain management
- Role-based access control
- High availability
- APIs and pxGrid integration

Firewall & AVC
NGIPS
AMP
Security Intelligence

…Available in physical and virtual options

Manage across many sites
Control access and set policies
Investigate incidents
Prioritize response
Easily manage individual NGFWs

Firepower Device Manager

Integrated on-box option for single instance deployment

- Easy set-up
- Role-based access control
- High availability
- Physical and virtual options
- NAT and Routing
- Intrusion and Malware prevention
- Device monitoring
- VPN support

Set up easily
Control access and set policies
Investigate incidents
Prioritize response
New Capabilities in 6.1 Release
<table>
<thead>
<tr>
<th>Enterprise Management</th>
<th>Threat Innovation</th>
<th>Unified Image</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geo-location + Whois lookup</td>
<td>True-IP Policy</td>
<td>Inline Security Group Tags (SGT)</td>
</tr>
<tr>
<td>AMP Private Cloud</td>
<td>SSL ClientHello</td>
<td>Shared NAT</td>
</tr>
<tr>
<td>FMC HA</td>
<td>YouTube EDU enforcement</td>
<td>Rate limiting Policies</td>
</tr>
<tr>
<td>ISE remediation</td>
<td>Safe Search Enforcement</td>
<td>Site-to-site VPN support</td>
</tr>
<tr>
<td>Interface objects</td>
<td>Active authentication enhancements</td>
<td>Routing enhancements</td>
</tr>
<tr>
<td>REST API</td>
<td>Citrix VDI Authentication</td>
<td>Firepower Device Manager (on box manager)</td>
</tr>
<tr>
<td>VDI User Input API</td>
<td></td>
<td>Traffic Rate Limiting</td>
</tr>
<tr>
<td>KVM Virtualization Support</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrated risk reports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event QoS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Common Across Firepower Platforms

Threat Defense Only
Available in multiple deployment options

Physical, virtual, and cloud options
- AWS
- Azure

Also available as standalone solutions
- NGIPS only
- Dedicated AMP

And on high-end performance appliances...

- Cisco Firepower™ 4100 Series and 9300
- Cisco Firepower Threat Defense on ASA 5500-X
- Cisco FirePOWER™ Services on ASA 5585-X

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Only Cisco delivers…

… superior protection and visibility to address new demands, more things, more things, more things, more things.

Threat Focused

- Stop more threats
- Gain more insight
- Detect earlier, act faster
- Reduce complexity
- Get more from your network

Fully Integrated
Thank you