Cisco Next Generation Firewalls

Dragan Novaković
Security Consulting Systems Engineer
20.4.2016.
What we announced @CiscoLive Berlin

Cisco Firepower NGFW
Cisco Firepower™ NGFW is the industry’s first fully integrated threat-focused next-generation firewall that keeps customers safer, mitigates advanced threats more quickly, and streamlines operations better. This allows customers to stop more threats and get more from their resources and positions security as a growth engine to seize new business opportunities.

Cisco Firepower 4100 Series Appliances
Cisco Firepower 4100 Series appliances provide a threat-focused NGFW security platform for Internet edge and other high-performance environments and deliver better security at faster speeds with a smaller footprint.

Cisco Firepower Management Center 6.0
Cisco Firepower Management Center provides complete and unified management over Cisco Firepower NGFW, Cisco Firepower NGIPS, and Cisco® AMP deployments, enabling users to go from managing the firewall to controlling application use to investigating and remediating malware outbreaks with ease.
Enable your business with a fully integrated, threat-focused solution

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

Cisco Firepower™ NGFW

Threat Focused
Fully Integrated

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Stop more threats across the entire attack continuum

BEFORE

DURING

AFTER

Cisco Firepower™ NGFW

Discover threats and enforce security policies

Detect, block, and defend against attacks

Remediate breaches and prevent future attacks
Gain more insight with increased visibility

“You can’t protect what you can’t see”
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
Get more from your network through integrated defenses

Shared intelligence

Shared contextual awareness

Consistent policy enforcement

Cisco Firepower™ Management Center
Cisco NGFW Platforms

New Appliances

Cisco Firepower™ 4100 Series and 9300

Cisco Firepower Threat Defense on ASA 5500-X

Cisco FirePOWER™ Services on ASA 5585-X

All* Managed by Cisco Firepower Management Center

*5585-X management available 2H CY16
Cisco 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

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
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

* Contact Cisco for services availability

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Firepower 9300 and 4100 Technical Overview
Platform-Based Security Architecture

Management

Security Services and Applications

Security Services Platform

Infrastructure Element Layer

Common Security Policy and Management

Cisco Security Applications

Third-Party Security Applications

Orchestration

Security Management APIs

Cisco ONE APIs

Platform APIs

Cloud Intelligence APIs

Physical Appliance

Virtual

Cloud

Device API: OnePK™, OpenFlow, CLI

Cisco Networking Operating Systems (Enterprise, Data Center, Service Provider)

ASIC Data Plane

Route–Switch–Compute

Software Data Plane

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
<table>
<thead>
<tr>
<th>Next Generation Platform Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Modular Compute</strong></td>
</tr>
<tr>
<td>System hardware components can be upgraded independently</td>
</tr>
<tr>
<td><strong>Architectural Scale</strong></td>
</tr>
<tr>
<td>Leverage the best of security processing components (x86, NPU, Crypto) and scale with Clustering</td>
</tr>
<tr>
<td><strong>No Single Failure Point</strong></td>
</tr>
<tr>
<td>All hardware and software components are redundant and as independent as possible</td>
</tr>
<tr>
<td><strong>Deployment Agnostic</strong></td>
</tr>
<tr>
<td>Provide the same benefits in physical, virtual, and hybrid SDN environments</td>
</tr>
<tr>
<td><strong>Dynamic Service Insertion</strong></td>
</tr>
<tr>
<td>Dynamic service insertion based on policy and context</td>
</tr>
<tr>
<td><strong>Rapid Inline Changes</strong></td>
</tr>
<tr>
<td>Services be added, removed, upgraded, and modified without disrupting existing flows</td>
</tr>
<tr>
<td><strong>3rd Party Integration</strong></td>
</tr>
<tr>
<td>Architecture built to quickly add new services as market evolves</td>
</tr>
<tr>
<td><strong>Unified API</strong></td>
</tr>
<tr>
<td>Offer a unified SDK/API for all services, including unified licensing and logging.</td>
</tr>
</tbody>
</table>
Firepower 9300 Overview

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

**Network Modules**
- 10GE/40GE and future 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 Module

- Overall chassis management and network interaction
  - Network interface allocation and module connectivity (960Gbps internal fabric)
  - Application image storage, deployment, provisioning, and service chaining
  - Clustering infrastructure for supported applications
  - Smart Licensing and NTP for entire chassis
Supervisor Simplified Hardware Diagram

Internal Switch Fabric (up to 24x40GE)

Security Module 1

Security Module 2

Security Module 3

RAM

x86 CPU

On-board 8x10GE interfaces

NM Slot 1

NM Slot 2

System Bus

Ethernet

2x40Gbps

2x40Gbps

2x40Gbps

5x40Gbps

5x40Gbps

2x40Gbps

5x40Gbps
Security Modules

- Two configurations
  - **SM-36** “Extreme”: 72 x86 CPU cores (up to 80Gbps)
  - **SM-24** “Enterprise”: 48 x86 CPU cores (up to 60Gbps), NEBS Ready

- Dual 800GB SSD in RAID1 by default

- Built-in hardware Smart NIC and Crypto Accelerator
  - Flow Offload
  - VPN connection acceleration
  - Future transit TLS inspection with FTD
Security Module Simplified Diagram

- RAM: 256GB
- x86 CPU 1: 24 or 36 cores
- x86 CPU 2: 24 or 36 cores
- Smart NIC and Crypto Accelerator
- Backplane Supervisor Connection
- 2x100Gbps
- 2x40Gbps

System Bus
Ethernet
Firepower 9300 Software

- Supervisor and security modules use multiple independent images
- All images are digitally signed and validated through Secure Boot
- Security application images are in Cisco Secure Package (CSP) format

Security Module 1
- DDoS
- ASA
- FXOS

Security Module 2
- ASA
- FXOS

Security Module 3
- ASA
- FXOS

Supervisor

- Supervisor stores CSP application images
- Decorator application from third-party (KVM)
- Primary application from Cisco (Native)
- FXOS upgrades are applied to Supervisor and resident provisioning agent on modules
Security Applications Overview

- Applications are security services that run on Firepower 9300 modules
- Primary application consumes full resources of an entire module
  - ASA or FTD; no plans for standalone NGIPS image
  - All modules in a chassis run same primary application
- A decorator application shares a security module with a primary
  - Traffic flows from network interface “through” decorator to primary application
  - Service chaining with Radware vDefensePro decorator and ASA/FTD
Future Vision: Security Service Chaining

- Contextual policy- and outcome based service insertion
- Meta data exchange with Network Services Header (NSH)

Service Function (SF) processes packet, attaches meta data, and returns to SFF.

Service Classifier (SC) and Service Function Forwarder (SFF) direct incoming traffic through necessary services.

SF, SC, and SFF may influence service path based on policy, context, and meta data.

Stateful Data Path

DDoS

FTD

?
ASA 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 ASA

```bash
policy-map OFFLOAD_POLICY
  class TRUSTED_FLOWS
    set connection advanced-options flow-offload
```

- Targeting 30Gbps+ per single flow (TCP/UDP) and <4us of latency
- Unicast IPv4 TCP/UDP/GRE and VLAN encapsulation only, no CMD/SGT

- Conditional offloading and selective inspection in the future
Introducing Firepower 4100

- Same software and hardware architecture as Firepower 9300

<table>
<thead>
<tr>
<th></th>
<th>Firepower 4110</th>
<th>Firepower 4120</th>
<th>Firepower 4140</th>
<th>Firepower 4150</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Throughput</td>
<td>20Gbps</td>
<td>40Gbps</td>
<td>60Gbps</td>
<td>TBD</td>
</tr>
<tr>
<td>NGFW Throughput</td>
<td>10Gbps</td>
<td>15Gbps</td>
<td>20Gbps</td>
<td>TBD</td>
</tr>
<tr>
<td>Connection Rate</td>
<td>68K-150K/sec</td>
<td>90K-250K/sec</td>
<td>125K-350K/sec</td>
<td>TBD</td>
</tr>
</tbody>
</table>

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Firepower 4100 Architecture

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

On-board 8x10GE interfaces

Internal Switch Fabric
(up to 18x40GE)

Smart NIC and Crypto Accelerator
- 4110: 1x100Gbps
- 4120-4150: 2x100Gbps
- 4110: 1x40Gbps
- 4120-4150: 2x40Gbps

System Bus

Ethernet

NM Slot 1

NM Slot 2

x86 CPU 1

x86 CPU 2

RAM
Firepower Threat Defense
Converged Software – Firepower Threat Defense

New Converged Software Image: Firepower Threat Defense
- Contains all Firepower Services plus select ASA capabilities
- Single Manager: Firepower Management Center*

Same subscriptions as FirePOWER Services, enabled by Smart Licensing:
- Threat (IPS + SI + DNS)
- Malware (AMP + ThreatGrid)
- URL Filtering

* Also manages Firepower Appliances, Firepower Services (not ASA Software)
What features are available?

- Everything from Firepower 6.0
- Phased introduction of features from ASA
- FTD 6.0.1
  - IPv4 and IPv6 Connection state tracking and TCP normalization
  - Access Control
  - NAT (Full support)
  - Unicast Routing (except EIGRP)
  - ALGs (only default configuration)
  - Intra chassis Clustering on Firepower 9300
  - Stateful Failover (HA)
Advantages of Firepower Threat Defense

• New Next Generation Firewall offering
• Brings together the best features from ASA and Firepower, all under one OS
• Zero-copy packet inspection
• Single management application
• Duplicate functionality removed
Unified Access Control policies

- Access policies broken down into 2 sets of rules
- Advanced ACLs - Evaluate L2 – L4 attributes and give a verdict
  - Permit
  - Deny
  - Trust
- NGFW ACLs – Evaluate L7 attributes
  - Allow
  - Block
  - TrustPath
Unified Objects Configuration

Objects in 5.4

Objects in 6.0

Security Intelligence
- Network Lists and Feeds
- DNS Lists and Feeds
- URL Lists and Feeds

Sinkhole

Prefix List
- IPv4 Prefix List
- IPv6 Prefix List

Route Map

Access List
- Standard
- Extended

AS Path

Community List

Policy List
What Platforms run Firepower Threat Defense?

- Cisco Firepower Threat Defense on Firepower™ 4100 Series and 9300
- Cisco Firepower Threat Defense on ASA 5500-X
- Cisco FirePOWER Services on ASA 5585-X
- Cisco FirePOWER on 7000/8000 Series Appliances

All* Managed by Cisco Firepower Management Center

*5585-X ASA module management being investigated for 2HCY16
Deployment Modes and Use Cases
Deployment Modes

• Basic deployment modes: **Firewall modes (choose one)**
  • Routed
  • Transparent

• Other interface modes: **IPS/IDS modes**
  • Inline
  • Inline Tap
  • Passive
Firepower Threat Defense interface modes

- Routed/Transparent
- Policy Tables
- Inline Pair 1
- Inline Pair 2
- Inline Tap
- Passive Interfaces
- Inline Set
Firepower Threat Defense

CISCO COLLECTIVE SECURITY INTELLIGENCE

- High Availability
- Intrusion Prevention
- Analytics & Automation
- Malware Protection
- URL Filtering
- Network Firewall and Routing
- Application Visibility & Control
- Network Profiling
- Identity Based Policy Control

Integrated Software - Single Management
Use Case
Internet Edge Firewall

Requirement

Connectivity and Availability Requirement:
- Firewall for High Availability (Redundancy)
- Firewall should support Router or Transparent Mode
- vPC/Port-Channel for interface redundancy and link speed aggregation

Security Requirement:
- Dynamic NAT/PAT and Static NAT
- AVC, URL filtering, IPS and Malware protection
- SSL Decryption

Solution

Security Application: Firepower Threat Defense application with FMC
ASA

HA and Clustering
VPN
Protocol Inspection
Data Center Security
Network Firewall
Mix Multi Context Mode
Identity Based Policy Control
Service Provider Security

ASDM/CSM/RESTful API for Management
Use Case
Internet Edge Firewall with VPN Support

Requirement

**Connectivity and Availability Requirement:**
- Firewall for High Availability (Redundancy)
- Firewall in the Router Mode
- vPC/Port-Channel for interface redundancy and link speed aggregation

**Security Requirement:**
- Dynamic NAT/PAT and Static NAT
- Application Inspection
- ACL to control the traffic flows
- VPN support (S2S, SSL and AnyConnect)

Solution

**Security Application:** ASA Firewall
Q&A