Cisco NGFW

Fully Integrated, Threat-Focused Next-Generation Firewall

Fabio Panada
Consultant Security Engineer
April 2016
Get ahead of attackers with threat-centric security solutions

In our live Security Experts Webinars discover all the items needed to help set up the best security architecture.

- What a Next Generation Firewall should be
- Advanced Malware Protection
- Protect your email and web gateways
- ISE/Access Control

And many other hot security topics so check our Security Experts Page and register to our upcoming webinars
Digital Transformation on a Massive Scale

- Devices Today: 15B
- Devices in 2030: 500B
- Opportunity Next 10 Years: $19T
- Threat Actors
- Attack Surface
- Attack Sophistication

Global Cybercrime Market: $450B to $1T
TeslaCrypt
Cryptolocker variant

• Data is the New Target
• Imitates CryptoLocker Screen
• Uses Bitcoin for payment
SECURITY EVERYWHERE

Attack Continuum

Before

- Endpoint
- Branch
- Edge
- Campus

During

- Data Center

After

- Cloud
- Operational Technology

© 2016 Cisco and/or its affiliates. All rights reserved.
Visibility Across Threat Vectors
You Can’t Find What You Can’t See

Endpoint  Branch  Edge  Campus  Data Center  Cloud  Operational Technology
Combined with the Best Threat Intelligence Capabilities

World-Class Threat Research

250 Threat Researchers

100TB Threat Intelligence

19.7B Threats Per Day

1.1M Incoming Malware Samples Per Day

1B Sender Base Reputation Queries Per Day

8.2B Web Filtering Blocks Per Month

1.4M AV Blocks Per Day

1.8B Spyware Blocks Per Month
More Effective Against Sophisticated Attacks

*Much Faster Than Most Organizations Discover Breaches*

Industry

100 DAYS

VS.

Cisco

Less than

1 Day

We are committed to addressing this problem

"Security is Cisco’s number 1 priority. We are going big and making strategic investments to become our customers’ and partners’ most trusted security advisor."

John Chambers
Executive Chairman, Cisco
April 2016

In the last 18 months, we invested over $3.7B in security
What is a NGFW?

• Typical Firewall Features

• Application Visibility & Control

• Integrated Network IPS

• Extra Firewall Intelligence
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

Threat Focused
Fully Integrated
Stop more threats across the entire attack continuum

Before

- Discover threats and enforce security policies
- Detect, block, and defend against attacks
- Remediate breaches and prevent future attacks

Cisco NGFW

During

After
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
Product and Services
Introducing Cisco NGFW

Fully Integrated
- FW / applications / IPS
- Cisco® AMP – network / endpoint
- Analysis and remediation
- Cisco security solutions

Threat Focused
- Networkwide visibility
- Industry-best threat protection
- Known and unknown threats
- Track / contain / recover

Unified Management
- Across attack continuum
- Manage, control, and investigate
- Automatically protect

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

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
Cisco Firepower 4100 Series

Introducing four new high-performance models

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

- 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

Performance and Density Optimization

Multiservice Security

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

* Contact Cisco for services availability
Features
Automated, Integrated Defenses

Context and Threat Correlation

- Dynamic Security Control
- Multi-vector Correlation
- Retrospective Security

Impact Assessment

Priority 1
Priority 2
Priority 3
Automated, Integrated Defenses

Dynamic Security Control

Adapt Policy to Risks
Automated, Integrated Defenses

Multivector Correlation

Early Warning for Advanced Threats

Host A

Host B

Host C

Context and Threat Correlation

Dynamic Security Control

Multivector Correlation

Retrospective Security
Advanced Malware Protection - Preventive

All detection is less than 100%

One-to-One Signature  Fuzzy Finger-Printing  Machine Learning  Advanced Analytics  Dynamic Analysis

Reputation Filtering and File Sandboxing
Automated, Integrated Defenses

Retrospective Security

Shrink Time Between Detection and Cure
Cisco AMP Everywhere

AMP for Networks (AMP on a Cisco FirePOWER NGIPS)

AMP on Cisco® ASA Firewall with FirePOWER Services

AMP on Web and Email Security Appliances

AMP for Endpoints

AMP Private Cloud Virtual Appliance

AMP Threat Grid
Malware Analysis + Threat Intelligence Engine
Appliance or Cloud

AMP for Cloud Web Security and Hosted Email

*AMP for Endpoints can be launched from AnyConnect

Windows OS

Virtual

MAC OS

Android Mobile

Linux for Servers and Data Centers

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