Global vision.
Local knowledge.

Cisco Forum Kyiv
Country • Day Month Year
Firepower Next Generation Firewall
Subtitle goes here

William Young
Security Solutions Architect, Global Security Architecture Team
December 2018
The move to digital business has increased exposure to attacks

- 90% of organizations not "fully aware" of the devices accessing their network
- 2/3 of all IP traffic
- 21B IoT devices
- 80% of all traffic will be encrypted

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Threats are constantly evolving and getting smarter

- Motivated and targeted adversaries
- Increased attack sophistication
- Insider threats

data breach averages

- 191 days time to detection
- 66 days time to contain
# 3 Security Concerns of IT Leaders

<table>
<thead>
<tr>
<th>Prevention</th>
<th>They aren’t confident in their ability to prevent the next big breach.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visibility</td>
<td>They lack visibility needed to be able to see and stop threats quickly.</td>
</tr>
<tr>
<td>Resources</td>
<td>They have limited budgets, staff and time.</td>
</tr>
</tbody>
</table>
Ask more from your firewall. Ask if it can...

- Prevent breaches automatically to keep the business moving.
- Deep network and security visibility to detect and stop threats fast.
- Automate operations to save time, reduce complexity, and work smart.
Prevent breaches automatically to keep the business moving
**Talos**

Talos is the intelligence backbone for all Cisco Security Products and Services.

### Products & Intelligence

<table>
<thead>
<tr>
<th>Intelligence</th>
<th>End Point</th>
<th>Network</th>
<th>Cloud</th>
<th>Email</th>
<th>Web</th>
<th>Open Source</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>ThreatGrid</td>
<td>AMP ClamAV</td>
<td>FirePower/ASA ISR Meraki</td>
<td>OpenDNS CES</td>
<td>ESA</td>
<td>ClamAV</td>
<td>SpamCop SenderBase</td>
<td>WSA</td>
</tr>
<tr>
<td>Malware Protection</td>
<td>Malware Protection</td>
<td>Malware Protection</td>
<td>Malware Protection</td>
<td>Malware Protection</td>
<td>Malware Protection</td>
<td>Malware Protection</td>
<td>Malware Protection</td>
</tr>
<tr>
<td>URL, Domain, IP Reputation</td>
<td>IP Reputation</td>
<td>URL, Domain, IP Reputation</td>
<td>AVC</td>
<td>URL, Domain, IP Reputation</td>
<td>AVC</td>
<td>URL, Domain, IP Reputation</td>
<td>Policy &amp; Control</td>
</tr>
</tbody>
</table>
Cisco Firewalls have you covered

<table>
<thead>
<tr>
<th>Product</th>
<th>Protection</th>
<th>Protection</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMP</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>CWS</td>
<td>✔️</td>
<td>N/A</td>
<td>✔️</td>
</tr>
<tr>
<td>Firewall</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Threat Grid</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Umbrella</td>
<td>✔️</td>
<td>N/A</td>
<td>✔️</td>
</tr>
<tr>
<td>WSA</td>
<td>✔️</td>
<td>N/A</td>
<td>✔️</td>
</tr>
</tbody>
</table>

WannaCry  
May 2017

NotPetya  
June 2017

VPNFilter  
May 2018

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Block or allow access to URLs and domains

Security Intelligence, URL Filtering, DNS Sinkhole

Classify 280M+ URLs
Filter sites using 80+ categories
Manage Acceptable Use Policy
Block latest malicious URLs
Understand threat details and quickly respond

Next-Generation Intrusion Prevention System (NGIPS)

Scan network traffic
Correlate data
Detect stealthy threats
Respond based on priority

Data packets
01011101001
010
010001101
010010 10 10

App & Device Data
Communications

Blended threats

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

Prioritize response
Automate policies
ISE

Block
Accept
# Automated Impact Assessment

Correlates all intrusion events to an impact of the attack against the target

<table>
<thead>
<tr>
<th>Impact Flag</th>
<th>Administrator Action</th>
<th>Why</th>
</tr>
</thead>
<tbody>
<tr>
<td>🟥</td>
<td>Act immediately; vulnerable</td>
<td>Event corresponds to vulnerability mapped to host</td>
</tr>
<tr>
<td>🟢</td>
<td>Investigate; potentially vulnerable</td>
<td>Relevant port open or protocol in use, but no vulnerability mapped</td>
</tr>
<tr>
<td>🟡</td>
<td>Good to know; currently not vulnerable</td>
<td>Relevant port not open or protocol not in use</td>
</tr>
<tr>
<td>🟠</td>
<td>Good to know; unknown target</td>
<td>Monitored network, but unknown host</td>
</tr>
<tr>
<td>⚫</td>
<td>Good to know; unknown network</td>
<td>Unmonitored network</td>
</tr>
</tbody>
</table>
Indications of Compromise (IoCs) Detection & Threat Correlation

- IPS Events
  - Malware Backdoors
  - Exploit Kits
  - Web App Attacks

- Security Intelligence Events
  - CnC Connections
  - Admin Privilege Escalations

- Malware Events
  - Connections to Known CnC IPs; DNS Servers, Suspect URLs
  - Malware Detections
  - Office/PDF/Java Compromises
  - Malware Executions
  - Dropper Infections

Indications of Compromise (3)

<table>
<thead>
<tr>
<th>Category</th>
<th>Event Type</th>
<th>Description</th>
<th>First Seen</th>
<th>Last Seen</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exploit Kit</td>
<td>Intrusion Event - exploit-kit</td>
<td>The host may have encountered an exploit kit</td>
<td>2013-09-17 16:46:28</td>
<td>2013-09-20 06:35:31</td>
</tr>
<tr>
<td>CnC Connected</td>
<td>Security Intelligence Event - CnC</td>
<td>The host may be under remote control</td>
<td>2013-09-17 16:52:11</td>
<td>2013-09-20 03:55:45</td>
</tr>
<tr>
<td>CnC Connected</td>
<td>Intrusion Event - malware-cnc</td>
<td>The host may be under remote control</td>
<td>2013-09-17 20:09:23</td>
<td>2013-09-19 17:32:49</td>
</tr>
</tbody>
</table>
Firepower Recommendations Knows what I Do Not
Uncover hidden threats in the environment

Advanced Malware Protection (AMP)

Breadth and Control points:
- Email
- Endpoints
- Web
- Network
- IPS
- Devices

Telemetry Stream

- File Fingerprint and Metadata
- File and Network I/O
- Process Information
- Talos + Threat Grid Intelligence

Continuous feed

Continuous analysis
AMP in Action

Focus on these users first

These applications are affected

The breach impacted these areas

This is the scope of exposure over time

Here is the origin and progression of the threat

Network and Endpoint Correlation
IN FIREPOWER MANAGEMENT CENTER
The results speak for themselves

4.6 Hours
Median time to detection with Cisco security*

Weeks
Industry average time to detection

* Source: Cisco 2018 Annual CyberSecurity Report
Deep network and security visibility to detect and stop threats fast
“You can’t protect against what you can’t see”

Gain more insight with increased visibility

Typical IPS

Typical NGFW

Cisco Firepower™ NGFW
Provide next-generation visibility into app usage

Application Visibility & Control

Cisco database

- 4,000+ pre-defined apps

See and understand risks

Enforce granular access control

Prioritize traffic and limit rates

Create detectors for custom apps

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Extend AVC to proprietary and custom apps

OpenAppID - Crowdsourcing Application Detection

Self-Service

Easily customize application detectors
Detect custom and proprietary applications
Share detectors with other users
Uncover hidden threats at the edge

TLS/SSL decryption engine

Decrypt traffic in hardware and software
Inspect deciphered packets
Track and log all TLS sessions
Visibility Provides Context
Automate operations to save time, reduce complexity, and work smarter
Save time and work smarter with NGFW automation

- **Automated policy application and enforcement** frees up time so you can focus on high priority items
- **Automatic IPS tuning** blocks more threats and reduces the volume of alerts
- **Prioritized threat alerts** show you where to focus on what matters
Effective security requires an integrated approach with a Cisco firewall at its foundation
Ensure compliance before granting access
Identity Services Engine (ISE)

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

Propagate
• User Context
• Device Profile
• Access Policies

ISE
BYOD
Guest Access
Segmentation

pxGrid

Management Console

TrustSec

ISE

Policy automation

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Integrate third-party security intelligence
Cisco Threat Intelligence Director

Ingest Security Intelligence
Correlate Observations
Generate Rich Incident Reports
Refine Security Posture

Cisco Security Sensors
- Firepower NGFW
- FirePOWER NGIPS
- AMP

STIX TAXII CSV

Threat Intelligence Director

Firepower Management Center

Observables
Events

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Device APIs and Events - Scale and Efficiency

Eventing

- Syslog servers
- Event connector
- FTD
- CDO
- Automation scripts
- Homegrown or 3rd party tools
- FDM
- FMC

Management

- SIEM
- SIEM
- FMC
- FMC
- FMC
- Homegrown or 3rd party tools
- Syslog servers
- Management
- Eventing
Secure workloads consistently across the data center and public cloud
Extend security to remote users and branches
Remote and site-to-site VPN

- AnyConnect
- IKEv2 support
- Third-party VPN

Extend access remotely  Protect important data  Maintain application performance  Support multiple sites

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Prevent network and application downtime

Firepower DDoS Mitigation

Available on the Firepower 9300 and 4100 series appliances.

- SYN flood attacks
- DDoS attacks
- Nonstandard packet attacks

Maintain up to **42 Gbps** total mitigation capacity

Handle **627,000** connections per second

Block **5,400,000** packets of flood traffic per second

Stop attacks within seconds of detection

Block or allow traffic automatically

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Cisco has an NGFW solution for every business...

<table>
<thead>
<tr>
<th>Small and Midsized Business</th>
<th>Midrange</th>
<th>Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5506-X / 5506W-X / 5506H-X / 5508-X / 5516-X</td>
<td>ASA 5525-X/ ASA 5545-X/ ASA 5555-X</td>
<td>Firepower 4110/4120/4140/4150</td>
</tr>
<tr>
<td>NGFWs for SMBs and distributed enterprises with integrated threat defense, a low TCO, and simplified security management.</td>
<td>Enterprise-class security for the internet edge, with superior threat defense, sustained performance, and simple management.</td>
<td>From the internet edge to carrier grade security for data centers and other high-performance settings, with multiservice security, flexible architecture, and unified management.</td>
</tr>
</tbody>
</table>
Virtual and Cloud Solutions

AVC  
NGIPS  
Firewall  
URL  
VPN (IPSEC and SSL)

Managed by FMC and FDM

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Pick from many deployment modes

Firewall deployment modes

Inline or Passive
- Inline
- Inline Tap
- Passive

Fail-to-wire NetMods
Available on 2100, 4100 and 9300

Additional options
- Routed
- Transparent
- Virtual or Physical

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Deliver scalable performance across many sites

Firewall Clustering

**Link Scalability**
- Increase throughput
- Handle more connections

**Distributed Plan**
- Combine multiple individual firewalls and manage as one

**Inter-site Clustering**
- Location A
- Location B
Multi-Instance for true Multi-Tenancy

- Firepower 4100 and 9300 only
- Instantiate multiple logical devices on a single module or appliance
- Complete traffic processing and management separation
- CPU/memory/disk resources are dedicated to an instance at provisioning
- Physical and logical interface and VLAN separation at Supervisor
Flow Offload

Full Inspection
- Dynamically program Offload engine after flow establishment
- Ability to switch between Offload and full inspection on the fly

Flow Offload
- Limited state tracking, NAT/PAT, TCP Sequence Randomization
- 30-40Gbps per single TCP/UDP flow, 2.9us UDP latency, 2M tracked flows
Management Options

Centralized
Firepower Management Center (FMC)
Enables comprehensive security administration and automation of multiple appliances

On-box
Firepower Device Manager (FDM)
Enables easy on-box management of common security and policy tasks

Cloud-based
Cisco Defense Orchestrator (CDO)
Enables cloud-based policy management of multiple deployments

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Firepower Management Center (FMC)

Centralized management for multi-site deployments

- Multi-domain management
- Firewall & AVC
- Role-based access control
- NGIPS
- High availability
- AMP
- APIs and pxGrid integration
- Security Intelligence

...Available in physical and virtual options

Manage across many sites  Control access and set policies  Investigate incidents  Prioritize response
Firepower Device Manager (FDM)

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
Automate Configuration
Enhanced Control
Cisco Defense Orchestrator (CDO)

Simplify security policy management in the cloud with Cisco Defense Orchestrator Security

Plan and model security policy changes before deploying them across the cloud

Deploy changes across virtual environments in real time or offline

Receive notifications about any unplanned changes to security policies and objects

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
Address modern security needs and challenges
With eight business-critical use cases

- Campus NGFW
- Internet Edge
- Cloud Data Center Edge
- Local Data Center Edge
- Acceptable Use
- ACI Integration
- Complex remote access
- Rapid Threat Containment
Stop threats from getting in by extending secure access to all users.

Extend secure access to other locations

I want to…

Stop threats from getting in by extending secure access to all users.

Firewall Highlights

- High bandwidth
- High availability
- Hardware and virtual options

Security feeds

URL | IP | DNS

SSL Decryption Engine

AVC

- Allow
- Block

NGIPS

Headquarters

Branch

Remote user

Distributed Enterprise

Firewall

VPN

Internet

Firewall

Branch WAN and Remote Users
Defend the network with Rapid Threat Containment

I want to…
Isolate compromised resources quickly before the problem grows.

Isolate compromised resources quickly before the problem grows.

Automatic Isolation

Firepower Management Center
Receive alert of intrusion event
Issue quarantine command

ISE
pxGrid
Alerts

ISE
pxGrid
Alerts

TrustSec
Employee Tag
Guest Tag
Supplier Tag
Quarantine Tag

www
pxGrid
Alerts

© 2018 Cisco and/or its affiliates. All rights reserved.
Migration
Migration Options

FMC Based Migration  

CISCO  

API Based Firepower Migration Tool  

New
API Based ASA To FTD Migration

**Independent from FMC**
- Takes away the pain of installing another FMC for migration
- Independent windows executable
- Independent releases with enhancements and bug fixes

**Rest API based**
- Supports migration of features supported in FMC Rest API
- Will support migration to FDM in the future
- Scalable

**Improved Workflow and reporting**
- Ability to edit the configuration being migrated
- Pre and post migration reports
- Live running logs, graceful error handling and resume from failure
- Object conflict detection and resolution
API Based Firepower Migration Tool
Easy Deployment

- Windows Executable
- Chrome Browser
- Import

5585-X

.cfg/.txt

• 55xx, 2100, 4100, 9300, and Virtual
• FMC 6.2.3+ and beyond

Reimage to FTD

FP4100

FP4100
Deploy security in multiple environments flexibly with NGFW

- Consistent security efficacy
- Consolidated security posturing
- Open architecture
- APIs and automation
- Flexible licensing model
Key Features of the 6.3 Release

- Extending deployment opportunities
  - Multi-Instance
  - Air-gapped licensing
  - Unified Eventing and Contextual Cross-launch
  - New Network Modules
  - ISA 3000 FTD enhancements
  - On-box Firepower Device Manage (FDM) HA
  - Additional FDM enhancements
  - TLS in Hardware for the 2100

- CoA for RA VPN
- FQDN based network objects
- New migration tool
- Other Enhancements
  - Dynamic Flow Offload
  - Clustering enhancements
  - Backup and restore for RMA
  - Snort restart improvements
  - FMC REST API enhancements
Next steps

1. Learn more about what Firepower NGFW can do for you at https://cisco.com/go/ngfw

2. Schedule a demo today for a hands-on experience at https://dcloud.cisco.com

3. Set up a POV to see how it can improve your network. Contact your local Cisco security representative
Thank You!