Unified Threat Management
NGFW

Christian Heinel
Technical Manager, Cyber Security, Northern Europe

April 2016
What we just launched

<table>
<thead>
<tr>
<th>Firepower NGFW</th>
<th>Firepower 4100 Series</th>
<th>Firepower Management Center 6.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>The industry’s first fully integrated, threat-focused next-generation firewall with unified management.</td>
<td>A threat-focused NGFW security platform; the industry’s first 1RU platform with 40Gb interfaces.</td>
<td>Complete and unified management of Firepower NGFW, Firepower NGIPS and Cisco AMP deployments.</td>
</tr>
</tbody>
</table>
Branding Terms

What You Know

ASA with FirePOWER Services

ASA Appliances with ASA and Firepower software, application firewalling and threat defense.

The ASA and FirePOWER functions have separate managers.

Just Launched

Firepower Threat Defense
New unified software

Firepower Appliances
New Firepower 4100 Series and 9300 appliances.

Firepower NGFW
New NGFW platform

Firepower Management Center
New unified manager
What is a NGFW?

- Typical Firewall Features
- Application Visibility & Control
- Integrated Network IPS
- Extra Firewall Intelligence
Firepower NGFW Overview
Typical NGFWs are focused too narrowly on apps and are too hard to manage.

Focused on apps, not threats

Another silo to manage
They protect before an attack but are less effective during or after one.
Next Generation Firewall (NGFW) Essentials

- Clustering & High Availability
- NGIPS
- Analytics & Automation
- Advanced Malware Protection
- Network Firewall Routing | Switching
- Application Visibility & Control
- Built-in Network Profiling
- Identity-Policy Control & VPN
- WWW
- URL Filtering
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 2015

In the last 18 months, we invested over $3.7B in security
The Problem is **Threats**
Turning Cisco towards Threat Centricity:

**Cognitive Security** - Network Behaviour Analysis

**ThreatGrid** - Malware Research Grid + SandBox

**SourceFire** - NGIPS, AMP, NGFW, ThreatIntel

**OpenDNS** - DNS inspection in the Cloud

**Lancope** – NetFlow Security Analysis
Gain more insight with increased visibility

“You can’t protect what you can’t see”
Detect infections earlier and act faster

Industry TTD rate:* 100 days

Cisco: 17.5 hours

- Automated attack correlation
- Indications of compromise
- Local or cloud sandboxing
- Malware infection tracking
- Two-click containment
- Malware analysis

Source: Cisco® 2016 Annual Security Report

*Median time to detection (TTD)
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
Product and Services
Cisco ASA Firewalls

- **ASA 5505** (150 Mbps, 4K conn/s)
- **ASA 5506-X** (750 Mbps, 5K conn/s)
- **ASA 5508-X** (1 Gbps, 10K conn/s)
- **ASA 5512-X** (500 Mbps, 10K conn/s)
- **ASA 5515-X** (750 Mbps, 15K conn/s)
- **ASA 5516-X** (1.8 Gbps, 20K conn/s)
- **ASA 5525-X** (2 Gbps, 20K conn/s)
- **ASA 5545-X** (3 Gbps, 30K conn/s)
- **ASA 5555-X** (4 Gbps, 50K conn/sec)
- **ASA Av** (100Mbps-2Gbps, 20-60K conn/s)
- **ASA 5555-X** (4 Gbps, 65K conn/s)
- **ASA 5585 SSP20** (10 Gbps, 140K conn/s)
- **ASA 5585 SSP40** (40 Gbps, 350K conn/s)
- **ASA 5585 SSP60** (40 Gbps, 350K conn/s)
- **ASA 5585 SSP10** (4 Gbps, 140K conn/s)
- **ASA 5585 SSP20** (20 Gbps, 240K conn/s)
- **ASA 5585 SSP40** (20 Gbps, 240K conn/s)
- **ASA 5585 SSP60** (20 Gbps, 240K conn/s)
- **Firepower 9300** (60-240 Gbps)
- **Firepower 4100** (20-60 Gbps)
- **ASA SM** (16-20 Gbps, 300K conn/s)
- **ASA 5512-X** (500 Mbps, 10K conn/s)
- **ASA 5516-X** (750 Mbps, 15K conn/s)
- **ASA 5525-X** (2 Gbps, 20K conn/s)
- **ASA 5545-X** (3 Gbps, 30K conn/s)
- **ASA 5555-X** (4 Gbps, 50K conn/sec)
- **ASA Av** (100Mbps-2Gbps, 20-60K conn/s)
- **ASA 5555-X** (4 Gbps, 65K conn/s)
- **ASA 5585 SSP20** (10 Gbps, 140K conn/s)
- **ASA 5585 SSP40** (40 Gbps, 350K conn/s)
- **ASA 5585 SSP60** (40 Gbps, 350K conn/s)
- **ASA 5585 SSP10** (4 Gbps, 140K conn/s)
- **ASA 5585 SSP20** (20 Gbps, 240K conn/s)
- **ASA 5585 SSP40** (20 Gbps, 240K conn/s)
- **ASA 5585 SSP60** (20 Gbps, 240K conn/s)
- **Firepower 9300** (60-240 Gbps)
- **Firepower 4100** (20-60 Gbps)
- **ASA SM** (16-20 Gbps, 300K conn/s)

**Teleworker** | **Branch Office** | **Internet Edge** | **Campus** | **Data Center**
Cisco NGFW Platforms

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

*5585-X management available 2H CY16

All* Managed by Cisco Firepower Management Center
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
FirePower Threat Defense Management
Firepower Threat Defense (FTD) is a NGFW SW Platform that Delivers Unified Code (Single OS) and Single Management

ASA with FirePOWER Service

- **OS1**: ASA (L2-L4)
- **OS2**: FirePOWER Services (L7)

FTD

- Single OS
- Benefits: Continuous feature migration, Full Feature Set
- Simple Deployment, Single Management
FTD 6.0.1 features

Stateful Firewall

- Access Control
- NAT
- HA
- Routing

NGFW Features

- NGIPS (Snort)
- AVC
- URL
- Malware and File inspection
- Security Intelligence
- Contextual Visibility
- Correlation
- Authentication and Authorization
Firepower Management Center Overview

- Only manager required for Firepower Threat Defense
- Added functionality to manage the features brought in from ASA
- Can also manage Firepower appliance and services deployments
- Unified policy management for Firepower appliances/services and Firepower Threat Defense
- Enhanced configuration management built on tested technology
Summary:

• FTD: Converged OS of ASA and FirePower
• Single Manager (FMC): ASA feat + FirePower
• FMC continues to manage: ASA w/FP
• 2H 2016 – Adding more features to FMC from ASA
Thank you.