Cisco Forschung & Lehre Forum für Mecklenburg Vorpommern
Security Update

Roland Müller (rmueller@cisco.com)
System Engineer

Januar 2015
Agenda

- 1+1=3 ASA mit Firepower Services
- AMP – Advanced Malware Protection
- ISE 1.3 und AnyConnect 4.0
1+1=3: Cisco ASA mit FirePOWER Services
Sourcefire is Now Part of Cisco

- Cisco welcomes 700 employees
- Martin Roesch, Sourcefire founder and author of Snort®, joins Cisco as vice president and chief security architect
- Sourcefire brings a team of expert engineers and professionals with a deep knowledge of security and open source
- Based in Maryland, an area widely recognized as a Center of Excellence for security innovation
- Sourcefire employees will support Cisco’s Security Business Group
Integrated Threat Defense Across the Attack Continuum

**Before**
- Discover
- Enforce
- Harden

**During**
- Detect
- Block
- Defend

**After**
- Scope
- Contain
- Remediate

Firewall/VPN
- Detailed App Control
- Modern Threat Control

NGIPS
- Security Intelligence
- Web Security

Advanced Malware Protection
- Retrospective Security
- IoCs/Incident Response

Visibility and Automation
FirePOWER Services for Cisco ASA

FirePOWER Services for 5500-X (Software)

FirePOWER Services for 5585-X (Blade)

Subscriptions: Threat (IPS and AVC), URL Filtering, AMP
Cisco ASA with FirePOWER Services

► Cisco® ASA firewalling combined with Cisco Sourcefire® next-generation IPS (NGIPS)
► Integrated threat defense over the entire attack continuum
► Best-in-class security intelligence, application visibility and control (AVC), and URL filtering
Superior Integrated and Multilayered Protection

Cisco® Collective Security Intelligence Enabled

- Clustering and High Availability
- Intrusion Prevention (Subscription)
- Application Visibility and Control
- Built-in Network Profiling
- Identity-Policy Control and VPN
- Advanced Malware Protection (Subscription)
- FireSIGHT Analytics & Automation
- URL Filtering (Subscription)
- WWW

Cisco ASA

- World’s most widely deployed, enterprise-class Cisco ASA stateful firewall
- Cisco Application Visibility and Control (AVC) with detailed control
- Industry-leading Cisco FirePOWER next-generation IPS (NGIPS)
- Reputation- and category-based URL filtering
- Cisco Advanced Malware Protection (AMP)
FirePOWER Services: New Security Subscriptions for Cisco ASA Product Family

FirePOWER Services for Cisco ASA 5500-X (Software)

- ASA 5512-X
- ASA 5515-X
- ASA 5525-X
- ASA 5545-X
- ASA 5555-X

FirePOWER Services for Cisco ASA 5585-X (Blade)

- ASA 5585-SSP10
- ASA 5585-SSP20
- ASA 5585-SSP40
- ASA 5585-SSP60

Performance and Scalability
Five Subscription Packages to Choose From for Each Appliance

- AVC is part of the default offering
- 1 and 3 year terms
- SMARTnet is ordered separately with the appliance
# Exceptional Network Visibility

<table>
<thead>
<tr>
<th>Categories</th>
<th>Cisco® FirePOWER Services</th>
<th>Typical IPS</th>
<th>Typical NGFW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threats</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Users</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
</tr>
<tr>
<td>Web Applications</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
</tr>
<tr>
<td>Application Protocols</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
</tr>
<tr>
<td>File Transfers</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
</tr>
<tr>
<td>Malware</td>
<td>✓</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Command and Control Servers</td>
<td>✓</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Client Applications</td>
<td>✓</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Network Servers</td>
<td>✓</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Operating Systems</td>
<td>✓</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Routers and Switches</td>
<td>✓</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Mobile Devices</td>
<td>✓</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Printers</td>
<td>✓</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>VoIP Phones</td>
<td>✓</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Virtual Machines</td>
<td>✓</td>
<td>×</td>
<td>×</td>
</tr>
</tbody>
</table>
NGIPS: Open Source Snort®

- Global standard for Intrusion Detection and Prevention
- World’s largest threat response community
- Interoperable with other security products
- Owned and controlled by Sourcefire/Cisco
- www.snort.org
Automated, Integrated Threat Defense
Superior Protection for Entire Attack Continuum

Context and Threat Correlation

- Impact Assessment
- Priority 1
- Priority 2
- Priority 3

Multivector Correlation

- Early Warning for Advanced Threats
- Host A
- Host B
- Host C
- 5 IoCs
- 3 IoCs

Dynamic Security Control

- Adapt Policy to Risks

Retrospective Security

- Reduce Time Between Detection and Cure
Indications of Compromise (IoCs)

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

- **SI Events**
  - CnC Connections
  - Admin Privilege Escalations

- **Malware Events**
  - Connections to Known CnC IPs
  - Malware Detections
  - Office/PDF/Java Compromises
  - Malware Executions
  - Dropper Infections

In the diagram, there is a table titled "Indications of Compromise (3)", showing the following events:

- **Exploit Kit**
  - Event Type: Intrusion Event - exploit-kit
  - Description: The host may have encountered an exploit kit
  - First Seen: 2013-09-17 16:46:28
  - Last Seen: 2013-09-20 06:35:31

- **CnC Connected**
  - Security Intelligence Event - CnC
  - First Seen: 2013-09-17 16:52:11
  - Last Seen: 2013-09-20 03:55:45

- **CnC Connected**
  - Intrusion Event - malware-cnc
  - First Seen: 2013-09-17 20:09:23
  - Last Seen: 2013-09-19 17:32:49
FirePOWER Services: Application Control

- Control access for applications, users and devices
- “Employees may view Facebook, but only Marketing may post to it”
- “No one may use peer-to-peer file sharing apps”

Over 2,200 apps, devices, and more!
FirePOWBER Services: URL Filtering

• Block non-business-related sites by category
• Based on user and user group
FirePOWER Services: Advanced Malware

1) File Capture
2) File Storage
3) Send to Sandbox
4) Execution Report

Available In Defense Center

Malware Alert!

Network Traffic

Collective Security Intelligence Sandbox
Deploying ASA w/ FirePOWER Services

- High Availability with ASA Failover
- Available on all ASA platforms
- State-sharing between Firewalls for high availability
- L2 Transparent or L3 Routed deployment options
- Failover Link
- **ASA provides valid, normalized flows to** FirePOWER module
- State sharing does not occur between FirePOWER Services Modules
Deploying ASA w/ FirePOWER Services: Scaling IPS with ASA5585-X Clustering

- Up to 8 ASA5585-X IPS
- Stateless load balancing by external switch
- L2 Transparent or L3 Routed deployment options
- Support for vPC, VSS and LACP
- Cluster Control Protocol/Link
- State-sharing between Firewalls for symmetry and high availability
- Every session has a primary and secondary owner ASA
- ASA provides traffic symmetry to FirePOWER module
- *State sharing does not occur between FirePOWER Services Modules
Multi-Context ASA Deployments

- ASA can be configured in multi context mode such that traffic going through the ASA can be assigned different policies.

- These interfaces are reported to the FirePOWER blade and can be assigned to security zones that can be used in differentiated policies.

- In this example, you could create one policy for traffic going from Context A Outside to Context A Inside. And then a different policy for Context B Outside to Context B Inside.

- Note: There is no management segmentation inside the FirePOWER module similar to the context idea inside ASA configuration.
FirePOWER Services Demonstration
Monitor-Only Mode (Demonstration Purposes Only currently)

• Monitor Mode allows FirePOWER Services to analyze traffic without being placed in the data path. The ASA is connected to a SPAN port on a switch or router, and copies of both inbound and outbound packets are sent to the FirePOWER Service. This copied traffic bypasses the ASA policy and goes directly to the FirePOWER Services which will apply policies to determine what traffic would have been blocked. After analysis of the traffic, the packets are discarded.
Today’s advanced malware is not just a single entity

It is a **Community** that hides in plain site

Missed by Point-in-time Detection
Cisco Advanced Malware Protection delivers…

Point in Time Protection

Retrospective Security

File Reputation & Sandboxing

Continuous Analysis
Delivers the first line of detection

- One-to-One Signature
- Fuzzy Fingerprinting
- Machine Learning
- Advanced Analytics
- Dynamic Analysis

Reputation Filtering and File Sandboxing
But most importantly AMP provides continuous retrospective security.

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

Telemetry Stream

File Fingerprint and Metadata
File and Network I/O
Process Information

Continuous feed

Continuous analysis
That continues to analyze what happens along the attack continuum.

Advanced levels of detection, tracking and response.

- Retrospection
- Retrospective Detection
- Behavioral Indications of Compromise
- Trajectory
- Threat Hunting
Giving you the assurance and visibility to know exactly where to start

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
An unknown file is present on IP: 10.4.10.183, having been downloaded from Firefox at 10:57. Seven hours later the file is then transferred to a third device (10.3.4.51) using an SMB application. The file is copied yet to a fourth device (10.5.60.66) through the same SMB application a half hour later.

The Cisco Collective Security Intelligence Cloud has learned this file is malicious and a retrospective event is raised for all four devices immediately. At the same time, a device with the FireAMP endpoint connector reacts to the retrospective event and immediately stops and quarantines the newly detected malware.

8 hours after the first attack, the Malware tries to re-enter the system through the original point of entry but is recognized and blocked.
Device Trajectory
Endpoint AMP

OpenIOC: Generic Botnet Communication
Description: Accessed URL matches characteristics of several malware families.
At 08:11:38, Fri May 23 2014 UTC

Detected Trojan.Spy.ZBot.FGD as bot002.exe (6b473f7..be53ef)
[PE Executable].

Executed by explorer.exe, Microsoft® Windows® Operating
System 6.0.2900.5512 (1e675cb..5ef455) [PE Executable] executing
as cisco@HU-WinXP-AMP03.

Downloaded from http://144.254.102.100/dh/bot002.exe.
The file was not quarantined. In audit only mode.
At 09:05:04, Sat Jan 18 2014 UTC
[ more details ]
## Comprehensive Environment Protection with AMP

<table>
<thead>
<tr>
<th>Cisco Advanced Malware Protection</th>
<th>AMP Protection</th>
<th>Content</th>
<th>Network</th>
<th>Endpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email and Web</td>
<td>AMP Protection</td>
<td>www</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Networks</td>
<td></td>
<td></td>
<td>Content</td>
<td></td>
</tr>
<tr>
<td>Devices</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Threat Vector
- Email and Web
- Networks
- Devices

### Method
- License with ESA or WSA
- Stand Alone Solution
- Enable AMP on FirePOWER Appliance
- Firepower Service on ASA

### Ideal for
- New or existing Cisco Email or Web Security customers
- IPS/NGFW/ASA customers
- Install on endpoints
- Windows, Mac, Android, VMs
Cisco Advanced Malware Protection
Built on unmatched collective security intelligence

Cisco Talos

1.6 million
global sensors
35%
worldwide email traffic
100 TB
of data received per day
13 billion
web requests
150 million+
deployed endpoints
24x7x365
operations
600+
gineers, technicians,
and researchers

---

180,000+ File Samples per Day
FireAMP™ Community
Advanced Microsoft
and Industry Disclosures
Snort and ClamAV Open Source
Communities
Honeypots
Sourcefire AEGIS™ Program
Private and Public Threat Feeds
Dynamic Analysis

---
Cisco Acquired ThreatGRID

“If Cisco executes on integration as well as they have been with SourceFire’s products and team this could be a dramatic challenge to FireEye.”

--Richard Stiennon

ThreatGRID + Cisco = Enhanced Protection Against Advanced Threats

Better Together

Cisco

- Market leading AMP product portfolio with...
- Protection throughout the attack continuum
- Coverage across the extended network
- Point-in-time & continuous technology including cloud-based dynamic analysis

ThreatGRID

- Private cloud sandboxing for dynamic malware analysis
- Analysis for additional file types
- API integration and automation
- Detects master boot record

ThreatGRID’s technology enhances Cisco’s Advanced Malware Protection Portfolio

- Private cloud-based products expands our ability to protect customers with stringent in-house data retention requirements.
- More threat data to aggregate & correlate from across the extended network means better context and threat intelligence for customers.
Cisco ISE 1.3 und AnyConnect 4.0 – What’s New
Cisco Identity Services Engine (ISE)
Delivering the Visibility and Control for Secure Network Access

Cisco ISE is the Market Leader
The Different Ways Customers Use ISE

**Guest Access Management**
Easily provide guests limited-time, limited-resource Internet access

**BYOD and Enterprise Mobility**
Seamlessly & securely onboard devices with the right levels of access

**Secure Access across the Entire Network**
Simplify & unify enterprise network access policy across wired, wireless, & VPN

**With Cisco TrustSec®**
Identity-aware Network Segmentation and Access Policy Enforcement
User Experience

All New Guest Experience

Introducing Admin Work Centers

BYOD & Certificate Management Made Easy
Hotspot

Goal: Get them on the Internet with AUP acceptance no matter who they are and remember who they are next time so you don’t get in their way.

Acceptable Use Policy
I promise to be good.

You Made It!
You are now connected to the Internet.
Looking for a great website? Just visit the DINOCO Store.

Day Ends
Self Service with Email Verification

1. Fill In A Simple Form
2. Check Your Email
3. Connect to WFI

Username: HanSolo
Password: nerfherder
Self Service with SMS

Goal: Get them on the Internet as long as you have a 3rd party identifier that proves who the user is.
Self Registration with Sponsored Approval

1. ISE sends email requesting approval

2. Logs into Sponsor Portal and Approves or rejects

3. Approved credentials
   username: trex42
   password: littlearms
Hi! Can I get on your Wi-Fi?

Sure. I just need a little information.

Print, email & SMS credentials. Cool!
The All New Guest Administration

A Guest Button

With our new navigation, getting to the Guest admin has never been easier.

One Stop Setup

Once you’re there, all the pieces you need are accessed in one place.

Prepackaged Flows

Ships with the default flows used by 90% of our customers: Hotspot, Self-Service (with or without approval), & Sponsored.
Walk Through BYOD Onboarding

- Out of the box flow walks users through onboarding.
- Fully customizable user experience with Themes.
- My Devices gives end users control to add and manage their devices.
- Mobile and desktop ready out of the box.
ISE 1.3: Internal Certificate Authority

Simplifying certificate management for BYOD devices

Managing certificates for BYOD adds significant complexity and expense when using Microsoft Public Key Infrastructure.

The ISE Certificate Authority is designed to work in concert as a self contained solution or with your existing Enterprise PKI to simplify BYOD deployments.

- **Single Management Console** – Manage endpoints and their certs. Delete an endpoint ISE deletes the cert.

- **Simplified deployment** – Supports stand alone and subordinate deployments. Removes corporate PKI team from every BYOD interaction.

*Designed for BYOD and MDM use-cases only, not a general purpose CA*
Simplified Integration

- Multi-Forest Active Directory
- Streamlined VPN
- AnyConnect Unified Agent
Multi-Forest Active Directory Support

ISE 1.3 is designed for growing businesses. With support for multiple Active Directory domains, ISE 1.3 enables authentication and attribute collection across the largest enterprises.

- Support for 50 concurrent Active Directory join points
- No need for 2-way trust relationship between domains
- Advanced algorithms for dealing with identical usernames.
Cisco ISE Posture Agents

Cisco NAC Agent

Cisco AnyConnect 4.0
AnyConnect 4.0 – ISE Posture

- An ISE posture AnyConnect module
  - Windows and OS X support
- Integration with the AC end-user experience (single posture tile for ISE and ASA posture)
  - Further strengthened by ISE 1.3 Posture Lease functionality
- AC deployment from ISE
  - Including an AC ISE posture module profile editor
- Coexistence with NAC Agent for ease of migration
  - This will help existing ISE and NAC Appliance customers
- Monthly compliance module updates
  - Same as today with the NAC Agent
Context and Speed

Streamlined Threat Defense

Streamlined Operation with new REST APIs
Enabling the Potential of Network-Wide Context Sharing

**INFRASTRUCTURE FOR A ROBUST ECOSYSTEM**

- Single framework – develop once, instead of multiple APIs
- Customize and secure what context gets shared and with which platforms
- Bi-directional – share and consume context
- Enables any pxGrid partner to share with any other pxGrid partner
- Integrating with Cisco ONE SDN for broad network control functions
Use Case: Identity and device aware threat management

Increase confidence around event severity levels in SIEMs and TD consoles; make events actionable in the network. SIEM/TD share “worst offenders” with ISE for user/device policy decisions.

Policy: Detect sensitive data access on mobile devices; quarantine such users.

Data: “Sensitive Data”
Type: “Mobile Device”

Context: Share with SIEM
USER : DEVICE TYPE : CONN STATUS
ISE REST APIs

- **Internal ISE User API** – Create and Manage ISE users programmatically.
- **Session Directory API** – Access to all the details for a given MAC or IP address.
- **Endpoints API** – Input new endpoints and assign them to groups. Ex. add corporate printers

- **Guest API** – Create and Manage Guest accounts.
- **NAD/NDG (Network access device & network device group) API** – Add and manage access control network devices configured within ISE. Ex. (teleworker devices)
- **Bulk Operation Support** – for Internal User, Endpoint, NAD and Guest APIs
- **Extended EPS API** – manage Endpoint Protection
- **pxGrid** – Enabling the potential of network wide context sharing.
Questions ?
Thank you.