TOMORROW starts here.
Design and Deployment of SourceFire NGIPS and NGFWL

BRKSEC - 2024

Marcel Skjald
Consulting Systems Engineer
Enterprise / Security Architect
Abstract
Overview of Session

- This technical session covers the FirePOWER security appliance product line and how it uniquely uses context to deliver true next generation network security capabilities including NGIPS, NGFW, and AMP (Next Generation IPS, Next Generation Firewall, and Advanced Malware Protection).

- The session will begin with a detailed review of the FirePOWER architecture including hardware acceleration, packet, flow and stream processing, and then move on to introduce why network context from FireSIGHT is a vital component in delivering these next generation services.

- Followed by a detailed review of Advanced Malware Protection, and how it uses context in detailing Malware behaviour.

- Deployment Scenarios.
Agenda

- Why do we need NGIPS or Advanced Malware Protection?
- What is FirePOWER? Performance and functional characteristics
- Packet and flow processing (day in the life of a stream)
- What is FireSIGHT?
- Awareness and the Network Map
- Why this context is vital in modern networks
- FirePOWER: Security deployment modes
  - NGIPS
  - NGFW
  - Advanced Malware Protection (AMP)
- Deployment Scenarios / Considerations
Why do we Need NGIPS & Advanced Malware Detection?

- Hackers
- State Based Actors
- Criminals
- Insider Threats
- Compliance
- Due Diligence
- Knowledge!

27,375,000 malware detection updates in FireAMP during 2013
Where did it all Start?

Marty Roesch
Threat Focused Approach to Network Security

Access Control
- Remote Access VPN
- Gateway VPN Switching
- Routing
- NAT
- Stateful Inspection

App Control
- Detection of applications
- Allow/block apps and app sub-functions
- Allow/block apps by user
- Allow/block apps by type, tag, category, risk rating

Threat Prevention
- Vulnerability facing rules
- Threat facing rules
- Enterprise accuracy and performance

Context Awareness
- Correlate host and user activity
- Passive OS Fingerprinting
- Passive Service Identification
- Passive Vulnerability mapping
- Passive Network Discovery
- Auto Policy Recommendations
- Auto Impact Assessment

Typical Firewall
Typical IPS
Typical NGFWs
FirePOWER NGIPS
FirePOWER – NGFW
FirePOWER Platform - Overview
What is FirePOWER?

- Industry-leading security platform
- Unmatched performance from a single-pass, low-latency design
- Configuration flexibility
- Standard platform for delivering the Sourcefire network capability
- NGIPS, NGFW & AMP
FirePOWER Platform

**Configurable Bypass or Fail Closed Interfaces**
*For IDS, IPS or Firewall deployments*

**Device Stacking**
*Scale monitoring capacity through stacking*

**Lights Out Management**
*Minimal operational impact*

**Connectivity Choice**
*Change and add connectivity inline with network requirements*

**LCD Display**
*Quick and easy headless configuration*

**Hardware Acceleration**
*For best in class throughput, security, Rack size/Mbps, and price/Mbps*

**SSD**
## FirePOWER Platform

### IPS Throughput

<table>
<thead>
<tr>
<th>Throughput</th>
<th>Model Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>40 Gbps</td>
<td>8290</td>
</tr>
<tr>
<td>30 Gbps</td>
<td>8270</td>
</tr>
<tr>
<td>20 Gbps</td>
<td>8260</td>
</tr>
<tr>
<td>10 Gbps</td>
<td>8250</td>
</tr>
<tr>
<td>6 Gbps</td>
<td>8140</td>
</tr>
<tr>
<td>4 Gbps</td>
<td>8130</td>
</tr>
<tr>
<td>2 Gbps</td>
<td>8120</td>
</tr>
<tr>
<td>1.5 Gbps</td>
<td>7125</td>
</tr>
<tr>
<td>1.25 Gbps</td>
<td>7120</td>
</tr>
<tr>
<td>1 Gbps</td>
<td>7115</td>
</tr>
<tr>
<td>750 Mbps</td>
<td>7110</td>
</tr>
<tr>
<td>500 Mbps</td>
<td>7030</td>
</tr>
<tr>
<td>250 Mbps</td>
<td>7010</td>
</tr>
<tr>
<td>100 Mbps</td>
<td>7020</td>
</tr>
<tr>
<td>50 Mbps</td>
<td>7010</td>
</tr>
</tbody>
</table>

### All appliances include:
- Integrated lights-out management
- Sourcefire acceleration technology
- LCD display

---

**Modular Connectivity**

- Mixed / SFP

---

**Stackable Connectivity**

- Fixed Connectivity

---

**Cisco live!**

---

© Cisco and/or its affiliates. All rights reserved.
FirePOWER Scalability

- Up to four 8250 chassis can be stacked

<table>
<thead>
<tr>
<th>Number of chassis</th>
<th>IPS Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10Gbps</td>
</tr>
<tr>
<td>2</td>
<td>20Gbps</td>
</tr>
<tr>
<td>3</td>
<td>30Gbps</td>
</tr>
<tr>
<td>4</td>
<td>40Gbps</td>
</tr>
</tbody>
</table>
New FirePower Appliances – 8300 Series

Current 8200 Offerings

<table>
<thead>
<tr>
<th>IPS Throughput</th>
<th>8290</th>
<th>8270</th>
<th>8260</th>
<th>8250</th>
</tr>
</thead>
<tbody>
<tr>
<td>40 Gbps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30 Gbps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20 Gbps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 Gbps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

New 8300 Offerings

<table>
<thead>
<tr>
<th>IPS Throughput</th>
<th>8390</th>
<th>8370</th>
<th>8360</th>
<th>8350</th>
</tr>
</thead>
<tbody>
<tr>
<td>60 Gbps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>45 Gbps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30 Gbps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15 Gbps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# 8300 Series – Performance Specifications

<table>
<thead>
<tr>
<th></th>
<th>Rack Height</th>
<th>NGIPS Throughput</th>
<th>Maximum Monitoring Interfaces (1Gbps)</th>
<th>x86 Cores/ threads and # Microengines</th>
<th>Netmod Bays</th>
<th>Stacking</th>
</tr>
</thead>
<tbody>
<tr>
<td>8350</td>
<td>2U</td>
<td>15Gbps</td>
<td>28</td>
<td>20/40 and 80</td>
<td>7</td>
<td>Yes, with additional 8350 appliances.</td>
</tr>
<tr>
<td>8360</td>
<td>4U</td>
<td>30Gbps</td>
<td>24</td>
<td>40/80 and 160</td>
<td>6</td>
<td>Yes, with additional 8350 appliances.</td>
</tr>
<tr>
<td>8370</td>
<td>6U</td>
<td>45Gbps</td>
<td>20</td>
<td>60/120 and 240</td>
<td>5</td>
<td>Yes, with additional 8350 appliances.</td>
</tr>
<tr>
<td>8390</td>
<td>8U</td>
<td>60Gbps</td>
<td>16</td>
<td>80/160 and 320</td>
<td>4</td>
<td>Yes, with additional 8350 appliances.</td>
</tr>
</tbody>
</table>
## FirePOWER - 7010, 7020, 7030

- **Half Width Chassis – Fixed 8 Port Copper**
  - Low Latency
  - LCD Screen
  - Integrated LOM
  - Solid State Drive

### Specifications

<table>
<thead>
<tr>
<th>Model</th>
<th>Acceleration</th>
<th>RAM</th>
<th>IPS Throughput</th>
<th>Modes</th>
</tr>
</thead>
<tbody>
<tr>
<td>3D7030</td>
<td><img src="image1" alt="firePOWER" /></td>
<td>4GB</td>
<td>250 Mbps</td>
<td>NGIPS, NGFW, AMP</td>
</tr>
<tr>
<td>3D7020</td>
<td><img src="image2" alt="firePOWER" /></td>
<td>4GB</td>
<td>100 Mbps</td>
<td>NGIPS, NGFW, AMP</td>
</tr>
<tr>
<td>3D7010</td>
<td><img src="image3" alt="firePOWER" /></td>
<td>4GB</td>
<td>50 Mbps</td>
<td>NGIPS, NGFW, AMP</td>
</tr>
</tbody>
</table>
# Defense Center

<table>
<thead>
<tr>
<th>Performance and Functionality</th>
<th>DC750</th>
<th>DC1500</th>
<th>DC3500</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Sensors Managed [1]</td>
<td>10</td>
<td>35</td>
<td>150</td>
</tr>
<tr>
<td>Maximum Network Map Size - Hosts</td>
<td>2,000</td>
<td>50,000</td>
<td>300,000</td>
</tr>
<tr>
<td>Maximum Network Map Size - Users</td>
<td>2,000</td>
<td>50,000</td>
<td>300,000</td>
</tr>
<tr>
<td>Maximum IPS Event Storage</td>
<td>20 Million</td>
<td>30 Million</td>
<td>150 Million</td>
</tr>
<tr>
<td>Maximum IPS Event Rate (per second)</td>
<td>2,000</td>
<td>5,000</td>
<td>10,000</td>
</tr>
<tr>
<td>Maximum Flow Data Rate (per second)</td>
<td>2,000</td>
<td>5,000</td>
<td>10,000</td>
</tr>
<tr>
<td>Management Interface</td>
<td>10/100/1000 RJ45</td>
<td>10/100/1000 RJ45</td>
<td></td>
</tr>
<tr>
<td>Memory (RAM)</td>
<td>2GB</td>
<td>6GB</td>
<td>12GB</td>
</tr>
<tr>
<td>Event Storage Space</td>
<td>100GB</td>
<td>125GB</td>
<td>400GB</td>
</tr>
<tr>
<td>Can function as Master Defense Center</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

## Redundancy Features

<table>
<thead>
<tr>
<th></th>
<th>DC750</th>
<th>DC1500</th>
<th>DC3500</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supports High Availability</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Dual Power Supplies</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>RAID Support</td>
<td>No</td>
<td>RAID 1</td>
<td>RAID 5</td>
</tr>
</tbody>
</table>
FirePOWER – Virtual

- Virtual Sensor
  - Inline or passive deployment
  - Full NGIPS Capabilities
  - Deployed as virtual appliance
  - Use Cases
    - SNORT Conversion
    - Small / Remote Sites
    - Virtualized workloads (PCI)

- Virtual Defense Center
  - Manages up to 25 sensors
    - physical and virtual
    - single pane-of-glass
  - Use Cases
    - Rapid Evaluation
    - Pre-production Testing
    - Service Providers
FirePOWER Architecture
The Power of Hardware & Software Combined

Enables industry leading, energy efficient performance for Sourcefire NGIPS | NGFW

Custom designed, specialised network processor accelerates data acquisition and classification.
Single Pass Architecture
Single Pass Architecture

480Gbps Layer 2-4 packet classification

Multiple 20Gbps Layer 2-7 flow classification

Detection Engines

- DAQ
- Decode
- Pre-process
- Analysis
- Output

2 x 40 microcores, each @ 1,800 instructions/packet @ 30 million pps

Cluster NetMod

to stacked device...

480 Gbps Load Balancer

20 Gbps Load

480 Gbps Load Balancer...
FirePOWER Architecture – V5.X
Life of a Flow

- Hardware processing
- Initial processing
  - IP Blacklist (Security Intelligence)
  - Flows that are blocked/trusted via AC rules
- Network Layer Processing
  - IP Defrag Frag, Stream, Rate Based Attack
- Application Identification
- AC Rule Evaluation
- Network Discovery
- IPS & File Processing
Life of a Flow

- Hardware Processing
  - Look for flow in flow state table
  - Create if not there
  - If flow has disposition of Block or Trust, take immediate action
- Evaluate hardware rules
- If block or trust, mark entry in flow state table
- Take action on rule
- If inspect
  - Store information about AC rule and Start Inspection
Life of a Flow

- Initial processing
  - Packet decoding
  - IP Blacklist (Security Intelligence)
  - immediately mark flow as blocked, update hardware flow state
  - monitor - mark flow, log later

- Network Layer Processing
  - IP Defragmentation/Connection Tracking/TCP Stream reassembly
  - Connection tracking by IPs, Ports, VLAN, IP Protocol, MPLS Label, In/Out zones unique ID

- Application Identification
  - When needed for AC rules
Life of a Flow

- **AC Rule evaluation**
  - Can match Zones, VLAN, IPs, Ports & User/Group based on packet header

- **Need App ID for matching Applications and URLs**
  - Packets continue to flow until Application is identified and the rule criteria can be matched or considered a non-match
  - If Application not yet determined, IPS policy from Default is used (“No Rules Active” if that is Block or Trust)

- **If action of block/trust**
  - Immediately mark flow, update hardware flow state

- **If action of allow**
  - Select IPS policy?
  - Select File policy?
Life of a Flow

- **Network Discovery**
  - Only if within Networks Discovery Policy
  - Hosts, users, applications

- **App ID**
  - Leverage information from earlier if done for AC rule

- **Network Map Events**
Life of a Flow

- **IPS**
  - IPS Event logging for Decode/Frag/Stream events
    - May block flow at this point
  - Application Preprocessors
    - HTTP Inspect, FTP/Telnet, SMTP, POP, IMAP, DCE/RPC, DNS, DNP3, Modbus, GTP, SSH, SSL
  - IPS Rules
    - Leverage Application Protocol ID to select rules
  - IPS Events
    - if block, mark flow as blocked, update hardware flow state
Life of a Flow

- File Processing

- Leverage HTTP, SMTP, POP, IMAP, FTP preprocessors

- File type ID
  - Usually within first part of the file

- Malware signature calculation & lookup
  - Requires entire file

- Blocking & Logging of File events
FireSight - Context
Got a lot of Data? – Well what was the question?
Why is Context Important?

Event + network & user context

Event: Attempted Privilege Gain
Target: 96.16.242.135 (vulnerable)
Host OS: Blackberry
Apps: Mail, Browser, Twitter
Location: Whitehouse, US
User ID: bobama
Full Name: Barack Obama
Department: Executive Office

Event + network context

Event: Attempted Privilege Gain
Target: 96.16.242.135 (vulnerable)
Host OS: Blackberry
Apps: Mail, Browser, Twitter
Location: Whitehouse, US

Event

Event: Attempted Privilege Gain
Target: 96.16.242.135
Dashboard - Context

Browse all application traffic…

Look for risky applications

What else have these users been up to?

On what operating systems?

What does their traffic look like over time?
FireSIGHT - CONTEXT

- OS & version identified
- Server applications and version
- Client Applications
- Client Version
- Application
- Who is at the host
- What other systems / IPs did user have, when?
Context - Geolocation

- Visualise and map countries, cities of hosts, events
Network AMP - Context

The time of entry

Systems Infected

File Trajectory for 8fe98673...267e06b9
Advanced Malware Protection - AMP
Complete advanced malware protection suite to protect networks and devices

- Dedicated Advanced Malware Protection (AMP) appliance
- Advanced Malware Protection Subscription for FirePOWER appliances
- Advanced malware protection for hosts virtual and mobile devices
AMP - Overview

**Advanced Malware Protection**

- Malware detection of files across the wire
- In-line *Retrospective Security* for continuous analysis and detection including retrospective alerts
- Security Intelligence for outbound / C&C

**Defence Centre**

**Event Stream**

**Control: FireAMP Connectors**

(Client/Mobile/Virtual)

Provide:
- Enhanced Intelligence
- Cleanup Capabilities

**Fingerprint**

**Retrospective Security**

- Continuous File Analytics
- Reputation Determination
AMP – Device trajectory

Device Trajectory for Java-0-Day

Root Cause

Other Threats of Interest

What it’s Doing?
AMP Context – Threat Root Cause

Threat Root Cause

Select Dates

Overview Details Timeline

<table>
<thead>
<tr>
<th>Program</th>
<th>Threat Name</th>
<th>Version</th>
<th>Threats Introduced</th>
<th>Computers Affected</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>explorer.exe</td>
<td>6.0.2900.5512</td>
<td>11</td>
<td>6</td>
<td>6 executed 5 moved</td>
<td></td>
</tr>
<tr>
<td>n.exe</td>
<td>6</td>
<td>6</td>
<td>1</td>
<td>2 created 2 executed 2 moved</td>
<td></td>
</tr>
<tr>
<td>java.exe</td>
<td>7.0.100.18</td>
<td>5</td>
<td>1</td>
<td>3 created 1 executed 1 moved</td>
<td></td>
</tr>
</tbody>
</table>

Detected Kazy:Troj_Generic-tdp as n (c9dbfc2..dc5600) [HTML].

Created by zaccess8308073210892168095.exe (87715c2..041f20) [HTML] executing as u@ZACCESSDRIVEBY2.

The file was not quarantined. In audit only mode.

At 22:05:11, Mon Feb 10 2014 UTC

File full path: C:\$Recycle.Bin\VS-1-5-21-1089625888-3054005746-3039903294-1000\%f20893dbb7e410a1126d2ca0eecb75n

File SHA-1: 9fbc6367265c8e04747004f4b1226e084c9bd79.

File MD5: 69bc8b1dcdfe7443d604b844b58d193.

File size: 53248 bytes.

Parent file SHA-1: 0800c75067600eab0f1341c3299f7b4126b6b.

Parent file MD5: bbf7933cd0da2b2152e040381e2.

Parent file size: 174592 bytes.

Parent process id: 4016.

Parent process SIDs: 5-1-5-21-1089625888-3054005746-3039903294-1000.

Detected by the SHA engines.
### AMP Context – Explorer Details

<table>
<thead>
<tr>
<th>Event Description</th>
<th>Type</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Demo_Tinba detected a Suspected Botnet connection</td>
<td>Botnet</td>
<td>12:40 PM EST, 2/11/2014</td>
</tr>
<tr>
<td>Demo_TDSS executed malware detected as Eldorado:Alureon-tpd in file unknown</td>
<td>Executed Malware</td>
<td>12:40 PM EST, 2/11/2014</td>
</tr>
<tr>
<td>Demo_Tinba executed malware detected as W32.Variant:Tinba.15h1.1201 in file unknown</td>
<td>Executed Malware</td>
<td>12:40 PM EST, 2/11/2014</td>
</tr>
<tr>
<td>Demo_Sality executed malware detected as W32.Sality:SmallHKN.d3da2.vv in file unknown</td>
<td>Executed Malware</td>
<td>12:40 PM EST, 2/11/2014</td>
</tr>
<tr>
<td>Demo_Rimecud executed malware detected as Rimecud:MalPack-tpd in file unknown</td>
<td>Executed Malware</td>
<td>12:40 PM EST, 2/11/2014</td>
</tr>
<tr>
<td>Demo_Ramnit executed malware detected as W32.Ramnit.A in file unknown</td>
<td>Executed Malware</td>
<td>12:20 PM EST, 2/11/2014</td>
</tr>
<tr>
<td>Demo_Stabuniq executed malware detected as W32.Variant:Stabuniq.15nx.1201 in file unknown</td>
<td>Executed Malware</td>
<td>12:03 PM EST, 2/11/2014</td>
</tr>
<tr>
<td>Demo_TDSS detected Eldorado:Alureon-tpd as tdss.exe</td>
<td>Quarantine: Not Seen</td>
<td>9:11 AM EST, 2/11/2014</td>
</tr>
<tr>
<td>Demo_TDSS detected Eldorado:Alureon-tpd as tdss.exe</td>
<td>Quarantine: Not Seen</td>
<td>9:09 AM EST, 2/11/2014</td>
</tr>
<tr>
<td>Demo_TDSS detected Eldorado:Alureon-tpd as tdss.exe</td>
<td>Quarantine: Not Seen</td>
<td>9:09 AM EST, 2/11/2014</td>
</tr>
</tbody>
</table>
AMP Context – IOC’s

- Indicators of Compromise
  - Monitor and Analyse files potential Malware traits
  - Monitors the now & retrospectively convicts files
  - Filters and sorts the most important events
  - Tells the analyst what is happening to reduce TCO
  - Quick links to trajectory
  - Search for SHA’s (fingerprints, list all computers that have the file)
Deployment Scenarios / Considerations
Deployment Scenarios / Usage – NGIPS / NGFW

- Data Centre GW
- Partner Networks / OGO’s
- Branch Office Links
- ISP feeds
- DMZs
- Segregated PCI LAN
- Out of band management LAN
- VLAN’s
- Internal (Core) LAN
- Critical Infrastructure LAN

- Traditional IDS / IPS
- Malware Detection
- Data Exfiltration (insider threat)
- Bandwidth Hogs
- Improper use of Corporate systems
  - (Websites / BitTorrent)
- Compliance PII / PCI data breaches
- Application usage / control and adherence to policies
- BYOD
- Due Diligence
Deployment Scenarios / Usage – Virtual

- Partner Networks / OGO’s
- Branch Office Links
- DMZs
- Segregated PCI LAN
- Out of band management LAN
- VLAN’s
- Internal (Core) LAN
- Critical Infrastructure LAN
- Deployed Infrastructure (Defence)
- Cloud Services

- Traditional IDS / IPS
- Malware Detection
- Data Exfiltration (insider threat)
- Bandwidth Hogs
- Improper use of Corporate systems
  - (Websites / BitTorrent)
- Compliance PII / PCI data breaches
- Application usage / control and adherence to policies
- BYOD
- Due Diligence
- Resilience!
Q & A
Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 March 12:00pm - 2:00pm

Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations.
www.CiscoLiveAPAC.com