Techtorial SEC-4

Next-Generation FW a IPS v Cisco ASA

Jiří Tesař, CSE Security

jitesar@cisco.com, CCIE #14558, SFCE #124266
Offering Overview
(H/W, Subscriptions, Management)
ASA + Sourcefire = New, Adaptive, Threat-focused NGFW

Cisco ASA

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

Cisco Collective Security Intelligence Enabled

CISCO ASA
FirePOWER Services
New Security Subscriptions for Cisco ASA Product Family
ASA with FirePOWER Services: Offering Structure

1. Base Hardware
   - New ASA 5585-X Bundle SKUs with FirePOWER Services Module
     - Upgrade: FirePOWER Services Spare Module/Blade for ASA 5585-X Series
   - New ASA 5500-X SKUs with SSD running FirePOWER Services Software
     - Upgrade: SSD + FirePOWER Services Upgrade License
   - FirePOWER Services Software >= 5.3.1
   - Appliance SMARTnet Services

2. Security Subscription Services
   - IPS, URL, Advanced Malware Protection (AMP) Subscription Services
   - 1, 3, and 5 Year Term Options

3. Management Systems
   - FireSIGHT Management Center (HW Appliance or Virtual) version >= 5.3.1
   - SMARTnet/SASU
   - Cisco Security Manager (CSM)
Managing Cisco ASA FirePOWER Services

Two Managers with Cross-launch

Cisco FireSIGHT Management Center
Models: 750, 1500, 3500, Virtual Appliance

Cisco Security Manager (CSM) or ASDM
CSM version 4.7
# FireSIGHT Management Center Appliances

<table>
<thead>
<tr>
<th>Max. Devices Managed*</th>
<th>750</th>
<th>1500</th>
<th>2000 (upcoming)</th>
<th>3500</th>
<th>4000</th>
<th>Virtual</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10</td>
<td>35</td>
<td>70</td>
<td>150</td>
<td>300</td>
<td></td>
</tr>
<tr>
<td>Event Storage</td>
<td>100 GB</td>
<td>125 GB</td>
<td>1.8 TB</td>
<td>400 GB</td>
<td>4.8/6.3 TB</td>
<td></td>
</tr>
<tr>
<td>Max. Network Map (hosts / users)</td>
<td>2K/2K</td>
<td>50K/50K</td>
<td>150K/150K</td>
<td>300K/300K</td>
<td>600K/600K</td>
<td></td>
</tr>
<tr>
<td>Events per Sec (EPS)</td>
<td>2000</td>
<td>6000</td>
<td>12000</td>
<td>10000</td>
<td>20000</td>
<td></td>
</tr>
</tbody>
</table>

Virtual FireSIGHT Management Center
Up to 2 or 10 Managed Devices - Special PIDs

Virtual FireSIGHT Management Center
Up to 25 Managed Devices

* Max number of devices is dependent upon sensor type and event rate
- Five (5) feature license packages are available
- AVC is part of the default offering
- 1, 3 and 5 year terms are available
- SMARTnet is ordered separately with the appliance
How to add FirePOWER Services to an ASA-5500-X

- Purchase ASA5500X-SSD120=
  - Adds Solid State Disc drive to ASA platform
  - Two drives required for ASA-5545 / 5555 (mirror redundancy)

- Purchase $0 ASA55xx-CTRL-LIC=
  - Adds perpetual “Protect and Control” license

- Purchase FS-VMW-x-SW-K9
  - FireSIGHT Management Center Virtual Appliance
  - 2 and 10 device SKU’s can NOT be upgraded later

- Purchase additional licenses as needed (not required)
  - URL / IPS / AMP offered as 1 or 3 year subscriptions
Licensing Key Points

• All licenses are installed on the FMC - Licenses work as a pool for each given appliance model, ie.. You have 20 5525-X licenses so as you add 5525-Xs to your FMC they simply pull from the pool.

* Licenses are simply a count that gets used up by the devices added to the FMC

• Licensing amongst FirePOWER services (SourceFire running on the ASA) and FirePower appliances is the same with the key caveat being VPN. VPN on FirePower appliances is the key exception where VPN on FirePower appliances is a perpetual license.

✧ Break down of Licensed Features:
  ✧ ASA appliance with FP Services/Appliance – protect and control = enables firepower services (IPS and AVC core functionality) - perpetual license
  ✧ URL - url filtering subscription
  ✧ IPS Subscription – Note: IPS subscription feature is not tied to a license (contract only)
  ✧ Malware Protection - AMP subscription

• To enable malware protection, you must have a protect license

• Term licenses (URL, IPS subscription, Malware) have a start and end date thus ensure renewals are up to date as functionality will exist but updates etc.. will cease.
# Cisco ASA with FirePOWER Services Licensing

<table>
<thead>
<tr>
<th>Component</th>
<th>License Name and Features Enabled</th>
<th>License Type</th>
<th>Fulfillment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco ASA Appliance with FirePOWER Services</td>
<td>Protect (IPS)</td>
<td>Perpetual License</td>
<td>Ships with Appliance/Upgrade License</td>
</tr>
<tr>
<td></td>
<td>Control (AVC)</td>
<td>Integrated</td>
<td>Ships with Appliance</td>
</tr>
<tr>
<td>URL Filtering</td>
<td>URL Filtering Subscription</td>
<td>Term License</td>
<td>Ships with URL Subscriptions</td>
</tr>
<tr>
<td>Malware Protection</td>
<td>AMP Subscription</td>
<td>Term License</td>
<td>Ships with AMP Subscriptions</td>
</tr>
<tr>
<td>FireSIGHT Management Center</td>
<td>FireSIGHT</td>
<td>Perpetual License</td>
<td>Ships with Appliance/Software Download</td>
</tr>
</tbody>
</table>
# Cisco ASA 5500-X FirePOWER Series

## ASA and SFR Resource Division

<table>
<thead>
<tr>
<th>Model</th>
<th>CPU</th>
<th>RAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA5555-X</td>
<td>Xeon 3430 2.8GHz 4 cores (3 available to IPS)</td>
<td>16G (50/50 split)</td>
</tr>
<tr>
<td>ASA5545-X</td>
<td>Xeon 3430 2.6GHz 4 cores (3 available to IPS)</td>
<td>12G RAM (50/50 split)</td>
</tr>
<tr>
<td>ASA5525-X</td>
<td>X3430 2.4GHz 4 cores (3 available to IPS)</td>
<td>8G RAM (50/50 split)</td>
</tr>
<tr>
<td>ASA5515-X</td>
<td>I3 3.0GHz 2 cores (1 available to IPS)</td>
<td>8G RAM (50/50 split)</td>
</tr>
<tr>
<td>ASA5512-X</td>
<td>Pentium 2.8GHz 2 cores (1 available to IPS)</td>
<td>4G RAM (50/50 split)</td>
</tr>
</tbody>
</table>
## Cisco ASA 5585-X FirePOWER Series

### SFR Resources

<table>
<thead>
<tr>
<th>Model</th>
<th>CPU</th>
<th>RAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA5585-X SSP-60</td>
<td>2 x E5645 2.46GHz 12 cores</td>
<td>48G</td>
</tr>
<tr>
<td>ASA5585-X SSP-40</td>
<td>2 x L5518 2.13GHz 8 cores</td>
<td>24G</td>
</tr>
<tr>
<td>ASA5585-X SSP-20</td>
<td>1 x L5518 2.13GHz 4 cores</td>
<td>12G</td>
</tr>
<tr>
<td>ASA5585-X SSP-10</td>
<td>1 x E5504 2.0GHz 4 cores</td>
<td>6G</td>
</tr>
</tbody>
</table>
How to deploy FirePOWER on a 5585-X Platform.

- Power down the unit and slide the module in the **top** slot
- Connect the M0/0 port to the network
- Install boot software
- Partition
- Configure IP address
- Install system software
- Launch FireSIGHT (Defense Center)
- Install license(s)
- Configure Policies
- Punt traffic up to the FP for filtering
Installation Steps

1. **Ensure requirements are met**
2. **Uninstall any existing Cisco IPS or CX module (if applicable)**
3. **Download ASA FirePOWER Boot Image and System Software packages from Cisco**
4. **Copy the ASA FirePOWER boot image to the ASA Flash**
5. **Start the recovery procedure to install the boot image**
6. **Host the FirePOWER system software package on an HTTP(S) or FTP server**
7. **Use the initial setup dialog and system install command to install the system software package**
8. **Once installed, open a console session to complete the system configuration wizard.**
9. **Add the FirePOWER sw-module into FireSIGHT Management Center.**
10. **Configure ASA to redirect traffic to the module**
Requirements

- FirePOWER services is **pre-installed** on ASA5500-X **FirePOWER bundles**
  - I.e. ASA5525-**FPWR-BUN** SKU
- Installation for FirePOWER services on a ASA5500-X platform requires an **SSD** drive
  - ASA5500-X-**SSD12= SKU**

```
ciscoasa# show inventory
Name:  "Chassis", DESCR:  "ASA 5515-X with SW, 6 GE Data, 1 GE Mgmt, AC"
PID:  ASA5515, VID:  V01, SN:  FGL1620413M

Name:  "Storage Device 1", DESCR:  "Unigen 128 GB SSD MLC, Model Number: UGB88RRA128HM3-EMY-DID"
PID:  N/A, VID:  N/A, SN:  11000046630
```
Install

ASA5585X (Blade)
- Connect to the console port
- Configure ROMMON
- Execute tftp command
- Login to boot image

ASA5500X (VM)
sw-module module sfr recover configure image disk0:/asasfr-5.3.1.img
sw-module module sfr recover boot
session sfr console

Before you can connect to the console the boot image needs to be up. Check for recovery
show module sfr details | inc Status

Then check if the console port is ready.
show module sfr details | inc Console

Install Videos (http://ast-falcon-re.cisco.com/elektra/demos/)
Detailed ASA SFR Packet Flow

FirePOWER does not drop flows, it marks them for drop by the ASA

1. Receive PKT
2. Ingress Interface
3. Existing Conn
4. ACL Permit
5. Match Xlate
6. Inspections sec checks
7. NAT IP Header
8. Egress Interface
9. L3 Route
10. L2 Addr
11. XMIT PKT

FirePOWER does not drop flows, it marks them for drop by the ASA.
Functional Distribution of Features

**FirePOWER Services**
- URL Category/Reputation
- NGIPS
- Application Visibility and Control
- Advanced Malware Protection

**ASA**
- File Type filtering
- File capture
- NAT
- Routing
- ACL
- VPN Termination
- Failover & Clustering

**Cisco**
- TCP Normalization
- TCP Intercept
- IP Option Inspection
- IP Fragmentation
- Botnet Traffic Filter

**Presentation_ID**
Cisco and/or its affiliates. All rights reserved.
Cisco Public
Packet Flow Overview

Packet flow between the solution components

1. Ingress processing – inbound ACLs, IP defragmentation, TCP normalization, TCP intercept, protocol inspection, clustering/HA traffic control, VPN decryption, etc.

2. Sourcefire Services processing – URL filtering, AVC, NGIPS, AMP, etc.

3. Egress processing – outbound ACLs, NAT, routing, VPN encryption, etc.

Packets are redirected to the FirePOWER Services module using the Cisco ASA Modular Policy Framework (MPF)

- MPF is a well known component of ASA architecture.
- MPF supports fail-open, fail-closed and monitor only options
- MPF class map, policy map and service policy determine which traffic is send to the FirePOWER Services module
Example of MPF configuration to send all traffic to the FirePOWER Services module:

```
policy-map global_policy
class class-default
  sfr fail-open

service-policy global_policy global
```

Checking traffic forwarding to the FirePOWER Services module:

```
ciscoasa(config)# show service-policy sfr

Global policy:
  Service-policy: global_policy
  Class-map: match_all
    SFR: card status Up, mode fail-open
      packet input 71505, packet output 71563, drop 56, reset-drop 0
```
ASA5500-X FirePOWER Management Interface

- Management interface for ASA and FirePOWER module on ASA5500-X platform
- The FirePOWER module uses Management Interface for
  - all updates (base OS, OS upgrade packages)
  - all feature updates (rules, reputation data)
  - all Management Center interaction (Mgmt, event-data)
- FireSIGHT policy management is performed through the management interface
Management-only ASA statement cannot be removed from the M0/0 interface

- If the ASA has a nameif assigned to the M0/0 interface, the FirePOWER module must have its management IP address in the same subnet

- You cannot route traffic through the M0/0 interface if nameif has been configured on that interface. *The ASA will drop this traffic.*

- If the ASA has no nameif assigned to the M0/0 interface, the FirePOWER module functions similarly to hardware module with a dedicated management interface

Communication from the FirePOWER module to external networks that pass through the ASA is inhibited if nameif is configured on the Management0/0 interface.
ASA5500-X FirePOWER Management Interface Considerations (Cont.)

- **Layer 3 Environment for ASA and FirePOWER Management both using M0/0**
- **ASA will be managed via the M0/0 Management Interface**
- **FirePOWER module will be managed via the M0/0 Management Interface**
- **ASA and FirePOWER Management share the same Layer 3 subnet**
- **Default gateway** of FirePOWER module pointed to an **external router/switch**
- Route on ASA needed to route traffic to FirePOWER module management via the default gateway

```
FirePOWER# show module SFR detail
Mgmt IP addr: 192.0.2.2
Mgmt Network Mask: 255.255.255.0
Mgmt Gateway: 192.0.2.254
```

```
interface Management0/0
nameif management
security-level 0
ip address 192.0.2.1 255.255.255.0
no shutdown
```
ASA5500-X FirePOWER Management Interface Considerations (Cont.)

- Best practice is to separate ASA and FirePOWER management interfaces
- ASA managed in-band (from the “inside” interface)
- FirePOWER module managed via the Management Interface
- No nameif assigned to the ASA M0/0 Interface
- ASA Inside Interface and FirePOWER Management can share the same Layer 2 domain and IP subnet
- Access from the “inside” to the FirePOWER module through switch/router, without ASA involvement

FirePOWER# show module SFR detail
Mgmt IP addr: 192.0.2.2
Mgmt Network Mask: 255.255.255.0
Mgmt Gateway: 192.0.2.254

Best Practice

interface Management0/0
no nameif
security-level 0
management-only
no shutdown

Interface
GigabitEthernet0/0
nameif inside
security-level 0
ip address 192.0.2.254
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
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 HA
- Every session has a primary and secondary owner ASA
- ASA provides traffic symmetry to FirePOWER module

Design Zone for Cisco Security
- View Design Guide for Threat Management with NextGen IPS
- View Implementation Guide for Threat Management with NextGen IPS
- View Implementation Guide for Threat Management with Passive Mode NextGen IPS
Clustering and Asymmetry

Traffic going to the Datacenter

- ASA 1 sees the traffic and becomes the owner
- Asymmetry is introduced on the return path
- ASA 2 sees the traffic and has never seen it before so asks, on the Cluster Control Link, who owns the flow
- ASA 1 signals that it owns the flow
- ASA 2 sends ASA 1 the packet from the flow in question over the CCL
- FirePOWER Services for ASA module inside ASA 1 sees the entire flow
- The module in ASA 2 sees no packets from that flow
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.
Multi-Context ASA Deployments

10.89.145.91
ASA5525

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Security Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin/ctx-admin-inside</td>
<td>ASA</td>
<td>Admin Context Inside</td>
</tr>
<tr>
<td>admin/ctx-admin-outside</td>
<td>ASA</td>
<td>Admin Context Outside</td>
</tr>
<tr>
<td>admin/public/mgmt</td>
<td>ASA</td>
<td></td>
</tr>
<tr>
<td>context-1/ctx-1-inside</td>
<td>ASA</td>
<td>Context1 inside</td>
</tr>
<tr>
<td>context-1/ctx-1-outside</td>
<td>ASA</td>
<td>Context1 Outside</td>
</tr>
<tr>
<td>eth0</td>
<td>Management</td>
<td></td>
</tr>
</tbody>
</table>
FirePOWER Services Demonstration Monitor-Only Mode

IDS Mode

- By selecting Monitor Only, you put the SFR into IDS mode.
  - Traffic will be copied from the ASA to the SFR module, but the SFR module will not be in the data path.
  - This will allow you to confirm that the policies on the SFR are working properly.

- Once you confirm this, you will disable monitor only mode, putting the SFR into IPS mode.
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.

The firewall must be in transparent mode.

The sensing interface must be in traffic forwarding mode:

```
interface gi0/0
  no nameif
  traffic-forward sfr monitor-only
  no shutdown
```
IPS and IPS+AVC test comparing throughput of FirePOWER Services for ASA to FirePOWER appliances.

Tested using the same 440 byte HTTP Transactional test used by Sourcefire.

High end 8250 and 8350 appliances are off the page.

<table>
<thead>
<tr>
<th>SFR 7120</th>
<th>5585-10</th>
<th>SFR 7125</th>
<th>5585-20</th>
<th>SFR 8130</th>
<th>SFR 8140</th>
<th>5585-40</th>
<th>5585-60</th>
<th>82xx 83xx</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS</td>
<td>100</td>
<td>1200</td>
<td>1250</td>
<td>2000</td>
<td>4000</td>
<td>6000</td>
<td>3500</td>
<td>6000</td>
</tr>
<tr>
<td>IPS + AVC</td>
<td>800</td>
<td>1200</td>
<td>2100</td>
<td>3500</td>
<td>2100</td>
<td>3500</td>
<td>++</td>
<td></td>
</tr>
</tbody>
</table>
Support Resources

- Ordering Guide, Data Sheets, Sizing Guide, Promos, Presentations:

- Sales Resources:

- Install Quick Start Guide:
SourceFire Security Analytics
FireSIGHT Management Console

AMP for Endpoints

- FirePOWER Sensor
- FirePOWER Sensor
- FirePOWER Services ASA
- FirePOWER Services ASA
Event Processing & Analytical Tools

FireSIGHT Management Console

- Real-time Event Processing and Correlation
- Event Database
- Configuration Database
- Analytical Tool Set
Data Sources

- **FirePower**
  - Open Source IPS Engine
  - Network Discovery
  - Application Identification
  - NGFW Engine
  - AMP for Networks

- **AMP for Endpoints**
  - Endpoint Malware Intelligence
  - BigData Cloud Analytics

- **FireSIGHT Management Console**
  - Correlation Technologies
FirePOWER Event Data

- **Intrusion Events**
  - Threat detection events triggered based on snort rules

- **File & Malware Events**
  - File type detection
  - Malware detection & control
  - Sandbox status

- **Connection Events**
  - Robust flow information
  - Application ID
  - User ID
  - Security Intelligence
  - Referential integrity of other events

- **Network Discovery Events**
  - Host intelligence data

- **Statistics Events**
  - Time series counters
AMP for Endpoints Events
- Endpoint Malware Detection
- Quarantine Data
- Restore Information
- Scan Data
- Indicators of Compromise

FireSIGHT Management Console Events
- Indicators of Compromise
- Correlated Statistics
- Event Augmentation
# Policy-Driven Visibility and Control

### Filter Access and Apply Protection by Application, User, and Traffic Path

## Interesting Use Cases

Enter a description

- [Save](#)  
- [Cancel](#)  
- [Save and Apply](#)

Device Targets: 0 devices

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Source Zones</th>
<th>Dest Zones</th>
<th>Source Net...</th>
<th>Dest Net...</th>
<th>VLA...</th>
<th>U...</th>
<th>Applications</th>
<th>Services</th>
<th>URLs</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Mobile Security 1</td>
<td>Intern</td>
<td>any</td>
<td>any</td>
<td>Ten</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>Block</td>
</tr>
<tr>
<td>2</td>
<td>Read Only Facebook</td>
<td>Intern</td>
<td>Exten</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>Block</td>
</tr>
<tr>
<td>3</td>
<td>Web Block List</td>
<td>Intern</td>
<td>Exten</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>Block</td>
</tr>
<tr>
<td>4</td>
<td>Block All P2P</td>
<td>Intern</td>
<td>Exten</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>Block</td>
</tr>
<tr>
<td>5</td>
<td>inbound Email</td>
<td>Extern</td>
<td>Intern</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>SMTP</td>
<td>any</td>
<td>Allow</td>
</tr>
<tr>
<td>6</td>
<td>Outbound Web Browsing</td>
<td>Extern</td>
<td>Intern</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>HTTP</td>
<td>any</td>
<td>any</td>
<td>Allow</td>
</tr>
</tbody>
</table>

### Standard Rules

**This category is empty.**

### Default Action

| Access Control: Block All Traffic | Displaying 1 - 6 of 8 rules | Page 1 of 1 |

1 Row Selected
Policy-Driven Visibility and Control
Filter Access and Apply Protection by Application, User, and Traffic Path

Interesting Use Cases

Device Targets: 0 devices

Administrator Rules
This category is empty.

Standard Rules

1 Mobile Security 1
   Source: Intern
   Destination: any
   Source Zone: any
   Destination Zone: any
   Source Net: any
   Destination Net: any
   VLAN: any
   User: any
   Applications: any

2 Read Only Facebook
   Source: Intern
   Destination: Extern
   Source Zone: any
   Destination Zone: any
   Source Net: any
   Destination Net: any
   VLAN: any
   User: any
   Applications: any

3 Web Block List
   Source: Intern
   Destination: Extern
   Source Zone: any
   Destination Zone: any
   Source Net: any
   Destination Net: any
   VLAN: any
   User: any
   Applications: any

4 Block All P2P
   Source: Intern
   Destination: Extern
   Source Zone: any
   Destination Zone: any
   Source Net: any
   Destination Net: any
   VLAN: any
   User: any
   Applications: any

5 Inbound Email
   Source: Extern
   Destination: Intern
   Source Zone: any
   Destination Zone: any
   Source Net: any
   Destination Net: any
   VLAN: any
   User: any
   Applications: any

6 Outbound Web Browsing
   Source: Extern
   Destination: Intern
   Source Zone: any
   Destination Zone: any
   Source Net: any
   Destination Net: any
   VLAN: any
   User: any
   Applications: any

Root Rules
This category is empty.

Default Action
1 Row Selected
Policy-Driven Visibility and Control
Filter Access and Apply Protection by Application, User, and Traffic Path

Top Events by Source Country

<table>
<thead>
<tr>
<th>Country Name</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>162</td>
</tr>
<tr>
<td>Germany</td>
<td>36</td>
</tr>
<tr>
<td>China</td>
<td>18</td>
</tr>
<tr>
<td>Japan</td>
<td>13</td>
</tr>
<tr>
<td>France</td>
<td>11</td>
</tr>
<tr>
<td>Russia</td>
<td>4</td>
</tr>
<tr>
<td>North Korea</td>
<td>2</td>
</tr>
<tr>
<td>Pakistan</td>
<td>1</td>
</tr>
<tr>
<td>Iraq</td>
<td>1</td>
</tr>
<tr>
<td>Iran</td>
<td>1</td>
</tr>
</tbody>
</table>

Last updated 1 minutes ago

<table>
<thead>
<tr>
<th>Initiator IP</th>
<th>Initiator Location</th>
<th>Responder IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>76.100.209.66</td>
<td>USA</td>
<td>10.4.32.112</td>
</tr>
<tr>
<td>10.4.10.131</td>
<td></td>
<td>10.4.32.112</td>
</tr>
<tr>
<td>10.4.10.131</td>
<td></td>
<td>10.4.32.112</td>
</tr>
<tr>
<td>10.4.33.95</td>
<td></td>
<td>10.5.32.206</td>
</tr>
<tr>
<td>89.188.101.82</td>
<td>ISR</td>
<td>10.5.32.206</td>
</tr>
<tr>
<td>200.189.215.85</td>
<td>BRA</td>
<td>10.5.32.44</td>
</tr>
<tr>
<td>10.4.31.237</td>
<td></td>
<td>10.5.32.206</td>
</tr>
<tr>
<td>10.4.11.216</td>
<td></td>
<td>10.5.39.206</td>
</tr>
</tbody>
</table>

Root Rules
This category is empty.

Default Action

Access Control: Block All Traffic
Displaying 1 - 6 of 8 rules

Presentation_ID
Cisco and/or its affiliates. All rights reserved.
Chaining FW with IPS and File Analysis

Cisco Security BU - Production Demo AC Policy

Cisco Provided. For best results, do not modify.

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Source Zones</th>
<th>Destination Zones</th>
<th>Source Network</th>
<th>Destination Network</th>
<th>VLA</th>
<th>Users</th>
<th>Applications</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>URLS</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Monitor Everything</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td></td>
<td>Any (Reputations 1-5)</td>
</tr>
<tr>
<td>2</td>
<td>High Risk URLs</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>Risks: Very High</td>
<td>any</td>
<td>any</td>
<td></td>
<td>Any (Reputations 1-2)</td>
</tr>
<tr>
<td>3</td>
<td>High Risk Apps</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td></td>
<td>Risks: High</td>
</tr>
<tr>
<td>4</td>
<td>Block Non-Work Related</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>Finance</td>
<td>any</td>
<td>any</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>IPS and File Detection</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>Business Relevance</td>
<td>(2 more...)</td>
<td>any</td>
<td></td>
<td>Allow</td>
</tr>
</tbody>
</table>

Root Rules

This category is empty.

Default Action

Intrusion Prevention: Cisco Security BU - Production Demo IPS Policy
### Editing Rule - High Risk Apps

<table>
<thead>
<tr>
<th>Name</th>
<th>Action</th>
<th>IPS</th>
<th>Files</th>
<th>Logging</th>
<th>---</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Risk Apps</td>
<td>Interactive Block with react</td>
<td>Cisco Security BU - Production Demo IPS Policy</td>
<td>Cisco Security BU - Production Demo IPS Policy</td>
<td>connections, files: dc</td>
<td></td>
</tr>
</tbody>
</table>

**Intrusion Policy**
- Cisco Security BU - Production Demo IPS Policy

**File Policy**
- Cisco Security BU - Production Demo File / Malware Policy
Real-time Analytics
The Problem with Legacy Next-Generation Firewalls

Focus on the Apps

But miss the threat...

Legacy NGFWs can reduce attack surface area but advanced malware often evades security controls.
Network Discovery – Context Context Context!

- **PASSIVE** Real-time Network Awareness
  - Host OS
  - Services
  - Device Type
  - Client Applications
  - User

- **FireSIGHT Management Console** Network Map
  - Context through asset state
    - Contextual IP Defrag Policy
    - Correlation
    - Vulnerability Mapping
Impact Assessment

- Relies on information from passive discovery: OS, client and server application
- Correlates all Intrusion Events to an Impact of the attack against the target
- Allows analysts to focus on the smaller subset of events that they could be vulnerable to

<table>
<thead>
<tr>
<th>IMPACT FLAG</th>
<th>ADMINISTRATOR ACTION</th>
<th>WHY</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Act Immediately, Vulnerable</td>
<td>Event corresponds to vulnerability mapped to host</td>
</tr>
<tr>
<td>2</td>
<td>Investigate, Potentially Vulnerable</td>
<td>Relevant port open or protocol in use, but no vuln mapped</td>
</tr>
<tr>
<td>3</td>
<td>Good to Know, Currently Not Vulnerable</td>
<td>Relevant port not open or protocol not in use</td>
</tr>
<tr>
<td>4</td>
<td>Good to Know, Unknown Target</td>
<td>Monitored network, but unknown host</td>
</tr>
<tr>
<td>5</td>
<td>Good to Know, Unknown Network</td>
<td>Unmonitored network</td>
</tr>
</tbody>
</table>
Cisco FireSIGHT Simplifies Operations
Impact Assessment and Recommended Rules Automate Routine Tasks
Indications of Compromise

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

- SI Events
  - CnC Connections
  - Connections to Known CnC IPs

- Malware Events
  - Malware Detections
  - Malware Executions
  - Office/PDF/Java Compromises
  - Dropper Infections

IOC: "tag" on a host that indicates that an event indicating likely host infection has occurred. IOCs are tallied against each host.
Correlation for Remediation

Summary

Universal Remediation Module

Correlation Rule: “if DoS detected”

Specific Remediation Instance

Correlation Policy
Correlation for Behavior Anomaly Detection

**Summary**

- **Traffic Profile**
- **Correlation Rule:** “if anomaly detected”
- **Generate alert**

**Correlation Policy**
Correlation
Can be complex

Rule Information
Rule Name: Critical phone Attacks
Rule Description: Attacks on Executives Android-based phones
Rule Group: Executive Attacks

Select the type of event for this rule
If an intrusion event occurs and it meets the following conditions:

- Impact Flag is 1 - red (Vulnerable)

Host Profile Qualification
Only generate an event if the host(s) involved have the following properties:

- Destination Host: Destination Host
- Operating System: has the following properties
  - OS Vendor: Google
  - OS Name: Android
  - OS Version: any
- Destination Host: is Jailbroken

User Identity Qualification
Only generate an event if the user(s) involved have the following properties:

- Identity on Destination: Department is Executives
ISE + SourceFire Remediation Demo
AMP: File based malware prevention

- ASA with FirePOWER Services
- Dedicated FirePOWER Appliance
- Web & Email Security Appliances
- Cloud Based Web Security & Hosted Email
- Private Cloud

Fire reputation and file sandboxing
Continuous & Zero-Day Detection
Advanced Analytics And Correlation
Advanced Malware Protection

Reputation Filtering

Behavioral Detection

All detection is less than 100%

One-to-One Signature
Fuzzy Finger-printing
Machine Learning
Indications of Compromise
Dynamic Analysis
Advanced Analytics
Device Flow Correlation

Reputation Filtering and File Sandboxing
AMP Provides Continuous Retrospective Security

Breadth of Control Points
- Email
- Endpoints
- Web
- Network
- IPS
- Devices

Telemetry Stream

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

Continuous Feed

Inspection verdicts
Retrospective Analysis: File Trajectory

Quickly understand the scope of malware problem

Looks **ACROSS** the organization and answers:

- What systems were infected?
- Who was infected first (“patient 0”) and when did it happen?
- What was the entry point?
- When did it happen?
- What else did it bring in?
FirePOWER Services on the ASA + AMP

FireSIGHT Management Console
(Defense Center)

Configuration (policy) - File Trajectory - AMP Events Correlation

(Cross-launch SSO)

Link to AMP Public Cloud for Endpoint Connector Events

Cisco Security Manager

ASA Cluster with Sourcefire Virtual Sensor

File Submitted for Dynamic Analysis

File Disposition queried against AMP Cloud (SHA256, Spero)

VRT Dynamic Analysis Cloud

Manual Dynamic Analysis for Endpoint Connectors

AMP Cloud

Endpoint Connectors
An unknown file is present on IP: 10.4.10.183, having been downloaded from Firefox at 10:57. The unknown file is then transferred to a third device (10.3.4.51) using an SMB application and copied to a fourth device (10.5.60.66) 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.
On-Demand Analytics
## Event Viewer

### Events By Priority and Classification

#### Drilldown of Event, Priority, and Classification

- **Table View of Events**
- **Packets**

#### Search Constraints (Edit Search)

<table>
<thead>
<tr>
<th>Event Details</th>
<th>Priority</th>
<th>Impact</th>
<th>Inline Result</th>
<th>Source IP</th>
<th>Source Country</th>
<th>Destination IP</th>
<th>Destination Country</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>ICMP Type</th>
<th>ICMP Code</th>
<th>VLAN ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014-03-24 10:50:13</td>
<td>high</td>
<td>3</td>
<td></td>
<td>10.5.61.104</td>
<td></td>
<td>10.6.12.92</td>
<td></td>
<td>55750</td>
<td>udp</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>2014-03-24 11:12:14</td>
<td>high</td>
<td>3</td>
<td></td>
<td>10.5.61.104</td>
<td></td>
<td>10.6.12.92</td>
<td></td>
<td>36286</td>
<td>udp</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>2014-03-24 11:04:56</td>
<td>high</td>
<td>3</td>
<td></td>
<td>10.5.61.104</td>
<td></td>
<td>10.6.12.92</td>
<td></td>
<td>60822</td>
<td>udp</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>2014-03-24 11:49:42</td>
<td>high</td>
<td>3</td>
<td></td>
<td>10.5.61.104</td>
<td></td>
<td>10.6.12.92</td>
<td></td>
<td>48245</td>
<td>udp</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>2014-03-24 11:49:61</td>
<td>high</td>
<td>3</td>
<td></td>
<td>10.5.61.104</td>
<td></td>
<td>10.6.12.92</td>
<td></td>
<td>38098</td>
<td>udp</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>2014-03-24 11:15:09</td>
<td>high</td>
<td>3</td>
<td></td>
<td>10.5.61.104</td>
<td></td>
<td>10.6.12.92</td>
<td></td>
<td>40751</td>
<td>udp</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>2014-03-24 11:26:59</td>
<td>high</td>
<td>3</td>
<td></td>
<td>10.5.61.104</td>
<td></td>
<td>10.6.12.92</td>
<td></td>
<td>67782</td>
<td>udp</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>2014-03-24 12:07:25</td>
<td>high</td>
<td>3</td>
<td></td>
<td>10.5.62.95</td>
<td></td>
<td>10.1.1.57</td>
<td></td>
<td>810</td>
<td>tcp</td>
<td></td>
<td>2049 (afsd)</td>
<td>tcp</td>
</tr>
<tr>
<td>2014-03-24 12:02:12</td>
<td>high</td>
<td>3</td>
<td></td>
<td>10.5.61.104</td>
<td></td>
<td>10.6.12.92</td>
<td></td>
<td>38597</td>
<td>udp</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>2014-03-24 09:29:15</td>
<td>high</td>
<td>3</td>
<td></td>
<td>10.5.61.104</td>
<td></td>
<td>10.6.12.92</td>
<td></td>
<td>55963</td>
<td>udp</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>2014-03-24 08:56:37</td>
<td>high</td>
<td>3</td>
<td></td>
<td>10.5.61.121</td>
<td></td>
<td>10.1.1.57</td>
<td></td>
<td>872 (rsync)</td>
<td>tcp</td>
<td></td>
<td>2049 (afsd)</td>
<td>tcp</td>
</tr>
<tr>
<td>2014-03-24 08:11:33</td>
<td>high</td>
<td>3</td>
<td></td>
<td>10.5.61.104</td>
<td></td>
<td>10.6.12.92</td>
<td></td>
<td>35743</td>
<td>udp</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>2014-03-24 07:58:29</td>
<td>high</td>
<td>3</td>
<td></td>
<td>10.5.61.104</td>
<td></td>
<td>10.6.12.92</td>
<td></td>
<td>60210</td>
<td>udp</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>2014-03-24 07:45:45</td>
<td>high</td>
<td>3</td>
<td></td>
<td>10.5.61.104</td>
<td></td>
<td>10.6.12.92</td>
<td></td>
<td>40920</td>
<td>udp</td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>2014-03-24 07:24:22</td>
<td>high</td>
<td>3</td>
<td></td>
<td>10.5.61.104</td>
<td></td>
<td>10.6.12.92</td>
<td></td>
<td>57993</td>
<td>udp</td>
<td></td>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>

Last login on Monday, 2014-03-24 at 17:28:22 PM from dhcp5.0-36.sfeng.sourcefire.com
Context Explorer

- Data exploration tool
- Visualizations of IoC, Network, Intrusion, File, App, User, and Geo info
- Advanced filtering across data silos
- Drill downs into detailed event analysis
- Accessible from analysis tools to provide context
Flexible Reporting

- Highly customizable and reusable report templates
- Generate reports based on dashboards and event views
- Scheduling support
- Multiple output formats
- Variable support for template reuse
Useful links:

ASA with FirePOWER Services Download link:
http://software.cisco.com/download/release.html?
mdfid=286271171&flowid=70723&softwareid=286277393&release=5.3.1.1&relind=AVAILABLE&rellifecycle =&reltype=latest

Release Notes:

Installation guide:

User guide:
## Web Security Portfolio Basics

<table>
<thead>
<tr>
<th>Feature</th>
<th>NGFW (ASA FP)</th>
<th>CWS (Cloud Web Security)</th>
<th>WSA (Web Security Appliance)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web/URL Filtering</strong></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Application Controls</strong></td>
<td>Ports (all) Protocols (all)</td>
<td>Ports (80, 443) Protocols (HTTP(S))</td>
<td>Ports (21, 80, 443) Protocols (HTTP(S), FTP)</td>
</tr>
<tr>
<td><strong>Malware Protection</strong></td>
<td>Advanced Malware Protection (reputation + content analysis)</td>
<td>Advanced (reputation + content analysis)</td>
<td>Advanced (reputation + content analysis)</td>
</tr>
<tr>
<td><strong>Remote User Security</strong></td>
<td>VPN Backhaul</td>
<td>Direct to cloud</td>
<td>VPN Backhaul</td>
</tr>
<tr>
<td><strong>Deployment</strong></td>
<td>On the firewall</td>
<td>Cloud forward via ASA, ISR, WSA, AnyConnect</td>
<td>On Premise Redirect</td>
</tr>
<tr>
<td><strong>Policy &amp; Reporting</strong></td>
<td>On Premise</td>
<td>In the Cloud</td>
<td>On Premise</td>
</tr>
<tr>
<td><strong>Licensing / Subscription</strong></td>
<td>Based on ASA model 1Y / 3Y / 5Y</td>
<td>Based on user count 1Y / 3Y / 5Y</td>
<td>Based on user count 1Y / 3Y / 5Y</td>
</tr>
</tbody>
</table>