Cisco Support Community
Expert Series Webcast
Threat Defense for a Secure Enterprise Branch

Kureli Sankar, TME, CCIE Security #35505
Kural Arangasamy, TME

March 22, 2016
Upcoming Events

https://supportforums.cisco.com/expert-corner/events
Become an Event Top Contributor

Participate in Live Interactive Technical Events and much more
http://bit.ly/1jlI93B

If you want to host an event, send an email to csc-events@external.cisco.com

https://supportforums.cisco.com/expert-corner/top-contributors
Rate Content

Encourage and acknowledge people who generously share their time and expertise

Now your ratings on documents, videos, and blogs count give points to the authors!!!

So, when you contribute and receive ratings you now get the points in your profile.

Help us to recognize the quality content in the community and make your searches easier. Rate content in the community.

https://supportforums.cisco.com/blog/154746
Cisco Support Community Expert Series Webcast

Kureli Sankar
TME, Enterprise Infrastructure and Solutions Group
CCIE Security # 35505

Kural Arangasamy
TME, Enterprise Infrastructure and Solutions Group
Ask the Expert Event following the Webcast

Now through April 1st


Join the discussion for these Ask The Expert Events:
Thank You For Joining Us Today!

If you would like a copy of the presentation slides, click the PDF file link in the chat box on the right or go to:

Submit Your Questions Now!

Use the Q & A panel to submit your questions and the panel of experts will respond.

Please take a moment to complete the survey at the end of the webcast
Agenda

♫ Security Features
  ♫ Zone Based Firewall
  ♫ Snort IPS
  ♫ CWS
  ♫ FirePOWER

♫ Demo
Polling Question 1

How important is Branch Threat Defense in your opinion?

A. Very important
B. Important
C. Somewhat important
D. Not important at all
“By 2016, 30% of advanced targeted threats—up from less than 5% today—will specifically target branch offices as an entry point.”
Changes at the Branch Lead to Security Challenges

- Increased Threat Surface Area
  Mobile, Cloud, IoT, DIA

- Increased Threat Sophistication
  Average time to discover 80 days*

- Increased Complexity for Mitigation
  Average time to resolve 123 days

*Ponemon Institute Study
**Gartner, Forecast Analysis: Worldwide Enterprise Network Services, Q2 2014 Update
The Approach to Securing Your Branch – Threat Centric Security

- Secure Connectivity
- Advanced Threat Defense
- Centralized Policy Management

Visibility & Defense Across the Entire Attack Continuum

Before
Discover
Enforce
Harden

During
Detect
Block
Defend

After
Scope
Contain
Remediate

Attack Continuum
Cisco’s Branch Security Solution

**Secure Connectivity**
- Dynamic Multipoint VPN (DMVPN)
- SSL VPN
- AnyConnect and SSL VPN
- Site to Site IPsec
- NaaS/NaaE
- IWAN

**Centralized Policy and Management**
- APIC-EM

**Branch Threat Defense**
- Cisco IOS Zone-Based Firewall
- Snort IPS
- Cloud Web Security (CWS)
- FirePOWER threat defense

**The Cisco Advantage**
- Real-time detection and remediation
- Secure connectivity
- Centralized policy and management
Direct Internet Access (DIA)

- Secure WAN transport
- Leverage local Internet path
- Threat Detection techniques
- Improve application performance
- Reduced WAN bandwidth consumption
Direct Internet Access

The retail branch

- Direct Internet Access
- Corporate Network
- Firewall

SEGMENTATION: VRF, TrustSec, ZBFW
PCI COMPLIANCE: ZBFW, SNORT IPS
GUEST WEB ACCESS: CWS
Agenda

✦ Security Features
  ✦ Zone Based Firewall
  ✦ Snort IPS
  ✦ CWS
  ✦ FirePOWER

✦ Demo
## Use Cases

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Vertical</th>
<th>Security Requirements</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCI and Regulatory Compliance</td>
<td>Retail, Healthcare, Financial, Government</td>
<td>FW, IPS, Content Filtering (optional)</td>
<td>ZBFW, Snort IDS/IPS, CWS</td>
</tr>
<tr>
<td>Guest Users Internet Access</td>
<td>Retail, Healthcare, Hospitality</td>
<td>FW, Web Security, IPS (optional)</td>
<td>ZBFW, Snort IDS/IPS, CWS</td>
</tr>
</tbody>
</table>
Use Case: Secure Branch to Meet Compliance Needs

**Value Prop**
- Best of Routing & Security at Head Quarters
- Good Enough Security at the Branch to Meet Compliance
- Snort IPS at the Branch
- Advanced Behavior Analysis at the Head-end

Examples:
- Retail stores
- Hospitals / Pharmacies
Use Case: Secure Branch Guest Internet Access

**MVP**
- FW/NGFW (ZBFW)
- URL Filtering (CWS)
- IPS (optional) (Snort)

**Internet Traffic**

- **VPN**
- **Enterprise Network**
- **Internet**
- **Branch office**
- **Headquarters**
- **Employee**
- **Guests**

**Value Prop**
- Best of Routing & Security at Head Quarters
- Good Enough Security at the Branch to Restrict Guest Access
- Advanced Behavior Analysis at the Head-end

Examples:
- Retail stores / Auto Dealerships
- Hospitals / Pharmacies
- Financials
- Schools / Universities

© 2015 Cisco and/or its affiliates. All rights reserved.
Zone Based Firewall

- Segmentation
- Stateful Firewall
- DoS Mitigation
- Resource Management
Zone Based Firewall

PC
Laptop
Server

G1/0/0
G1/1/0
G1/0/1

dmz
inside
self
outside

Internet
Step.1 Classify traffic

```
class-map type inspect match-any in-to-out-class
  match protocol ftp
  match protocol tcp
  match protocol udp
```

Step.2 Define actions in Policy map

```
policy-map type inspect in-to-out-pol
  class type inspect in-to-out-class
    inspect

  class type inspect class-default
    drop log \(\rightarrow\) logging is optional
```

Step.3 Define Security Zones

```
zezone security inside
nzezone security outside

! Interface GigabitEthernet 1/0/0
  Description ***connect-to-Internet***
  Zone-member security outside

! Interface GigabitEthernet 1/1/0
  Description ***connect-to-private***
  Zone-member security inside
```

Step.4 Define inter-Zone Rules

```
Zone-pair security inside-to-outside source inside destination outside
  service-policy type inspect in-to-out-pol
```
Appendix

• ZBF – Zone Based Firewall
• DMZ – Demilitarized Zone
• DoS – Denial Of Service
ZBF - Resources

ZE SYN cookie configuration guide:

XE - Zone Based Firewall configuration guide:

IOS - Zone Based Firewall configuration guide:

ISR TCP intercept configuration guide:
Snort IPS/IDS on ISR-4K
Snort IPS

- Help meet PCI compliance mandate at the Branch Office
- Threat protection built into ISR 4000 branch routers
- Complement ISR 4000 Integrated Security
- Lightweight Threat Defense with low TCO and automated signature updates
- monitoring available

- Over 4 million downloads
- 500,000 registered users
- Widely deployed IPS in the world

Cisco ISR 4000 Series

Now Orderable!

Splunk monitoring available

Over 4 million downloads
500,000 registered users
Widely deployed IPS in the world
- Snort IPS runs on a Linux Container using control plane resources.
- Traffic is punted to Snort Container using Virtual Port Group interface.
- Reserved CPU and memory for Snort process enables deterministic performance.
- VPGs to communicate between container and data plane
- VPG1 <==> eth2 (data plane)
- VPG0 <==> eth1 (management)
- eth3 can be mapped to dedicated mgmt port G0 of the router
Snort IPS – Management & Monitoring

1. On Premise WEB-UI*
2. Signature Update
3. Centralized Provisioning & Monitoring

* Web UI will be available in a future release
Snort IPS – Configuration Steps

1. Copy Snort OVA to flash and install
2. Configure and activate Snort VM
3. Configure IPS policies
4. Enable IPS, selected i/f or globally

Generic Container configuration

Snort IPS Specific configuration
Configuration – Virtual Service Activation

**Exec Mode:**
virtual-service install name myips package flash:ios-snort.ova

**Config Mode:**
interface VirtualPortGroup0
   ip address 10.0.1.1 255.255.255.252
interface VirtualPortGroup1
   ip address 192.0.2.1 255.255.255.252

**Config Mode:**
virtual-service myips
profile high
vnic gateway VirtualPortGroup0
guest ip address 10.0.1.2
vnic gateway VirtualPortGroup1
guest ip address 192.0.2.2
activate

Install virtual service
Configure Virtual Interfaces
Configure Virtual Service Interfaces and activate the service
IPS Policy Configuration

- utd engine standard
- threat protection
- policy security
- signature update server cisco username <uname> password <paswd>
- signature update occur-at daily 0 0
- logging server 10.0.20.20 syslog level warning

Enable IPS

- utd
  - engine standard
  - all-interfaces
  - interface GigabitEthernet0/0/0
  - utd enable
# Snort - Community vs Subscriber Rule Set

1. Memory – 8 G RAM
2. License – SEC-K9
3. Subscription
4. Container OVA installation
5. Container service activation
6. Enabling IPS/IDS
7. Enable Snort configuration
8. Reporting
9. Signature updates
10. Ability to whitelist

<table>
<thead>
<tr>
<th></th>
<th>Community Rule Set</th>
<th>Subscriber Rule Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pricing</td>
<td>free</td>
<td>paid</td>
</tr>
<tr>
<td>Number of rules</td>
<td>3000+</td>
<td>30,000+</td>
</tr>
<tr>
<td>Coverage in advance of exploits</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Signature availability</td>
<td>30 days later</td>
<td>Fastest access to Talos signature updates</td>
</tr>
<tr>
<td>Snort Engine “Latest-1” compatibility</td>
<td>90 days only</td>
<td></td>
</tr>
<tr>
<td>SLA</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Level 3 support</td>
<td>No</td>
<td>Bugzilla</td>
</tr>
</tbody>
</table>
Snort – Troubleshooting Commands

- show virtual-service list
- show utd engine standard config
- show virtual-service detail
- show platform hardware qfp active feature utd stats
- show platform hardware qfp active feature utd config
- show platform hardware qfp active feature utd stat divert
Snort – Debug Commands

debug platform packet copy packet out size 2048
debug platform packet-trace enable
debug platform packet-trace packet 64 circular fia-trace

Note: Conditional debugging needs to be enabled along with packet tracing

debug platform condition interface g0/0/0 both
debug platform condition condition start

Note: Optionally the utd debugging can be enabled along with packet tracing
debug platform condition feature utd dataplane submode divert level info
Appendix

- VPG – Virtual Port Group
- DIA – Direct Internet Access
- CSR – Cloud Services Router
- WL – White Listing
- OVA – Open Virtual Appliance
- UTD – Unified Threat Defense
- APIC-EM – Application Policy Infrastructure Controller – Enterprise Module
- IWAN – Intelligent WAN
Snort IPS/IDS - Resources

At-A-Glance


Data Sheet

Agenda

✧ Security Features
  ✧ Zone Based Firewall
  ✧ Snort IPS
  ✧ CWS
  ✧ FirePOWER

✧ Demo
### Use Cases

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Vertical</th>
<th>Security requirements</th>
<th>Security Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest Users Internet Access</td>
<td>Retail, Healthcare, Public Sector</td>
<td>FW, Web Security, IPS (optional)</td>
<td>ZBF, CWS and Snort IDS/IPS</td>
</tr>
</tbody>
</table>
Use Case: Secure Branch Public Cloud / Partner Access

**MVP**
- FW/NGFW (ZBFW)
- DBR
- IPS (Snort)
- URL Filtering (CWS)

**Value Prop**
- Domain Based Routing, routes only the cloud specific traffic directly
- ZBFW provides pinholes for return traffic from cloud services
- CWS provides additional protection from cloud services
- Additional security services if needed (CWS AMP, CTA etc.)

Examples:
- Retail Stores Accessing Supplier Websites
- Hospital / Pharmacy Accessing Insurance websites
- Cloud Based Enterprise Services (webex, salesforce etc.)

© 2015 Cisco and/or its affiliates. All rights reserved.
Use Case: Secure Branch Direct Internet Access

Integrated Cloud-based Threat Defense

**MVP**
- NGFW (ZBFW)
- IPS (Snort)
- URL Filtering (CWS)
- SGT based Routing

**Value Prop**
- Best of Routing & Security at Head Quarters
- UTM like Features at the Branch to Protect Branch Users
- Advanced Behavior Analysis at the Head-end
- Advanced dynamic routing at Branch to reroute suspicious users

Examples:
- Retail stores
- Hospitals / Pharmacies
- Schools / Universities

Corporate Traffic

Suspicious traffic redirected to head-end or 3rd party for advanced analysis

Network Behavior Analysis at the Head Quarters Via NetFlow

Enterprise Network

Internet Traffic

VPN

Branch office

Employees

Guests

Internet

Headquarters

© 2015 Cisco and/or its affiliates. All rights reserved.
Use Case: Branch to Branch Direct Access

MVP
FW (ZBFW)
IPS (Snort)
SGT based Routing

Corporate VPN + Internet Traffic

Suspicious traffic can be forcefully redirected to head-end for advanced analysis

Value Prop
- Best of Routing & Security at Head Quarters
- Good enough security at Branch to contain Branch Infection
- Advanced Behavior Analysis at the Head-end

Examples:
Retail stores / Auto Dealerships
Hospitals / Pharmacies
Schools / Universities
Advanced Architecture
Enterprise Branch Requirement

- Meet Regulatory/Compliance Requirement
- Reduce Compliance Scope
- Local Direct Internet Access for Trusted Users & Guests
- Centralized Monitoring & Policy Management
- Ensure Internet Access Adheres to Corporate Policy

Solution for an Intelligent & Secure Enterprise Branch

- Identity/Role based Access
- Segmentation & Security Policy Enforcement
- Advanced Flow Analytics
- Security Event Monitoring
- Policy based Traffic Redirect and QoS Management

Use Case: Context Aware Threat Defense for an Enterprise Branch

Network as a Sensor (NaaS) / Enforcer (NaaE), TrustSec, ZBFW, FirePOWER or Snort IPS, CWS

Non-Compliant Devices & Suspicious Users Internet Traffic Redirection to HQ

Head Quarters

| Servers | ISE | Lancope | FireSight | Splunk |

BYOD & Suspicious Users Internet Traffic

VPN

Internet

Head Quarters

Branch

ISR 4451-X

SM·X EtherSwitch

BYOD

Employee

Guest

MVP

FW/NGFW (ZBFW, FirePower)

IPS (Snort or FirePower)

URL Filtering (FirePower or CWS)

SGT based Segmentation

SGT based Routing

Non-Compliant Devices & Suspicious Users Internet Traffic Redirection to HQ

Enterprise Branch Requirement

Meeting Regulatory/Compliance Requirement

Reduce Compliance Scope

Local Direct Internet Access for Trusted Users & Guests

Centralized Monitoring & Policy Management

Ensure Internet Access Adheres to Corporate Policy

MVP

FW/NGFW (ZBFW, FirePower)

IPS (Snort or FirePower)

URL Filtering (FirePower or CWS)

SGT based Segmentation

SGT based Routing

Employee

Guest

BYOD

Use Case: Context Aware Threat Defense for an Enterprise Branch

Network as a Sensor (NaaS) / Enforcer (NaaE), TrustSec, ZBFW, FirePOWER or Snort IPS, CWS

Non-Compliant Devices & Suspicious Users Internet Traffic Redirection to HQ

Head Quarters

| Servers | ISE | Lancope | FireSight | Splunk |

BYOD & Suspicious Users Internet Traffic

VPN

Internet

Head Quarters

Branch

ISR 4451-X

SM·X EtherSwitch

BYOD

Employee

Guest

MVP

FW/NGFW (ZBFW, FirePower)

IPS (Snort or FirePower)

URL Filtering (FirePower or CWS)

SGT based Segmentation

SGT based Routing

Enterprise Branch Requirement

- Meet Regulatory/Compliance Requirement
- Reduce Compliance Scope
- Local Direct Internet Access for Trusted Users & Guests
- Centralized Monitoring & Policy Management
- Ensure Internet Access Adheres to Corporate Policy

Solution for an Intelligent & Secure Enterprise Branch

- Identity/Role based Access
- Segmentation & Security Policy Enforcement
- Advanced Flow Analytics
- Security Event Monitoring
- Policy based Traffic Redirect and QoS Management

Kural Arangasamy
Polling Question 2

What comes to your mind when we talk about BTD?  
(check all that applies)

A. Regulatory compliance (ex. PCI-DSS)
B. Guest Internet Access
C. Public Cloud Access (ex. office 365, salesforce)
D. BYOD
Agenda

✧ Security Features
  ✧ Zone Based Firewall
  ✧ Snort IPS
  ✧ CWS
  ✧ FirePOWER

✧ Demo
CWS (Cloud Web Security) on ISR-4K
CWS – Tunnel Based Redirection

SEC-K9 License on the router
CWS Provisioning & Subscription
HSEC License if needed (more than 85 MB Crypto throughput or more than 225 Tunnels)
A. Is the user allowed to visit this host at this time?
B. Does the host have a good reputation?

Logging of all request and response events
CWS: Policy creation on CWS portal

Policy
Action
Who
What
When

Activate the rule
CWS - Tunnel Based Redirection Configuration

**Step. 1 Import Certificate**
Router(config)#crypto pki trustpoint cws-trustpoint
Router(ca-trustpoint)#revocation-check none
Router(ca-trustpoint)#enrollment terminal
Router(ca-trustpoint)#exit
Router(config)#cry pki authenticate cws-trustpoint

**Step. 2 Define a redirect list**
Router(config)#access-list 80 per 10.10.20.0 0.0.0.255

**Step. 3 Define a whitelist (optional)**
Router(config)#ip access-list extended cws-whitelist
Router(config-ext-nacl)#permit ip any 10.0.0.0 0.255.255.255
Router(config-ext-nacl)#permit ip any 172.16.0.0 0.15.255.255
Router(config-ext-nacl)#permit ip any 192.168.0.0 0.0.255.255

**Step. 4 Parameter Map**
Router(config)#parameter-map type cws-tunnel global
Router(config-profile)# primary
Router(config-cws-pri)# tower ipv4 108.171.130.255
Router(config-cws-pri)# secondary
Router(config-cws-sec)# tower ipv4 108.171.133.254
Router(config-cws-sec)# license 0 947D9DC0781B425AED0BB0B30C345321
Router(config-profile)# redirect-list 80
Router(config-profile)# whitelist
Router(config-cws-tun-wl)#acl name cws-whitelist
Router(config-cws-tun-wl)#download interval 10

**Step. 5 Apply CWS OUT**
Router(config)#int g0/0/2
Router(config-if)#cws-tunnel out tunnel-number 60

**Step. 6 Apply CWS IN**
Router(config)#int g0/0/1
Router(config-if)#cws-tunnel in
### CWS - Proxy VS Tunnel Connector

<table>
<thead>
<tr>
<th>Features</th>
<th>Proxy ISR-G2 (IOS)</th>
<th>Tunnel ISR-4K (XE)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redirection</td>
<td>Proxy</td>
<td>Tunnel</td>
</tr>
<tr>
<td>Telemetry</td>
<td>Yes</td>
<td>No (March 2016)</td>
</tr>
<tr>
<td>Tower Pooling</td>
<td>Yes</td>
<td>Through Tunnel Keepalives</td>
</tr>
<tr>
<td>MetaData</td>
<td>X-Scansafe Headers</td>
<td>NSH (Network Services Headers)</td>
</tr>
<tr>
<td>Whitelisting</td>
<td>ACL &amp; HTTP Headers Based</td>
<td>ACL &amp; Domain Based</td>
</tr>
<tr>
<td>Authentication</td>
<td>Yes</td>
<td>No (March 2016)</td>
</tr>
<tr>
<td>Default User-Group</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
CWS – Resources


Appendix

- CWS – Cloud Web Security
- IWAN – Intelligent WAN
- CSR - Cloud Services Router
- RRI – Reverse Route Injection
- L4F – Layer 4 Forwarding
- AMP – Advance Malware Protection
- WL – White Listing
Polling Question 3

Are you interested in all integrated single box solution to provide FW, URL filtering, Advance Malware Protection and IPS/AVC?

A. Yes, I prefer single box

B. No, I prefer different boxes to do each job
Agenda

✧ Security Features
   ✧ Zone Based Firewall
   ✧ Snort IPS
   ✧ CWS
   ✧ FirePOWER

✧ Demo
## Use Cases

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Vertical</th>
<th>Security Requirements</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partial Direct Internet Access (Public Cloud, Partner Sites)</td>
<td>Retail, Healthcare, Manufacturing</td>
<td>FW, Web Security, IPS</td>
<td>Snort IDS/IPS, CWS (Identity Policies) or FirePOWER Threat Defense</td>
</tr>
<tr>
<td>Full Direct Internet Access</td>
<td>Retail, Healthcare, Manufacturing</td>
<td>FW, Web Security, IPS, Malware Protection, AVC</td>
<td>FirePOWER Threat Defense</td>
</tr>
</tbody>
</table>
Use Case: Secure Branch Public Cloud / Partner Access

**Value Prop**
- Domain Based Routing, routes only the cloud specific traffic directly
- ZBFW provides pinholes for return traffic from cloud services
- CWS provides additional protection from cloud services
- Additional security services if needed (CWS AMP, CTA etc.)

**Examples:**
- Retail Stores Accessing Supplier Websites
- Hospital / Pharmacy Accessing Insurance websites
- Cloud Based Enterprise Services (webex, salesforce etc.)
Use Case: Secure Branch Direct Internet Access
Integrated On-Premise Advanced Threat Defense

**MVP**
- NGFW (ZBFW, FirePOWER)
- NGIPS (FirePOWER)
- URL Filtering (FirePOWER)
- AMP (FirePOWER)

Suspicious traffic redirected to head-end or 3rd party for advanced analysis

**Value Prop**
- Best of Routing & Security at Head Quarters and Branch
- Advanced Behavior Analysis at the Head-end

Examples:
- Financials
Cisco FirePOWER Threat Defense for ISR
Cisco FirePOWER Threat Defense for ISR

**FirePOWER Threat Defense**

**BEFORE**
- Discover
- Enforce
- Harden

**DURING**
- NGIPS
- Security Intelligence
- URL Filtering
- Advanced Malware Protection
- Retrospective Security
- IoC/Incident Response

**AFTER**
- Scope
- Contain
- Remediate

**Visibility and Automation**

**Cisco® 4000 Series ISR**

**Cisco UCS®**

**OR**

**Cisco ISR G2 Series**

**AppX + Security License**

Free Up Valuable Square Footage Generate More Revenue $$$
## Snort vs FirePOWER Threat Defense for ISR

<table>
<thead>
<tr>
<th></th>
<th>Threats</th>
<th>Application visibility and control</th>
<th>Contextual awareness</th>
<th>Impact assessment</th>
<th>Automated IPS tuning</th>
<th>User identities</th>
<th>FireSIGHT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snort IPS</td>
<td>✔️</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>FirePOWER IPS and Apps</td>
<td>✔️ ✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>

© 2015 Cisco and/or its affiliates. All rights reserved.
## Snort vs. FirePOWER Threat Defense for ISR

<table>
<thead>
<tr>
<th>Feature</th>
<th>Snort</th>
<th>FirePOWER</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDS</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IPS</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Signature set</td>
<td>Snort</td>
<td>FirePOWER</td>
</tr>
<tr>
<td>Application Control and URL Filtering</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Next Gen FW</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>SSL Traffic inspection</td>
<td>No</td>
<td>Yes, with the help of SSL decryption appliance</td>
</tr>
<tr>
<td>Advanced Malware Protection</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Centralized Management</td>
<td>APIC EM IWAN App (March 2016)</td>
<td>FireSIGHT appliance</td>
</tr>
<tr>
<td></td>
<td>Cisco Prime Infrastructure (Nov 2015)</td>
<td></td>
</tr>
<tr>
<td>Centralized Monitoring</td>
<td>No (third-party tools)</td>
<td>FireSIGHT appliance</td>
</tr>
<tr>
<td>Application/Endpoint visibility and profiling</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Performance</td>
<td>Less than 1 Gbps</td>
<td>Upto 40 Gbps</td>
</tr>
<tr>
<td>Compute required</td>
<td>1 core CPU</td>
<td>4 vCPUs</td>
</tr>
</tbody>
</table>
FirePOWER - Deployment Architecture

Branch Office

Centralized monitoring

FireSIGHT Management Center

<table>
<thead>
<tr>
<th>FireSIGHT Management Center Model</th>
<th>Max. Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>FS-VMW-SW</td>
<td>25</td>
</tr>
<tr>
<td>FS 750</td>
<td>10</td>
</tr>
<tr>
<td>FS 1500</td>
<td>35</td>
</tr>
<tr>
<td>FS 2000</td>
<td>70</td>
</tr>
<tr>
<td>FS 3500</td>
<td>150</td>
</tr>
<tr>
<td>FS 4000</td>
<td>300</td>
</tr>
</tbody>
</table>
• Host the Sensor on the UCS-E
• Replicate and push all the traffic to be inspected to the Sensor
  • SF sensor examines traffic

**Only for POC purpose**

Do not install SF sensor and Management VM on the same UCS-E unless it is strictly for testing.
On the ISR-G2, the replicated traffic can be sent to SourceFire Virtual Sensor as untagged traffic thru UCSEx/0 interface or as DOT1Q VLAN on UCSEx/1 interface.
On the ISR-4K, the replicated traffic can be sent to SourceFire Virtual Sensor using either UCSEEx/0/0 interface or UCSEEx/0/1 interface, both interfaces can be configured as trunk ports.
Cisco FirePOWER Threat Defense for ISR—Configuration Steps

Configure UCS-E (backplane) interface on the router - ISR-G2

```
  utd
  ids redirect interface Vlan10
  ids 000c.2923.abdc (mac address of the sensor interface)
  mode ids-global
  !
  interface ucse1/1
  description Internal switch interface connected to Service Module
  switchport mode trunk
  no ip address
  !
  Interface vlan10
  ip address 10.10.10.1 255.255.255.0
```
Cisco FirePOWER Threat Defense for ISR—Configuration Steps

Configure UCS-E (backplane) interface on the router – ISR 4K 3.16.1

```bash
interface ucse2/0/0
  no ip address
  no negotiation auto
  switchport mode trunk
  service instance 1
    ethernet encapsulation untagged bridge-domain 1

! interface BDI1
  ip unnumbered GigabitEthernet0/0/1

! utd (data plane)
  all-interfaces
  redirect interface BDI1
  engine advanced
```
Cisco FirePOWER Threat Defense for ISR- IPS

- Host the Sensor on the UCS-E
- IPS is in inline mode
- Packets ingress via the UCS-E front panel port
- SF sensor examines traffic; allowed packets egress the WAN interface
Switch Config

spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 10 hello-time 1
spanning-tree vlan 10 forward-time 4

interface GigabitEthernet3/17
description connected to UCS-E front panel Ge 2
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10
switchport mode trunk

interface GigabitEthernet3/4
description connected to Router’s LAN int g0/0/1
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10
switchport mode trunk

Router Config

spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 10 hello-time 1
spanning-tree vlan 10 forward-time 4
bridge-domain 1
interface GigabitEthernet0/0/1
description LAN interface
no ip address
negotiation auto
spanning-tree cost 100
service instance 10 ethernet
encapsulation dot1q 10
rewrite ingress tag pop 1 symmetric
bridge-domain 10
interface ucse1/0/1
switchport mode trunk
spanning-tree cost 10
service instance 10 ethernet
encapsulation dot1q 10
rewrite ingress tag pop 1 symmetric
bridge-domain 10
interface BDI10
ip address 106.0.0.1 255.255.255.0
Cisco FirePOWER Threat Defense for ISR-IPS

- Host the Sensor on the UCS-E
- IPS is in inline mode
- Packets ingress via the LAN interface of the router
- SF sensor examines traffic; allowed packets egress the WAN interface of the router

Work In Progress
ETA – June 2016
Cisco FirePOWER Threat Defense for ISR - IPS

L2 Switch

 ISR-4451 with UCS-E 140S

G0/0/3
10.150.217.132
vrf inside

Internet

G0/0/2
10.150.217.132
U1/0/0 – trunk port
10.20.252.1

FirePOWER Mgmt

FireSIGHT Mgmt

VNIC0

MGMT

FirePOWER

FireSIGHT

ESXi

CIMC

172.16.1.8

Laptop

172.16.1.2

U1/0/1.10 – vlan 10
10.10.1.10
vrf inside

Kureli’s Mac

at home
VNICO \(\leftrightarrow\) U1/0/0

VNICO1 \(\leftrightarrow\) U1/0/1
ip route vrf inside 0.0.0.0 0.0.0.0 10.10.1.20
interface GigabitEthernet0/0/3
description LAN side
ip vrf forwarding inside
ip address 172.16.1.3 255.255.255.0

interface ucse1/0/1.10
description LAN side FirePOWER
encapsulation dot1Q 10
ip vrf forwarding inside
ip address 10.10.1.10 255.255.255.0
ip route vrf inside 0.0.0.0 0.0.0.0 10.10.1.20

interface GigabitEthernet0/0/2
description WAN side
ip address 10.150.217.132 255.255.255.0
ip nat inside
ip nat inside source list nat-acl interface GigabitEthernet0/0/2 overload
ip route 0.0.0.0 0.0.0.0 10.150.217.1

interface ucse1/0/0.20
description WAN side FirePOWER
encapsulation dot1Q 20
ip address 10.10.1.10 255.255.255.0
ip nat inside

Service Chaining vWAAS+FP

1. Ingress WAN traffic from the ISR WAN port is redirected to vWAAS on sub-intfc ucse1/0/0.30 running on the UCS-E vnic0 vlan30.
2. vWAAS will redirect traffic back to the ISR router.
3. Use standard routing to route traffic from vWAAS to sub-intfc ucse1/0/0.20 to the UCS-E blade.
4. Traffic will be routed to the outside interface of the FP VM set to vlan20 on vnic0 vswitch.
5. Traffic is analyzed by the inline IPS service, allowed packets are sent out via the inside interface of the FP VM.
6. UCSE1/0/1.10 sub-intfc is placed in “ip vrf inside” to segregate at layer 3 from outside network and traffic is routed to LAN via GEO0/0/3 which is also on ip vrf inside.
Appendix

- AMP – Advance Malware Protection
- WL – White Listing
- CIMC – Cisco Integrated Management Console
- PI – Prime Infrastructure
- WAAS – Wide Area Application Services
- UCS-E – Unified Computing System
- BDI – Bridge Domain Interface
- IDS – Intrusion Detection System
- IPS – Intrusion Prevention System
FirePOWER - Resources

• Router Security – FirePOWER Threat Defense for ISR

• Configuration Guide - FirePOWER Threat Defense for ISR

• Router Security – FirePOWER Threat Defense for ISR
  BDM, TDM, Step-by-Step Guides (includes performance numbers)
  Troubleshooting Guide, Ordering Guide, FAQ
  http://wwwwin.cisco.com/tech/srtg/rbs/security.shtml#tab-vpn=0&ext-comp-1078=1&tab-CWS=0&tab-td=3&tab-fp=0&ext-comp-1077=1
Polling Question 4

What products are you interested in? (Check all that applies)

A. IPS/IDS
B. AVC - Application Visibility and Control
C. URL Filtering solution
D. Advanced Malware Protection
Agenda

❖ Security Features
  ❖ Snort IPS
  ❖ CWS
  ❖ FirePOWER
  ❖ Zone Based Firewall

❖ Demo
Submit Your Questions Now!

Use the Q & A panel to submit your questions and our expert will respond
Ask the Expert Event following the Webcast

Now through April 1st


Join the discussion for these Ask The Expert Events:
Collaborate within our Social Media

Learn About Upcoming Events

LinkedIn http://bit.ly/csc-linked-in
Cisco has support communities in other languages!

If you speak Spanish, Portuguese, Japanese, Russian or Chinese we invite you to participate and collaborate in your language

Spanish
https://supportforums.cisco.com/community/spanish

Portuguese
https://supportforums.cisco.com/community/portuguese

Japanese
https://supportforums.cisco.com/community/csc-japan

Russian
https://supportforums.cisco.com/community/russian

Chinese
http://www.csc-china.com.cn
More IT Training Videos and Technical Seminars on the Cisco Learning Network

View Upcoming Sessions Schedule
https://cisco.com/go/techseminars
Thank you for participating!

- Redeem your 35% discount offer by entering code: CSC when checking out:

Visit Cisco Press at:

Please take a moment to complete the survey

Thank you for Your Time!
TOMORROW starts here.