Cisco live!

What You Make Possible
Deploying Next Generation Firewalling with ASA-CX

Christian Heinel, Systems Engineer
Deploying Next Generation Firewalling with ASA-CX

Abstract

This session will explain the technology and capabilities behind Cisco’s new context aware firewall: Cisco ASA-CX.
We will introduce a new approach to firewall policy creation based on contextual attributes such as user identity, device type and application usage. In the session we will demonstrate how to create and enforce policies that allows control over application behavior for both local and remote users. We will show the ASA-CX management platform named PRSM. Deployment and design considerations including use cases will be covered. Technologies discussed during this session will be firewall installation, firewall management, SSL decryption, identity based firewalling, web security and application visibility and control.

The target audience are security administrators dealing with next generation firewalling.

The attendees will benefit from the sessions:

BRKSEC-3771 "Advanced Web Security deployment with WSA",
BRKSEC-3020 "Cisco Advanced Firewalls Inside-Out“
TECSEC-2999 "CISCO ASA Product Line: A 360-Degree Perspective"
Cisco Live 2013 - Relevant Related Sessions

- BRKSEC-3771 "Advanced Web Security deployment with WSA and ASA CX"
- BRKSEC-3020 "Cisco Advanced Firewalls Inside-Out"
- TECSEC-2999 "CISCO ASA Product Line: A 360-Degree Perspective"
Presentation Hand-outs

• Some slides are meant for references only, such as performance tables, technical specifications, and screenshots.

• These will not be covered in depth, but is included in the hand-outs.

• These will be marked with:
Agenda

Session time: 120 minutes

- Introduction
- Management architecture
- Supported platforms and performance
- Software architecture and packet flow
- Redirecting traffic to ASA CX
- Discovery, objects and object Groups
- Deploying ASA CX policies
  - Access Policies
  - Authentication & Identity Policies
  - Decryption Policies
  - Advanced Inspection Policies
- Place in the network & routed or transparent mode
- High Availability
Introduction to Next Generation Firewalling
Next Generation Firewalling

Definition?

“A class of firewalls designed to filter network and Internet traffic based upon the applications or traffic types using specific ports. The application-specific granular security policies provided by Next Generation Firewalls help them detect application-specific attacks, giving them the potential to catch more malicious activity than more traditional firewalls.”

Source:
http://www.webopedia.com/TERM/N/next_generation_firewall_ngfw.html
Next Generation Firewalling

Definition?

“Next Generation Firewalls (NGFWs) blend the features of a standard firewall with quality of service (QoS) functionalities in order to provide smarter and deeper inspection. In many ways a Next Generation Firewall combines the capabilities of first-generation network firewalls and network intrusion prevention systems (IPS), while also offering additional features such as SSL and SSH inspection, reputation-based malware filtering and Active Directory integration support.”

Source:
http://www.webopedia.com/TERM/N/next_generation_firewall_ngfw.html
The world Is Changing – The Era of an Internet Make Over

The Paradox for us as Security Professionals

VS.

Mobility          Threats / APT
Cloud            Virtualization
Devices          Collaboration
Apps             BYOD
HTTPS/SSL        IPv6

SECURITY
Why Do I Need / Want Next Generation Firewalling?

- Pure visibility of network and application usage?
- Identity Firewalling?
- What do I want to block?
- What CAN I block?
- Malware protection?
- Acceptable Use?
- Threat Defense?
The Goal of ASA CX – Next Generation Firewall

Monitor & Control users, apps, devices, location WITH Stateful firewalking
Cisco ASA CX

Quiz:

Why is it called CX?
Cisco ASA CX
Main Features

- User ID / Active & Passive Authentication
- Application visibility & Control – Broad and Web
- SSL/TLS Decryption
- HTTP inspection
- Web Reputation
- URL filtering
- Reporting
- Eventing
- Layer 3/7 access rules
Cisco ASA CX

1st Generation vs. Next Generation – Can we rely only on NGFW?

URL Category/Reputation
HTTP Inspection
AVC
TLS Proxy
TCP Proxy

Multiple Policy Decision Points

ASA CX
ASA

TCP Normalization
TCP Intercept
IP Option Inspection
IP Fragmentation

NAT
Routing
ACL
VPN Termination
Compatibility with existing ASA Features

The following features are **NOT** supported in Version 1.x release:

- ASA running in Multi-context (therefore no active-active failover)
- ScanSafe connector integration
- Clustering
- Co-existence with IPS
- Co-existence with Iron Port WSA “Mobile User Security” solution (mus)

The following features **ARE** supported

- IPv6
- Transparent mode

Management Architecture
ASA CX Management Overview

Prime Security Manager – PRSM - /ˈprɪzəm/

• PRSM is the only management platform for ASA CX
• Based entirely on HTML-5 interactive GUI
• Web UI is for policy and device configuration, eventing and reporting.
• CLI is for troubleshooting / recovery
• Same tool for single device as multi-device management
• Feature support available day-1 of CX features
ASA CX Management Architecture

ASA CX

HTTPS

PRSM

HTTPS

Admin
ASA CX Management Architecture
ASA CX Management Architecture

- Reporting
- Event Viewer
- Policy Tables
- CX Device Administration
- PRSM Administration
ASA CX Management Architecture

ASA CX

RESTful XML

Binary Logging

PRSM

Note: ASA can forward Syslog to PRSM
ASA CX Management Architecture

Updates for:

- Application signatures
- WBRS – Web Reputation Scores
- URL filter
- Trusted CA roots

- Note: APP sig, WBRS & URL filter requires subscription license
PRSM – Deployment Options
Local or Centralized Deployment? “Same, Same, But Different”

• Local on ASA CX; PRSM provides:
  • Configuration
  • Eventing
  • Reporting

• Centralized on dedicated server; PRSM provides the above plus:
  • Multi-Device support
  • Role based access control
  • Device discovery/object import
  • Push vs. Pull w/deployment
  • Storage/historical events
  • Distributed deployment (management separated from enforcement)
  • Configuration synchronization across HA environs / larger scale management
PRSM – Multi-Device Deployment Options

• Virtual Machine
  • Delivered as single file with .ova extension
  • Open Virtual Appliance (OVA) format
  • VMware vSphere Hypervisor 4.1 (Update 2)
  • Downloadable from www.cisco.com

• UCS Bundle
  • UCS C220 M3 Server + ESXi 4.1 U2 + VM
  • Virtual Machine
## Tested And Supported Hardware

<table>
<thead>
<tr>
<th>Supported Devices</th>
<th>25 Pairs (50 devices)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>4 vCPU (2 GHz)</td>
</tr>
<tr>
<td>RAM</td>
<td>8 Gb</td>
</tr>
<tr>
<td>Software</td>
<td>ESXi 4.1 Update 2</td>
</tr>
<tr>
<td>Objects</td>
<td>2000</td>
</tr>
<tr>
<td>Policies</td>
<td>2000</td>
</tr>
<tr>
<td>Syslog &amp; CX EPS</td>
<td>15000 (10.500 &amp; 4500)</td>
</tr>
</tbody>
</table>
Supported Platforms and Performance
Supported Hardware Platforms

ASA 5500-X supported
ASA 5585-X SSP10 & 20 supported

Performance and Scalability

ASA 5512-X (1 Gbps, 10K cps)
ASA 5515-X (1.2 Gbps, 15K cps)
ASA 5525-X (2 Gbps, 20K cps)
ASA 5545-X (3 Gbps, 30K cps)
ASA 5555-X (4 Gbps, 50K cps)
ASA 5585-X SSP-60 (10 Gbps, 125K cps)
ASA 5585-X SSP-40 (20 Gbps, 200K cps)
ASA 5585-X SSP-20 (40 Gbps, 350K cps)

Branch Office Internet Edge Campus Data Center

ROADMAP
## ASA 5585-X Hardware Comparison

<table>
<thead>
<tr>
<th>Specification</th>
<th>SSP-10</th>
<th>SSP-20</th>
<th>SSP-40 (NOT SUPPORTED w/CX)</th>
<th>SSP-60 (NOT SUPPORTED w/CX)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Platform Base</strong></td>
<td>2RU chassis</td>
<td>2RU chassis</td>
<td>2RU chassis</td>
<td>2RU chassis</td>
</tr>
<tr>
<td><strong>ASA SSP CPU</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CX SSP CPU</td>
<td>1xL5508 2.0 GHz 2C4T</td>
<td>1xL5518 2.13 GHz 4C/8T</td>
<td>2xL5518 2.13 GHz 8C/16T</td>
<td>2xE5645 2.46 GHz 12C/24T</td>
</tr>
<tr>
<td>ASA SSP DRAM</td>
<td>6GB DDR3-800</td>
<td>12GB DDR3-1066</td>
<td>12GB DDR3-1066</td>
<td>24GB DDR3-1066</td>
</tr>
<tr>
<td>CX SSP DRAM</td>
<td>6GB DDR3-800</td>
<td>12GB DDR3-1066</td>
<td>24GB DDR3-1066</td>
<td>48GB DDR3-1066</td>
</tr>
<tr>
<td>SSP Customer Ports</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal Nic</td>
<td>1xNiantic B0</td>
<td>1xNiantic B0</td>
<td>2xNiantic B0</td>
<td>2xNiantic B0</td>
</tr>
<tr>
<td>ASA SSP Flash</td>
<td>2GB eUSB</td>
<td>4GB eUSB</td>
<td>4GB eUSB</td>
<td>4GB eUSB</td>
</tr>
<tr>
<td>CX SSP Flash</td>
<td>8GB eUSB</td>
<td>8GB eUSB</td>
<td>8GB eUSB</td>
<td>8GB eUSB</td>
</tr>
<tr>
<td>CX SSP HD</td>
<td>2x600GB</td>
<td>2x600GB</td>
<td>2x600GB</td>
<td>2x600GB</td>
</tr>
<tr>
<td>Power</td>
<td>2xAC, DC Future</td>
<td>2xAC, DC Future</td>
<td>2xAC, DC Future</td>
<td>2xAC, DC Future</td>
</tr>
<tr>
<td>ASA CX CARD [Reg EXP]</td>
<td>Preakness-2G</td>
<td>Preakness-2G</td>
<td>Preakness-10G</td>
<td>2xPreakness-10G</td>
</tr>
<tr>
<td>Crypto Capacity</td>
<td>1xCavium 1620 – 1.5 Gbps AES 256</td>
<td>2xCavium 1620 – 3.0 Gbps AES 256</td>
<td>3xCavium 1620 – 4.5 Gbps AES 256</td>
<td>4xCavium 1620 - 6 Gbps AES 256</td>
</tr>
</tbody>
</table>
# ASA 5500-X Hardware Comparison

<table>
<thead>
<tr>
<th></th>
<th>ASA 5512-X</th>
<th>ASA 5515-X</th>
<th>ASA 5525-X</th>
<th>ASA 5545-X</th>
<th>ASA 5555-X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form Factor</td>
<td>1RU Short Chassis (19” Rack-Mountable)</td>
<td>1RU Short Chassis (19” Rack-Mountable)</td>
<td>1RU Short Chassis (19” Rack-Mountable)</td>
<td>1RU Long Chassis (19” Rack-Mountable)</td>
<td>1RU Long Chassis (19” Rack-Mountable)</td>
</tr>
<tr>
<td>64Bit Multi Core Processors</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Maximum Memory</td>
<td>4 GB</td>
<td>8 GB</td>
<td>8 GB</td>
<td>12 GB</td>
<td>16 GB</td>
</tr>
<tr>
<td>Maximum Storage</td>
<td>4 GB eUSB</td>
<td>8 GB eUSB</td>
<td>8 GB eUSB</td>
<td>8 GB eUSB</td>
<td>8 GB eUSB</td>
</tr>
<tr>
<td>Base I/O Ports</td>
<td>6 x 1GbE Cu 1 x 1GbE Cu Mgmt</td>
<td>6 x 1GbE Cu 1 x 1GbE Cu Mgmt</td>
<td>8 x 1GbE Cu 1 x 1GbE Cu Mgmt</td>
<td>8 x 1GbE Cu 1 x 1GbE Cu Mgmt</td>
<td>8 x 1GbE Cu 1 x 1GbE Cu</td>
</tr>
<tr>
<td>Expansion I/O Module</td>
<td>6 x 1GbE Cu or 6 x 1GbE SFP</td>
<td>6 x 1GbE Cu or 6 x 1GbE SFP</td>
<td>6 x 1GbE Cu or 6 x 1GbE SFP</td>
<td>6 x 1GbE Cu or 6 x 1GbE SFP</td>
<td>6 x 1GbE Cu or 6 x 1GbE SFP</td>
</tr>
<tr>
<td>VPN Crypto Hardware Accelerator</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IPS Hardware Accelerator</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
# ASA 5500-X Performance Comparison

<table>
<thead>
<tr>
<th>Performance</th>
<th>ASA 5512-X</th>
<th>ASA 5515-X</th>
<th>ASA 5525-X</th>
<th>ASA 5545-X</th>
<th>ASA 5555-X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Firewall</td>
<td>1 Gbps</td>
<td>1.2 Gbps</td>
<td>2 Gbps</td>
<td>3 Gbps</td>
<td>4 Gbps</td>
</tr>
<tr>
<td>EMIX Firewall</td>
<td>500 Mbps</td>
<td>600 Mbps</td>
<td>1 Gbps</td>
<td>1.5 Gbps</td>
<td>2 Gbps</td>
</tr>
<tr>
<td>Concurrent Threat Mitigation</td>
<td>250 Mbps</td>
<td>400 Mbps</td>
<td>600 Mbps</td>
<td>900 Mbps</td>
<td>1.3 Gbps</td>
</tr>
<tr>
<td>(Firewall + IPS)</td>
<td>200 Mbps</td>
<td>250 Mbps</td>
<td>300 Mbps</td>
<td>400 Mbps</td>
<td>700 Mbps</td>
</tr>
<tr>
<td>Max IPSec VPN Throughput</td>
<td>200 Mbps</td>
<td>250 Mbps</td>
<td>300 Mbps</td>
<td>400 Mbps</td>
<td>700 Mbps</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Platform Capabilities</th>
<th>ASA 5512-X</th>
<th>ASA 5515-X</th>
<th>ASA 5525-X</th>
<th>ASA 5545-X</th>
<th>ASA 5555-X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Firewall Conns</td>
<td>100,000</td>
<td>250,000</td>
<td>500,000</td>
<td>750,000</td>
<td>1,000,000</td>
</tr>
<tr>
<td>Max Conns/Sec</td>
<td>10,000</td>
<td>15,000</td>
<td>20,000</td>
<td>30,000</td>
<td>50,000</td>
</tr>
<tr>
<td>Max PPS (64 Byte UDP)</td>
<td>450,000</td>
<td>500,000</td>
<td>700,000</td>
<td>900,000</td>
<td>1,100,000</td>
</tr>
<tr>
<td>Max VLANS Supported</td>
<td>50</td>
<td>100</td>
<td>200</td>
<td>300</td>
<td>500</td>
</tr>
<tr>
<td>HA Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Max IPSec/SSL VPN peers</td>
<td>250</td>
<td>250</td>
<td>750</td>
<td>2500</td>
<td>5000</td>
</tr>
</tbody>
</table>
ASA 5500-X Performance With CX - Comparison

Traffic profile is EMIX

<table>
<thead>
<tr>
<th>Feature</th>
<th>ASA 5512-X</th>
<th>ASA 5515-X</th>
<th>ASA 5525-X</th>
<th>ASA 5545-X</th>
<th>ASA 5555-X</th>
</tr>
</thead>
<tbody>
<tr>
<td>AVC + WSE</td>
<td>200 Mbps</td>
<td>350 Mbps</td>
<td>650 Mbps</td>
<td>1 Gbps</td>
<td>1.4 Gbps</td>
</tr>
</tbody>
</table>
EMIX Traffic Profile

- FTP: 34.744%
- SMTP: 27.506%
- HTTP: 5.149%
- IMAPv4-Advanced: 2.361%
- BitTorrent Peer: 2.722%
- DNS: 27.518%
## ASA 5585-X Performance With CX - Comparison

<table>
<thead>
<tr>
<th></th>
<th>ASA CX SSP 10</th>
<th>ASA CX SSP 20</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throughput Multi-Protocol</td>
<td>2 Gbps</td>
<td>5 Gbps</td>
</tr>
<tr>
<td>Concurrent Connections</td>
<td>500,000</td>
<td>1,000,000</td>
</tr>
<tr>
<td>New Connections per second</td>
<td>40,000</td>
<td>75,000</td>
</tr>
</tbody>
</table>

Source: Placeholder for Notes is 12pts
ASA 5585-X H/W architecture

CX is ONLY supported in Slot 1
= Upper slot
ASA 5585-X H/W architecture

- Two Hard Drives Raid 1 (Event Data)
- 10GE and GE ports
- Two GE Management Ports
- CX SSP
- ASA SSP
ASA 5500-X H/W Architecture

• 120 GB SSD (5585-X uses spinning 600 GB)
• “show inventory” on ASA will show SSD details
• ASA provides syslogs & SNMP Traps for SSD insertion & removal
• ASA will shutdown CX service when all storage devices have been removed

• RAID:
  • Supported only on 5545-X & 5555 -X (and 5585-X)
  • RAID CLI is on ASA vs. 5585-X where RAID CLI is on CX

• Shares management port with ASA (Cannot be used for regular data!)
• Feature parity across all ASA platforms
CX Pre-installation Flow For ASA 5500-X

For new ASA appliances:
- Manufacturing installs CX completely before shipping
- CX is booted automatically when ASA is started
- Login to CX console from ASA CLI and setup management IP
- Configure CXSC redirection on ASA for traffic redirection

For existing ASA appliances with spare SSD:
- Install one or two SSDs on ASA depending on the model
- Copy 9.1.1 ASA image which supports CX onto flash filesystem
- CX uses 3GB space on ASA flash filesystem, so ensure we have more than 3GB free space on ASA flash
- Reload ASA with 9.1.1 version
- Use CX boot image to bootstrap CX and then install CX system package
- Boot image is launched from ASA CLI
- There is a single boot image for all 5500-X platforms but this image is different from the 5585-X boot image !!!
- ASA5500x will use asacx-5500x-boot-9.1.1.img
CX Installation Flow For ASA 5500-X

- Copy CX Boot image to ASA flash
  
  ```
  copy tftp://<server>/asacx-5500x-boot-9.1.1.img flash:
  ```

- Configure the Boot Image to be used on ASA
  
  `sw-module module cxsc recover configure image disk0:/asacx-5500x-boot-9.1.1.img`

- Boot the image from ASA
  
  `sw-module module cxsc recover boot`  
  This can take up to several minutes

- Session command from ASA is used to console into CX
  
  `session cxsc console`

- Setup disk partitions from CX console
  
  `partition`

- Setup management IP from CX console
  
  `setup`

- Install complete CX system package from CX console and reboot
  
  `system install http://<server>/<path>/asacx-sys-9.1.1.pkg`
Software Architecture And Packet Flows
Software Architecture

- Packet data
- RPC Data

Management Plane

HTTP Engine
AVC, URL, WBRS

Authentication
Identity

Eventing
Reporting

Inspection engines

TLS Proxy

Data Plane – L2-L4, Identity, Broad AVC

Control Plane

AD
CDA
Open Ldap
Cisco Context Directory Agent

Open Ldap

Cisco Public

© 2013 Cisco and/or its affiliates. All rights reserved.
Packet Processing Flow Diagram

Red = ASA ingress
Yellow = Traffic matched for CX inspection
Green = Traffic allowed – ASA egress

All traffic ALWAYS enters and exits the ASA (SSP)
All traffic enters ASA, and if policy verdict is "allow" it exists ASA, not CX. All traffic hits the Broad AVC engine if subject to CX inspection.
If Broad AVC classifies traffic as HTTP/HTTPS – Web AVC inspection engine is applied.
Redirecting Traffic to ASA CX SSP
ASA CX – Redirecting traffic to ASA CX SSP

Selecting Traffic

- Redirection is done using Service Policies as a part of ASA MPF
- Traffic for inspection can be matched on interface, source/destination, protocol ports and even user identity (Identity Firewall / IDFW)
- Traffic from different segments/locations can be matched step-by-step, which is useful in new deployments or during migrations.
ASA CX – Redirecting traffic to ASA CX SSP
Selecting Traffic

• Performance considerations and non-user flows could/should impact the service policy for efficiency and optimal use

• Service Policies can be configured in two ways:
  • Using ASDM/CLI on ASA – “auth proxy” keyword must be explicit defined
  • In multi-device mode through PRSM – “auth proxy” keyword is ALWAYS used
  • TIP: In secure environments where active AUTH is not used, remember to disable manually if redirection is performed using PRSM
  • Note: More details on Authentication later
ASA CX – Redirecting Traffic to ASA CX SSP

Selecting Traffic

Using CLI

```
policy-map global_policy
  class class-default
    cxsc fail-open auth-proxy
  service-policy global_policy global
```

Using PRSM - Multi Device mode only
Discovery, Objects and Object Groups
ASA CX – Multi Device Management
Device Discovery

Device discovery is the process of adding ASA and ASA CX devices to PRSM

- Only available in multi device mode

- Policies, settings and objects are "imported" into the PRSM database from both ASA and CX
  - Only supported settings will be imported from ASA

- Object & Policy Names must be unique unless System Defined or Identical
  Renaming will usually occur during device discovery

- After discovery the device is put into it’s own device group
  - This ensures that any existing service is maintained and uninterrupted

- After discovery CX devices cannot be accessed locally via GUI!
ASA CX – Multi Device Management

Device Discovery

### Devices

<table>
<thead>
<tr>
<th>Device name / Description</th>
<th>IP Address</th>
<th>Software version</th>
<th>Model</th>
<th>Serial number</th>
<th>Device group</th>
</tr>
</thead>
<tbody>
<tr>
<td>FALCON-ASA (Routed)</td>
<td>172.16.2.250</td>
<td>9.1(1)</td>
<td>ASA5585-SSP-10</td>
<td>JAF1530CRHG</td>
<td>363</td>
</tr>
</tbody>
</table>

**Associated device name / Description**

<table>
<thead>
<tr>
<th>Device name / Description</th>
<th>IP Address</th>
<th>Software version</th>
<th>Model</th>
<th>Serial number</th>
<th>Commit version</th>
<th>Device group</th>
</tr>
</thead>
<tbody>
<tr>
<td>FALCON-ASA-CX</td>
<td>172.16.5.200</td>
<td>9.1.1 (1)</td>
<td>ASA5585-SSP-CX10</td>
<td>JAF1530CNEH</td>
<td>1088</td>
<td>Default device group</td>
</tr>
</tbody>
</table>
ASA CX – Multi Device Management

Device Discovery

Credentials for the ASA device

Please enter a name and optional description to identify the device in PRSM

Device type: ASA

Device name

Description

Please provide the following information required to discover device

Hostname/IP

Port: 443

Username

Password

* required fields

Discover Cancel
ASA CX – Multi Device Management

Device Discovery

After discovery GUI access is restricted to CX device:

Managed Mode

This device is being managed by Cisco Prime Security Manager (multiple-device mode) running on https://172.16.2.212.

Redirect to Cisco Prime Security Manager (multiple-device mode)

Download logs

Switch to Single-Device Mode

Caution: Switching to single-device mode terminates the management relationship with the PRSM server and allows you to directly manage the device. However, the device is not deleted from the PRSM inventory. To avoid deployment problems in the future, please delete the device from the PRSM server's inventory. To return to managed mode, you must import the device again into the PRSM multiple-device mode server.
ASA CX – Multi Device Management
Device Discovery - Limitations

On ASA:

- When discovered use PRSM for supported settings, and ASDM/CLI/CSM for non supported settings (ie. VPN/NAT)

- Don't use other applications to control settings that is ‘owned’ by PRSM such as:
  - Syslog servers

- Commiting PRSM Managed ASA Settings are deployed to and changed in ASA incl: MPF svc policy, syslog servers and logging settings

- Some unmanaged settings are discovered, and can be edited on CX, but it will not be deployed to ASA incl: Interface list, Network and Service objects.
  - Use ASDM/CLI to edit these in addition to CX
  - Consider the discover ONE WAY
ASA CX – Multi Device Management

Device Discovery - Limitations (cont.)

On CX:

- All policies and objects are discovered, but some settings might not be imported
  - Remember duplicate names need to be ‘sufFIXED’

- Directory Realms: AD realm is only imported if none exists in PRSM
  - Only one AD realm is supported! This might prevent the device from being discovered.

- Enabled Decryption policies and settings are imported if:
  - Settings are are identical to those in PRSM (if not, import fails)
  - Decryption is disabled in PRSM – it will then be enabled automatically

- Users are NOT imported – these are not removed, but will be disabled

- Log settings are imported and no changes will take place as these are device specific.
ASA CX – Working With Objects
Object Types And Their Use

- Objects can be imported from ASA, from ASA CX or created
- Note: Object type naming can be confusing –
  - Try to remember the three objects used in ASA:
    - Network object
    - Service object
    - Network group
    - Only available in multi-device mode
    - Can be edited and controlled in PRSM but will not be changed on ASA – see previous slide.
    - Used to match SRC, DST, Ports, Protocols, FQDN
      - Can be IPv6
ASA CX – Working With Objects

Object types and their use (cont.)

ASA CX object types:

• ASA CX Network Group
  IP, networks, ASA network objects and groups, and nested CX Network Groups

• Service Group
  Protocols and ports, and nested services groups

• Identity object
  Authenticated users, groups and nested groups
  Predefined objects: Known users & Unknown Users
ASA CX – Working With Objects
Object types and their use (cont.)

- **URL object**
  Only valid in the DST tuple. Matches both HTTP and HTTPS, URL, Domains and URL category
ASA CX – Working with Objects
Object Types And Their Use (cont.)

ASA CX object types:

• UserAgent object

Many predefined objects
Useful for server user-agents that need access to specific services or clients that cannot respond to active AUTH prompts.

Not a safe control as spoofing is common

```
GET / HTTP/1.1
Host: developmentserver.com
User-Agent: Mozilla/5.0 (iPad; U; CPU OS 3_2 like Mac OS X; en-us) AppleWebKit/531.21.10 (KHTML, like Gecko) Version/4.0.4 Mobile/7B334b Safari/531.21.10
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
```
ASA CX – Working with Objects
Object Types And Their Use (cont.)

ASA CX object types:

- Application object
  Can be a specific supported application or application type
  Ex. Application: BitTorrent, DNS, Google Translate
  Ex. Application type: Instant Messaging

- Application-Service Object
  The ability to tightly couple application and service (port)
• Application-Service Object
  The ability to tightly couple application and service (port)
ASA CX – Working with Objects
Object Types and Their Use (cont.)

ASA CX object types:

- **Destination object GROUPS:**
  Network objects AND URL objects can be combined in DST

- **Source object GROUPS:**
  Network objects AND identity AND userAgent and AnyConnect/SecMob objects can be combined in SRC
Deploying ASA CX Policies
### ASA CX – The Policy Model

#### Overview of The ASA CX Policy Model

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Policy</td>
<td>Yes its a FW... Deny or Allow?</td>
</tr>
<tr>
<td>Identity Policy</td>
<td>Who are you....? Tie Identity to traffic</td>
</tr>
<tr>
<td>Decryption Policy</td>
<td>When and what to decrypt.</td>
</tr>
</tbody>
</table>
ASA CX – The Policy Model

Policies in General

• Policies are evaluated top-down → Order is important

• Policy model honors: First match

• Policy order is:
  • Identity
  • Decryption
  • Access
ASA CX – The Policy Model

Policies in General

If no policy matches, implicit policies are applied to the flow:

Access policy sets end with implicit allow all

Decryption policy sets end with implicit do not decrypt

Identity policy sets end with implicit do not require authentication

NOTE: A policy which identical to another policy in SRC – DST – ACTION is not allowed and cannot be created.
Deploying ASA CX Access Policies
ASA CX – Access Policy

Access Policy Creation

• Access Policies are your "traditional" firewall policies
  • Action is ALLOW or DENY

• Other options in access policies includes
  • Policy on/off
  • Eventing on/off
  • Capture packets on/off

• To match access policies connection must match "Triplet":
  • Source (user, network, sec mob object, group, UserAgent....)
  • Destination (network, URL, FQDN...)
  • Application/Service/port
ASA CX – Access Policy

Access Policy Creation

1. Identify bad application usage in event viewer
2. Create a simple access policy that blocks the device from using YMSG
3. Commit and deploy change
4. Observe blocked comms and deny events in event viewer
Authentication & Identity Policies
Identity and Authentication Overview

Identity and Authentication serves to main purposes:

- **Visibility**: Obtain user identity for reporting and eventing purposes
- **Authorization**: Create rules in ACCESS POLICY based on user/groups

Identity is obtained through authentication in two ways:

- **Passive authentication**
- **Active authentication**

Both methods have pros and cons.
### ASA CX – Identity Policies

#### Active vs. Passive Authentication

<table>
<thead>
<tr>
<th>Passive Authentication</th>
<th>Active Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD authentication only</td>
<td>Kerberos, NTLM, Basic</td>
</tr>
<tr>
<td>Always transparent to the user</td>
<td>Can be transparent to the user</td>
</tr>
<tr>
<td>Supports all traffic types</td>
<td>Must be initiated by HTTP</td>
</tr>
<tr>
<td>Uses Agent software to monitor AD logins –</td>
<td>Performes ‘real’ authentication, requires no agent.</td>
</tr>
<tr>
<td>Best effort authentication….</td>
<td></td>
</tr>
<tr>
<td>Must be on AD member client</td>
<td>Must use client/agent that can authenticate</td>
</tr>
<tr>
<td>Only MS Active Directory</td>
<td>MS AD, openLDAP</td>
</tr>
<tr>
<td>Not suitable for Citrix/Virtual desktop</td>
<td>Not suitable for Citrix/Virtual desktop</td>
</tr>
<tr>
<td>environments</td>
<td>environments</td>
</tr>
</tbody>
</table>
ASA CX – Identity Policies
Passive Authentication Architecture

Traffic controlled by Access Policies which leverage Identity

Internet

Cisco ASA + CX

Domain username and group information (LDAP)

Domain Username/Group to IP Mapping (Radius)

User Login Event Security Log (WMI)

Active Directory Domain Controller

Cisco CDA Server

User Login Event

Domain user

Traffic controlled by Access Policies which leverage Identity
ASA CX – Identity Policies
Passive Authentication Policy

Enabling Identity passive mappings:

• Use action of “Get identity using AD agent” in the Identity Policy

• Note: A combination of both Passive and Active auth can be used as a fallback mechanism if Passive authentication fails to obtain the identity
ASA CX – Identity Policies
Active Authentication Flow

- First connection **MUST** be HTTP – if successful authentication, all traffic is mapped to ID

- ASA CX sees HTTP request from a client to a remote website

- ASA CX redirects the client to the ASA inside interface (port 885 by default) Redirect is accomplished by sending a proxy redirect to the client (HTTP return code 307) spoofing the remote website

- Sends client authentication request (HTTP return code 401)

- After authentication, the ASA CX redirects the client back to the remote website (HTTP return code 307)
ASA CX – Identity Policies
Active Authentication Tips

• Remember to enable auth proxy in the redirect policy
  • Through PRSM it is automatically done, but not through CLI
  • Port number can be changed from TCP/885 using ‘number’ keyword
    • cxsc auth-proxy port number  (Number MUST be >1024)
  • Make sure no firewalls are blocking users from connecting to ASA auth proxy
ASA CX – Identity Policies
Active Authentication Tips

- Time settings are important – skew between ASA and DC’s and clients will break auth

- Users who fail authentication will be shown in dashboard as REALM\anonymous

- Users with no USER/IP mapping will be shown in dashboard as IP address

- Some clients cannot respond to authentication requests – these could be exempted from authentication using ”exclude” objects in the policy.
ASA CX – Identity Policies
Make Active Authentication Transparent

• For optimal experience enable "advanced" as the Active authentication method
  • This allows for negotiation of strongest auth method Kerberos, NTLM, Basic

• Kerberos and NTLM can support a transparent "browser” authentication, if:
  • Configured in the client browser
  • The user has already authenticated to the windows domain

• Browser configuration can be done manually or pushed via Enterprise software deployment tools.

Note: Windows integrated authentication does not support proxy – so make sure to exclude ASA inside IP from any proxy servers between the client and the auth proxy daemon.
ASA CX – Access Policy
Identity Policy Creation and How To Use In Access Policy

1. DEMO of Passive authentication with new user
2. Create policy with specific user in SRC – show AD integration
3. Use this to ALLOW this user access to Yahoo Messenger
4. Track username in “dashboard/event viewer”
Decryption Policies
ASA CX – Decryption Policies

Why Implement TLS Decryption on Traffic?

• The purpose of CX is to detect malicious traffic, monitor, measure and control user traffic.

• This cannot be accomplished well on encrypted traffic without decryption.

• Using decryption will provide the following on encrypted flows:
  Gain insight into traffic i.e. application visibility
  Block malicious sites by using reputation
  Block file uploads and downloads
  Control access based on application behaviour

• Remember: TLS/SSL might be secure, but not necessarily ‘safe’
ASA CX – Decryption Policies

TLS Decryption - Overview

• Based on the ‘Decryption Policy” ASA CX determines whether to decrypt a flow.

• If the matching policy dictates to decrypt – ASA CX will act as a man-in-the-middle, decrypt the flow and re-encrypt it the access policy allows the flow.

• To intercept, decrypt and re-encrypt ASA CX uses either a self-signed certificate or the administrator can upload a CA certificate to the ASA.

• The client MUST trust the ASA CA certificate as a trusted root for decryption to work.

• FQDN, issue dates and expiry as well as CRL’s are NOT checked by ASA CX. This is ‘still’ up to the client application (i.e. browser) to check.
ASA CX – Decryption Policies
TLS Decryption – Untrusted Server Certificates

• The destination tuple in decryption policies can be based on FQDN

• ASA CX will only match FQDN’s if the server certificate can be trusted by CX.

• If FQDN is needed, and the site server certificate cannot be trusted the flow is dropped.

• It is possible to manually add certificates to the ASA CX trusted root certificate store
ASA CX – Decryption Policies

TLS Decryption – Man In The Middle Flow

ASA CX acts as a CA and issues a certificate ‘on behalf of” the real web-site.

1. Negotiate algorithms.

2. Authenticate server certificate.

3. Generate proxied server certificate.


5. Generate encryption keys.

6. Encrypted data channel established.

Cert is generated dynamically with destination name but signed by ASA CX.

1a. Negotiate algorithms.

2a. Authenticate server certificate.

3a. Generate proxied server certificate.

4a. Client Authenticate “server” certificate.

5a. Generate encryption keys.

6a. Encrypted data channel established.
ASA CX – Decryption Policies

TLS Decryption – Decryption Policy

Create Policy

Policy Name*: Decrypt_webmail

Enable Policy: On

Source: Any

Create new object

For URL objects used in decryption policies, URLs containing paths are ignored.

Destination:

URLs to Decrypt

WebMail

Create new object

Service: Any

Create new object

Action: Decrypt potentially malicious traffic

Web reputation:

Default Reputation Profile

Create new profile

DST can be both specific URLs and URL categories

Decryption policies can be linked to Web Reputation Profile
ASA CX – The Policy Model
The Ambiguous Scenario – Order Matters!

- A scenario can occur where ASA CX cannot determine the policy
Result: The flow will be dropped – can happen if CERT is untrusted

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td><a href="http://www.example.com">www.example.com</a></td>
<td>Do not decrypt</td>
</tr>
<tr>
<td>Any</td>
<td>Any</td>
<td>Do not decrypt</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td><a href="http://www.example.com">www.example.com</a></td>
<td>Do not decrypt</td>
</tr>
<tr>
<td>HR</td>
<td>Any</td>
<td>Do not decrypt</td>
</tr>
<tr>
<td>Any</td>
<td>Any</td>
<td>Decrypt</td>
</tr>
</tbody>
</table>
• Decryption requires a K9 license – free but subject to export regulations

• HTTPS is the only protocol subject to inspection after decryption

• Only traffic which initiated with a SSL/TLS handshake will be decrypted, all other traffic are handled as unencrypted traffic. I.e. SMTPoTLS will not be decrypted.
ASA CX – Decryption Policies
TLS Decryption – Tips and Caveats (cont.)

• If the DST tuple is matched using URL objects, use only domain names. Objects which contain path information are ignored by the policy.

• Some applications do not support MITM/Decryption. This include many banking applications. URL categories can be used to exempt these from decryption – but consider the operational ressource impact.

• Enabling decryption on the system will affect system performance and might impact application performance as well.

• **TIP:** Creating a policy with DST ‘www.example.com’ and Action: Do Not Decrypt can provide valuable network visibility, but without decrypting the actual traffic payload.
Advanced Inspection Policies
ASA CX – Advanced Inspection Policies
Managing Threats and Application Behaviour

• In addition to standard access policies, ‘allow’ policies can be inspected and controlled with more granularity for content such as:

  • Web based threats: By adding a ‘Web Reputation Profile’
  • Block file upload or download: By adding a ‘File Filtering Profile’
  • Web Application Behaviour: By Allowing or Denying a certain behaviour
ASA CX – Advanced Inspection Policies
Cisco Cloud Threat Intelligence – Span & Scale

- Cisco Security Intelligence Operations is a threat monitoring network receiving threat intelligence from many different sources such as:
  - Web Security and Email Security appliances
  - IDS/IPS sensors
  - Cloud Web Security
  - 3rd party sources

- Threat information is correlated across threat vectors not just single source of truth

- Reputation scores are constantly deducted and regulated then submitted into Cisco Security Products including ASA CX

- Note: Web Reputation is very different from blacklisting
ASA CX – Advanced Inspection Policies
Understanding Web Reputation Scores

Dedicated or hijacked sites persistently distributing key loggers, root kits and other malware. Almost guaranteed malicious.

Aggressive Ad syndication and user tracking networks. Sites suspected to be malicious, but not confirmed

Sites with some history of Responsible behavior or 3rd party validation

-10  -5  0  +5  +10

Phishing sites, bots, drive by installers. Extremely likely to be malicious.

Well managed, Responsible content Syndication networks and user generated content

Sites with long history of Responsible behavior. Have significant volume and are widely accessed
ASA CX – Advanced Inspection Policies

Web Reputation Profiles

• Web Reputation Profiles can be added to "ALLOW" policies to filter out potentially malicious traffic.
  Action will show as: "Conditional Allow’

• Web Reputation Profiles can be used with "decryption policies” to limit decryption to traffic which might pose a threat.
  Note: Web Reputation works only for HTTP/HTTPS traffic.

• Web Reputation Scores can be viewed in the event-viewer
Tip: Your traditional firewall clean-up rule could be the following:
ASA CX – Advanced Inspection Policies

File Filtering Profiles

- File filtering policies enable blocking of upload/download of specified MIME types on HTTP and decrypted HTTPS traffic only.

- Similar to Web Reputation Profiles, File filtering can only be applied to policies with the ‘allow’ action.

- ASA CX detects the main type by inspecting the "content type header”.

- Mime types can be matched using wildcards or specific sub types:
  - Ie. audio/* or audio/mp4

- End User Notifications are provided – see DEMO.
ASA CX – Advanced Inspection Policies
Web AVC – Controlling Application Behaviour

• For HTTP and decrypted HTTPS application behaviour can be controlled, if supported by the specific application

• This allows for enforcing policies where allowing access to an application can be balanced with acceptable usage
  • ie. Generally allow access to Facebook, but block chat and games.

• Behaviour controls can only be enabled on ‘allow policies’

• Behaviours will automatically populate the GUI where supported
  • Controls can also be seen in the application database
ASA CX – Advanced Inspection Policies
Web AVC – Controlling Application Behaviour

Set application behaviours
Set global behavior to

Dropbox
- Download: Allow
- Dropbox Sharing: Allow
- Upload: Allow
## ASA CX – Advanced Inspection Policies

### Web AVC – Controlling Application Behaviour

<table>
<thead>
<tr>
<th>Application</th>
<th>Behaviors</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Facebook Events</strong></td>
<td>Post, Tag</td>
</tr>
<tr>
<td>Facebook is an event calendaring and management</td>
<td></td>
</tr>
<tr>
<td>system for Facebook users.</td>
<td></td>
</tr>
<tr>
<td><strong>Facebook General</strong></td>
<td>Post, Tag, Install</td>
</tr>
<tr>
<td>Facebook is a social networking service and</td>
<td></td>
</tr>
<tr>
<td>website.</td>
<td></td>
</tr>
<tr>
<td><strong>Facebook Messages and Chat</strong></td>
<td>Attachment Upload,</td>
</tr>
<tr>
<td>Facebook Messages and Chat is Facebook’s web-based instant</td>
<td>Attachment</td>
</tr>
<tr>
<td>messaging service.</td>
<td>Download, Facebook Video</td>
</tr>
<tr>
<td></td>
<td>Chat</td>
</tr>
<tr>
<td><strong>Facebook Notes</strong></td>
<td>Post, Tag</td>
</tr>
<tr>
<td>Facebook Notes is a Facebook-based blogging</td>
<td></td>
</tr>
<tr>
<td>service.</td>
<td></td>
</tr>
<tr>
<td><strong>Facebook Photos</strong></td>
<td>Upload, Post, Tag</td>
</tr>
<tr>
<td>Facebook Photos is Facebook's photo sharing</td>
<td></td>
</tr>
<tr>
<td>application, which features albums, tagging,</td>
<td></td>
</tr>
<tr>
<td>facial recognition technology, and</td>
<td></td>
</tr>
<tr>
<td>commenting on photos.</td>
<td></td>
</tr>
</tbody>
</table>
ASA CX – Access Policy
Blocking Malware and File Download with ASA-CX

1. Block malicious .exe file from phishing email
2. Block live malware via WRBS

Email me after the session to obtain DEMO videos via Dropbox: Cheinel(a)cisco.com
ASA CX – Managing the solution
Management Operations - Eventing

- PRSM supports real time and historical integrated eventing
- The event viewer can be customized and personalized greatly with custom filters and the "column chooser".
- Created views and filters can be saved and reused
- ASA Syslogs can be forwarded to PRSM eventing
- Drill down to single events from the reporting dashboards are supported
  - i.e. for investigating malicious traffic transactions or specific user traffic
- TIP: Clicking details on a single event, will display all relevant columns as well as the ‘policy correlator’
Here is the trick for the "policy correlator" view:
### Identity
Used by device groups: Default device group

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Application</th>
<th>Action/Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANY</td>
<td>ANY</td>
<td></td>
<td>Do not require authentication</td>
</tr>
</tbody>
</table>

Realm: ADS.falcon.lab

### Access
Used by device groups: Default device group

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Application</th>
<th>Action/Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANY</td>
<td>ANY</td>
<td></td>
<td>Conditional Allow</td>
</tr>
</tbody>
</table>

Profiles:
- Default Reputation
- Profile
ASA CX – Managing the solution
Event Storage Requirements

Small deployment of 250 users (25 EPS)

<table>
<thead>
<tr>
<th>Days (12 Hour)</th>
<th>EPS</th>
<th>Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>25</td>
<td>324 MB</td>
</tr>
<tr>
<td>30</td>
<td>25</td>
<td>9.72 GB</td>
</tr>
<tr>
<td>60</td>
<td>25</td>
<td>19.44 GB</td>
</tr>
<tr>
<td>90</td>
<td>25</td>
<td>29.16 GB</td>
</tr>
</tbody>
</table>

NOTE: Results may vary greatly depending on application and usage
ASA CX – Managing the solution
Event Storage Requirements

Medium -deployment of 1,000 users (100 EPS)

<table>
<thead>
<tr>
<th>Days (12 Hour)</th>
<th>EPS</th>
<th>Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>100</td>
<td>1.3 GB</td>
</tr>
<tr>
<td>30</td>
<td>100</td>
<td>38.88 GB</td>
</tr>
<tr>
<td>60</td>
<td>100</td>
<td>77.76 GB</td>
</tr>
<tr>
<td>90</td>
<td>100</td>
<td>116.64 GB</td>
</tr>
</tbody>
</table>

NOTE: Results may vary greatly depending on application and usage
ASA CX – Managing the solution
Event Storage Requirements

Medium - Large deployment of 10,000 users (1000 EPS)

<table>
<thead>
<tr>
<th>Days (12 Hour)</th>
<th>EPS</th>
<th>Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1000</td>
<td>13 GB</td>
</tr>
<tr>
<td>30</td>
<td>1000</td>
<td>390 GB</td>
</tr>
<tr>
<td>60</td>
<td>1000</td>
<td>780 GB</td>
</tr>
<tr>
<td>90</td>
<td>1000</td>
<td>1.17 TB</td>
</tr>
</tbody>
</table>

NOTE: Results may vary greatly depending on application and usage
ASA CX – Managing the solution
Event Storage Requirements

Very Large deployment of 50,000 users (5000 EPS)

<table>
<thead>
<tr>
<th>Days (12 Hour)</th>
<th>EPS</th>
<th>Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5000</td>
<td>64.8 GB</td>
</tr>
<tr>
<td>30</td>
<td>5000</td>
<td>1.9 TB</td>
</tr>
<tr>
<td>60</td>
<td>5000</td>
<td>3.88 TB</td>
</tr>
<tr>
<td>90</td>
<td>5000</td>
<td>5.83 TB</td>
</tr>
</tbody>
</table>

NOTE: Results may vary greatly depending on application and usage
ASA CX – Managing the solution
Day to Day Management Operations – Role Based Access Control

- PRSM in Multi-Device mode supports RBAC
- Admins can be authenticated using AD – but must be created in PRSM
- RBAC controls both what admins can ‘see’ and ‘do’
- The following roles are applicable:
  - Administrator – creates ALL users and can access to ALL features
  - Security Administrator – R/W to security policies and some device features
  - Reporting Administrator – Can view dashboards, but no changes allowed
  - Help Desk User – Can view dashboards, policy and device configurations but no changes allowed.
ASA CX – Managing the solution
Role Based Access Control – refer to user guide for detailed matrix

<table>
<thead>
<tr>
<th>Menu</th>
<th>Role</th>
<th>Administrator</th>
<th>Security Administrator</th>
<th>System Administrator</th>
<th>Reporting Administrator</th>
<th>Help Desk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies &gt; Objects</td>
<td></td>
<td>R/W</td>
<td>R/W</td>
<td>No</td>
<td>No</td>
<td>RO</td>
</tr>
<tr>
<td>Policies &gt; Applications</td>
<td></td>
<td>R/W</td>
<td>R/W</td>
<td>No</td>
<td>No</td>
<td>RO</td>
</tr>
<tr>
<td>Policies &gt; Device Groups</td>
<td></td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>No</td>
<td>RO</td>
</tr>
<tr>
<td>Device &gt; Devices (including the device configuration page)</td>
<td></td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>No</td>
<td>RO</td>
</tr>
</tbody>
</table>
Place in the Network & Routed or Transparent Mode
ASA CX – Routed / Transparent Mode

- ASA CX can be deployed with ASA both in routed and transparent mode
- In transparent mode CX can ‘easily’ be inserted and with little to no topology/ip change provide visibility and control into network behaviour.
- Deploy where IP schemes cannot be changed
- No VPN support – thus no AnyConnect integration
- No dynamic routing support
- No DHCP relay nor QOS support (ASA)
ASA CX – Places in the Network (PIN)
Considerations For Deployment

• ASA CX is primarily targeted at Internet/Edge deployments

• In current version security controls are centered around ‘user & client’ outbound protections

• WBRS and URL filtering are external Internet dependant services

• Most use-cases touch Internet based apps
  • Only Web-AVC allows for granular usage controls
ASA CX – Places in the Network (PIN)
Considerations For Deployment

- Other PIN’s may be considered for gaining visibility and control in specific use cases:
  - ASA CX in Remote Access WAN environments – AnyConnect integration
  - Centralized Virtual Desktop environments
  - Specific Data Center deployments for managing access to very specific applications/services
    - NOTE: Consider performance, no. of connections, ssl load, protocol support and the need for traditional firewall controls vs. CX controls in the DC!
ASA CX – High Availability
ASA CX devices – High Availability

- ASA CX is currently not supported when ASA is configured in Multi-context
- NO active/active failover support
- ASA CX Active/Standby failover works similar to that of IPS modules integrated in ASA
- No failover technology built into ASA CX itself as of today
- High Availability and uninterrupted service can still be achieved
- Introducing the concept of Device Groups and Policy sets
ASA CX devices – High Availability

<table>
<thead>
<tr>
<th>Scenario</th>
<th>How to achieve</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Active &amp; Standby CX.</td>
<td>By using device groups and policy sets you can ensure “synchronization” and consistency across active/standby device</td>
</tr>
<tr>
<td>If primary CX goes down, ASA fails over to Standby Device.</td>
<td>HTTP Replication enables users to browse, stream and download files freely without end-user interruption during a failover.</td>
</tr>
<tr>
<td>Non-disruptive Web Browsing &amp; File Download</td>
<td>Failover is triggered if CX fails</td>
</tr>
<tr>
<td>Monitor health – CX &lt;-&gt; ASA Heartbeat Sensor</td>
<td></td>
</tr>
</tbody>
</table>
Scenario

How to achieve

Manage Active & Standby CX.

If primary CX goes down, ASA fails over to Standby Device.

By using device groups and policy sets you can ensure "synchronization" and consistency across active/standby device.

Non-disruptive Web Browsing & File Download

HTTP Replication enables users to browse, stream and download files freely without user interruption during a failover.

Monitor health – CX < ASA Heartbeat Sensor

Failover is triggered if CX fails ASA CX devices – High Availability

Device Groups

5525-A

Device Groups

5525-A-CX

Device Groups

5525-b

Device Groups

5525-b-CX

Device Groups

5525-X Failover Pair
2 Devices
ASA CX devices – High Availability

<table>
<thead>
<tr>
<th>Scenario</th>
<th>How to achieve</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Active &amp; Standby CX.</td>
<td>By using <strong>device groups and policy sets</strong> you can ensure “synchronization” and consistency across active/standby device.</td>
</tr>
<tr>
<td>If primary CX goes down, ASA fails over to Standby Device.</td>
<td>HTTP Replication enables users to browse, stream and download files freely without end-user interruption during a failover.</td>
</tr>
<tr>
<td>Non-disruptive Web Browsing &amp; File Download</td>
<td>Failover is triggered if CX fails</td>
</tr>
</tbody>
</table>

Only available in centralized PRSM!
# ASA CX devices – High Availability

<table>
<thead>
<tr>
<th>Scenario</th>
<th>How to achieve</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Active &amp; Standby CX.</td>
<td>By using device groups and policy sets you can ensure “synchronization” and consistency across active/standby device</td>
</tr>
<tr>
<td>If primary CX goes down, ASA fails over to Standby Device.</td>
<td></td>
</tr>
<tr>
<td>Non-disruptive Web Browsing &amp; File Download</td>
<td>HTTP Replication enables users to browse, stream and download files freely without end-user interruption during a failover.</td>
</tr>
<tr>
<td>Monitor health – CX &lt;-&gt; ASA Heartbeat Sensor</td>
<td>Failover is triggered if CX fails</td>
</tr>
</tbody>
</table>

|
How to Manage Active & Standby CX

By using device groups and policy sets you can ensure "synchronization" and consistency across active/standby device.

Web Browsing & File Download

HTTP Replication enables users to browse, stream and download files freely without user interruption during a failover.

CX < ASA Heartbeat Sensor

If primary CX goes down, ASA fails over to Standby Device.
## ASA CX High Availability

### Caveats to Consider

<table>
<thead>
<tr>
<th>Scenario</th>
<th>What happens</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Stateful Failover</strong></td>
<td>No stateful failover of transactions going through CX-1.</td>
</tr>
<tr>
<td></td>
<td>In-progress connections – These sessions will be processed by ASA-2 correctly; they are not sent to CX-2</td>
</tr>
<tr>
<td></td>
<td>New Sessions – These sessions are sent to CX-2</td>
</tr>
<tr>
<td><strong>Events</strong></td>
<td>Events are shown from both systems but are not aggregated together</td>
</tr>
<tr>
<td><strong>CX User Authentication</strong></td>
<td>CX user authentication may not fail over for the in-progress transactions</td>
</tr>
<tr>
<td><strong>Decryption</strong></td>
<td>Decrypted sessions may not fail over for the in-progress transactions</td>
</tr>
</tbody>
</table>
Key Take Aways & Summary
ASA CX– Key Take Aways

• ASA CX delivers Next Generation capabilities in ‘addition’ to ASA firewall capabilities

• PRSM is mandatory – Centralized deployment is always recommended, and required for config sync in HA deployments

• CX is currently supported on all 5500-X platforms except 5585-X SSP40 and SSP60

• Passive and active authentication gives you deep insight into user behaviour

• Consider where to deploy decryption – many applications might be unsupported, requiring exceptions.

• ASA CX current features are targeted mainly for Internet/Edge deployments
Recommended Reading for BRKSEC-2699

Cisco Firewalls
Concepts, design and deployment for Cisco Stateful Firewall solutions

Alexandre M.S.P. Moraes, CCIE® No. 6063
Call to Action

• **Visit** the Cisco Campus at the World of Solutions to experience the following demos/solutions in action:

  Security Intelligence Operations / Scott Simkin  
  Next Generation Security Services – Firewall / Almitra Karnik

• **Meet** the Engineer  
  Book a MTE meeting on Cisco ASA CX – contact me after the session

• **Discuss** your project’s challenges at the Technical Solutions Clinics
Your feedback is important to us.

Complete the session survey at: www.ciscolivelondon.com/onsite or via the Cisco Live Mobile App