Deploying Next-Generation Firewall Services on the ASA

BRKSEC-2024

Poonguzhali (Kureli) Sankar
CCIE Security # 35505
Technical Marketing Engineer

Phillip Strelau
Customer Support Engineer
Agenda

**Introduction to NGFW**
Deployment
Software Architecture
Licensing
How to configure policies
Management and Eventing
Use cases
Troubleshooting tips
Cisco ASA Next-Generation Firewall Services
Security Without Compromise

**Cisco® SIO**
Comprehensive, Next-Generation Security Services

**Proven Stateful Inspection Firewall**

**Network Integrated Security**

Complete protection and policy

- **ONLY CISCO** Industry-leading web reputation for malware protection
- **ONLY CISCO** Stateful inspection firewall and class-leading AnyConnect® VPN
- **ONLY CISCO** Network-wide identity and device access policy
What is Context Aware Security?

• ASA CX software includes three new software modules:
  – Application Visibility and Control (AVC)
  – Web Security Essentials (WSE)
  – NG-IPS

• Adds unprecedented visibility, granular control and maximizes protection
  – Who (Identity and Authentication)
  – What (Application, URL Category, Reputation)
  – How (Devices, OS, User Agent, Posture)
  – Where (Local, Remote)
Application Visibility And Control - (AVC)
Control Granular Behaviors Of Popular Applications

- Broad...
  - ... classification of all traffic
  - More than 1200 apps

- MicroApp Engine
  - Deep classification of targeted traffic
  - More than 150,000 MicroApps

- App Behavior
  - Control user interaction with the application

- MicroApps
  - Farm Ville
  - More than 150,000 MicroApps

- Apps
  - Facebook
  - Skype
  - YouTube
  - Twitter
  - Google+
Enterprise-Grade URL Filtering - WSE
Industry-Leading Coverage And Efficacy

Marketing
Legal
Finance

60 Languages
200 Countries
50 Million URLs
10,000 Customers
Reputation Analysis
The power of real-time context

IP Reputation Score

17.0.2.12
Kiev
HTTPS
Web server < 1 Month
Web Security Essentials – (WSE)

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

-10

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

-5

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

0

Well managed, Responsible content Syndication networks and user generated content

+5

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

+10

Sites with long history of Responsible behavior. Have significant volume and are widely accessed

Default web reputation profile

Suspicious (-10 through -6)

Not suspicious (-5.9 through +10)
Threats in Motion – NG-IPS

Let us assume that something, somewhere, in your network is doing something you don’t want.

- You don’t know where to look.
- You don’t know what to look for.

But when it acts and reaches across the network, you will see it and know.
Why use AVC and WSE?

- Increase protection – save money
  - Infected PCs cost about 4 hours to rebuild
  - Control bandwidth-hungry sites
  - Increase productivity by blocking non-productivity related apps.
  - Avoid sensitive company data uploaded to the cloud.
  - Allow WebEx and block all other remote control apps.
Why use AVC and WSE?

- Increase visibility - save time
  - Loss of services result in production loss
  - Inappropriate content at work place may raise lawsuits
  - Avoid bandwidth misuse
  - Block micro applications on allowed websites
  - Identify and clamp applications using well known ports
Why use AVC and WSE?

Best choice compared to other 3rd party products

- Licenses are per device basis and not per seat
- Watches all IP traffic and not select ports and protocols
- Detects access to proxies and blocks them
- Recognizes over 1200 applications and more than 150,000 micro-applications
# Web Security Portfolio Basics

<table>
<thead>
<tr>
<th>Feature</th>
<th>NGFW (ASA CX)</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)</td>
<td>Ports (80, 443) Protocols (HTTP(S))</td>
<td>Ports (21, 80, 443) Protocols (HTTP(S), FTP)</td>
</tr>
<tr>
<td>Protocols (all)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Malware Protection</strong></td>
<td>Basic</td>
<td>Advanced</td>
<td>Advanced</td>
</tr>
<tr>
<td>(reputation)</td>
<td></td>
<td>(reputation + content</td>
<td>(reputation + content</td>
</tr>
<tr>
<td>Analysis)</td>
<td></td>
<td>analysis)</td>
<td>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>
What platforms support NGFW Services?

- 5512-55-X – Software Based

ASA 5512-X
ASA 5515-X
ASA 5525-X
ASA 5545-X
ASA 5555-X
ASA5512-X & 5515-X Back Panel

- I/O Expansion Slot
- Status LED's
- Serial Console
- 6 x 1GE Cu Ports
- USB Port
- Dedicated Mgmt Port (1GE)
- Fixed Power Supply
ASA5525-X & 5545-X / 5555-X Back Panel

I/O Expansion Slot
Status LED’s
Serial Console
8 x 1GE Cu Ports
USB Port
Dedicated Mgmt Port (1GE)
Fixed Power Supply
Redundant Hot Swappable PSU
What platforms support CX Software Module?

Branch Locations

- **200 Mbps NGFW**
  - 100K Connections
  - 10,000 CPS
  - ASA 5512-X

- **350 Mbps NGFW**
  - 250K Connections
  - 15,000 CPS
  - ASA 5515-X

- **650 Mbps NGFW**
  - 500K Connections
  - 30,000 CPS
  - ASA 5525-X

Small/Medium Internet Edge

- **1.4 Gbps NGFW**
  - 1 MM Connections
  - 50,000 CPS
  - ASA 5555-X

- **1 Gbps NGFW**
  - 750K Connections
  - 30,000 CPS
  - ASA 5545-X

- **1 Gbps NGFW**
  - 250K Connections
  - 15,000 CPS
  - ASA 5525-X
What platforms support CX Hardware Module?

- 5585-X + CX module in top slot – Hardware Module

- Two Hard Drives Raid 1 (Event Data)
- 8 GB eUSB (System)
- 10GE and GE ports
- Two GE Management Ports
- SSP 40 and 60 Support New with NGFW 9.2
What platforms support CX Hardware Module?

- **ASA 5585-SSP10**
  - **2 Gbps** NGFW
  - **500K Connections**
  - **40,000 CPS**

- **ASA 5585-SSP20**
  - **5 Gbps** NGFW
  - **1 M Connections**
  - **75,000 CPS**

- **ASA 5585-SSP40**
  - **9 Gbps** NGFW
  - **1.8 M Connections**
  - **120,000 CPS**

- **ASA 5585-SSP60**
  - **13 Gbps** NGFW
  - **4 Gbps** NGFW + IPS
  - **4 M Connections**
  - **160,000 CPS**

**Campus / Data Center**

**Enterprise Internet Edge**

*New with 9.2*
Agenda

Introduction to NGFW Deployment
Software Architecture Licensing
How to configure policies
Management and Eventing
Use cases
Troubleshooting tips
How to deploy CX on a 5585-X Platform.

Power down the unit and slide the module in the top slot
How to deploy CX on a 5585-X Platform.

- The module is not hot swappable.
- ASA CX SSP must be at the same level as the SSP model
How to deploy CX on a 5585-X Platform.

- Desktop PC
- Laptop
- Layer 2 switch
- ASA5585-X
- single subnet
- Internet
- CX's Gateway should point to the ASA's inside interface IP
- Inside
- Outside
- CX M0/0
- DNS server
- Single subnet
- 24
How to deploy CX on a 5585-X Platform.

CX M0/0

Inside router/switch

CX’s Gateway should point to the inside router IP

Inside

outside

ASA5585-X

Desktop PC

Laptop

DNS server

SUBNET 2

SUBNET 1

SUBNET 3

SUBNET 4

SUBNET 5

Internet

Internet

Inside router/switch

CX’s Gateway should point to the inside router IP
How to deploy CX 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 PRSM GUI
- Install license file
- Configure Policies
- Punt traffic up to the CX for filtering
How to deploy CX on a 5585-X Platform.

Configuring the CX via the console port

Reboot the CX from the ASA CLI

ASA5585-X# hw-module module 1 reset
Module 1 should be shut down before resetting it or loss of configuration may occur.

Reset module 1? [confirm]
Reset issued for module 1.

OR

Reboot the CX from the CX CLI

asacx-host > system reload

Press Esc to interrupt the boot process so that you can configure rommon variables
How to deploy CX on a 5585-X Platform.

Configuring the CX via the console port

rommon #1> ADDRESS=14.36.109.54
rommon #2> SERVER=14.36.109.111
rommon #3> GATEWAY=14.36.1.1
rommon #4> IMAGE=asacx-boot.9.2.1.2-82.img
rommon #5> sync

Updating NVRAM Parameters...
How to deploy CX on a 5585-X Platform.

Configuring the CX via the console port

rommon #6> tftp
ROMMON Variable Settings:
ADDRESS=14.36.109.54
SERVER=14.36.109.111
GATEWAY=14.36.1.1
PORT=Management0/0
VLAN=untagged
IMAGE=asacx-boot-9.2.1.2-82.img
CONFIG=
LINKTIMEOUT=20
PKTTIMEOUT=4
RETRY=20

tftp asacx-boot-9.2.1.2-82.img@14.36.109.111 via 14.36.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Received 68993646 bytes
Launching TFTP Image...
How to deploy CX on a 5585-X Platform.

Configuring the CX via the console port

Login as following:
User-ID: admin
Default password: Admin123

…
starting Busybox inetd: inetd... done.
Starting ntpd: done
Starting syslogd/klogd: done

Cisco ASA CX Boot Image 9.2.1.2-82

asacx login: admin
Password:
How to deploy CX on a 5585-X Platform.

asacx-boot>partition
WARNING: You are about to erase all policy configurations and data.
You cannot undo this action.
Are you sure you want to proceed? [y/n]:y

....
Partition Successfully Completed on the Flash
....
Partition Successfully Completed on the Hard Drive
asacx-boot>
How to deploy CX on a 5585-X Platform.

Configuring the CX via the console port

asacx-boot>setup

Welcome to Cisco Prime Security Manager Setup
    [hit Ctrl-C to abort]
Default values are inside []

Enter a hostname [asa-191-cx]:asa-191-cx
Do you want to configure IPv4 address on management interface?(y/n) [Y]:y
Do you want to enable DHCP for IPv4 address assignment on management interface?(y/n) [N]:n
Enter an IPv4 address [14.36.109.54]:14.36.109.54
Enter the netmask [255.255.0.0]:255.255.0.0
Enter the gateway [14.36.1.1]:14.36.109.35
Do you want to configure static IPv6 address on management interface?(y/n) [N]:n
Stateless autoconfiguration will be enabled for IPv6 addresses.
Enter the primary DNS server IP address [4.2.2.2]:4.2.2.2
Do you want to configure Secondary DNS Server?(y/n) [N]:n
Do you want to configure Local Domain Name?(y/n) [Y]:y
Enter the local domain name [cisco.com]:cisco.com
Do you want to configure Search domains?(y/n) [N]:n
Do you want to enable the NTP service? [N]:y
Enter the NTP servers separated by commas:172.18.108.15
How to deploy CX on a 5585-X Platform.

Configuring the CX via the console port

```plaintext
asacx-boot> system install ftp://CX:cx@14.36.109.111/asacx-sys-9.2.1.2-82.pkg
Verifying.
Downloading.
Extracting.
Package Detail
Description: Cisco ASA-CX 9.2.1.2-82 System Upgrade
Requires reboot: Yes
```

NOTE: If this device is being managed by a PRSM server, you must also apply the same upgrade package to the PRSM server or you will not be able to deploy configurations from the PRSM server to this device.

Do you want to continue with upgrade? [y]: y
WARNING: Please do not interrupt the process or turn off the system.
Do so might leave system in unusable state.

Upgrading.
Stopping all the services ... Starting upgrade process ... Reboot is required to complete the upgrade.
Press Enter to reboot the system.
How to deploy software CX on 5512-55 Platform.

Step 1: Copy the CX boot image to the disk0:/ of the ASA.

5512-X-CX# copy tftp://14.36.109.111/asacx-5500x-boot-9.2.1.2-82.img disk0:/

Address or name of remote host [14.36.103.220]?
Source filename [asacx-5500x-boot-9.2.1.2-82.img]?
Destination filename [asacx-5500x-boot-9.2.1.2-82.img]?
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]
How to deploy software CX on 5512-55 Platform.

Step 2: Load the boot OS onto the CX module using the boot image from the ASA's flash:

```
5512-X-CX# sw-module module cxsc recover configure image disk0:/asacx-5500x-boot-9.2.1.2-82.img
5512-X-CX#
5512-X-CX# sw-module module cxsc recover boot
```

Module cxsc will be recovered. This may erase all configuration and all data on that device and attempt to download/install a new image for it. This may take several minutes.

Recover module cxsc? [confirm]
Recover issued for module cxsc.
How to deploy software CX on 5512-55 Platform.

Step 3: Session to the CX module and run the partition command

5515-X-CX# session cxsc console
Opening console session with module cxsc.
Connected to module cxsc. Escape character sequence is 'CTRL-^X'.

Cisco ASA CX Boot Image 9.2.1

asacx login: admin
Password: Admin123

asacx-boot>partition
How to deploy software CX on 5512-55 Platform.

Step 4: Run the setup command to set the CX Boot IP settings

asacx-boot>setup

Welcome to Cisco Prime Security Manager Setup
[hit Ctrl-C to abort]
Default values are inside []

Enter a hostname [asacx]:
asacx
Do you want to configure IPv4 address on management interface?(y/n) [Y]: Y
Do you want to enable DHCP for IPv4 address assignment on management interface?(y/n) [N]: N
Enter an IPv4 address [192.168.8.8]: 14.36.103.86
Enter the netmask [255.255.255.0]: 255.255.0.0
Enter the gateway [192.168.8.1]: 14.36.103.88
How to deploy software CX on 5512-55 Platform.

Step 5: Run the 'system install' command to download the system image from a http or ftp server and install it

asacx-boot> system install ftp://CX:cx@14.36.109.111/asacx-sys-9.2.1.2-82.pkg

Verifying
Downloading
Extracting
Package Detail

<table>
<thead>
<tr>
<th>Description:</th>
<th>Cisco ASA-CX 9.2.1.2-82 System Upgrade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requires reboot:</td>
<td>Yes</td>
</tr>
</tbody>
</table>

NOTE: If this device is being managed by a PRSM server, you must also apply the same upgrade package to the PRSM server or you will not be able to deploy configurations from the PRSM server to this device.

Do you want to continue with upgrade? [y]: y

Warning: Please do not interrupt the process or turn off the system.

Doing so might leave system in unusable state.

Upgrading
How to deploy CX on a 5585-X/5512-55 Platform.

Log into PRMS GUI http://14.36.109.54

User-ID: admin
Password: Admin123
How to deploy CX on a 5585-X/5512-55 Platform.

Log into PRSM GUI https://14.36.109.54

Supported browsers
- Windows 7, Mac OS X—Mozilla Firefox 22 Mozilla Firefox
- Windows 7, Mac OS X—Google Chrome 17
- Windows 7—Windows Internet Explorer 9 (64-bit)

User-ID: admin
Password: Admin123
Agenda

Introduction to NGFW Deployment
Software Architecture
Licensing
How to configure policies
Management and Eventing
Use cases
Troubleshooting tips
Packet flow diagram – ASA decision process

1. Recv 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

ASA CX

Drop

Yes

No

Yes

No

Yes

No
Functional distribution of ASA and ASA NGFW Software

- URL Category/Reputation
- HTTP Inspection
- AVC
- TLS Proxy
- TCP Proxy
- TCP Normalization
- TCP Intercept
- IP Option Inspection
- IP Fragmentation
- Botnet Traffic Filter
- Multiple Policy Decision Points
- NGFW IPS

- NAT
- Routing
- ACL
- VPN Termination

- NGFW Services Module
- ASA Module
ASA NGFW High level software architecture

- **Packet data**
- **RPC Data**

**Management Plane**

**Control Plane**

**Data Plane – L2-L4, Identity, Broad AVC**

**Eventing Reporting**

**Authentication Identity**

**HTTP Engine**
AVC, URL, WBRS

**Inspection engines**

**TLS Proxy**

**Cisco Context Directory Agent**
AD, CDA, Open Ldap
Packet flow diagram – ASA and CX

- ASA processes all ingress/egress packets
  - No packets are directly processed by CX except for management
- CX provides Next Generation Firewall Services
Packet Processing for non-HTTP traffic

All traffic enters ASA, and if policy verdict is "allow" it exits ASA, not NGFW. All traffic hits the Broad AVC engine if subject to NGFW inspection.
Packet Processing for HTTP(S) traffic

If Broad AVC classifies traffic as HTTP/HTTPS
Web AVC inspection engine is applied
Agenda

Introduction to NGFW
Deployment
Software Architecture
Licensing
How to configure policies
Management and Eventing
Use cases
Troubleshooting tips
Licensing

- Subscription based
  1,3,5 years
- Three Licenses
  AVC (Application Visibility Control)
  WSE (Web Security Essentials)
  NG-IPS
- Eval license can be renewed once for another 60 days.
Licensing - High Availability (OFF-BOX PRSM)

Licensing

- Only one license count is used for the HA pair.
- One single license can be applied to CX HA pair (in fact only the logical device will be shown for assigning the license). PRSM will automatically push the CX license to both the CX devices.

<table>
<thead>
<tr>
<th>Device name / Description</th>
<th>IP Address</th>
<th>Software version</th>
<th>Model</th>
<th>Commit version</th>
</tr>
</thead>
<tbody>
<tr>
<td>ha ASA</td>
<td>10.194.204.186</td>
<td>9.1(3)240</td>
<td>ASA5512</td>
<td>53</td>
</tr>
</tbody>
</table>
Licensing (decryption)

• ASA-CX ships with K8 or low encryption capabilities.
• K9 license turns on high encryption capabilities.
• K9 is locked to the serial number of the unit permanently.
• K9 is free to all users in qualified locations.
Licensing – How to apply

- Purchase license
- Register the PAK number
- Upload the license file
Agenda

Introduction to NGFW Deployment
Software Architecture Licensing
How to configure policies
Management and Eventing
Use cases
Troubleshooting tips
How to configure policies

Policy Sets
- Access
- Decryption
- Identity
- NG-IPS
How to configure policies

**D1 Policy Sets**

1. **Univ. Top [Shared - All devices]**
   - PS1 [Shared – D1, D2]
     - P1 [Exception – D1 only]
     - P2
     - P3
   - PS2 [Local – D1]
   - PS3 [Shared – D1, D2]
   - PS4 [Local – D1]
2. **Univ. Bottom [Shared - All devices]**

**D2 Policy Sets**

1. **U. Top [Shared - All devices]**
2. **PS5 [Local – D2]**
3. **PS6 [Local – D2]**
   - PS1 [Shared – D1, D2]
     - P1 [Exception – D1 only]
     - P2
     - P3
   - PS3 [Shared – D1, D2]
2. **U. Bottom [Shared - All devices]**
How to configure policies

How to create a policy to block Skype

• Click on add new policy
How to configure Policies

Block Skype

![Policy Configuration Diagram]

- **Policy Name**: Block Skype
- **Enable Policy**: On
- **Policy Action**: Deny
- **Source**: Any
- **Destination**: Any
- **Application Service**: Skype
- **Shared/Local**: All Shared Devices

**Interface roles**

- Tags: Enter associated keyword strings
- Ticket ID: Enter Ticket ID strings

---

© 2014 Cisco and/or its affiliates. All rights reserved.
How to configure policies

Block Categories

Create Policy

Policy Name: Rest traffic - URL filtering
Enable Policy: On
Policy Action: Deny

Source: Any
Destination: URL object
Application / Service: Any
Tags: Enter keyword tags
Ticket ID: Enter Ticket ID

* required fields

Save policy  Cancel
How to configure policies

Block Categories

Create URL object

Name*: Bad Sites
Object type: URL object
Description: CX network group
Tags: Enter keyword tags
Ticket ID: Enter Ticket ID

Include
URL: Any
Web category: Any
URL objects: Any

Exclude
URL: None
Web category: None
URL objects: None

URL strings may include wildcards (*). When a domain or host name is entered, all subdomains will be matched (e.g. "example.com" will match traffic to both "example.com" and "mail.example.com"). In situations where only the domain can be determined (e.g. decryption policies), URLs specifying a resource path are ignored.

Save object  Cancel
How to configure policies

Block Categories

https://securityhub.cisco.com/web/submit_urls
How to configure policies

Block category – which policy set uses the URL object Bad Sites?

![Policy Configuration Screen]

- **ASA-5512-Policy_Set**

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Application/Service</th>
<th>Action/Conditions</th>
<th>Interface Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANY</td>
<td>Bad Sites</td>
<td></td>
<td>Deny</td>
<td>ANY to ANY</td>
</tr>
</tbody>
</table>

Any traffic flow that does not match one of the access policies is allowed without conditions.
How to configure policies
Block Malware Using Web Reputation

Cisco Prime Security Manager

Repository
Add device
All devices (1)

Overview
Access policies
Decryption Settings
Malware Protection

Local Malware Protection Configuration

Malware protection: On or Off
Web reputation profile: Default web reputation profile

Intrusion Prevention
Malware Protection

Update successful
Save
How to configure policies
Configuring Web Reputation policy – Enable Malware Protection

Malware protection: On

Create Web reputation profile
- Name: Web Reputation -6 to -10
- Object type: Web reputation profile
- Description:
- Tags: Enter associated keyword strings
- Ticket ID: Enter Ticket ID strings

Low reputation -10 to -6
High reputation -5.9 to 10

When used in access policies, low reputation traffic is blocked. For decryption policies, low reputation traffic is decrypted.

* required fields
How to configure policies

Configuring Web Reputation policy – Configure Access Policy

[Diagram of Cisco Prime Security Manager interface showing Web Reputation policy configuration]
How to configure policies
Configuration Web Reputation Policy – Commit the Changes

Commit and Deploy Changes

You have pending changes. These changes will not go into effect until you commit them.

- Commit
- Discard

Impacted devices: F340.27.05-ASA5500-1 – CX

View changes

ASA-5512-Policy_Set

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

Profiles:
- Web reputation profile - Web
- Reputation -6 to -10
- NG IPS profile - device level
How to configure policies

- Punting traffic to the CX for processing – configured on the ASA

```
policy-map global_policy
  class inspection_default
    inspect dns migrated_dns_map_1
    inspect ftp
  
  class class-default
    cxsc fail-open
    service-policy global_policy global
```
How to deploy CX on a 5512-X Platform.

- Desktop PC: 14.36.109.13
- Laptop
- Layer 2 switch
- ASA5512-X: 172.18.124.203
  - Outside
  - CX M0/0
  - Blocking Skype
  - Blocking a few bad categories
  - Blocking Web Sites with reputation score -6 to -10
- Single subnet
- Internet
Testing from the PC to log into Skype and checking the ASA service-policy

ASA5512# sh service-policy cxsc

Global policy:
Service-policy: global_policy
Class-map: class-default
CXSC: card status Up, mode fail-open, auth-proxy disabled
   packet input 83105, packet output 83297,
   drop 12, reset-drop 11, proxied 0
Looking at the event on the PRSM GUI

<table>
<thead>
<tr>
<th>Receive Times</th>
<th>Event Type</th>
<th>Severity</th>
<th>Device</th>
<th>Source</th>
<th>Destination</th>
<th>Destination Port</th>
<th>Application</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/06/2014 3:13:26 PM</td>
<td>Flow Deny</td>
<td>Informational</td>
<td>F340.27.05-AS55...</td>
<td>14.36.109.13</td>
<td>176.96.66.162</td>
<td>80</td>
<td>Skype</td>
<td>A flow was denied due to policy violation.</td>
</tr>
<tr>
<td>05/06/2014 3:13:23 PM</td>
<td>Flow Deny</td>
<td>Informational</td>
<td>F340.27.05-AS55...</td>
<td>14.36.109.13</td>
<td>212.57.40.155</td>
<td>80</td>
<td>Skype</td>
<td>A flow was denied due to policy violation.</td>
</tr>
<tr>
<td>05/06/2014 3:13:22 PM</td>
<td>Flow Deny</td>
<td>Informational</td>
<td>F340.27.05-AS55...</td>
<td>14.36.109.13</td>
<td>46.158.24.235</td>
<td>80</td>
<td>Skype</td>
<td>A flow was denied due to policy violation.</td>
</tr>
<tr>
<td>05/06/2014 3:13:21 PM</td>
<td>Flow Deny</td>
<td>Informational</td>
<td>F340.27.05-AS55...</td>
<td>14.36.109.13</td>
<td>31.128.82.95</td>
<td>80</td>
<td>Skype</td>
<td>A flow was denied due to policy violation.</td>
</tr>
<tr>
<td>05/06/2014 3:13:07 PM</td>
<td>Flow Deny</td>
<td>Informational</td>
<td>F340.27.05-AS55...</td>
<td>14.36.109.13</td>
<td>212.187.172.78</td>
<td>443</td>
<td>Skype</td>
<td>A flow was denied due to policy violation.</td>
</tr>
<tr>
<td>05/06/2014 3:13:03 PM</td>
<td>Flow Deny</td>
<td>Informational</td>
<td>F340.27.05-AS55...</td>
<td>14.36.109.13</td>
<td>212.187.172.78</td>
<td>80</td>
<td>Skype</td>
<td>A flow was denied due to policy violation.</td>
</tr>
<tr>
<td>05/06/2014 3:13:01 PM</td>
<td>Flow Deny</td>
<td>Informational</td>
<td>F340.27.05-AS55...</td>
<td>14.36.109.13</td>
<td>178.121.172.148</td>
<td>443</td>
<td>Skype</td>
<td>A flow was denied due to policy violation.</td>
</tr>
</tbody>
</table>
Testing from the PC to load a URL that is blocked.

According to this category lookup link
https://securityhub.cisco.com/web/submit_urls

<table>
<thead>
<tr>
<th>Check</th>
<th>URL</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><a href="http://playboy.com">http://playboy.com</a></td>
<td>Pornography</td>
</tr>
</tbody>
</table>

Choose Category:  -- SELECT ONE --  

Submit
Testing from the PC to load a URL that is blocked.
Configuring IPS based policies

• File filtering profile
  – Blocks the download of specific MIME types
  – Blocks the upload of specific MIME types

• Web reputation profile
  – Specifies threshold value for web reputation filter
  – Default profile sets threshold to -6

• NGFW IPS profile
  – Specifies threshold values for NGFW IPS
  – Default: Block & Monitor 70, Allow & Monitor 40
Cisco ASA/CX NGFW IPS – Global Settings

- NGFW IPS Feature available through license
- NGFW IPS ON/OFF switch
- Blocking of traffic sourced from blacklisted IPs
- Option to exclude high reputation traffic
Threat Profiles

- Risk Based Control
- 3 ranges
  - Block and Monitor
  - Allow and Monitor
  - Don’t Monitor
- Customizable exceptions
Access Policy configuration for NGFW IPS

- Threat Profile Field
- Use Custom IPS Profile or the Device Level profile
- Different profiles can be applied to different subset of traffic
- Selection criteria include 5-tuple, user and application
NGFS IPS report dashboard
Why configure decryption based policy?

If blocking social networking is per policy and if these sites are accessible via https how does one block them?

- HTTPS connections are secure, **not** safe
- HTTPS traffic does not discriminate against malicious or compromised servers.

CX needs to play “**man in the middle**”.
Benefits of decrypting https traffic

- Gain insight into network traffic
- Block low reputation sites
- Block undesired file exchanges
- Control access based on defined objects

CX needs to play man in the middle.
How does decryption work?

Client Hello
Server Hello & Certificate

Server Certificate Issuer: Local CA

Handshake
Encrypted Data

ASA with CX software

Client Hello
Server Hello & Certificate

Server Certificate Issuer: Public CA

Handshake
Encrypted Data

Server
Tips and Limitations for Decryption

• A 3DES/AES (K9) license is required for strong encryption.
• HTTPS is the only protocol that is subsequently inspected after decryption.
• Flow has to begin with the SSL/TLS handshake in order to be inspected.
• You cannot use specific URL paths in decryption policies.
• Enabling decryption might decrease the throughput of the system.
• Some applications do not support decrypting traffic between the client and server.
How to configure decryption based policy.

Generate A New Certificate

Import a new certificate
How to configure decryption based policy.

Create decryption policy

Policy Name: Decryption Policy
Enable Policy: On
Source: Any
Destination: Any
Service: Any
Action: Decrypt potentially malicious traffic
Web reputation: Web Reputation - 6 to -10
Interface roles:
Source Interface Role: Any
Destination Interface Role: Any
Tags: Enter associated keyword strings
Ticket ID: Enter Ticket ID strings

* required fields
How to define identity (passive) based policy.

- Configure a Realm – AD or LDAP
- Configure CDA
  - Install CDA on a VM
  - Add the Active Directory Domain Controller to CDA
  - Add consumer device (CX) to CDA
  - Verify ip-to-user mapping
- Add CDA to PRSM
- Modify Authentication Settings (optional)
- Create identity objects
- Configure Identity Policy
- Monitor via Event viewer
How to define identity (passive) based policy.

- CDA VM
- AD Domain Controller
- PRSM VM (OFF BOX)
- ASA5512-X
- Outside
- Internet

Protocol Connections:
- WMI protocol
- Passive identity (tcp port 3779)
- RADIUS
- LDAP
- Active identity (tcp 389)
- tcp 443
How to configure identity (passive) based policy.

Configure CDA - Download ISO image

http://tools.cisco.com/squish/6556F
How to configure identity (passive) based policy.

Configure CDA

Install CDA on a VM or on a physical server.
Configure VM with IP address, DNS server, Gateway, NTP server etc.
How to configure identity (passive) based policy.

Configure CDA - Add the Active Directory Domain Controller to CDA
How to configure identity (passive) based policy.

Configure CDA – Add the CX/PRSM/ASA (consumer device)
How to configure identity (passive) based policy.

Configure CDA – Configure the Domain Controller
How to configure identity (passive) based policy.

Configure CDA - Verify ip-to-user mapping
How to define identity (passive) based policy.

Add CDA into off-box PRSM
How to configure identity (passive) based policy.

Configure a Realm – AD or LDAP

- **CX.com(AD)**
  - CX.com Domain (kusankar)
    - AD login name: `Administrator@cx.com`
    - Group attribute: `member`
  - URL: `ldap://14.36.162.100:389`
    - AD login name: `Service-PRSM@empire.lab`
    - Group attribute: `member`
How to define identity (passive) based policy.

Modify Authentication Settings (optional)

Local Authentication Settings

- Authenticated session duration (hours): 1
- Failed authentication timeout (minutes): 1
- Maximum authentication attempts: 5
- Group refresh interval (hours): 1
How to define identity (passive) based policy.

Configure Identity Policy

ASA CLI

```
policy-map global_policy
class inspection_default
    inspect dns migrated_dns_map_1
    inspect ftp
class class-default
cxsc fail-open
```
How to define (active) identity based policy.

1. Access Attempt
2. Challenge
3. Response (Username / Password)
4. Forward Credentials
5. Authentication Result
6. Access Granted or Denied

policy-map global_policy
class class-default
cxsc fail-open auth-proxy
How to define identity (active) based policy.

ASA CLI

```
policy-map global_policy
class inspection_default
  inspect dns migrated_dns_map_1
  .
  inspect ftp
class class-default
  cxsc fail-open auth-proxy
```

PRSM GUI

Active Authentication
How to define identity (active) based policy.

Configuring identity policy
How to define identity (active) based policy.
Agenda

Introduction to NGFW Deployment
Software Architecture Licensing
How to configure policies
Management and Eventing
Use cases
Troubleshooting tips
PRSM – Prime Security Manager

• PRSM from version 9.2 can also manage "classic" ASA firewall and NAT rules.
• ASA management is only supported when PRSM is in "multi device" mode (off box)
• Extended ACL’s incl. Time ranges is supported
• Webtype, standard and Ethertype ACLs are not supported.
• Note: When committing ASA changes, CLI changes can be reviewed
## Events

### Filter
Enter filter criteria

### View historic event
- Last 30 minutes

**13 May 2014, 1:09 AM (UTC) to 13 May 2014, 1:39 AM (UTC)**

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Event Type</th>
<th>Device</th>
<th>Source</th>
<th>Destination</th>
<th>Destination Port</th>
<th>Application</th>
<th>Reputation Score</th>
<th>Threat</th>
<th>Web Category</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/13/2014 1:39:54 AM</td>
<td>HTTP Complete</td>
<td>F340.27.05-ASA55...</td>
<td>Kureli Sankar</td>
<td>turnerhd-f.akama...</td>
<td>80</td>
<td>HyperText Transfer Protocol</td>
<td>5.9</td>
<td>Infrastructure and C...</td>
<td><a href="http://turnerhc">http://turnerhc</a>...</td>
<td></td>
</tr>
<tr>
<td>05/13/2014 1:39:52 AM</td>
<td>HTTP Complete</td>
<td>F340.27.05-ASA55...</td>
<td>Kureli Sankar</td>
<td>turnerhd-f.akama...</td>
<td>80</td>
<td>HyperText Transfer Protocol</td>
<td>5.9</td>
<td>Infrastructure and C...</td>
<td><a href="http://turnerhc">http://turnerhc</a>...</td>
<td></td>
</tr>
<tr>
<td>05/13/2014 1:39:50 AM</td>
<td>HTTP Complete</td>
<td>F340.27.05-ASA55...</td>
<td>Kureli Sankar</td>
<td>turnerhd-f.akama...</td>
<td>80</td>
<td>HyperText Transfer Protocol</td>
<td>5.9</td>
<td>Infrastructure and C...</td>
<td><a href="http://turnerhc">http://turnerhc</a>...</td>
<td></td>
</tr>
<tr>
<td>05/13/2014 1:39:50 AM</td>
<td>HTTP Complete</td>
<td>F340.27.05-ASA55...</td>
<td>Kureli Sankar</td>
<td>turnerhd-f.akama...</td>
<td>80</td>
<td>HyperText Transfer Protocol</td>
<td>5.9</td>
<td>Infrastructure and C...</td>
<td><a href="http://turnerhc">http://turnerhc</a>...</td>
<td></td>
</tr>
<tr>
<td>05/13/2014 1:39:47 AM</td>
<td>HTTP Complete</td>
<td>F340.27.05-ASA55...</td>
<td>Kureli Sankar</td>
<td>turnerhd-f.akama...</td>
<td>80</td>
<td>HyperText Transfer Protocol</td>
<td>5.9</td>
<td>Infrastructure and C...</td>
<td><a href="http://turnerhc">http://turnerhc</a>...</td>
<td></td>
</tr>
<tr>
<td>05/13/2014 1:39:47 AM</td>
<td>HTTP Complete</td>
<td>F340.27.05-ASA55...</td>
<td>Kureli Sankar</td>
<td>turnerhd-f.akama...</td>
<td>80</td>
<td>HyperText Transfer Protocol</td>
<td>5.9</td>
<td>Infrastructure and C...</td>
<td><a href="http://turnerhc">http://turnerhc</a>...</td>
<td></td>
</tr>
<tr>
<td>05/13/2014 1:39:44 AM</td>
<td>HTTP Complete</td>
<td>F340.27.05-ASA55...</td>
<td>Kureli Sankar</td>
<td>turnerhd-f.akama...</td>
<td>80</td>
<td>HyperText Transfer Protocol</td>
<td>5.9</td>
<td>Infrastructure and C...</td>
<td><a href="http://turnerhc">http://turnerhc</a>...</td>
<td></td>
</tr>
<tr>
<td>05/13/2014 1:39:44 AM</td>
<td>HTTP Complete</td>
<td>F340.27.05-ASA55...</td>
<td>Kureli Sankar</td>
<td>turnerhd-f.akama...</td>
<td>80</td>
<td>HyperText Transfer Protocol</td>
<td>5.9</td>
<td>Infrastructure and C...</td>
<td><a href="http://turnerhc">http://turnerhc</a>...</td>
<td></td>
</tr>
<tr>
<td>05/13/2014 1:39:43 AM</td>
<td>HTTP Complete</td>
<td>F340.27.05-ASA55...</td>
<td>Kureli Sankar</td>
<td>turnerhd-f.akama...</td>
<td>80</td>
<td>HyperText Transfer Protocol</td>
<td>5.9</td>
<td>Infrastructure and C...</td>
<td><a href="http://turnerhc">http://turnerhc</a>...</td>
<td></td>
</tr>
<tr>
<td>05/13/2014 1:39:41 AM</td>
<td>HTTP Complete</td>
<td>F340.27.05-ASA55...</td>
<td>Kureli Sankar</td>
<td>turnerhd-f.akama...</td>
<td>80</td>
<td>HyperText Transfer Protocol</td>
<td>5.9</td>
<td>Infrastructure and C...</td>
<td><a href="http://turnerhc">http://turnerhc</a>...</td>
<td></td>
</tr>
<tr>
<td>05/13/2014 1:39:39 AM</td>
<td>HTTP Complete</td>
<td>F340.27.05-ASA55...</td>
<td>Kureli Sankar</td>
<td>turnerhd-f.akama...</td>
<td>80</td>
<td>HyperText Transfer Protocol</td>
<td>5.9</td>
<td>Infrastructure and C...</td>
<td><a href="http://turnerhc">http://turnerhc</a>...</td>
<td></td>
</tr>
<tr>
<td>05/13/2014 1:39:37 AM</td>
<td>HTTP Complete</td>
<td>F340.27.05-ASA55...</td>
<td>Kureli Sankar</td>
<td>turnerhd-f.akama...</td>
<td>80</td>
<td>HyperText Transfer Protocol</td>
<td>5.9</td>
<td>Infrastructure and C...</td>
<td><a href="http://turnerhc">http://turnerhc</a>...</td>
<td></td>
</tr>
</tbody>
</table>
## Events – Customer tabs

### Customize columns
Drag/drop or double click column names to add to Selected.
Use Ctrl key to select multiple

<table>
<thead>
<tr>
<th>Available</th>
<th>Selected</th>
</tr>
</thead>
<tbody>
<tr>
<td>AVC App Behavior</td>
<td>Receive Times</td>
</tr>
<tr>
<td>Action</td>
<td>Event Type</td>
</tr>
<tr>
<td>Application Type</td>
<td>Device</td>
</tr>
<tr>
<td>Attacker</td>
<td>Source</td>
</tr>
<tr>
<td>Attacker IP</td>
<td>Destination</td>
</tr>
<tr>
<td>Auth Policy Name</td>
<td>Destination Port</td>
</tr>
<tr>
<td>Auth Realm Name</td>
<td>Application</td>
</tr>
<tr>
<td>Auth Retry Count</td>
<td>Reputation Score</td>
</tr>
<tr>
<td>Auth Server Name</td>
<td>Threat</td>
</tr>
<tr>
<td>AuthType</td>
<td>Web Category</td>
</tr>
<tr>
<td>Backtrace</td>
<td>URL</td>
</tr>
<tr>
<td>Byte Count</td>
<td>Policy Name</td>
</tr>
<tr>
<td>ClientOS</td>
<td></td>
</tr>
<tr>
<td>Config Version</td>
<td></td>
</tr>
</tbody>
</table>
Events – Two modes

Real time eventing – user defined refresh interval

Historic eventing – user defined time range
## Event - Details

An HTTP transaction passed policy constraints and completed normally.

### Event details

<table>
<thead>
<tr>
<th>Source</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Kurei Sankar</td>
</tr>
<tr>
<td>Realm</td>
<td>CX.com(AD)</td>
</tr>
<tr>
<td>IP address</td>
<td>14.36.109.13</td>
</tr>
<tr>
<td>Port</td>
<td>63711</td>
</tr>
<tr>
<td>Interface</td>
<td>inside</td>
</tr>
<tr>
<td>Identity</td>
<td>active</td>
</tr>
<tr>
<td>Remote device</td>
<td>No</td>
</tr>
<tr>
<td>Client OS name</td>
<td></td>
</tr>
<tr>
<td>Context name</td>
<td>kurei</td>
</tr>
</tbody>
</table>

### Destination

<table>
<thead>
<tr>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
</tr>
<tr>
<td>Port</td>
</tr>
<tr>
<td>Interface</td>
</tr>
<tr>
<td>Service</td>
</tr>
<tr>
<td>Host</td>
</tr>
<tr>
<td>URL</td>
</tr>
<tr>
<td>URL category</td>
</tr>
<tr>
<td>Web reputation</td>
</tr>
<tr>
<td>Threat type</td>
</tr>
</tbody>
</table>

### Transaction

<table>
<thead>
<tr>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection ID</td>
</tr>
<tr>
<td>Transaction ID</td>
</tr>
<tr>
<td>Component name</td>
</tr>
<tr>
<td>Bytes sent</td>
</tr>
<tr>
<td>Bytes received</td>
</tr>
<tr>
<td>Total bytes</td>
</tr>
<tr>
<td>Request content type</td>
</tr>
<tr>
<td>Response content type</td>
</tr>
<tr>
<td>HTTP response status</td>
</tr>
<tr>
<td>HTTP app detected phase</td>
</tr>
<tr>
<td>Configuration version</td>
</tr>
<tr>
<td>Error details</td>
</tr>
</tbody>
</table>

### TLS

- Decrypted flow
- Requested domain
- Ambiguous destination
- Server certificate name
- Server certificate issuer
- TLS version
- Server cipher suite
- Error Details
## Event - Details

### Identity Policy
- **Used by devices:** F340.27.05-ASA5500-1
- **Policy set type:** Identity
- **Number of Policies:** 1

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Application</th>
<th>Action/Conditions</th>
<th>Interface Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Custom - 14.36.109.x</td>
<td>ANY</td>
<td></td>
<td>Active authentication</td>
<td>ANY to ANY</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Realm: CX.com(AD) (Basic)</td>
<td></td>
</tr>
</tbody>
</table>

### ASA-5512-Policy_Set
- **Used by devices:** F340.27.05-ASA5500-1
- **Policy set type:** Access
- **Number of Policies:** 1

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Application</th>
<th>Action/Conditions</th>
<th>Interface Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 ANY</td>
<td>ANY</td>
<td></td>
<td>Conditional Allow</td>
<td>ANY to ANY</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Profiles:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Web Reputation -6 to -10</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Deny Threats</td>
<td></td>
</tr>
</tbody>
</table>
Reporting

Network Overview

Device summary

<table>
<thead>
<tr>
<th>Device Name</th>
<th>Alert</th>
<th>CPU</th>
<th>Memory</th>
<th>Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA CX</td>
<td>F340,27.05-ASA5500-1</td>
<td>No alerts</td>
<td>max 0%</td>
<td>avg 0%</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>min 0%</td>
<td>min 32%</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>avg 32%</td>
<td>avg 32%</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>max 0 b/s</td>
<td>min 0 b/s</td>
</tr>
</tbody>
</table>
Reporting

Generate report
Please choose options to generate a report. Your report will be generated in PDF format.

Report type
- Application and web destination
  - Top 25 applications
  - Top 25 application types
  - Top 25 web destinations
  - Top 25 web categories

Time range
- Last 30 minutes

Report logo
- Upload logo
- 100 pixels wide, 80 pixels tall, .jpg, .gif or .png,
  8KB max
- Use default logo

Application and web destination
- Administrative
- User and device
- Threat analysis
- Application and web destination

Generate
# Top 25 Users by transactions

**09 May 2014, 04:31:24 PM (UTC) to 16 May 2014, 04:31:24 PM (UTC)**

<table>
<thead>
<tr>
<th>User name</th>
<th>Transactions</th>
<th>Bytes</th>
<th>Applications</th>
<th>Top 5 by transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 CX.com(AD)(Kureeli Sankar)</td>
<td>79.0 K 78.0 K 132</td>
<td>3.0 GB 40.0 MB 3.0 GB</td>
<td>HyperText Transfer Protocol 77.0 K</td>
<td>Infrastructure and Content Delivery 75.0 K</td>
</tr>
<tr>
<td>2 14.36.109.57</td>
<td>11.0 K 11.0 K 0</td>
<td>1.0 GB 7.0 MB 1.0 GB</td>
<td>SSL 2.0 K</td>
<td>Computer Security 4.0 K</td>
</tr>
<tr>
<td>3 14.36.109.13</td>
<td>4.0 K 4.0 K 182</td>
<td>7.0 MB 655.0 KB 6.0 MB</td>
<td>Transport Layer Security Protocol 782</td>
<td>Search Engines and Portals 408</td>
</tr>
<tr>
<td>4 CX.com(AD)(Administ rator)</td>
<td>2.0 K 2.0 K 30</td>
<td>40.0 MB 1.0 MB 38.0 MB</td>
<td>HyperText Transfer Protocol 973</td>
<td>Search Engines and Portals 548</td>
</tr>
<tr>
<td>5 14.36.109.56</td>
<td>993 993 0</td>
<td>93.0 KB 46.0 KB 46.0 KB</td>
<td>Network Time Protocol 993</td>
<td>Search Engines and Portals 158</td>
</tr>
</tbody>
</table>
Agenda

Introduction to NGFW Deployment
Software Architecture Licensing
How to configure policies Management and Eventing

Use cases
Troubleshooting tips
Use Case 1: Managing High Availability

OFF box PRSM is mandatory
Configure stateful failover via CLI or ASDM
HTTP Replication must be enabled
Add the devices to the PRSM inventory
Use Case 1: Managing High Availability

- When one ASA is imported into PRSM, the other unit is discovered and both devices are imported together.
- In most respects PRSM treats pair as single device
- HA properties can be modified after import using PRSM
  - Add or modify Stateful failover link
  - Enable or disable HTTP replication
Use Case 2: How to upgrade PRSM?

Simply drag and drop

Dashboard | Events | Configurations | Components | Administration
---|---|---|---|---
Users | Licenses | PRSM logs | Server Certificates | Database backup | Upgrade | Change history | End user notification | Quit

Upgrade Manager

Upload an upgrade package

Drag files or click this area to upload
Use Case 3: How to control Application Usage

How to allow all IM applications, such as Yahoo Messenger, Google Talk, and AOL Instant Messenger, yet block all “audio” file transfers through IM applications.
Use Case 3: How to control Application Usage

Profile
- Bandwidth limit: No Limit
- Safe search: On
- File filtering: kusankar - audio file block
- Web reputation
- NG IPS

Interface roles
- Tags: Enter associated keyword
- Ticket ID: Enter Ticket ID strings

* required fields

View File filtering profile
- Name: kusankar - audio file block
- Object type: File filtering profile
- Description
- Tags: --
- Ticket ID: --
- Status: Committed
- Created: May 15, 2014 by admin
- Last modified: May 15, 2014 by admin

Usage
- Block file downloads: audio/*
- Block file uploads: audio/*
- audio
- audio/*
- audio/basic
- audio/midi
- audio/mp4
- audio/MP4A-LATM
- audio/mpeg
- audio/unknown
Use Case: 4 How to allow Facebook but block uploading photos and videos
Agenda

Introduction to NGFW
Deployment
Software Architecture
Licensing
How to configure policies
Management and Eventing
Use cases
Troubleshooting tips
Problem 1: Unable to session into the module

Symptom: “show module” shows that the module is fine and it is running the image 9.2.1.2.82 but, “session cxsc console” doesn’t work.

Troubleshooting steps:
1. Issue “show module cxsc log console” and look for clues
2. Check the code compatibility chart in the release note page for the CX code and make sure the CX code and the ASA code are compatible.
Problem 2: Latency issues loading certain websites

Symptom: Some websites load very slowly.

1. Is this particular traffic being inspected by CX?
   – Issue the command “show service-policy flow tcp host s.s.s.s host d.d.d.d eq 80” and make sure CX shows up in the path. We could use “packet-tracer” command as well.
2. Is decryption enabled for the flow?
3. Is NG-IPS enabled for the flow?
4. Try to exempt the traffic from being scanned by the CX module to narrow down the problem.
5. Verify and make sure the CX is running all the latest updates for AVC, WSE etc.
Problem 3: How to clear ASA console session to CX

**Symptom:** Unable to session into the module

ciscoasa# session cxsc console
ERROR: An existing console session is in progress with module cxsc. Only one is allowed at any point in time.
ciscoasa#

**Solution:**
ciscoasa# kill 0
Problem 4: Certificate and Decryption Problems with CX

Symptom: https sites do not load

This Connection is Untrusted
You have asked Firefox to connect securely to www.facebook.com, but we can't confirm that your connection is secure.

 Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Got me out of here!

Technical Details
www.facebook.com uses an invalid security certificate.
The certificate is not trusted because the issuer certificate is not trusted.
(Error code: sec_error_untrusted_issuer)

I Understand the Risks
If you understand what's going on, you can tell Firefox to start trusting this site's identification. Even if you trust the site, this error could mean that someone is tampering with your connection.

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

Add Exception...
Problem 4: Certificate and Decryption Problems with CX

![Certificate Viewer for Facebook.com](image)

Certificate Viewer for Facebook.com

- **Could not verify this certificate for unknown reasons.**
- **Issued To**: *facebook.com*
- **Issued By**: *cx.cisco.com*
- **Validity**:
  - **Issued On**: 6/20/2012
  - **Expires On**: 12/31/2013
- **Fingerprints**:
Problem 4: Certificate and Decryption Problems with CX

- Export the cert
- Install it in the client
Problem 5: High CPU issue what data do we gather?

From the CX CLI gather the following data

```
show tech
show opdata interface
show opdata framedrop
show opdata flowdrop
show opdata block
show opdata pdts summary
show opdata pdts all
```
Test for understanding (TFU)

1. What model ASAs support the software CX module?
   5512-5555

2. Why does the CX module need the boot software?
   To boot into rommon mode if needed.

3. Social networking category is blocked according to policy configured, but the browser is able to load the site. What could be the problem?
   May be the site is loading via https and decryption is not enabled.

4. What kind of certificate will not work for decryption?
   “end” cert or “wild-card” cert from a major certificate authority.

5. Where should one go in order to make sure the CX code is compatible with the ASA code?
   Release Note for CX

6. When opening a TAC case online what data is critical to include?
   “sh tech” and “logs”
Summary

Deploy NGFW services. Filter content and increase productivity

Action item: Please reach out to your local Cisco account team upon returning and have one of them come out; size and price the Next-Generation Firewall Services for your enterprise.
Useful CX links:


Useful PRSM links:

Code download:

Release Note:

Configuration guide:

Command Reference guide:
Useful CDA links:

CDA download:

CDA release note:

CDA: Configuration guide:

CDA Command reference:
Participate in the “My Favorite Speaker” Contest

Promote Your Favorite Speaker and You Could be a Winner

• Promote your favorite speaker through Twitter and you could win $200 of Cisco Press products (@CiscoPress)

• Send a tweet and include
  – Your favorite speaker’s Twitter handle <jmckg>
  – Two hashtags: #CLUS #MyFavoriteSpeaker

• You can submit an entry for more than one of your “favorite” speakers

• Don’t forget to follow @CiscoLive and @CiscoPress

• View the official rules at http://bit.ly/CLUSwin
Complete Your Online Session Evaluation

• Give us your feedback and you could win fabulous prizes. Winners announced daily.

• Complete your session evaluation through the Cisco Live mobile app or visit one of the interactive kiosks located throughout the convention center.

Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at CiscoLive.com/Online
Continue Your Education

• Demos in the Cisco Campus
• Walk-in Self-Paced Labs
• Table Topics
• Meet the Engineer 1:1 meetings
• WoS (World of Solutions)

• BRKSEC-2902 - Embrace Cloud Web Security with your Cisco Network
  Moscone West 3012, Tuesday May 20th 8am PDT

• BRKSEC-2042 Web Filtering and Content Control in the Enterprise
  Thursday May 22nd 12:30pm PDT
Thank you.