Secure Your Network with the ASA CX Context-Aware Firewall
Forward-Looking Statements

“Many of the products and features described herein remain in varying stages of development and will be offered on a when-and-if-available basis. This roadmap is subject to change at the sole discretion of Cisco, and Cisco will have no liability for delay in the delivery or failure to deliver any of the products or features set forth in this document.”
Network Security Challenges

Managing Complexity: Trying to Stay Above Water

Massive surge in applications, devices, mobility
Current access controls don’t go far enough

Compromise: Productivity or Security

Demands for anytime, anywhere, any device access
Porous borders, little control

Forced to choose: “Next-Gen” Firewall or Classic Firewall

Rebuilding access control: costly and risky
Application-based access control is not deterministic
ASA CX

End-to-End Intelligence
Granular Control
Safely Enable
  Applications
  Users
  Devices
Leading threat protection
Extensible architecture
ASA CX is part of SecureX

- Context-Aware Firewall
- Unified Endpoint Client
- Guest Access, Posture, Profiling
- Network-Wide Enforcement
Cisco ASA CX
Complete Context Awareness. Proven Cisco Technology.

Context-Aware
Cisco ASA CX

Classic ASA Firewall

Distributed
Appliance  Integrate  Virtual
Complete Context

Visibility with Control

Productivity with Security

Next-Generation with Stateful
Complete Context. Plus Threat Awareness.
Complete Context. Plus Threat Awareness.

Cisco SIO
SensorBase  Threat Operations Center  Dynamic Updates
Cisco Prime Security Manager

Simple
Efficient
Standards-based

Cisco ASA CX

Context-Aware
Threat Aware

Classic ASA Firewall

© 2010 Cisco and/or its affiliates. All rights reserved.
Thank you.

More information at cisco.com/go/asacx
ASA CX and PRSM

Brian Conklin – Technical Marketing Engineer
Danny Anello – Technical Marketing Engineer
Agenda

• ASA CX
  Overview
  Architecture

• Prime Security Manager (PRSM)
  Overview
  Management Architecture

• Demo

• Q&A
ASA CX

- Context-Aware Firewall
- Active/Passive Authentication
- Application Visibility and Control
- Reputation Filtering
- URL Filtering
- Secure Mobility
- SSP-10 and SSP-20 at FCS
- Availability on SSP-40 and SSP-60 after
ASA CX – Front View

Order separate blades or chassis bundle
CX Architecture
ASA CX – Front View

New
Two Hard Drives
Raid 1 (Event Data)

New
8 GB eUSB
(System)

10GE and GE ports

Two GE Management Ports
Send traffic to CX SSP

• Use MPF to direct traffic to the CX blade:

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

service-policy global_policy global
```

• PRSM Multi-device applies this when connecting to CX:
Policy types

- Authentication
  - How to identify user?

- Decryption
  - What to decrypt?

- Access
  - Allow or Deny?
### Policy types - Screenshot

#### Access
- **Features enabled:**
  - ![Feature 1]
  - ![Feature 2]
  - ![Feature 3]

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Application</th>
<th>Action/Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 ANY</td>
<td>ANY</td>
<td></td>
<td>Allow</td>
</tr>
</tbody>
</table>

#### Authentication
- **Features enabled:**
  - ![Feature 1]
  - ![Feature 2]
  - ![Feature 3]

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Action/Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 ANY</td>
<td>ANY</td>
<td></td>
</tr>
</tbody>
</table>

**Use Identity When Available**
- Realm: seclabs

#### Decryption
- **Features enabled:**
  - ![Feature 1]
  - ![Feature 2]
  - ![Feature 3]

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Action/Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

There are no policies in this policy set.
Authentication Realm

- **Realm**: Logical group of trusted Directory Servers (AD or LDAP)

- **Active Directory**
  - One Realm
  - One Domain (joins the domain)
  - AD Agent for passive authentication
  - Kerberos, NTLM, or Basic for active authentication

- **LDAP**
  - Multiple Realms
  - Basic authentication only
Decryption

- Decrypt TLS/SSL traffic across any port
- Self-signed (default) certificate or customer certificate/key
- Based on FQDN, URL Category, User/Group, Device type, IP address, or Port
- FQDN and URL Category are determined using server certificate
Access

- Allow or Deny the transaction based on full context

- Other possible actions:
  - Create Event (on by default)
  - Capture Packets (off by default)

- Also applied to HTTP Traffic:
  - File Filtering Profile
    - Apply added filtering based on MIME type
  - Reputation Profile
    - Apply added filtering based reputation score of destination
      (default profile drops -6.0 and below and is not active)
Day-in-the-life of a packet
(One possible flow. May be different for other traffic.)

Auth/Access Policy
Check L3/L4 and Identity Access Policies

Broad AVC
Determine Protocol and Application

TCP Proxy
Handle TCP 3-way handshake

TLS Proxy
Proxy encryption to decrypt traffic for inspection

HTTP Inspector
Determine Application, URL Category, Reputation, User Agent

Active Auth
If passive auth not available, authenticate using NTLM, Kerberos, or Basic auth

Access Policy
Allow or Deny verdict based on access policy

Packet Egress
Return packet back to the ASA SSP with an allow verdict
Compatibility with Existing ASA Features

- **IPv6**: supported
- **Failover**: active/standby
- **Transparent Mode**: supported
- **VPN**: supported
Prime Security Manager (PRSM)
Cisco Prime Security Manager (PRSM)

Build-in

- Configuration, Eventing, and Reporting

Off-box

- Multi-device Manager for ASA CX
- Role Based Access Control
- Virtual Machine or UCS Appliance

Virtual Machine supports VMWare ESX 4.1
Management Architecture
Management Architecture - Today

CLI

Manager

Syslog

Syslog Server or SIEM

SNMP
Management Architecture - Today

Manager

CLI

Admin

Syslog

Server or SIEM

Syslog

SNMP

X
Management Architecture – ASA CX/PRSM

ASA CX ➔ HTTPS ➔ PRSM

Admin

© 2010 Cisco and/or its affiliates. All rights reserved.
Management Architecture – ASA CX/PRSM

RESTful XML

ASA CX  Reliable Binary Logging  PRSM
Management Architecture – ASA CX/PRSM
Why Cisco Prime Security Manager?

Schema Driven
Single and multi-device management

Innovative Web 2.0 architecture

User persona centric GUI design
ASA CX and PRSM

Visibility with Control
Productivity with Security
Next-Generation with Stateful Firewall
Demo
ASA CX and PRSM
Thank you.