

*TOMORROW starts here.*



Cisco *live!*

# Advanced Web Security Deployment with WSA and ASA-CX

BRKSEC-3771

Andrew Wurster

Network Consulting Engineer

Your personal files are encrypted!



I hope you have backups. **It's legit**, it really encrypts. It **can jump across mapped network drives... encrypt anything with write access...** infection isn't dependent on being a local admin or UAC state... **antiviruses do not catch it... timer is real** and your opportunity to pay them goes away when it lapses.

**Reality: Crypto Locker in Australia**

Source: [Reddit](#)



Private key will be destroyed on  
10/19/2013  
6:09 PM

Time left  
**71 : 59 : 33**





“ “  
According to Cisco ...

**malicious traffic is visible on 100 percent of corporate networks...** there is evidence that sophisticated criminals or other players have penetrated these networks and may be operating undetected over long periods of time.

Source: [Cisco Annual Security Report, 2014](#)

**No time to lose. Let's get started...**

# Session Agenda

- Introduction and House Keeping
- Web Security Refresher
- Securing the Web with ASA-CX
- Advanced Concepts for Web Security Appliance
  - Transparent Redirection
  - Directory Integration
- WSA Operations
  - Logging, Monitoring, and Management
  - Troubleshooting and Debugging

# Pre-requisites

- Suggested Courses:
  - TECSEC-2663 - Cyber Security - Cisco Cyber Range Techtorial
  - BRKSEC-3770 - Advanced Email Security with ESA
  - BRKSEC-2073 - Advanced Threat Defence using NetFlow
  - BRKSEC-2663 - Before. During. After. Cisco's Integrated Security Strategy
  - BRKSEC-2010 - Emerging Threats - The State of Cyber Security
  - BRKSEC-2695 - Embrace Cloud Web Security with your Cisco Network
  - BRKSEC-3660 - Cisco Advanced ASA Firewalls Inside-Out
- Have basic working knowledge of
  - TCP/IP Fundamentals
  - Windows / Linux OS Basics
  - Web Protocol Fundamentals
  - Authentication Fundamentals
  - Cisco's Web Security Appliance

# Housekeeping

- Hold questions and comments – plenty of Question Time at the end
- Keep your gadgets in silent mode
- Take any calls outside
- Do unto others...
- Will re-post slides and distribute via email

- Andrew's tips look like this:



This is an important note!



- Have you had your coffee?!





# Web Security Refresher

360 昂GONG 坪PING 360

1972 km  
公里

People's Republic of China - Great Wall  
中華人民共和國 - 萬里長城

9632 km  
公里

United Kingdom - Big Ben  
英國 - 大笨鐘

Africa - Cape of Good Hope  
非洲 - 好望角

11881 km  
公里

12968 km  
公里

United States of America - Statue of Liberty  
美國 - 自由神像



Web Security Refresher



High Level Review

# Why You WebSec?



## GROWING THREATS

- Day 0 and APTs
- Evolving malware / virus strategies
- Uncontrolled rich web apps and social media



## EVOLVING NETWORKS

- Public WiFi and Home
- Guest and BYOD
- Branch / pop-up offices
- Mobile Workforce



## BUSINESS NEEDS

- Work with the *business*
- Use existing architecture
- Scale with the business and do more with less





Millennials are now entering the workplace and bringing with them **new working practices and attitudes to information and ... security...**

They believe in the demise of privacy—that it's simply defunct in practice, and it's in this paradigm that organisations must operate...

Source: Cisco's [Annual Security Report \(2013\)](#)

**Attacks are now a reality**







Melbourne  
20° NOW 13° MIN

Increasing sunshine  
Traffic Conditions

# THE AGE

INDEPENDENT. ALWAYS.

Subscribe to  
The Age this Christmas,  
now 50% off

FIND OUT MORE



MY NEWS

MY CLIPPINGS

MY COMMENTS

MY HISTORY

MY BENEFITS

SUBSCRIBE

LOG IN

REGISTER



## Ashes Victory

### Late wickets tumble to bring urn home

Australia has reclaimed the Ashes, beating England in the third Test in Perth to take an unassailable 3-0 lead in the five-match series.

Live: Day five, 3rd Ashes Test, Perth

VIDEO



01:44

### Australia wins the Ashes

Australia has won back the Ashes after just three of the five Test series, with a convincing victory at the WACA in Perth.

Advertisement

## Hey Joe, it's time to drop the Santa Claus act



**MICHAEL PASCOE** Assuming he believes the figures, here's the simplified bottom line. 77 Budget surplus scrapped



Things no one will tell fat girls ... so I will




Cop that Kanye: police chief lays



# MONASH University

Make  
Mona  
your f  
prefer

Monast  
Change  
Prefer  
Expo






Melbourne  
20° 13°  
NOW MIN  
Increasing sunshine  
Traffic Conditions



THE AGE  
INDEPENDENT. ALWAYS.

Enter search term

Christmas,  
FIND OUT MORE

SUBSCRIBE LOG IN REGISTER

MY NEWS MY CLIPPINGS MY COMMENTS MY HISTORY MY BENEFITS




### Late wickets tumble to bring urn home

Australia has reclaimed the Ashes, beating England in the third Test in Perth to take an unassailable 3-0 lead in the five-match series.

Live: Day five, 3rd Ashes Test, Perth





VIDEO





Australia wins the Ashes  
Australia has won back the Ashes after just three of the five Test series, with a convincing victory at the WACA in Perth.

01:44






Potential threats



Things no one will tell fat girls ... so I will

Advertisement



Cop that Kanye: police chief lays out

want a range or the better?



of nce

Make Mona your preferred



Monash Change Preferred Expo

162 Distinct Objects

2 x HTML docs

4 x Style Sheets

111 x Images

14 x Scripts

7 x Flash / Adv. Content

18 x Errors

Name Path	Method	Status Text	Type	Initiator	Size Content	Time Latency	Timeline
www.googleadservices.com/page		NOT MODIFIED		parser	8.2 KB	71 ms	
57568X1347946.skimlinks.js	GET	(pending)	Pending	www.theage.co.. Parser	13 B	Pending	
s.skimresources.com/js					0 B		
survey-launch.js?rj0046-fd	GET	(failed)	Pending	www.theage.co.. Parser	13 B	8 ms	
secure-au.immworldwide.com/s					0 B		
j?ci=rj0120&se=1&te=0	GET	(failed)	Pending	www.theage.co.. Parser	13 B	8 ms	
secure-au.immworldwide.com/c					0 B		
MetroMastheads.js	GET	(failed)	Pending	s_code.js:16 Script	13 B	8 ms	
www.adobetag.com/d1/fairfaxi					0 B		
ga.js	GET	304	text/javascript	(index):7026 Script	257 B	164 ms	
www.google-analytics.com		Not Modified			39.1 KB	161 ms	
fd.registrars.images.httppipe...	GET	304	applicat...	www.theage.co.. Parser	364 B	38 ms	
resources.theage.com.au/comm		Not Modified			1.1 KB	32 ms	
amc.js	GET	(failed)	Pending	(index):7074 Script	13 B	20 ms	
www.adobetag.com/d1/v2/ZDE					0 B		
?random=1387260328428&...	GET	302	text/html	conversion.js:18 Script	889 B	187 ms	
googleads.g.doubleclick.net/pa		Found			0 B	168 ms	
itunes_autolinkmaker.js	GET	304	applicat...	(index):7079 Script	309 B		
autolinkmaker.itunes.apple.com		Not Modified					

27 x Unique Domains

29 x Unique Hosts

107 x Kilobytes Downloaded

### Australia wins the Ashes

Australia has won back the Ashes after just three of the five Test series, with a convincing victory at the WACA in Perth.



MONASH University

Monash Change Preference Expo



# How do you keep up?

## Block access by URLs?

or maybe even IP blocks?!?

## Allow unfiltered access by AD group?

Ok getting better... sort of.

## Bypass controls for trusted IP's?

you are laughing because it's true. the hackers are laughing too 😊



360 昂 NGONG 坪 PING 360

1972 km  
公里

People's Republic of China - Great Wall  
中華人民共和國 - 萬里長城

9632 km  
公里

United Kingdom - Big Ben  
英國 - 大笨鐘

Africa - Cape of Good Hope  
非洲 - 好望角

11881 km  
公里

12968 km  
公里

United States of America - Statue of Liberty  
美國 - 自由神像

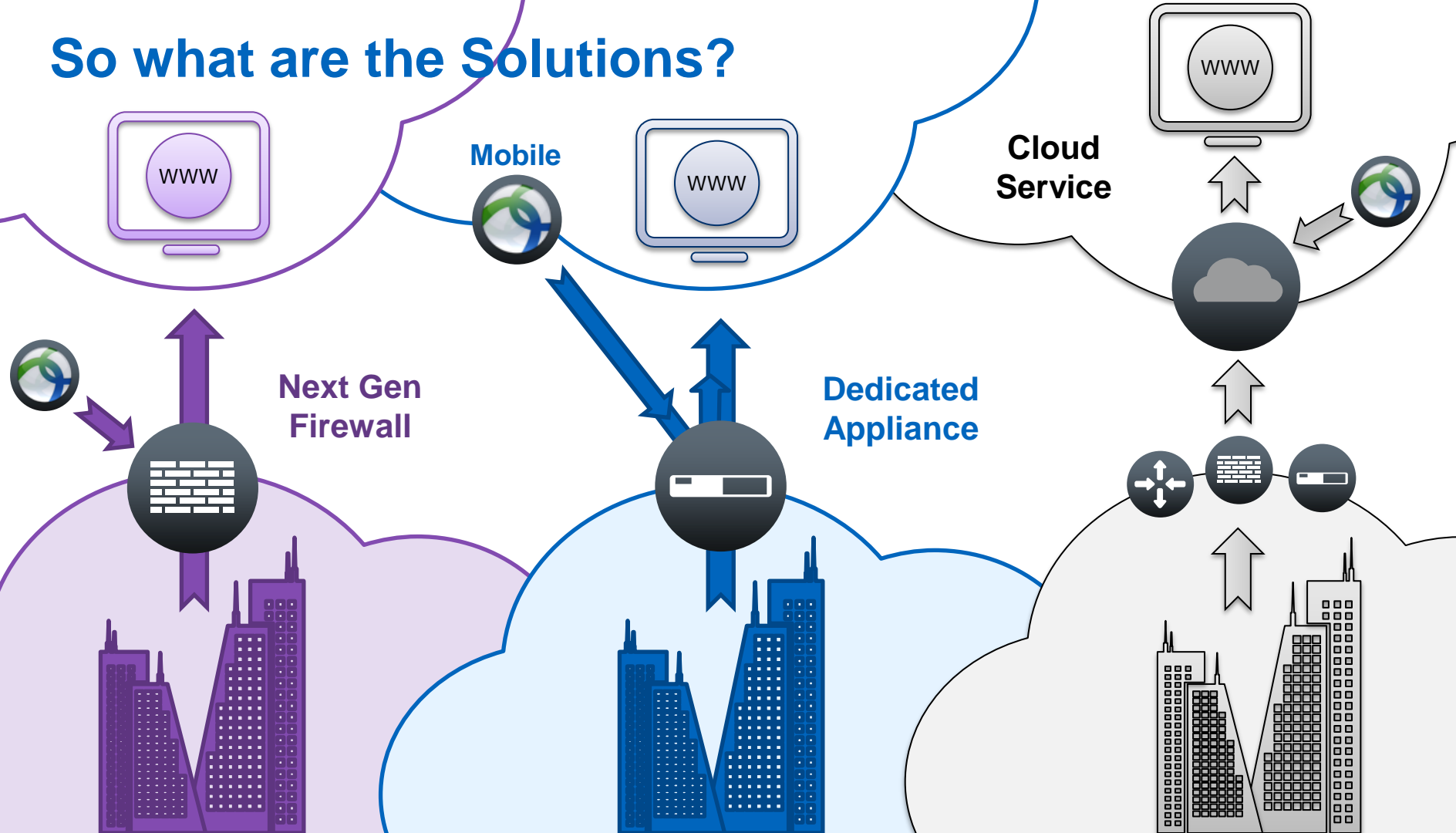


Web Security Refresher

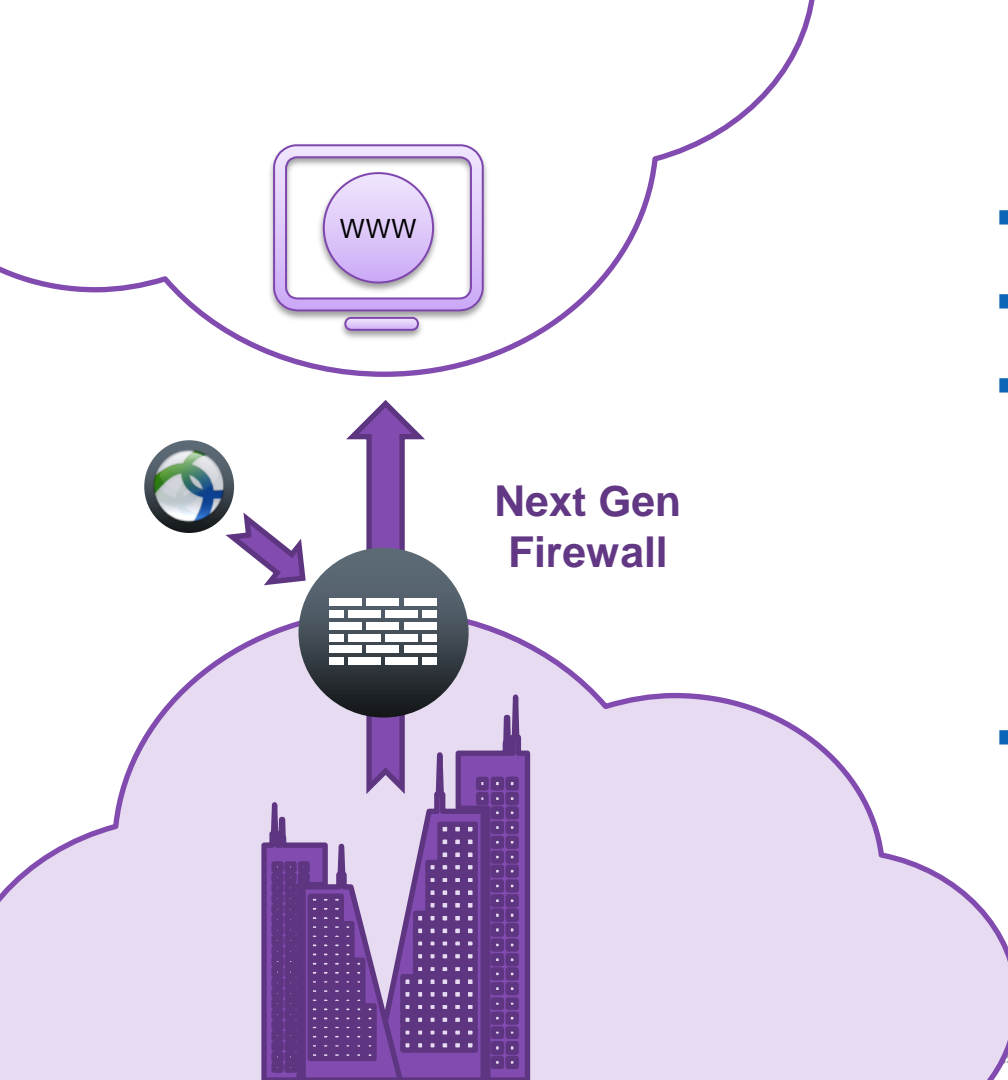


Solutions Overview

# So what are the Solutions?



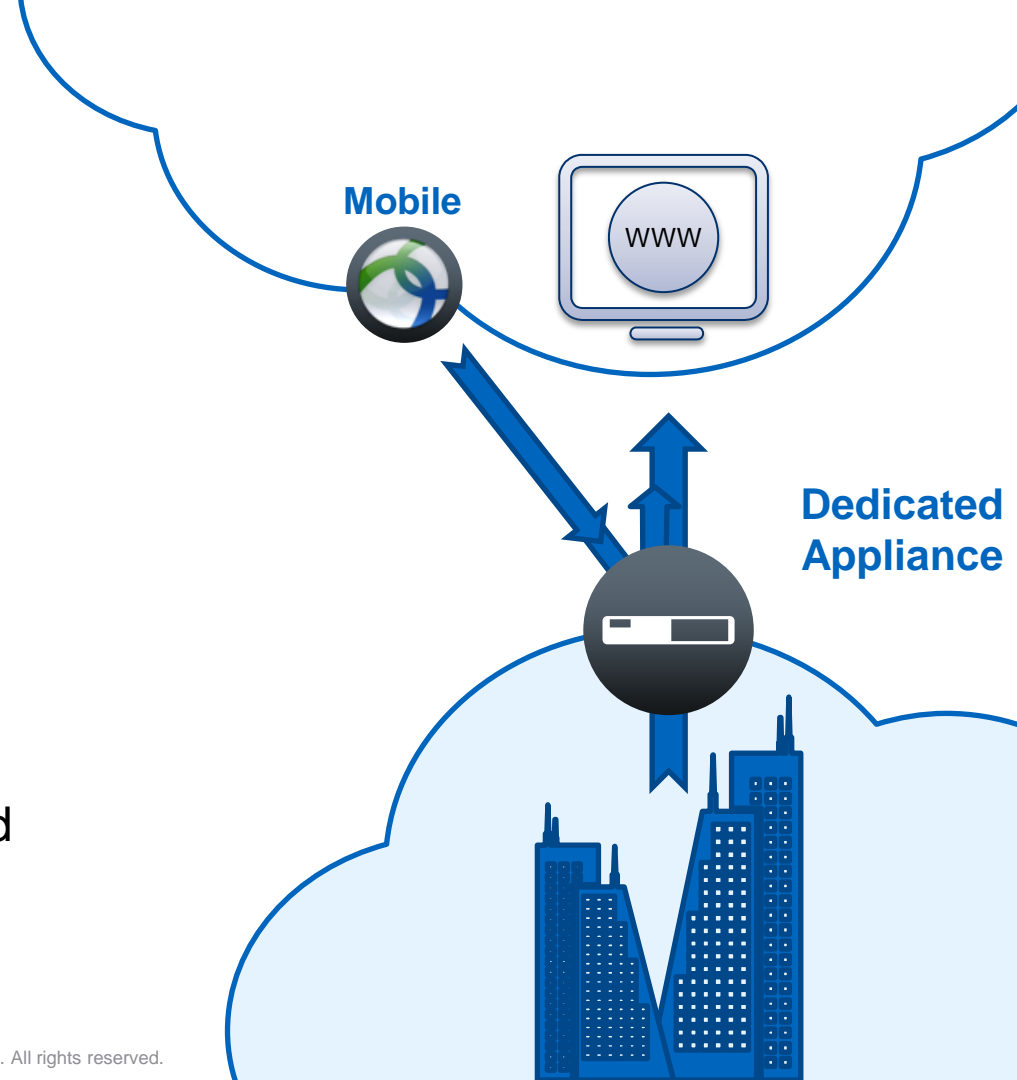
# On-premises: ASA CX



- ASA 5500-x with CX blade
- Placed at Edge or major Border
- Transparently capture / redirect outbound traffic
  - Includes HTTP / HTTPS
  - Inspect any port from underlying firewall service policy
  - Layer 2 transparency support
- Next Gen policy framework and UI

# On-premises: WSA

- Web Security Appliances
  - New Sx80 Models
- More Flexible Placement
  - Out of Band of regular traffic patterns
  - Near Edge or major Border
- Transparently capture / redirect outbound traffic
  - Includes HTTP / HTTPS
  - Inspect any port from WCCP engines
- Explicit (direct) connections permitted
- “Advanced” proxy features
  - PAC file server, SOCKS support, etc





# Solution Comparisons – Deployment Modes

	 WSA	 WSAv	 ASA-CX
Transparent			
Explicit			
Inline			
Out of Band			
High Availability			
Flex / Cloud			

# Solution Comparisons – Feature Support

	 WSA	 WSAv	 ASA-CX
HTTP(s) Proxy			
SSL Decryption			
Anti-X Scan			
URL Filtering			
Anomaly Detect			
Central Mgmt			

# Solution Comparisons – Feature Support (Cont)

	 WSA	 WSAv	 ASA-CX
DLP Support			
Non-Web Ports			
Caching			
Directory Auth			
AnyConnect			
Interoperability			



# Securing the Web with ASA-CX





1972 km  
公里  
People's Republic of China - Great Wall  
中華人民共和國 - 萬里長城

9632 km  
公里  
United Kingdom - Big Ben  
英國 - 大笨鐘

11881 km  
公里  
Africa - Cape of Good Hope  
非洲 - 好望角

12968 km  
公里  
United States of America - Statue of Liberty  
美國 - 自由神像

● Securing the Web with  
ASA-CX

● CX Platform Review

# What exactly is CX?

## Software Module (5515-55x)

- Runs CX OS on shared resources from ASA
- Controlled via ASA host and shared management interfaces
- Requires SSD in expansion bay



## Hardware Module (5585x)

- Runs CX OS on dedicated HW blade
- Controlled via ASA host or dedicated management interface
- Requires existing ASA 5585 chassis



# ASA CX Platform Architecture

## Data Plane - Hardware

- CX SSP receives from ASA SSP
- Traffic goes via backplane
- ASA SSP defines a traffic selector for redirection to CX

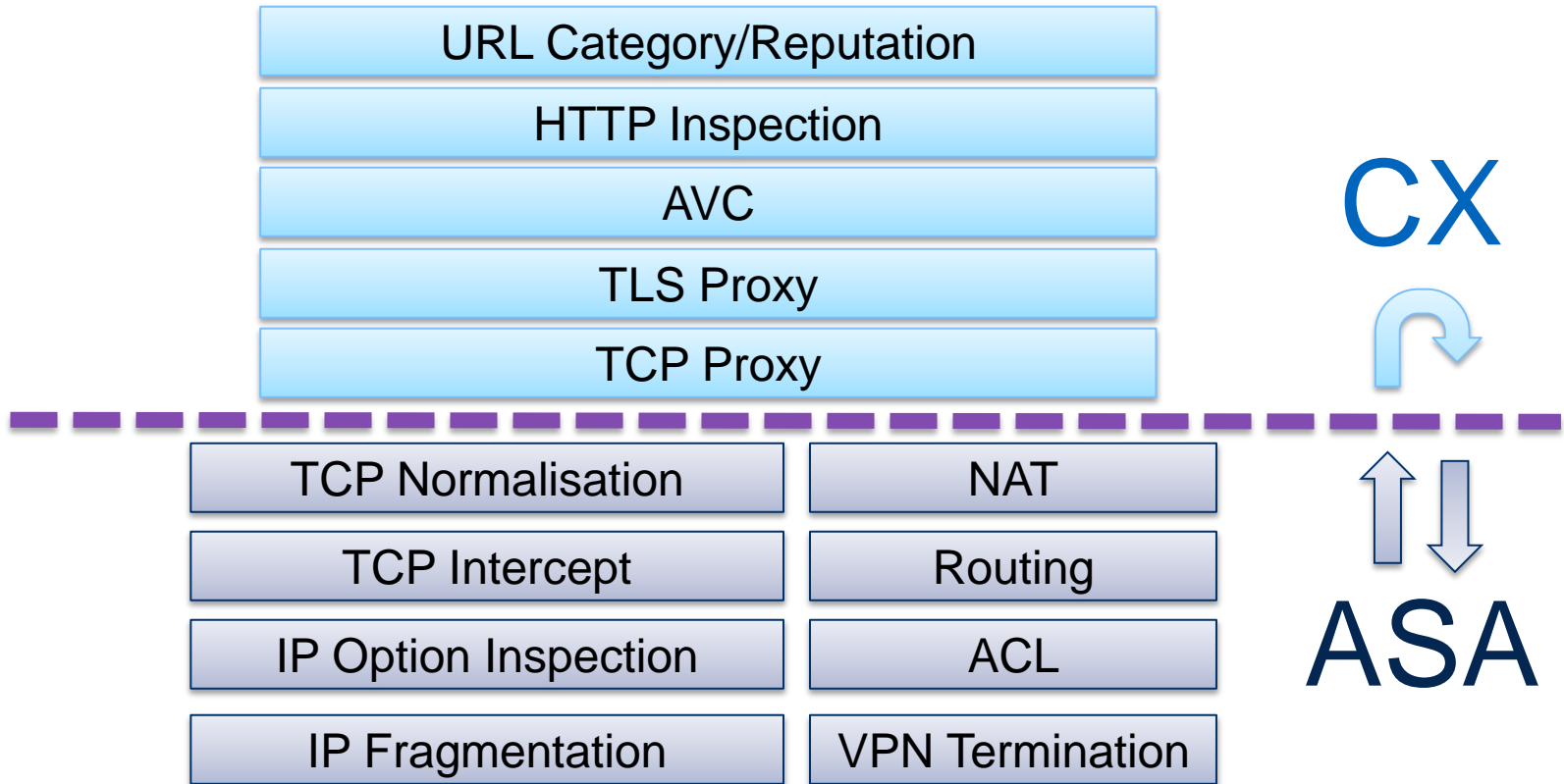
## Data Plane - Software

- CX receives from ASA Backplane
- Dedicated ASA resources for CX

## Management Plane

- Web UI for config / reports
- SMX (off-box) config / events
- AD agent session info
- Signature / software updates
- CLI for bootstrap / diagnostics

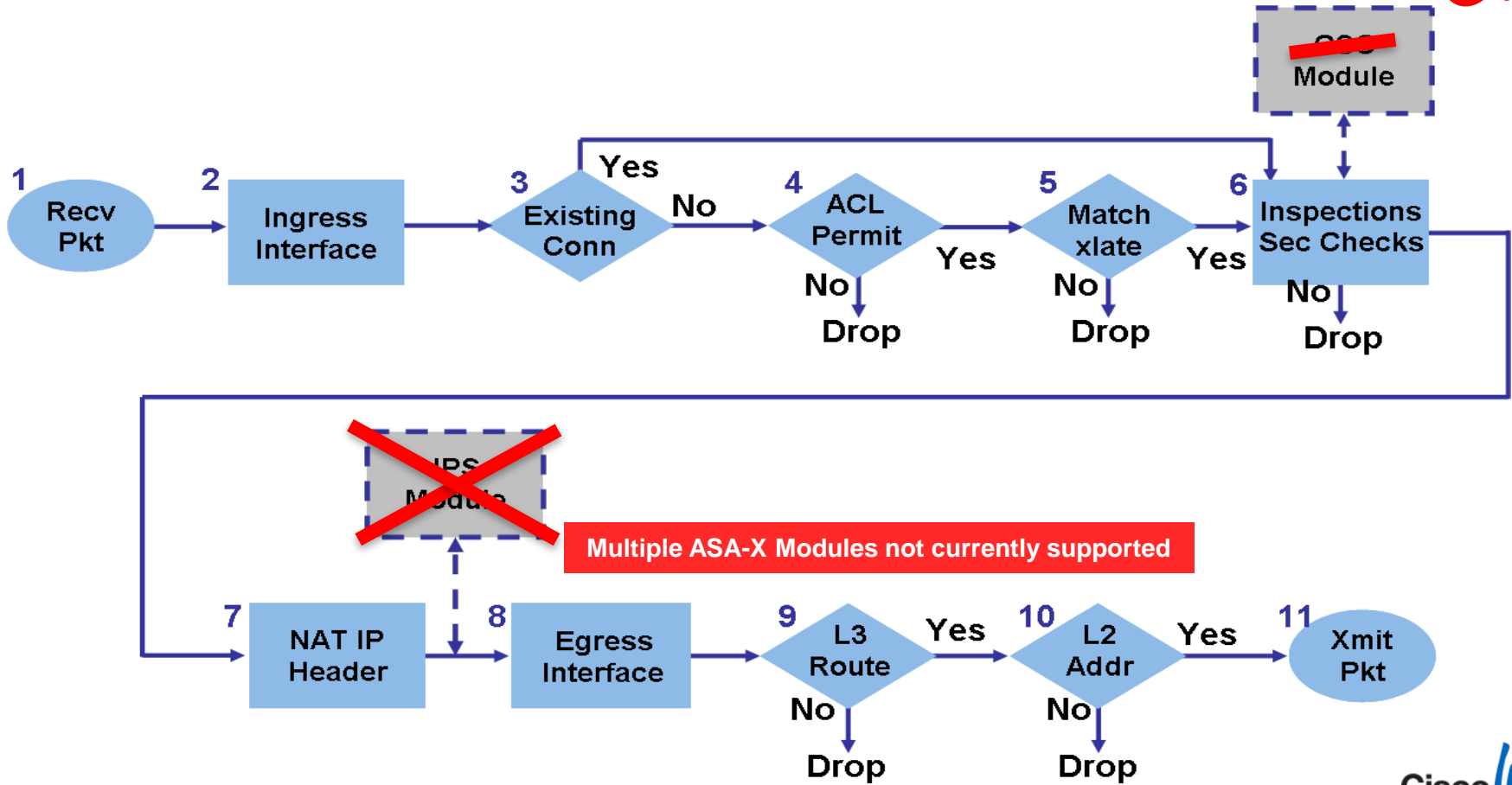
# Separation of Duties





# Packet Processing Flow Diagram

CX



Multiple ASA-X Modules not currently supported

# Configure Traffic Forwarding

```
access-list <match-to-CX>
class-map <class-to-CX>
  match access-list <match-to-CX>
policy-map <policy-to-CX>
  class <class-to-CX>
    CXSC <fail-open/fail-closed>
service-policy <policy-to-CX> <global/interface>
```

ASA  
CLI

## Traffic Redirection Settings

Traffic Redirection

Enable

TCP/UDP Ports

Any

e.g. tcp/80, udp/1-1000

Interfaces

All interfaces

PRSM



1972 km  
公里  
People's Republic of China - Great Wall  
中華人民共和國 - 萬里長城

9632 km  
公里  
United Kingdom - Big Ben  
英國 - 大笨鐘

11881 km  
公里  
Africa - Cape of Good Hope  
非洲 - 好望角

12968 km  
公里  
United States of America - Statue of Liberty  
美國 - 自由神像

● Securing the Web with  
ASA-CX

● CX Policies

# Context Aware Policy Types

Identity



Decryption



Access





# Beyond Ports and Addresses



**Who:** Identity and Authentication



**What:** Application, URL Category, Reputation



**How:** Device, OS, User Agent, Posture



**Where:** Access Location






**When:** Access Time

# First Look: Policy Types

Access

**Access** Policy set type: **Access**  
Number of Policies: 1



Features enabled:   

[Add new policy](#)

Source	Destination	Application/Service	Action/Conditions
--------	-------------	---------------------	-------------------

Decryption

**Decryption** Policy set type: **Decryption**  
Number of Policies: 1

Features enabled:  

[Add new policy](#)

Source	Destination	Action/Conditions
1 ANY	ANY	<b>Always decrypt for inspection</b>

[Delete policy](#) [Edit policy](#) [Duplicate policy](#) [Add above](#) [Move up](#) [Move down](#)

Identity

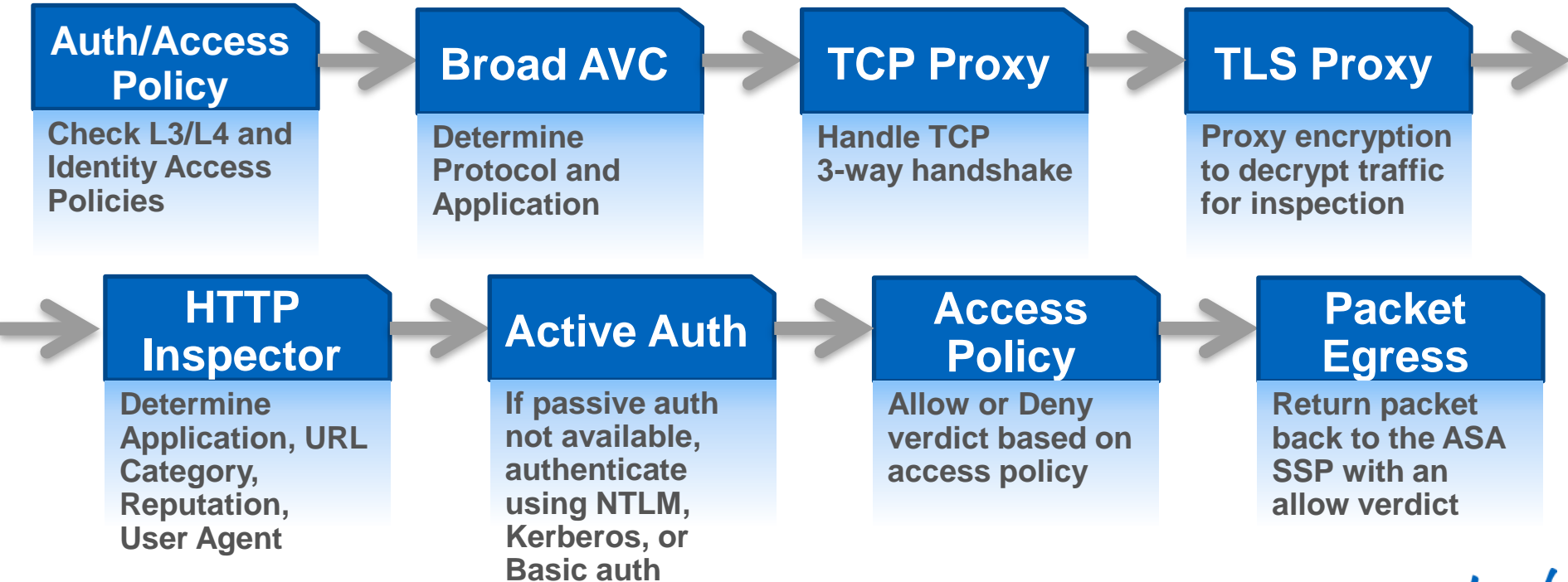
**Identity** Policy set type: **Identity**  
Number of Policies: 1

[Add new policy](#)

Source	Destination	Action/Conditions
1 ANY	ANY	<b>Do not require authentication</b> Realm: isebyodlab

[Delete policy](#) [Edit policy](#) [Duplicate policy](#) [Add above](#) [Move up](#) [Move down](#)

# A Day in the Life of an CX Packet



# Creating Identities: Authentication Realms

## ■ Active Directory

- One realm only
  - Single domain only (joins the domain)
- AD Agent for passive authentication
- Kerberos, NTLM, or Basic for active authentication

## ■ LDAP

- Multiple Realms
- Basic authentication only

The screenshot displays the configuration interface for two authentication realms. The top realm, **CYBERRANGE**, is of type **Standard LDAP**. Its configuration includes the URL `ldap://10.67.34.31:389`, the LDAP login name `CN=ASA CX T, Service,OU=Infrastructure,OU=CyberRange,DC=cybercisco,DC=com`, and the group attribute `dc=cybercisco,dc=com` with a value of `member`. The bottom realm, **CYBERCISCO**, is of type **Active Directory**. Its configuration includes the URL `ldap://10.67.34.31:3268` and the group attribute `member`. A green arrow points from the **CYBERCISCO** realm entry to a detailed configuration form for an Active Directory realm. This form includes the following fields:

- Name\***: CYBERCISCO
- Description**: (empty)
- Directory Type\***: Active Directory
- Primary domain\***: cybercisco.com (e.g. cisco.com)
- Join username\***: asa-cx-service (sAMAccountName)
- Join password\***: (masked with dots)

Below the fields are the options [Test domain join](#) and a note *\* Required*.



# Next Step: Identity Policies

- **Is “identity” required?**
  - Use identity when available (“Passive”)
- **Require identity:**
  - “Passive” Auth if available, otherwise use “Active” Authentication
- **How to identify user?**
  - Basic, NTLM, Kerberos or “Advanced”
- **Exclusions**
  - For the “shoehorn” approach!
  - Really handy for mobiles and legacy apps!

The screenshot shows a 'Create Policy' configuration window. At the top, there is a 'Policy Name' text input field and an 'Enable Policy' toggle switch set to 'On'. Below this, there are three sections for defining the policy's scope: 'Source', 'Destination', and 'Service'. Each section has a text input field with the value 'Any' and a 'Create new object' link. The 'Realm' is set to 'hospital' in a dropdown menu. The 'Action' is set to 'Get identity using AD agent' in a dropdown menu. A question 'Do you want to use active authentication if AD agent can't identify user?' is followed by a 'Yes' toggle switch. The 'Authentication type' is set to 'Advanced' in a dropdown menu, with a note below it stating 'Advanced tries Kerberos first, then NTLM and then Basic. See how to configure'. Finally, there is an 'Exclude user agent' text input field with the value 'Any' and a 'Create new object' link.

# Decision: Decryption Policies?

- **Decrypt TLS / SSL traffic across any port**
  - Self-signed certificate (default) **OR**
  - Specify certificate / key
- Based on:
  - **FQDN** (using server certificate)
  - **URL Category** (using certificate)
  - **Source User / Group**
  - **User Agent** (device type)
  - **Network Details**
  - **Reputation**

The screenshot shows a 'Create Policy' configuration page. At the top, there is a 'Policy Name' input field and an 'Enable Policy' toggle set to 'On'. Below this are three sections for defining the policy scope: 'Source', 'Destination', and 'Service', each with a dropdown menu set to 'Any' and a 'Create new object' link. A note states: 'For URL objects used in decryption policies, URLs containing paths are ignored.' The 'Action' section has a dropdown menu set to 'Decrypt potentially malicious traffic'. The 'Web reputation' section has a dropdown menu set to 'Default Reputation Profile' and a 'Create new profile' link. At the bottom, there are 'Tags' and 'Ticket ID' input fields. A footnote at the bottom left indicates '\* required fields'.

# Taking Action: Access Policies

- **Allow** or **Deny** based on **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 filtering based on reputation score

The screenshot shows the 'Create Policy' configuration page. It includes the following fields and controls:

- Policy Name \***: A text input field.
- Enable Policy**: A toggle switch set to 'On'.
- Eventing**: A toggle switch set to 'On'.
- Policy Action**: A dropdown menu set to 'Allow'.
- Capture packets**: A toggle switch set to 'Off'.
- Source**: A dropdown menu set to 'Any' with a 'Create new object' link below it.
- Destination**: A dropdown menu set to 'Any' with a 'Create new object' link below it.
- Application / Service**: A dropdown menu set to 'Any' with a 'Create new object' link below it.
- Profile**: A section with a right-pointing arrow icon.
- Tags**: A text input field with the placeholder text 'Enter keyword tags'.
- Ticket ID**: A text input field with the placeholder text 'Enter Ticket ID'.

\* required fields



1972 km 公里  
People's Republic of China - Great Wall  
中華人民共和國 - 萬里長城

9632 km 公里  
United Kingdom - Big Ben  
英國 - 大笨鐘

11881 km 公里  
Africa - Cape of Good Hope  
非洲 - 好望角

12968 km 公里  
United States of America - Statue of Liberty  
美國 - 自由神像

● Securing the Web with ASA-CX

● CX Deployment Tips



# Typical CX Deployment Concerns



Will it decrypt or store sensitive data?

Negative. All in memory; tune decryption policies as needed.

How do I silently evaluate or easily insert CX into my network?

Monitor-Mode can help here; so can L2 deployment.

Should I use CX versus WSA? Can they work together?

Depends, let's discuss the deployment needs a bit more...

How do I manage it?  
Can I use SMA / CSM?

No – but support is coming. See your account team for a roadmap.

# CX Policy Guidance



Use policies and other objects sparingly

Establish a naming convention and socialise it across your org

Create dedicated “testing” and “stating” policies

Only apply auth where needed, but can be default.

# More CX Tips...



Fail-close model in critical environments.

Craft WCCP and CX ACLs carefully.

Opt for dedicated PRSM rather than on-box.



1972 km 公里  
People's Republic of China - Great Wall  
中華人民共和國 - 萬里長城

9632 km 公里  
United Kingdom - Big Ben  
英國 - 大笨鐘

11881 km 公里  
Africa - Cape of Good Hope  
非洲 - 好望角

12968 km 公里  
United States of America - Statue of Liberty  
美國 - 自由神像

● Securing the Web with ASA-CX

● CX Wrap Up

# CX: Bringing it all Together

- Leverages existing ASA 5500-x hardware to provide nextgen FW
- Nextgen UI and OS; on top of rock solid, best-in-class HW
- Flexible deployment models
- Awesome, industry-leading AVC support, courtesy of SIO
- Actively being developed; only going to keep getting better





# ASA CX References

	General Availability	Latest Release	Future
CX Release	9.1.2-42	9.2.1-2	???
Min ASA Release	9.1.2(3)	9.1.2(3)	???
Release Date	22-Jul-2013	14 Jan 2014	~ Apr 2014

- [ASA CX and PRSM User Guide](#)
- [ASA CX Introduction Whitepaper](#)
- [ASA CX Data Sheet](#)
- [“Firewalling” Group in Cisco Support Community](#)
- [ASA CX Overview Video \(with Jimmy Ray!\)](#)
- [ASA CX Applications Portal](#)
- [CX / PRSM Compatibility](#)



# Advanced Web Security Appliance Concepts



1972 km  
公里  
People's Republic of China - Great Wall  
中華人民共和國 - 萬里長城

9632 km  
公里  
United Kingdom - Big Ben  
英國 - 大笨鐘

11881 km  
公里  
Africa - Cape of Good Hope  
非洲 - 好望角






12968 km  
公里  
United States of America - Statue of Liberty  
美國 - 自由神像

● Advanced WSA

● High Level Review

# Physical Appliance Models



Deployment	Appliance	Details
SMB / Branch	<b>WSA S170</b> 	1 dual core CPUs, 500GB (2x250), RAID 1, hot swappable HD
Midsize Office	<b>WSA S370</b> 	1 quad core, 1.8TB (4x450), RAID 10, hot swappable HD
	<b>WSA S380</b> 	1 hexa core, 2.4TB (4x600), RAID 10, hot swappable HD
Large Enterprise / Service Provider	<b>WSA S670</b> 	2 quad core, 2.7TB (6x450), RAID 10, hot swappable HD
	<b>WSA S680</b> 	2 octa core, 4.8TB (8x600), RAID 10, hot swappable HD


# Virtual Appliance Models




Web Users				
Web Users	Model	Disk	Memory	Cores
< 1,000	S000v	250 GB	4 GB	1
1,000-2,999	S100v	250 GB	6 GB	2
3,000-6,000	S300v	1024 GB	8 GB	4

**Server**

**Cisco UCS**



**ESXi 4. x 5.0  
Hypervisor**



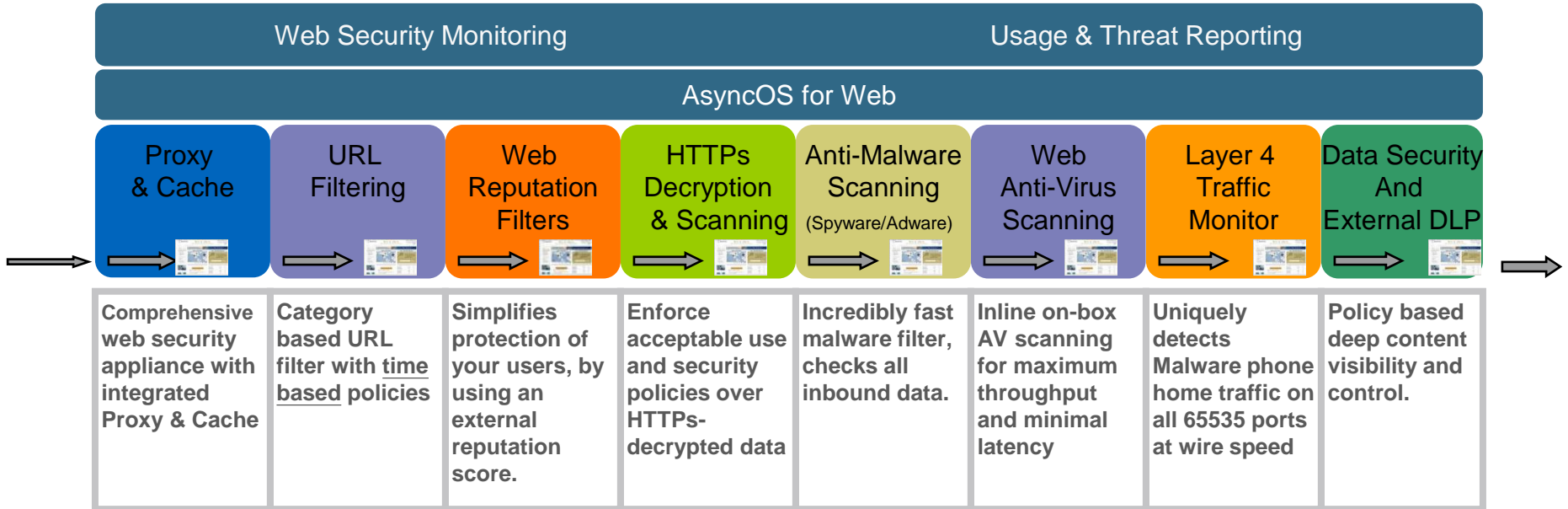
**vmware®**



# WSA's Web Security Pipeline



## Unknown Traffic In



## Clean Traffic Out





1972 km 公里  
People's Republic of China - Great Wall  
中華人民共和國 - 萬里長城

9632 km 公里  
United Kingdom - Big Ben  
英國 - 大笨鐘

11881 km 公里  
Africa - Cape of Good Hope  
非洲 - 好望角

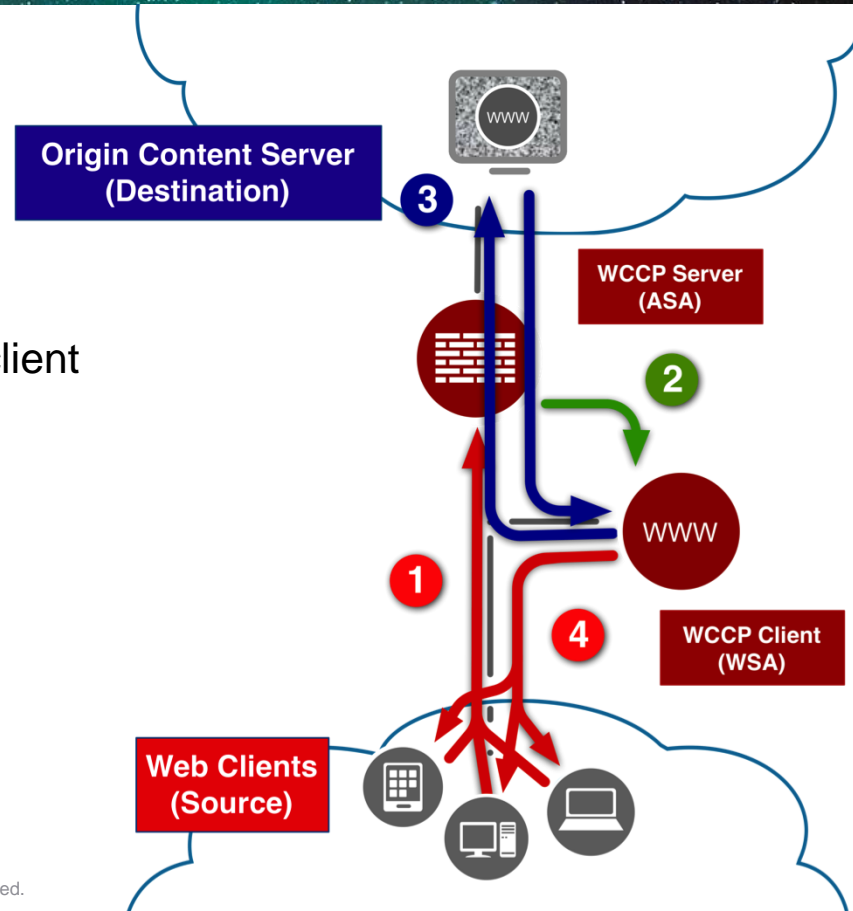
12968 km 公里  
United States of America - Statue of Liberty  
美國 - 自由神像

Advanced WSA

Transparent Redirection

# What is “Transparent Redirection”?

- Transparent Redirection = WCCP
  - WCCP client is the “cache” (WSA here)
  - WCCP server directs the connection (ASA here, but could be many things)
- Client unaware of the proxy
  - WSA often spoofs the destination to trick the client
  - Many benefits, but many pitfalls
- High Level Flows:
  - 1 Client request outbound
  - 2 Request redirected by ASA to WSA (WCCP)
  - 3 WSA evals request, proxies to server (OCS)
  - 4 WSA scans results and proxies back to client



# WCCP Deployment Considerations

- WSA is generally **WCCPv2**
  - Client could be anything (WAAS, 3<sup>rd</sup> party proxy/gateway, etc)
- Typical deployment pairings are
  - WSA -> **ASA** (now virtual!)
  - WSA -> **ISR**
  - WSA -> **ASR1K**
  - WSA -> **Nexus7K**
  - WSA -> **Cat6K**
- **Layer 2 vs. GRE** for return / redirect traffic
- **Ingress vs. Egress** for redirection point as concerned with L2 forwarding
- **Closer vs. Further** to/from clients; logical placement
- Service IDs and interested traffic

# WCCP Service Groups

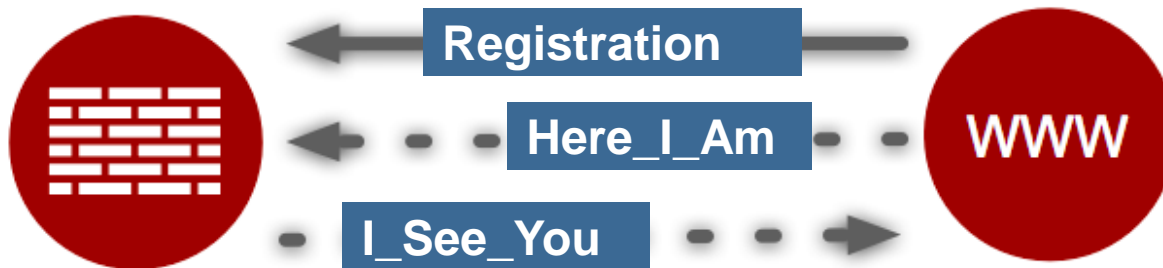
- Collection of WCCP clients and WCCP servers make up a Service Group
  - Up to 32 routers per service group
  - Up to 32 WCCP clients per service group
  - Up to **8 ports for redirection** to WSA
- Each service group has separate WCCP exchange, database, and FSM
- Service definition must be the same across all members
- **Service IDs are 0-255**
  - 90-98 for custom user ports
  - Others are pre-defined

Service Profile Name:	<input type="text" value="CyberRange_WCCP_Services"/>
Service:	<input type="radio"/> Standard service ID: 0 web-cache (destination port 80)
	<input checked="" type="radio"/> Dynamic service ID: <input type="text" value="90"/> 1-255
	Port numbers: <input type="text" value="80,443"/> <i>(up to 8 port numbers, separated by commas)</i>
	<input checked="" type="radio"/> Redirect based on destination port
	<input type="radio"/> Redirect based on source port (return path)



# WCCP Operation: Registration

- WCCP client (WSA) registers with WCCP server (ASA, Router, Switch)
- Server and client verify Service Group ID, confirm Security Key (if used)
- WCCP server can register multiple clients
- Server and client exchange “here i am” and “i see you“ packets for availability
  - UDP/2048 unicast exchanges (can multicast)



# WCCP Details: Distribution Algorithms

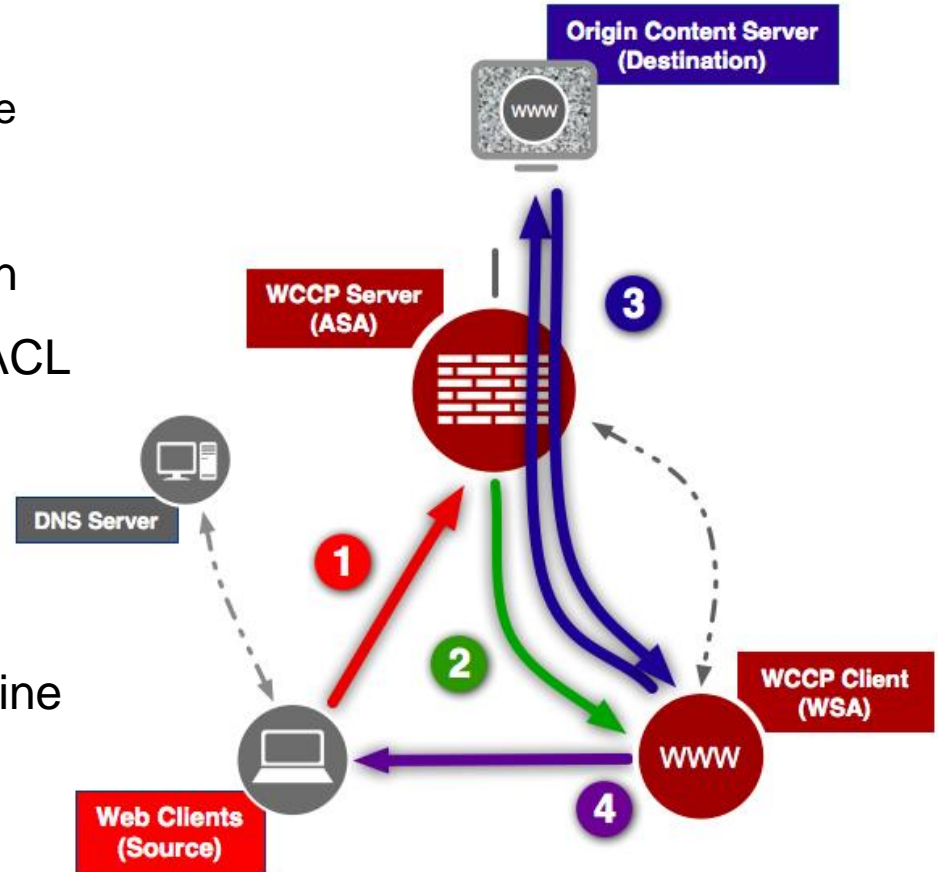
- Hash-based algorithm versus Mask-based
  - **Hash-based**: a software based hash algorithm to determine which WCCP appliance receives traffic. In hardware based platforms, the Netflow table is used to apply hardware assistance.
  - **Mask-based**: “TCAM” entries help assign WCCP entities. This method is fully handled by hardware.
- Algorithm is set and established by the WCCP client (WSA)
- If platform supports WCCP in hardware (i.e. Cat6K, ASR, etc)
  - Prefer **Mask-based** assignment
  - Prefer **Ingress / Input** redirection
  - Prefer **L2 Redirect** (if GRE also is in hardware)

# WCCP Details: Rewrites and Return Path

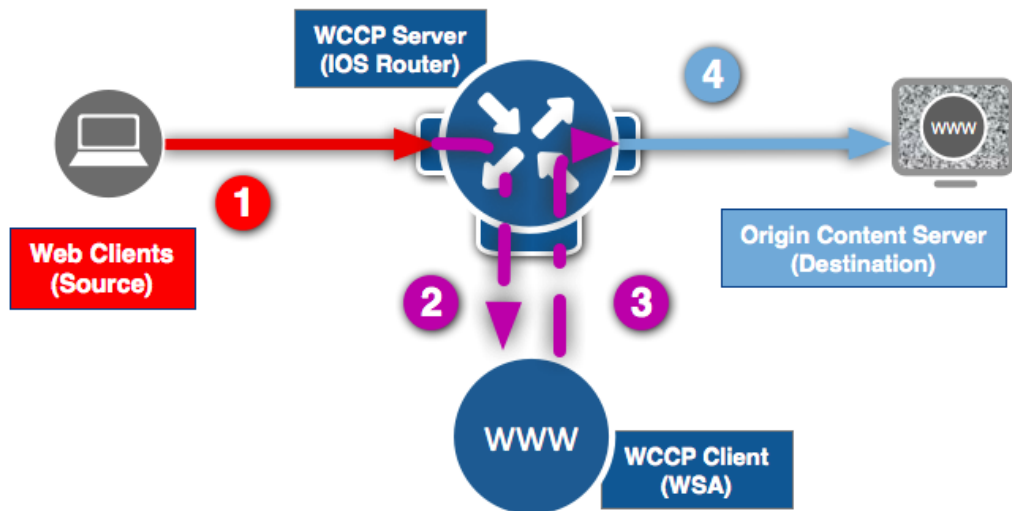
- **Redirect Method:** how traffic is sent to the client by the server
  - **WCCP GRE** - Entire packet WCCP GRE tunneled to the WCCP Client (WSA)
  - **Layer 2** - Frame MAC address rewritten to MAC of WCCP Client
- **Return Method:** how traffic is sent back from the server to the WCCP client if the traffic could not be serviced (aka “Proxy Bypass”)
  - **WCCP GRE** – Packet WCCP GRE returned router WCCP
  - **Layer 2** – Frame rewritten to router’s own MAC address

# WCCP with ASA

- ASA allows only “redirect in”
  - Client and WSA must be on same interface
- No DMZ Deployment possible
- Inside ACL is checked before redirection
- Destination Server must be allowed in ACL
- Redirection Method is GRE based
- Redirect ACL allows permit and deny
- Bypasses inspection and other checks
- Hardware module (including CX) still inline



# WCCP with Switches / Routers



- Very scalable and flexible design, including “DMZ” approach
- CAT6500 (recent SUPs)
  - allows redirect of L2 and GRE in Hardware
- Adjust MTU for GRE
- Attention to the bypass list to avoid loops and other nasties
  - Redirect-in and Redirect-out is supported
  - Permit and Deny ACE is allowed
  - Avoid flags, options & time- ranges



# Debugging WCCP

- Generally, WCCP registration either just works or it doesn't
  - Check **service IDs**, hashing methods, MD5 keys
  - Ensure your **configs are aligned on both sides** (i.e. redirect ACLs, encaps, etc)
- Debug on the client and server side to get the full picture
  - Run **Packet Captures** on both sides, as needed
  - Debugs
    - ASA: **debug wccp packet** | **debug wccp event**
    - WSA: “**WCCP Module Logs**” Log Subscription (not standard -> must manually add)
    - IOS: **debug ip wccp packet** | **debug ip wccp event**
- Network Constraints:
  - Any transit firewall is allowing both UDP 2048 and GRE for tunnelling



1972 km 公里  
People's Republic of China - Great Wall  
中華人民共和國 - 萬里長城

9632 km 公里  
United Kingdom - Big Ben  
英國 - 大笨鐘

11881 km 公里  
Africa - Cape of Good Hope  
非洲 - 好望角

12968 km 公里  
United States of America - Statue of Liberty  
美國 - 自由神像

Advanced WSA

Directory Integration

# Authentication Modes

- Authentication Realm Types Supported:
  - LDAP vs. **NTLM (Active Directory)**
- Method:
  - Basic: Credentials are sent unencrypted
  - NTLMSSP: Challenge-Response
  - Kerberos: Secure tickets
  - TUI: **Transparent ID lookup with Cisco Directory Agent (CDA)**
- Identifying the session / user:
  - **IP-based surrogates** vs. Cookie-based surrogates
- Advanced concepts:
  - Securing the session via SSL
  - **Hostnames for redirection** (for SSO), certs (separate SSL cert for each WSA)
  - Credential caching and timeouts, reauth enforcement

# Challenges with WCCP: Authentication Loops

- Multiple WSAs pose a problem in terms of redirection
  - If a user authenticates against one WSA, the resulting traffic could be redirected again!
  - Can be a really nasty problem to debug in a large environment
  - Especially weird behaviour at the end-user side
- Solution is to “exempt” the WSAs’ own addresses from redirection:

```
ip access-list extended <WCCP_redirection_ACL>
```

```
deny ip any host <WSA_interface>
```

```
deny ip host <WSA_interface> any
```

```
permit tcp any any eq www
```

```
permit tcp any any eq 443
```

- Can also: “**Load Balance based on client address**”

Dynamic service ID:  1-255

Port numbers:   
(up to 8 port numbers, separated by commas)

Redirect based on destination port

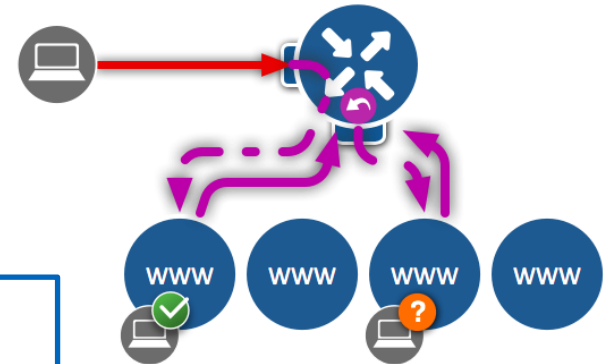
Redirect based on source port (return path)

For IP spoofing, define two services, one based on destination port and an source port (return path).

Load balance based on server address

Load balance based on client address

Applies only if more than one Web Security Appliance is in use.



# Passing the Auth: Upstream Proxy Considerations

- WSA can be deployed behind an existing proxy (even another WSA!)
  - NOTE: WSA can easily overload an upstream proxy if not careful

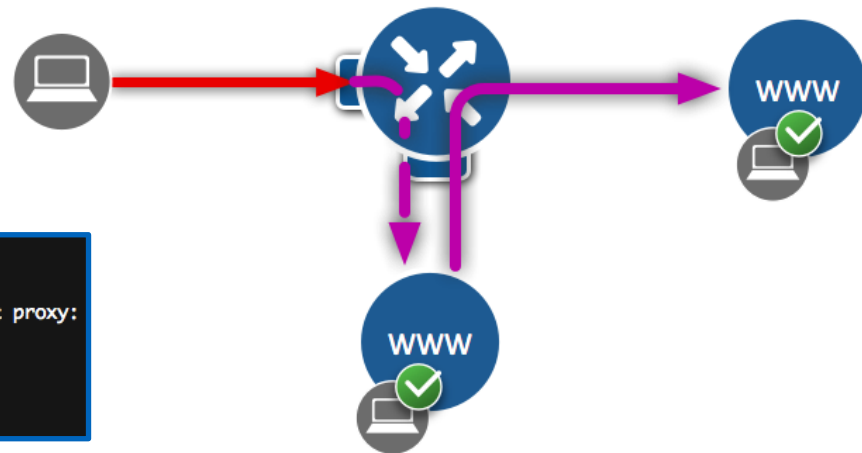
- On Downstream Proxy (CLI only)
  - `advancedproxyconfig > authentication`

```
Enter values for the authentication options:
```

```
When would you like to forward authorization request headers to a parent proxy:
```

1. Always
2. Never
3. Only if not used by the WSA

```
[2]> █
```



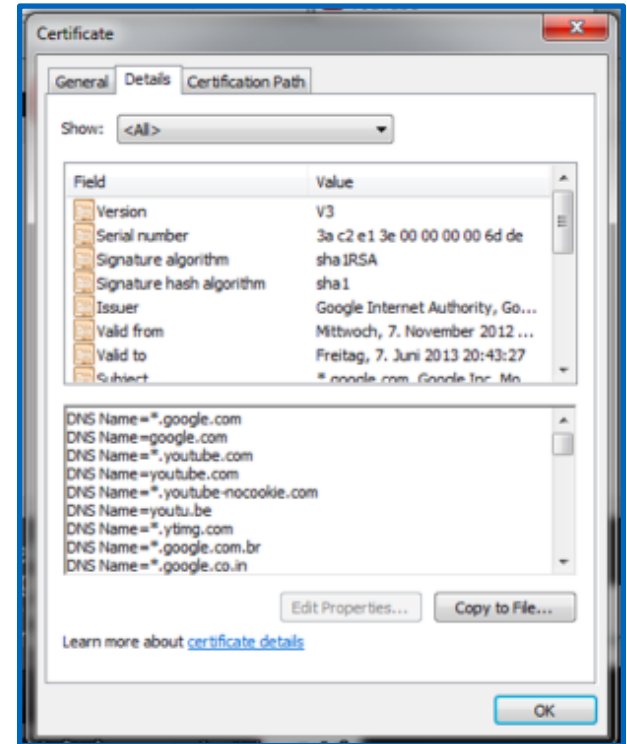
- On Upstream Proxy (if using WSA)
  - Security Services > Web Proxy > Advanced Settings

Generate Headers:	X-Forwarded-For: <input type="radio"/> Send <input checked="" type="radio"/> Do Not Send
	Request Side VIA: <input checked="" type="radio"/> Send <input type="radio"/> Do Not Send
	Response Side VIA: <input checked="" type="radio"/> Send <input type="radio"/> Do Not Send
Use Received Headers:	<input type="checkbox"/> Enable Identification of Client IP Addresses using X-Forwarded-For
	Trusted Downstream Proxy or Load Balancer <input type="text"/> <input type="button" value="Add Row"/>
	<input type="text"/> <input type="button" value="Delete"/>
	IP address



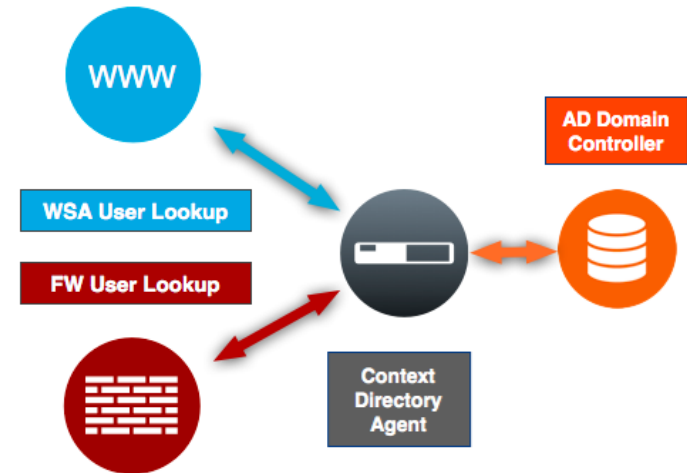
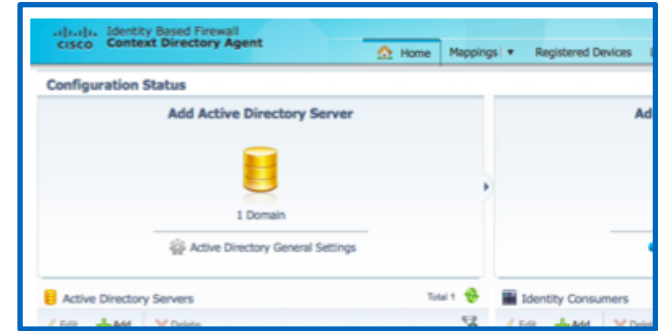
# HTTPS Considerations

- WSA first fetches the server cert, and parses out relevant data
- With this certificate, WSA has knowledge of:
  - Client IP
  - Destination IP
  - Server Certificate
  - Common Name (CN) from server certificate is used as a request URL, thus used for URL category matching
- Based on this information WSA can match Identity and Decryption Policy and determine whether to DECRYPT or PASS THROUGH the request
- All other info is now encrypted and otherwise **not available to WSA**



# Enter: Context Directory Agent

- Evolution from Cisco AD Agent
- Common framework to standardise how Cisco kit interacts with an AD domain or forest
- Improves administrators' ability for policy enforcement and control, without bugging the users too much 😊
- “Cisco Linux” based software
  - same as ACS, ISE, ASA-CX, etc
  - installed as canned Virtual Appliance
- Obtains **User-to-IP Mapping via WMI** from the AD Domain Controller
- Can be queried from other Cisco sources:
  - WSA, ASA, or ASA-CX, ISE **via RADIUS**

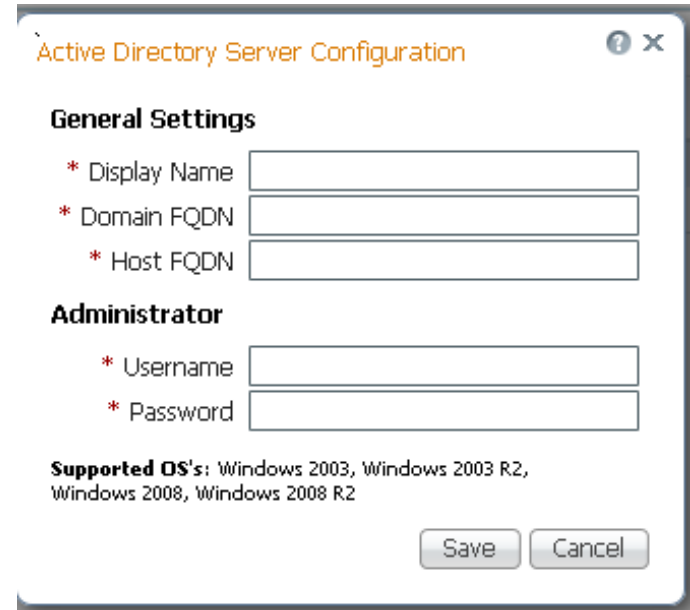


# Planning for Transparent Auth with CDA

- Allocate VM resources and deploy appliance
- Infrastructure Readiness
  - Firewall rules (RADIUS, HTTPS, NTP, etc)
  - Domain configs and CDA Service Account provisioning
  - AD Domain 2003, 2008 (2012 support with latest patch!)
- Build CDA; have network details on hand
- Bind CDA to the domain
  
- Caveats:
  - No NAT “stitching” capability; real addresses required

# CDA Pre-requisites

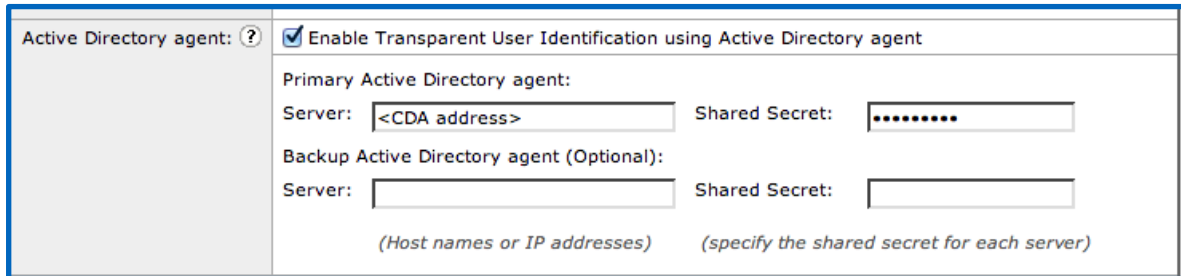
- AD Requirements for CDA Communication
  - Confirm version support; **patch AD DC's** (WMI memory leaks, etc)
  - Ensure user login events -> set the **“Audit Policy”** for the domain to **include successful logins** for the Windows Security Log
  - Ensure CDA user credentials have proper privileges in domain (**Domain Admin**)
    - non-domain admin accounts require additional settings and reg hacks!
  - Verify AD NTLM settings via Group Policy under security / login settings
  - Firewall rule to access **dllhost.exe** on DCs



The image shows a screenshot of the 'Active Directory Server Configuration' dialog box. The title bar reads 'Active Directory Server Configuration' with a help icon and a close button. The dialog is divided into sections: 'General Settings' with three required fields: 'Display Name', 'Domain FQDN', and 'Host FQDN'; 'Administrator' with two required fields: 'Username' and 'Password'. At the bottom, it lists 'Supported OS's: Windows 2003, Windows 2003 R2, Windows 2008, Windows 2008 R2' and has 'Save' and 'Cancel' buttons.

# Configuring the WSA for Transparent Auth

- Again, very simple... This process either works or it doesn't.
- Follow exact same steps as deploying normal AD realm
- Enable the “Transparent User Identification” setting
  - Configure CDA address
  - Enter pre-shared secret (encrypts credentials)
  - NOTE: secret is the same as a typical RADIUS pre-shared key



Active Directory agent: ?  Enable Transparent User Identification using Active Directory agent

Primary Active Directory agent:

Server:  Shared Secret:

Backup Active Directory agent (Optional):

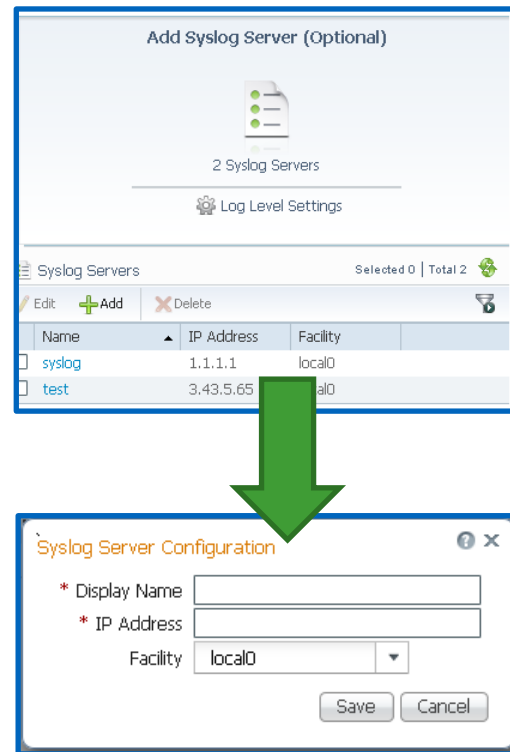
Server:  Shared Secret:

*(Host names or IP addresses) (specify the shared secret for each server)*



# CDA Debugging

- Check logs on CDA
  - set to DEBUG; default is NOTICE
  - check basics:
    - service account password
    - time skew
    - intermediate connectivity
- Check domain “security” logs for logon events from CDA service account
- Can export logs off box as well for analysis





# WSA Operations

# Foreword: Building Your Own “Big Data”

- Use the “metrics” approach:
  - Establish pre-defined goals and criteria or “metrics” according to your
  - Use data points and trends to show **continuous improvement**, however small
  - Derive the best value of your WSA deployment
- Exporting logs off-box = big data opportunities, with **huge potential**
  - Sampling data for **sizing future projects**
  - **Educated policy decisions**
  - **Reduce security risk**
- Help **\$ub\$idize** Cost of Ownership with data insights
  - IT service charge back models
  - Marketing data for business partners, internal use
  - Visualising data for CxO level consumption
- Oh, and by the way – **makes Ops life easier** 😊





1972 km 公里  
People's Republic of China - Great Wall  
中華人民共和國 - 萬里長城

9632 km 公里  
United Kingdom - Big Ben  
英國 - 大笨鐘

11881 km 公里  
Africa - Cape of Good Hope  
非洲 - 好望角

12968 km 公里  
United States of America - Statue of Liberty  
美國 - 自由神像

WSA Operations

Logging

# Understanding what you can work with

- Local log subscriptions on each WSA
- Centralised Logging / Tracking on SMA
  - Pulls data periodically from WSAs
  - Actual logs still available locally on WSAs
- Off-box Reporting App(s) for Splunk (SCP / FTP / SYSLOG)
- Export to any server (SCP / FTP / SYSLOG)
- Focus here is on **accesslogs**, but some others include:
  - system\_logs
  - cli\_logs
  - gui\_logs
  - prox\_track.log (not available as log subscription!)



# Get to Know Your Data Sources

Cisco S100V  
Web Security Virtual Appliance

Reporting Web Security Manager Security Services Network System Administration

Overview

System Overview

Web Proxy Traffic Characteristics System Resource Utilization Users

Policy Trace Alerts Log Subscriptions Return Addresses Users

Printable (PDF)

Reporting Web Security Manager Security Services Network System Administration

## Log Subscriptions

Configured Log Subscriptions

Add Log Subscription...

Log Name	Type	Log Files	Rollover Interval	All Rollover	Delete
accesslogs	Access Logs	ftp://stl-as-n07-wsa-1.cisco.com/accesslogs	Custom	<input type="checkbox"/>	
accesslogs_splunk_tc...	Access Logs	Syslog Push - Host stl-as-n07-splunk-1.cisco.com	None	<input type="checkbox"/>	
authlogs	Authentication Framework Logs	ftp://stl-as-n07-wsa-1.cisco.com/authlogs	Custom	<input type="checkbox"/>	
avc_logs	AVC Engine Logs	ftp://stl-as-n07-wsa-1.cisco.com/avc_logs	Custom	<input type="checkbox"/>	
bypasslogs	Proxy Bypass Logs	ftp://stl-as-n07-wsa-1.cisco.com/bypasslogs	Custom	<input type="checkbox"/>	

# Get to Know Your Data Sources

Rollover by Time:	None
Log Style:	<input checked="" type="radio"/> Squid <input type="radio"/> Apache <input type="radio"/> Squid Details
Custom Fields (optional):	%u
File Name:	
Log Compression:	<input type="checkbox"/> Enable
Log Exclusions (Optional):	<input type="text"/> <i>(Enter the HTTP status codes of transaction)</i>

## Suggested Custom Fields

%u %<Referer: %k %XF %q

Online Help for AsyncOS for Web Security Appliances  
https://stl-as-n07-wsa-1.cisco.com:8443/help/wsa\_help/index.html?Logging06.html#wp1155538

Back Forward Print View PDF Search Go

### Custom Formatting in Access Logs and W3C Logs

You can customize access logs and W3C access logs to include many different fields to capture comprehensive information about web traffic within the network. Access logs use format specifiers, and the W3C access logs use W3C log fields.

Table 24-11 describes the W3C log fields you can include in the W3C access logs and the custom format specifiers (for the access logs) they correspond with.

Table 24-11 Log Fields in W3C Logs and Format Specifiers in Access Logs

W3C Log Field	Format Specifier in Access Logs	Description
—	%XP	Unrecognized header. Use this field to log extra headers in client requests. This supports troubleshooting of specialized systems that add headers to client requests as a way of authenticating and redirecting those requests, for example, YouTube for Schools.
bytes	%B	Total bytes used (request size + response size, which is %q + %s)
c-ip	%a	Client IP Address
c-port	%F	Client source port
CMF	%M	Cache miss flags, CMF flags

Copyright 2012, Cisco Systems, Inc. All rights reserved.

# Know Your Sources: Access Logs

```
accesslogs_splunk_tcp: Info: 1390159677.065 5 192.168.100.252 TCP_MISS/200
441 HEAD
http://ds.download.windowsupdate.com/v10/1/microsoftupdate/redirect/muredir.cab?14
01191559 - DIRECT/ds.download.windowsupdate.com application/octet-stream
DEFAULT_CASE_12-CyberRange_Access-CyberRange_Inside_NoAuth-NONE-
NONE-NONE-DefaultGroup <IW_swup,9.2,0,"-",0,0,0,-,"-",-,-,-,"-",-,-,"-","-",-,-
,IW_swup,-,"-","-", "Windows Update", "Software Updates", "-","-",705.60,0,-
,"Unknown","- "> - "Windows-Update-Agent" - 144.135.8.162 "Software Updates" 177
```

Squid Base Fields

Vendor Specific

Recommended Additions

# Know Your Sources: Access Logs Basics

accesslogs\_splunk\_tcp: Info: 1390159677.065 5 192.168.100.252

**Response Size (bytes)**

**Timestamp**

**Client IP Address**

**Elapsed Time (ms)**

TCP\_MISS/200 441 HEAD http://ds.download.windowsupdate.com/ -

**Request Method**

**Request URL**

**User Identity**

**Cache Result / HTTP Status Code**

Example:  
"unsuspecting\_user@CyberRange"

DIRECT/ds.download.windowsupdate.com application/octet-stream

**Hierarchy / From**

**MIME Type**

# Know Your Sources: WSA Access Log Fields

```
DEFAULT_CASE_12-CyberRange_Access-CyberRange_Inside_NoAuth-NONE-  
NONE-NONE-DefaultGroup
```

**Action**

**Policy and Identity Names**

```
<IW_swup,9.2.0,"-",0,0,0,-,"-",,-,-,"-",,-,"-",,"-",,-,IW_swup,-,"-",,"-",  
"Windows Update","Software Updates","-",,"-",705.60,0,-,"Unknown", "-"> -
```

**ACL Decision Tag**

???



# Know Your Sources: WSA Custom Fields



"Windows-Update-Agent" - 144.135.8.162 "Software Updates" 177

**User Agent**

**HTTP Referrer**

Example:  
"http://www.news.com.au/"

**Destination  
IP Address**

**URL Category Name**

**Request Size (bytes)**

These fields help drive the new Splunk app, and can be considered best practice for InfoSec-savvy deployments.

# Know Your Sources: Splunk extractions

**access\_policy** acl\_decision\_tag **action bytes\_in bytes\_out** c\_ip cache **cause** cs\_bytes cs\_method cs\_mime\_type **cs\_url** cs\_url\_host cs\_url\_port **cs\_url\_query cs\_url\_scheme cs\_url\_stem** cs\_user\_agent cs\_username data\_security\_policy date\_hour date\_mday date\_minute date\_month date\_second date\_wday date\_year date\_zone **dest\_domain dest\_host dest\_ip dest\_port duration** end\_time eventtype external\_dlp\_policy hierarchy **host** http\_content\_type **http\_method http\_result http\_user\_agent identity** ids\_type index linecount outbound\_malware\_policy product punct routing\_policy s\_from s\_hierarchy sc\_bytes sc\_http\_status sc\_result source sourcetype splunk\_server **src\_ip** status tag tag::eventtype threat\_reason url vendor x\_acl\_tag **x\_avc\_app** x\_avc\_behavior x\_avc\_type x\_avg\_bw x\_bw\_throttled x\_custom\_fields x\_icap\_verdict x\_ids\_verdict x\_mcafee\_av\_virustype x\_mcafee\_detecttype x\_mcafee\_filename x\_mcafee\_scan\_error x\_mcafee\_scanverdict x\_mcafee\_virus\_name **x\_req\_dvs\_threat\_name** x\_request\_rewrite **x\_resp\_dvs\_threat\_name** x\_resp\_dvs\_verdictname x\_scan\_verdict x\_sophos\_filename x\_sophos\_scancode x\_sophos\_scanverdict x\_sophos\_virus\_name x\_user\_type **x\_wbrs\_score x\_wbrs\_threat\_type** x\_webcat\_code\_abbr **x\_webcat\_code\_full** x\_webcat\_req\_code\_abbr x\_webcat\_resp\_code\_abbr x\_webroot\_scanverdict x\_webroot\_spyid x\_webroot\_threat\_name x\_webroot\_trace\_id x\_webroot\_trr

That's a lot of information!

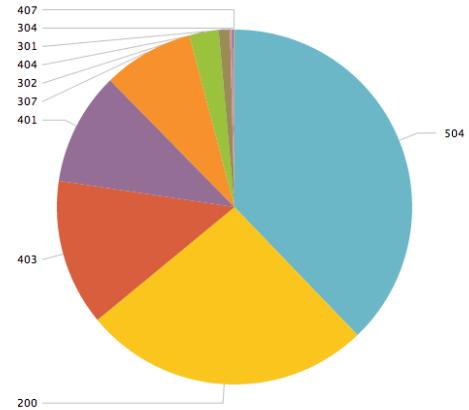
- 100+ fields
- **~25 instructor favorites**

# Fun Stuff to Check Out: HTTP Response Codes

- **200** – OK  
*The request sent by the client was successful*
- **301** – Moved Permanently  
*The resource has permanently moved to a different URI*
- **401** – Unauthorised (Authentication Required)  
*The request first requires authentication with the server*
- **403** – Forbidden  
*Access denied*
- **404** – Not Found  
*The server cannot find the requested URI*
- **407** – Proxy Authentication Required  
*The request first requires authentication with the proxy*

**Try Me!**

```
sourcetype="cisco_wsa_*"  
| top sc_http_status
```



# More Fun Stuff to Check Out: HTTP Headers

## Request Headers

```
GET http://www.google.com HTTP/1.1
Proxy-Authorization: NTLM [...snip...] ==
User-Agent: curl/7.24.0 (x86_64-apple-darwin12.0) libcurl/7.24.0 OpenSSL/0.9.8y
zlib/1.2.5
Host: www.google.com
Accept: */*
Proxy-Connection: Keep-Alive
```

```
HTTP/1.1 302 Found
Location: http://www.google.com.au/?gws_rd=cr&ei=DDbcUtmIE8SWkQX5zID4Ag
Cache-Control: private
Content-Type: text/html; charset=UTF-8
Set-Cookie: NID=67=eZivlpL3TkYmXeXHgXsU2vtdezQ5hrXw8XYvd [...snip...]
Date: Sun, 19 Jan 2014 20:31:08 GMT
Server: gws
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Alternate-Protocol: 80:quic
Content-Length: 262
Via: 1.1 WSAv-01.cybercisco.com:80 (Cisco-IronPort-WSA/7.7.5-194)
Connection: keep-alive
Proxy-Connection: keep-alive
```

## Response Headers

# Some Access Log Samples

## Cache Miss:

```
1245711783.527 79 172.20.11.222 TCP_MISS/200 14148 GET
http://www.ironport.com/ - DIRECT/www.ironport.com
text/html
```

## Cache Memory Hit:

```
1245712075.460 1 172.20.11.222 TCP_MEM_HIT/200 972 GET
http://www.ironport.com/_media/_technology2.gif - NONE/-
image/gif
```

## If Modified Since Hit:

```
1245713067.598 0 172.20.11.222 TCP_IMS_HIT/304 155 GET
http://www.outside.com/images/logo.gif - NONE/- -
```



Only the Squid part of the entry is displayed







360 昂公 坪平 360

1972 km 公里  
People's Republic of China - Great Wall  
中華人民共和國 - 萬里長城

9632 km 公里  
United Kingdom - Big Ben  
英國 - 大笨鐘

11881 km 公里  
Africa - Cape of Good Hope  
非洲 - 好望角

12968 km 公里  
United States of America - Statue of Liberty  
美國 - 自由神像

WSA Operations

Monitoring

# Key Performance Indicators to Watch

- SNMP Polling / SMA Reporting
  - CPU utilisation (proxy)
  - Memory footprint (proxy)
  - Disk I/O
  - Requests Per Second (RPS)
  - Response Time/Latency
- CLI Commands
  - Sample regularly for trending
  - status detail
- Log Data
  - Send off-box for more detailed analysis

The screenshot shows the Cisco Management Appliance Web interface. At the top, there are tabs for 'Management Appliance', 'Email', and 'Web'. Below these are sections for 'Reporting', 'Utilities', and 'Configuration Master 7.5'. The main content area is titled 'System Capacity' and includes a 'Time Range' dropdown set to '30 days' and a date range from '08 Jul 2013 00:00 to 07 Aug 2013 19:34 (GMT +10:00)'. Below this is a section titled 'Overview of Averaged Usage and Performance' which contains a table with the following data:

Web Security Appliance ▲	CPU Usage %	Response Time (ms)	Proxy Buffer Memory (Bytes)	Transactions Per Second
	1.6%	14	0B	0
	1.5%	10	0B	0
	1.5%	10	0B	0
	1.7%	3	0B	0
				0
				0

```
WSAv-01.cybercisco.com> status detail
Status as of:                Mon Feb 10 11:38:16 2014 EST
Up since:                    Fri Jan 17 12:00:07 2014 EST
System Resource Utilization:
CPU                           12.2%
RAM                           0.0%
Reporting/Logging Disk       14.8%
Transactions per Second:
Average in last minute        0
```

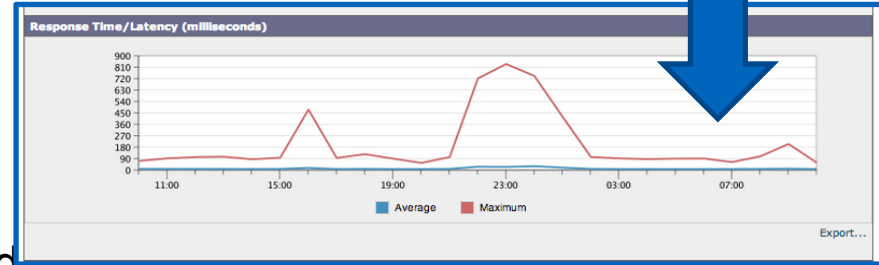
# KPI Trending



- Trending over time yields massive benefit
  - Strike a chord with the business
- Must have a “baseline” or starting point
- Can export the “raw” data off-box to CSV
  - Excel, Splunk, TI-84, etc
- More data is usually better, but don't send just anything without a plan.



Overview of Averaged Usage and Performance				
	CPU Usage %	Response Time (ms)	Proxy Buffer Memory (Bytes)	Transactions Per Second
Web Security Appliance A	1.5%	14	00	0
	1.5%	10	00	0
	1.5%	10	00	0
	1.5%	00	00	0
	1.5%	00	00	0
	1.5%	00	00	0



## Target “Comfort Levels”

	Optimum	At Capacity	Over Loaded
<b>Proxy CPU vs. Response Time</b>	<b>CPU &lt; 80%</b> <b>RT &lt; 3s</b>	<b>CPU &lt; 90%</b> <b>RT &lt; 5s</b>	<b>CPU &gt; 90%</b> <b>RT &gt; 5s</b>



# “How many access policies is too much”?



- There is no hard limit of configurable access policies.
- However, suggested **recommendation to not exceed:**
  - **30 Access Policies**
  - **30 Custom URL Categories**
  - **10 Regular Expressions** per Custom URL Category (use RegEx sparingly!)
- Cisco tests / QAs the following scenarios:
  - **“simple” configuration** of 1 single policy
  - **“complex” configuration** of 30 access policies
- Numbers and strategy, as of AsyncOS 7.5.x and 7.7.x
  - QA process / sharing of **perf. figures will continue to improve** in upcoming releases!

# Performance Testing Methodology and Caveats

## ■ Cisco Testing Notes

- Figures apply to AsyncOS 7.5.x only
- Tests assume **HTTPS decryption**
  - Simulate “typical user” **real-world traffic mix** (some % SSL, % malware, etc)
  - HTTPS connections stay open really, really long these days!
- Assume **5-25% cache hit rate**

## ■ Understanding the Measurements

- **Requests per Second != Total Connections** (or anything else)
- Expected **RPS is difficult to extrapolate** w/o detailed raw data to back it up
- Use **10% of total clients \* 1.5** conservative real-world multiplier to **guestimate RPS**
- **Max RPS** = highest sustained RPS where:
  - **CPU < 90%**
  - **Response Time / Latency < 5 seconds**
  - (this is where the “comfort levels” come from)



# Sizing and Performance Tuning Review

## Best Practice Guidelines

- **Do not exceed** 30 Access Policies
- **Do not exceed** 20 Identities
- **Reduce** Custom URL Category complexity
- Limit regular expression usage where possible
- **Do not exceed** 10 Regex entries per Custom Category
- Reuse Custom URL Categories where possible to avoid duplicates

## Cisco's Testing Evolution

- **Previous State** ( $\leq$  AsyncOS 7.5)
  - Internal-only, limited Datasets
- **Current State** (AsyncOS 7.7)
  - Revamped testing / sizing for Web 2.0
  - “Real World”, tiered usage profiles
- **Future State** ( $\geq$  AsyncOS 7.7)
  - Additional data sets
  - More customer-facing stats



1972 km 公里  
People's Republic of China - Great Wall  
中華人民共和國 - 萬里長城

9632 km 公里  
United Kingdom - Big Ben  
英國 - 大笨鐘

11881 km 公里  
Africa - Cape of Good Hope  
非洲 - 好望角

12968 km 公里  
United States of America - Statue of Liberty  
美國 - 自由神像

WSA Operations

Management

# So you have problems with your manager?

**Cisco S100V**  
Web Security Virtual Appliance

Upgrade Available | Logged in as: awurster on WSAv-01.cybercisco.com

Reporting | Web Security Manager | Security Services | Network | System Administration

### Overview

#### System Overview

Web Proxy Traffic Characteristics	System Res
Average transactions per second in past minute:	0
Average bandwidth (bps) in past minute:	0
Average response time (ms) in past minute:	0
Total current connections:	0

System Sta

Time Range: Week

13 Jan 2014 00:00 to 20 Jan 2014 06:38 (GMT +11:00)

#### Total Web Proxy Activity

Date	passthru	error	Total
14-Jan	~1,800	~1,200	~3,000
16-Jan	~5,800	~1,200	~7,000
18-Jan	~1,200	~1,000	~2,200
20-Jan	~1,000	~1,000	~2,000

Export...

### Web Security Overview

Last 7 days

#### Web Security Events

Date	allow	auth fail	block	decrypt	error	passthru	Total
Mon Jan 13	~17,000	~1,000	~1,000	~1,000	~1,000	~1,000	~21,000
Wed Jan 15	~8,000	~1,000	~1,000	~1,000	~1,000	~1,000	~13,000
Fri Jan 17	~5,000	~1,000	~1,000	~1,000	~1,000	~1,000	~10,000
Sun Jan 19	~2,000	~1,000	~1,000	~1,000	~1,000	~1,000	~7,000

#### Blocked Transaction Summary

Category	Percentage
error	~45%
auth fail	~15%
avc	~15%
reputation	~10%
policy	~15%

#### URL Category Mix

Category	Percentage
Streaming Video	~25%
Web-based Email	~20%
Computer Security	~15%
Internal	~10%
Travel	~5%
Search E...d Portals	~5%
Health a... Nutrition	~5%
Transportation	~5%
Business ... Industry	~5%
Compute... Internet	~5%

#### Web Security Threats

Category	Percentage
error	~45%
acceptable use	~35%
auth failure	~20%

#### Application Visibility and Control

Category	Percentage
other (9)	~35%
YouTube	~25%
Gmail	~20%
Windows Update	~10%
Google	~10%



1972 km 公里  
People's Republic of China - Great Wall  
中華人民共和國 - 萬里長城

9632 km 公里  
United Kingdom - Big Ben  
英國 - 大笨鐘

11881 km 公里  
Africa - Cape of Good Hope  
非洲 - 好望角

12968 km 公里  
United States of America - Statue of Liberty  
美國 - 自由神像

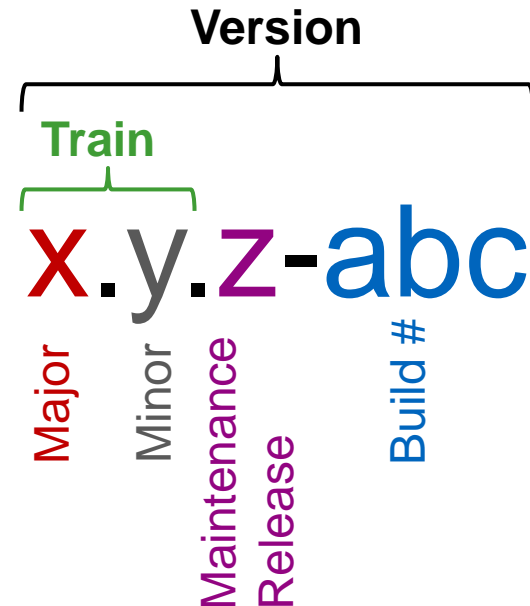
WSA Operations

AsyncOS Releases



# AsyncOS Software Lifecycle

- **New trains** introduce **new features**
- **Maintenance releases** undergo the **most testing**
  - Concentrate on bug fixes, avoid new features
  - Cumulative fixes typically
- Build # signifies exact build of entire version
- Build numbers increase regularly during development
  - The build you get is just a number.



```
WSA-test.lab> version
Current Version
=====
Product: Cisco IronPort S670 Web Security Appliance
Model: S670
Version: 7.5.2-118
```

Version	7.5.1
Full Version:	7.5.2-118
Train:	7.5

# AsyncOS Release Processes

- Major Releases (i.e. **7.x.0** or **8.x.0**) planned semi-annually
- Minor Releases (i.e. **7.5.x**) planned quarterly
- All Major and Minor releases have Build numbers (i.e. **7.5.2-abc** or **7.5.0-abc**)
- Generally a 6 month cadence for major releases
  - follow EOL / EOS for details on [hardware](#) and [software](#) lifecycles



# AsyncOS Release Planning Suggestions

- Read [release notes](#) thoroughly
- Execute iterative test plan in a test environment
- “Phase” rollouts across individual boxes and low-profile regions
- Can engage Cisco Advanced Services for “bug scrub” capability
- Subscribe to [Cisco Notification Service](#) for updates

# WSA and SMA Release Compatibility

- WSA and SMA code trains are separate branches of AsyncOS, but the pair are released in step
- Upgrading between different major releases in WSA or SMA generally requires an upgrade to both systems
- Refer to [SMA Compatibility Matrix](#) for more detail. Currently, we have:

Release	WSA 7.1.x	WSA 7.5.x	WSA 7.7.x
SMA 7.9.1	WSA 7.1.4	WSA 7.5.1 WSA 7.5.2	--
SMA 8.0	WSA 7.1.4	WSA 7.5.1 WSA 7.5.2	WSA 7.7.x
SMA 8.1	WSA 7.1.4	WSA 7.5.1 WSA 7.5.2	WSA 7.7.x



1972 km 公里  
People's Republic of China - Great Wall  
中華人民共和國 - 萬里長城

9632 km 公里  
United Kingdom - Big Ben  
英國 - 大笨鐘

11881 km 公里  
Africa - Cape of Good Hope  
非洲 - 好望角

12968 km 公里  
United States of America - Statue of Liberty  
美國 - 自由神像

WSA Operations

Troubleshooting and Debugging

# Debugging Tools: Logs



## Log Subscriptions

### Configured Log Subscriptions

Add Log Subscription...

Log Name	Type	Log Files	Rollover Interval	All <input type="checkbox"/> Rollover	Delete
accesslogs	Access Logs	<a href="ftp://CyberRange-Dev-WSAv.cisco.com/accesslogs">ftp://CyberRange-Dev-WSAv.cisco.com/accesslogs</a>	None	<input type="checkbox"/>	
authlogs	Authentication Framework Logs	<a href="ftp://CyberRange-Dev-WSAv.cisco.com/authlogs">ftp://CyberRange-Dev-WSAv.cisco.com/authlogs</a>	None	<input type="checkbox"/>	
avc_logs	AVC Engine Logs	<a href="ftp://CyberRange-Dev-WSAv.cisco.com/avc_logs">ftp://CyberRange-Dev-WSAv.cisco.com/avc_logs</a>	None	<input type="checkbox"/>	
bypasslogs	Proxy Bypass Logs	<a href="ftp://CyberRange-Dev-WSAv.cisco.com/bypasslogs">ftp://CyberRange-Dev-WSAv.cisco.com/bypasslogs</a>	None	<input type="checkbox"/>	
cli_logs	CLI Audit Logs	<a href="ftp://CyberRange-Dev-WSAv.cisco.com/cli_logs">ftp://CyberRange-Dev-WSAv.cisco.com/cli_logs</a>	None	<input type="checkbox"/>	
configdefragd_logs	Configuration Logs	<a href="ftp://CyberRange-Dev-WSAv.cisco.com/configdefragd_logs">ftp://CyberRange-Dev-WSAv.cisco.com/configdefragd_logs</a>	None	<input type="checkbox"/>	
dca_logs	DCA Engine Logs	<a href="ftp://CyberRange-Dev-WSAv.cisco.com/dca_logs">ftp://CyberRange-Dev-WSAv.cisco.com/dca_logs</a>	None	<input type="checkbox"/>	

Much much easier to work with logs off-box!

```
$ scp -r admin@stl-as-n07-wsa-1.cisco.com:accesslogs/* ~/tmp/
100% 1134KB 141.7KB/s 00:08 aclog.@20140206T140542.s
100% 805KB 201.1KB/s 00:04 aclog.@20140208T140527.s
```

## grep

```
CyberRange-Dev-WSAv.cyberrange.dev> grep -i
awurster accesslogs
```

```
1391563737.008 1144 172.20.1.99 TCP_MISS/404 1350
GET http://fubar.awurster.com/ -
DEFAULT_PARENT/proxy.cisco.com text/html
DEFAULT_CASE 12-DefaultGroup-DefaultGroup-NONE-
NONE-NONE-DefaultGroup <IW_pnet,0.0,0,"-
",0,0,0,1,"-", "-", "-", "-", "1,-", "-", "-", "-", IW_pnet, -
,"Unknown", "-", "Unknown", "Unknown", "-", "-", "9.44,0, -
,"Unknown", "-> -
```

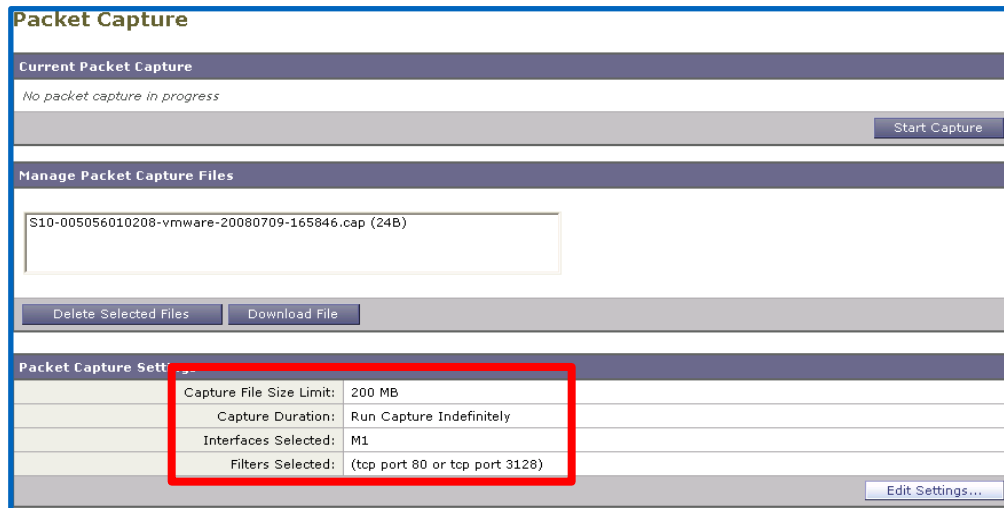
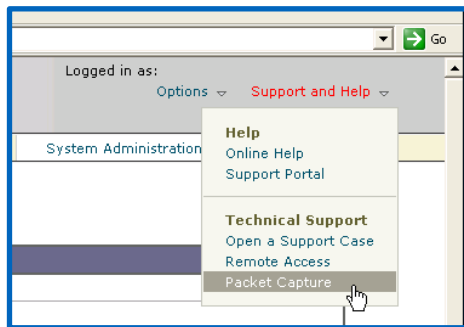
## tail

```
CyberRange-Dev-WSAv.cyberrange.dev> tail system_logs
```

```
Press Ctrl-C to stop.
Sat Feb 8 08:18:44 2014 Warning: DNS query network
error '[Errno 65] No route to host' to
'64.104.200.248' looking up 'update-
manifests.sco.cisco.com'
```

# Debugging Tools: Packet Capture

- GUI: **Support and Help -> Packet Capture**
- CLI: **packetcapture**



# Debugging Tools: CLI commands

## proxystat

used	/sec	hits	blocks	misses	kb/sec	kb/sec	saved	wrs	rds		
0.05		5	0	38	20	63	31	50.6	0	0	
0.06		2	0	14	7	358	347	3.1	0	0	

## status detail

Status as of: Thu Jul 08 01:29:02 2010 PDT  
Up since: Wed Jul 07 05:14:26 2010 PDT (20h 14m 36s)  
System Resource Utilization:  
CPU 19.4%  
RAM 52.3%  
Reporting/Logging Disk 7.2%  
Transactions per Second:  
Average in last minute 0

## version

Current Version  
=====  
Product: Cisco Web Security Appliance  
Model: S100  
Version: 9.1.2-695  
Build Date: 2020-06-01  
Install Date: 2010-06-01 21:51:03  
Serial #: 005056010201-vmware  
BIOS: NA  
RAID: 02  
RAID Status: Unknown  
RAID Type: NA  
BMC: NA

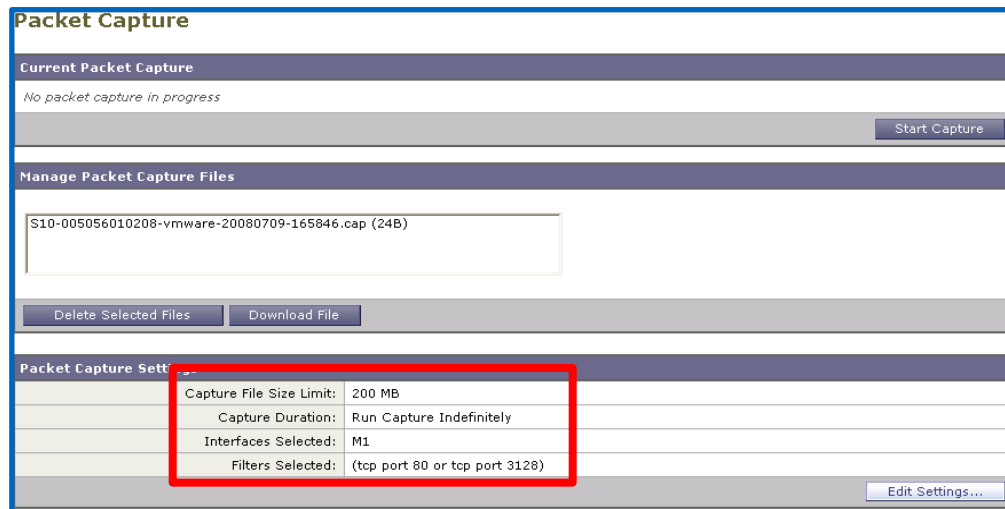
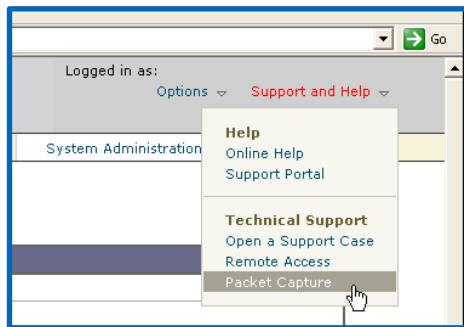
## help?

ping  
arp  
tracert  
nslookup  
dnsflush  
telnet  
tail  
grep  
diagnostic  
tcpdump  
netstat



# Debugging Tools: Packet Capture

- GUI: **Support and Help -> Packet Capture**
- CLI: **packetcapture**



# Debugging Tools: Policy Trace

- Simulate transactions to debug and verify policy configurations
- Enter everything you, know about the transaction.

### Policy Trace

<b>Destination</b>	
URL:	<input type="text" value="www.cisco.com"/>
<b>Transaction</b>	
<i>All fields below are optional.</i>	
Client IP Address:	<input type="text" value="172.20.1.100"/>
User:	No Authentication Realms are defined.
▸ Advanced	
<input type="button" value="Cancel"/>	
<b>Results</b>	
<b>User Information</b>	
User Name: None	
Group Membership: None	
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36	
<b>URL Check</b>	
WBR Score: 6.5	
URL Category: Computers and Internet	
Scanner "Webroot" Verdict (Request): Unknown	
Scanner "AVC" Verdict (Request): Unknown (Unknown)	
MIME-Type: text/html	
Object Size: 26714 bytes	
Scanner "AVC" Verdict (Response): Unknown (Unknown)	
Adaptive Scanning Verdict (Response): Unknown	

# Refresher: Support Requests and Cisco TAC

- Service requests can be created via
  - TAC Service request Tool <http://tools.cisco.com/ServiceRequestTool/create/launch.do>
  - Calling TAC hotline: 1 800 553 2447
  - From the appliance itself
- Generate config and diagnostics with “Support Request”
- Allow temporary remote access via “Support Tunnel”
- Minimum Information to provide:
  - Personal contact details and preferences
  - Contract details
    - Cisco Support Contract Number
    - Serial Number
  - Access Logs (for normal access related issues)
  - Optional information to provide:
    - Packet Captures



## Web Security Wrap-up



**What have you learned today?**

# So are you ready and able? You decide!



GROWING THREATS



EVOLVING NETWORKS



BUSINESS NEEDS





# Keeping in Touch

Find me on [Linked](#) 

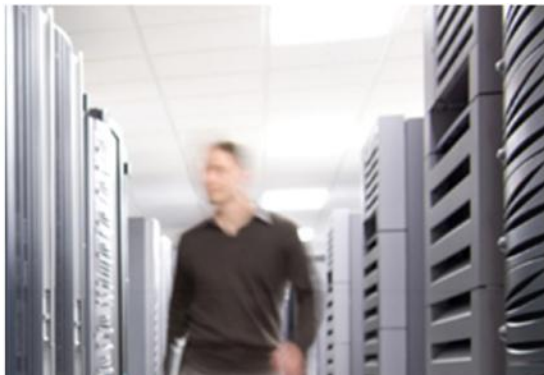


me: [awurster@cisco.com](mailto:awurster@cisco.com)

Check out my  [Repositories](#)

# Further Reading and Resources

- End User Guides
  - [http://www.cisco.com/en/US/products/ps10164/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/ps10164/products_user_guide_list.html)
- Release notes
  - [http://www.cisco.com/en/US/products/ps10164/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps10164/prod_release_notes_list.html)
- IronPort Customer Support Page
  - <http://www.cisco.com/web/services/acquisitions/ironport.html#~Overview>
- Knowledge Base
  - <https://ironport.custhelp.com/app/answers/list>
- Support Community
  - <https://supportforums.cisco.com/community/netpro/security/web>



Q & A

# Complete Your Online Session Evaluation

## Give us your feedback and receive a Cisco Live 2014 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site [www.ciscoliveaustralia.com/mobile](http://www.ciscoliveaustralia.com/mobile)
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 March 12:00pm - 2:00pm



## Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations.

[www.CiscoLiveAPAC.com](http://www.CiscoLiveAPAC.com)



**CISCO**™