

TOMORROW starts here.



Cisco *live!*

Embrace Cloud Web Security with your Cisco Network

BRKSEC-2695

Jonny Noble
Content Security TME

Session Abstract



Embrace Cloud Web Security with your Cisco Network

- Cisco Cloud Web Security enables any organisation with Cisco ASA, Cisco AnyConnect, WSA or ISR devices to deploy a premium cloud-based web security solution that protects their network from threats and provides the tools to control productivity, while providing administrators with centralised configuration and granular reporting capabilities for their web usage
- This breakout session will give a technical overview and live demo of the deployment options available for integration to the cloud from various Cisco network devices, followed by a Q&A session
- The target audience is security administrators and architects dealing with today's increasing Web Security challenges

Disruptions Come in Many Forms...



You can leverage Cloud Web Security today with your existing Cisco asset



This session will focus on a number of ways that Cisco's Cloud Web Security can be deployed with ease, all through existing Cisco infrastructure... or even without!

Introduction & Today's Agenda

Security Without Compromise

- What is CWS?
- The Threat Landscape
- Data Flow and Statistics
- Cloud Proxy Architecture

Live Demos

- ASA Connector
- ScanCenter Policies
- Reporting
- User Simulation



Deploying CWS with Your Cisco Infrastructure

- ASA
- ISR-G2
- WSA Connector
- AnyConnect
- Direct to Cloud

Managing CWS

- Centralised Management
- Web 2.0 Control
- Best of Class Reporting

For Your Reference...

- Additional information for your reference can be found on slides with this icon



**For Your
Reference**

- Presentation with **footnotes** available on www.tinyurl.com/embracethecloud

Agenda

Security Without Compromise

- What is CWS?
- The Threat Landscape
- Data Flow and Statistics
- Cloud Proxy Architecture



Live Demos

- ASA Connector
- ScanCenter Policies
- Reporting
- User Simulation

Deploying CWS with Your Cisco Infrastructure

- ASA
- ISR-G2
- WSA Connector
- AnyConnect
- Direct to Cloud

Managing CWS

- Centralised Management
- Web 2.0 Control
- Best of Class Reporting

What is CWS?

A Cloud Based Premium Service



Real-time scanning of all inbound and outbound HTTP/S web content



Robust, fast, scalable and reliable global datacenter infrastructure



Flexible deployment options via Cisco attach model and direct to cloud



Full support for roaming users

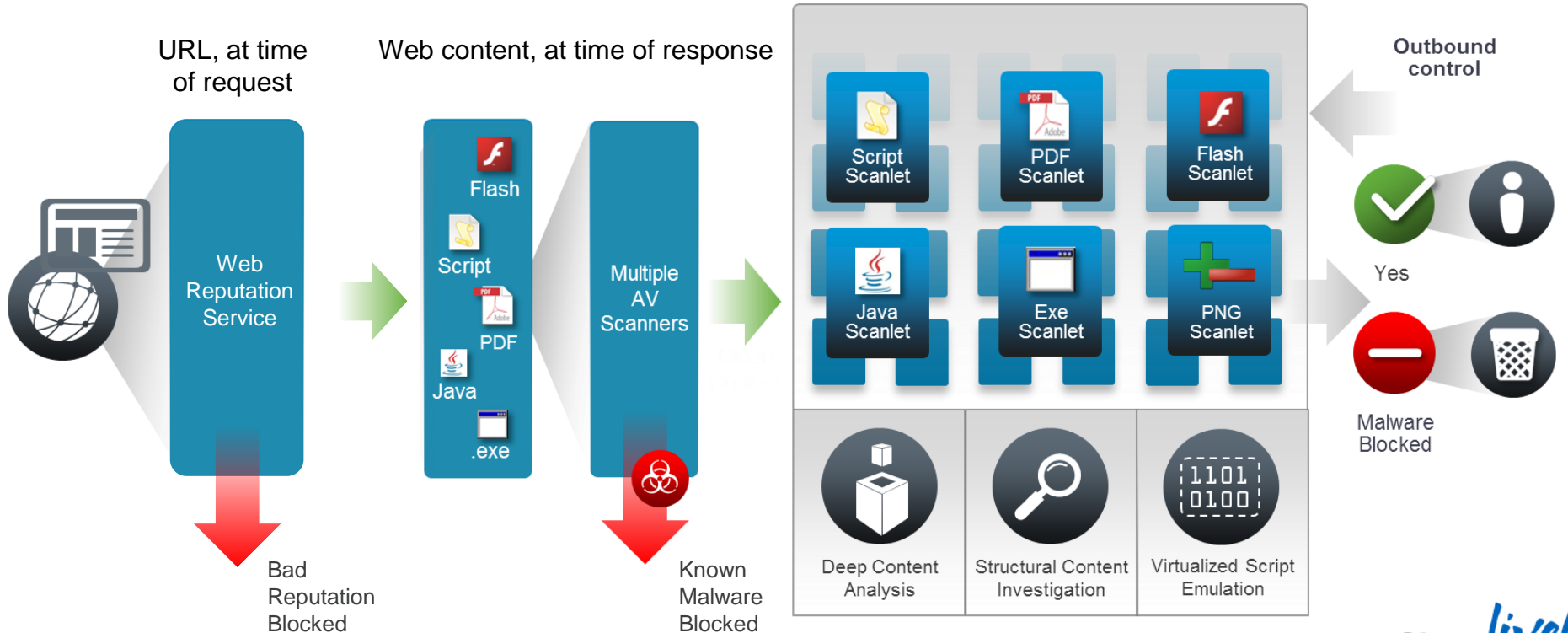


Centrally managed granular web filtering policies, with web 2.0 visibility and control



Close to real-time reporting with cloud retention, as part of the standard offering

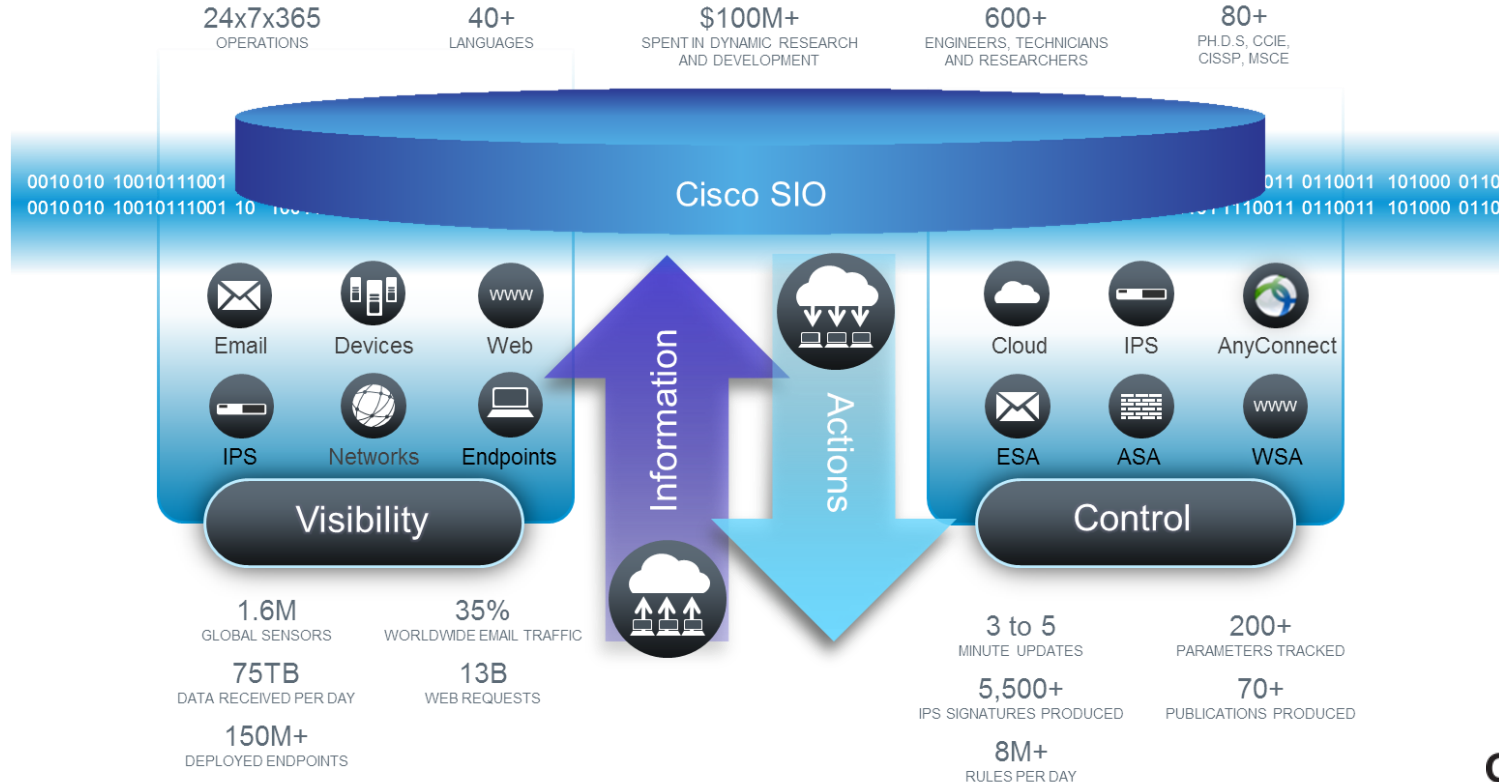
Multi-Layer Zero Hour Protection





SIO - Security Intelligence Operations

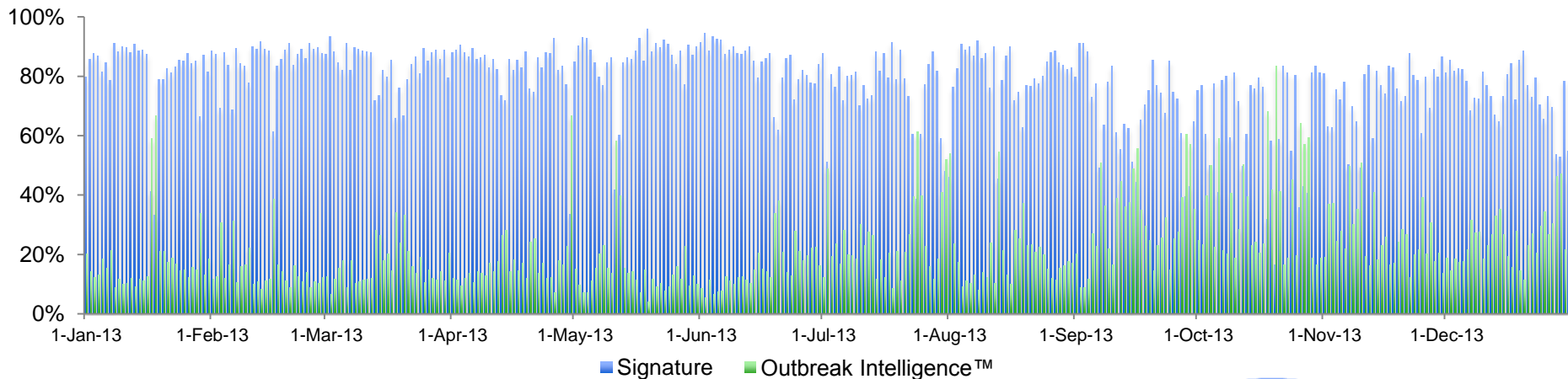
SIO receives feeds from Outbreak Intelligence



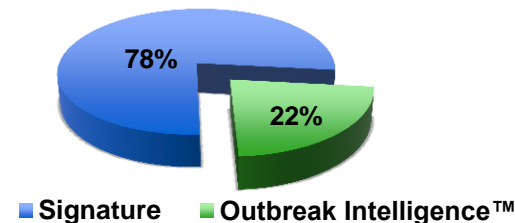
Outbreak Intelligence™ Vs. Signature Detection



Daily Blocks, 2013 (Source: Cisco Cloud Web Security)



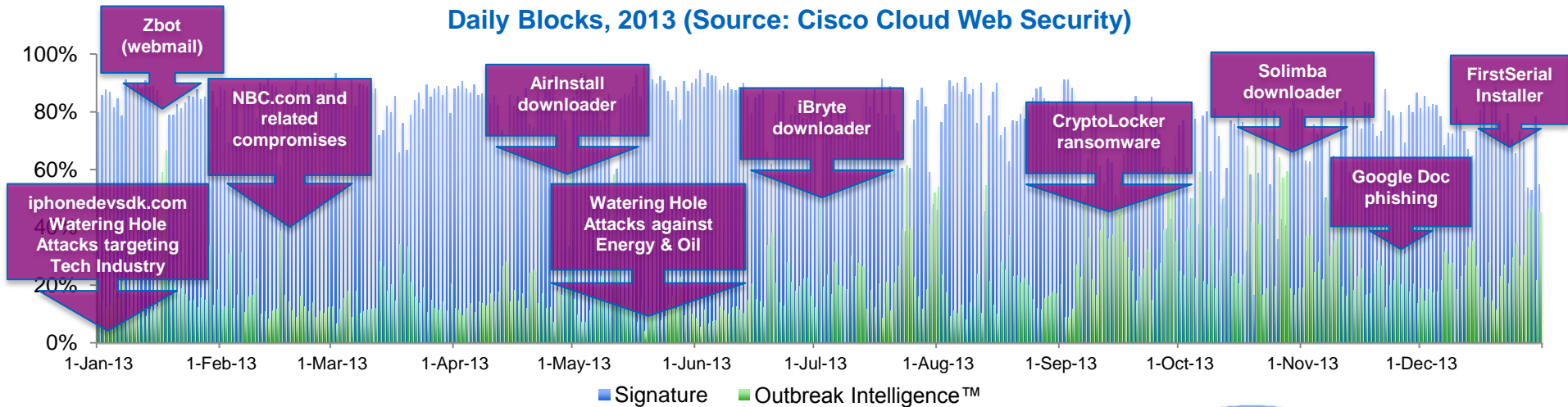
- This chart shows the day to day rate of OI detected threats vs. standard antivirus signatures.
- In 2013, 22% of Web malware was blocked by Cisco Outbreak Intelligence before signature detection became available
- Outbreak Intelligence provides early detection of new threats based on heuristic analysis of behavioural characteristics and machine learning



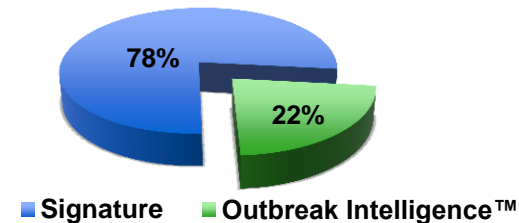
Outbreak Intelligence™ Vs. Signature Detection



Daily Blocks, 2013 (Source: Cisco Cloud Web Security)



- This chart shows the day to day rate of OI detected threats vs. standard antivirus signatures.
- In 2013, 22% of Web malware was blocked by Cisco Outbreak Intelligence before signature detection became available
- Outbreak Intelligence provides early detection of new threats based on heuristic analysis of behavioural characteristics and machine learning

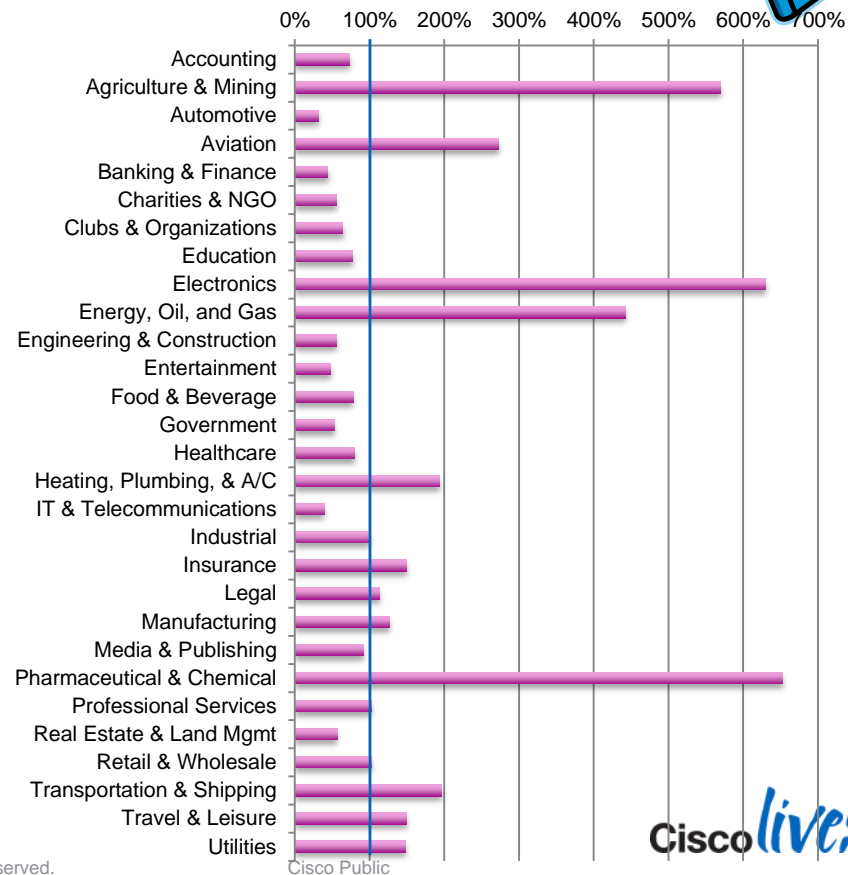


Vertical Risk: Web Malware Encounters, 2013



- Vertical risk is calculated by factoring the median block rate for all companies across all industry sectors, then calculating the median block rate in each specific sector
- A score above 100 signifies a higher than median rate of Web malware encounters, a score below 100 signifies a lower than median rate of Web malware encounters
- As seen in the chart, companies in the Electronics, Pharmaceutical, and Agriculture/Mining industries had the highest rate of Web malware encounters during 2013
- The Agriculture/Mining industry had one of the lowest encounter rates (back in 2008/2009), however, as scarcities in precious metals have worsened and food shortages have occurred as a result of weather disasters, this industry has increasingly come under more attacks

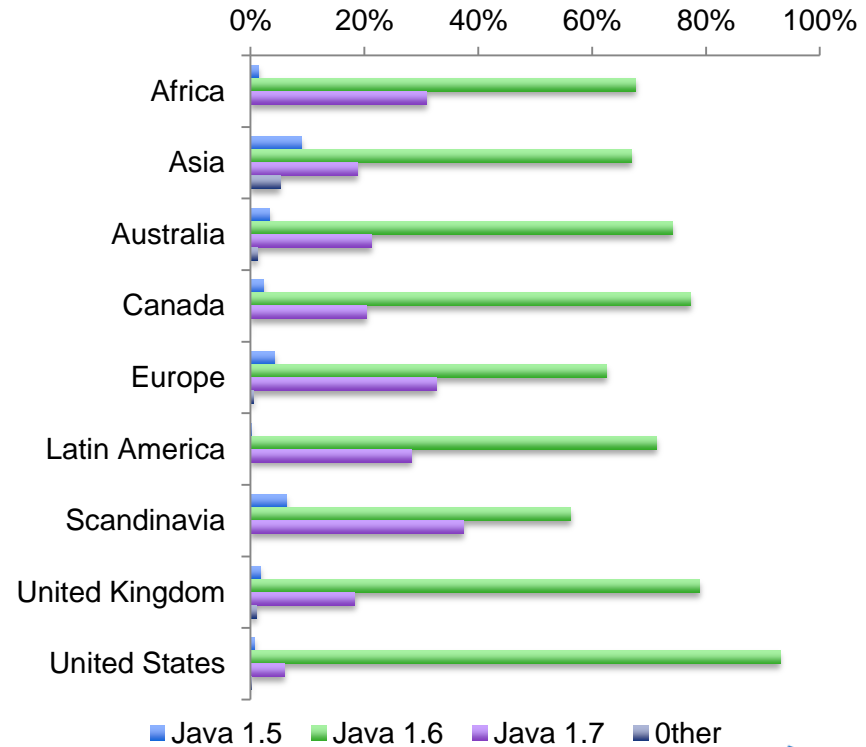
Source: Cisco Cloud Web Security



Java Malware Encounters by Region, 2013



- While timely patching is a critical component of good security posture, legacy tools and other dependencies may preclude updating to the latest versions
- An analysis of useragents reveals Java exploits by version:
 - 68% Java 1.6
 - 21% Java 1.7
 - 11% other Java



Source: Cisco Cloud Web Security

Global Data Centre Footprint



Multiple proxies within
each Data Centre



 Multiple data centres

 SP managed data centre

Some Basic Data Centre Statistics

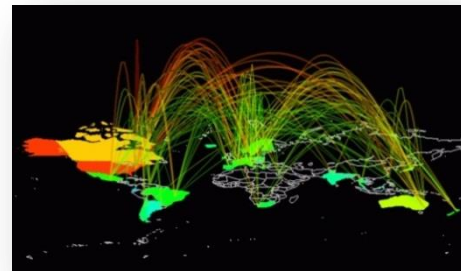


- 5,587,585,952 (5.6B) Requests in a typical business day *
- 197,607,002 (197.6M) Blocks in a typical business day (45.7M malware blocks) *
- 28 GB/s Traffic at peak *
- 136,116,611,072 (136B) Requests per month **
- 4,936,880,628 (4.9B) Blocks per month (1.3B malware blocks) **
- As a comparison: Google processes 3.3B requests/day ***
- 7.4 M rows of data processed per minute for reporting data

* 28 October 2013

** Measured throughout October 2013

*** Average daily data, based on 100B requests/month, as published on Wikipedia



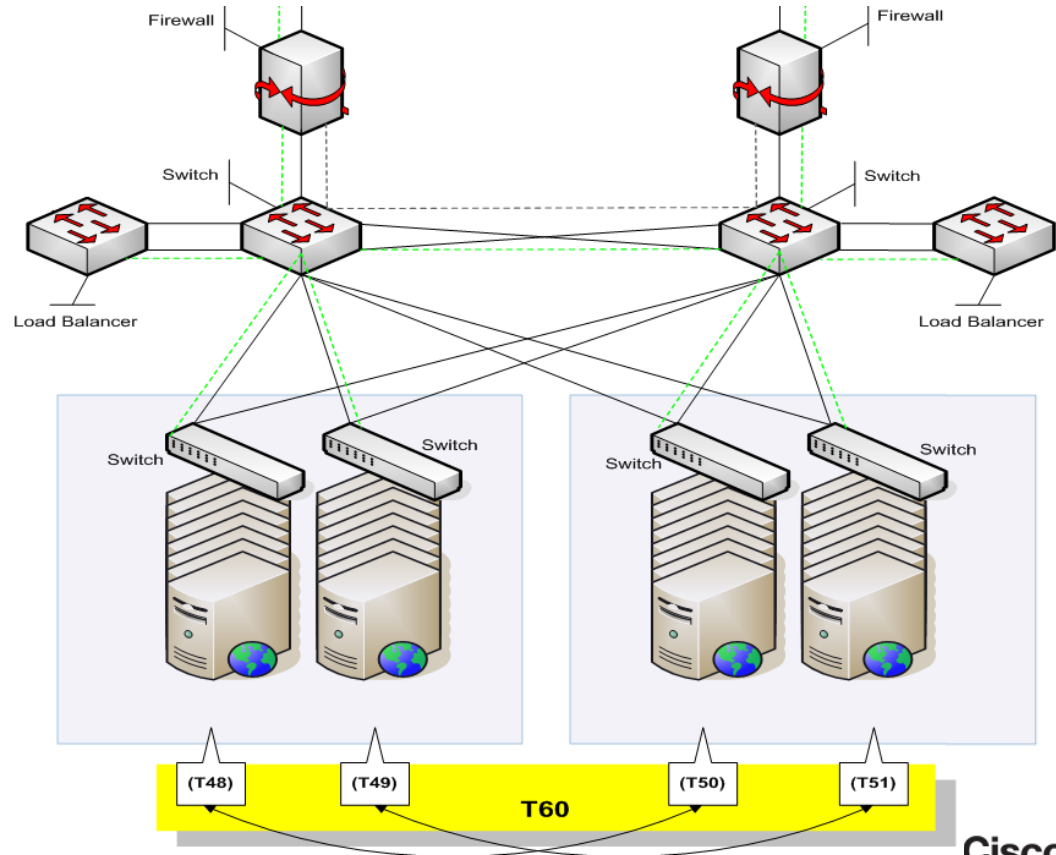
So What is a Cloud Proxy?



Proxy Layout - Today



- Each logical Proxy consists of:
 - Active/Passive Firewalls
 - Active/Passive Load Balancers
 - Application Switches
 - Distribution Switches
 - 2 x Chassis of 16 Blades each (32 Total)



Next Gen Cloud Infrastructure - Tomorrow



Built from the ground up to deliver the next gen Cloud delivered Security Services



Convergence



Intelligence



Automation



Higher throughput over existing infrastructure

Auto-Configuration detects best tower
Independently assigned egress IPs

Ability to deploy new services without
disruptions



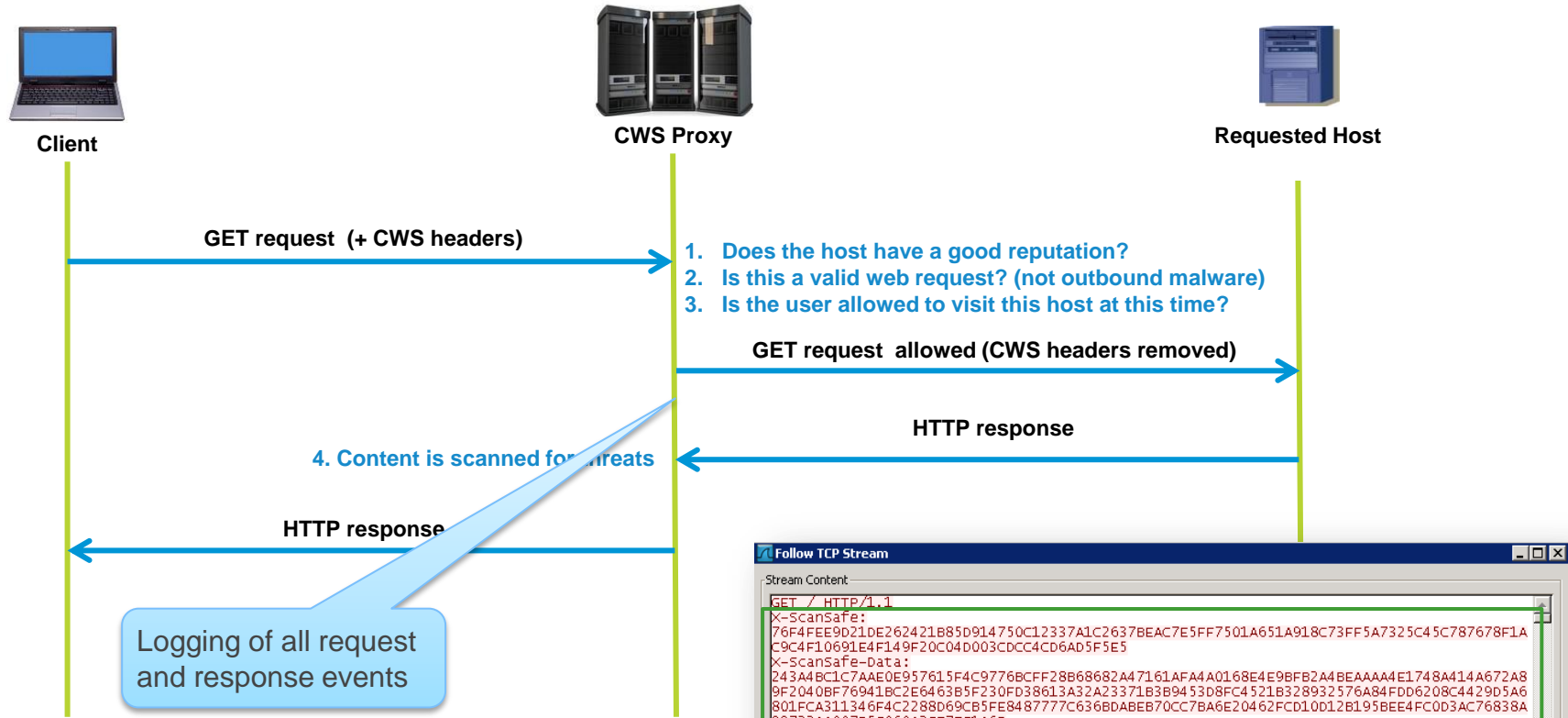
VM infrastructure on scalable Cisco UCS hardware
Multi-Service Capable + Capacity for product evolution

Additional Proxy Notes



- 1 incoming port (8080) + 443 on some towers for Secure Mobility clients
- Outgoing proxy IP is different from the incoming IP
- Allowed outgoing ports:
 - HTTP traffic is only allowed on ports 80, 81, 70, 84, 210, 280, 488, 591, 777, and 1025 - 65535
 - HTTPS traffic is only allowed on ports 443, 444, 563, 4005, and 8443
 - FTP traffic is only allowed on port 21
- ICMP protocols are not allowed for security reasons

CWS Data Flow



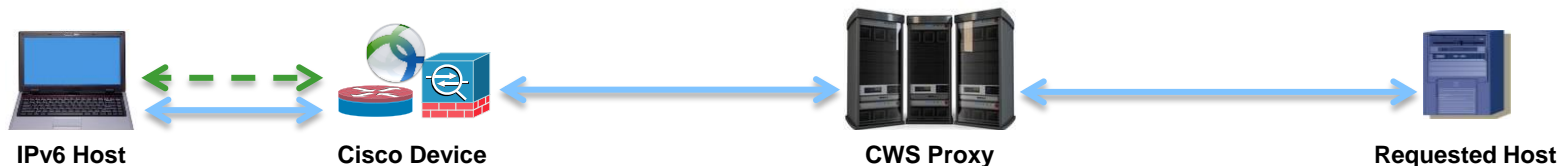
Unencrypted data in CWS headers:
 ScanSafeAgentVersion=AP-ISR-15.1(2)T;time=2010-04-29T17:09:59Z;
 X-Scansafe-License=12345678912345678912345678912345;cxn=1027;X-Client-IP=20.1.1.2;X-Authenticated-User=c2l2YQ==;X-Authenticated-Groups=SVQ=;

```

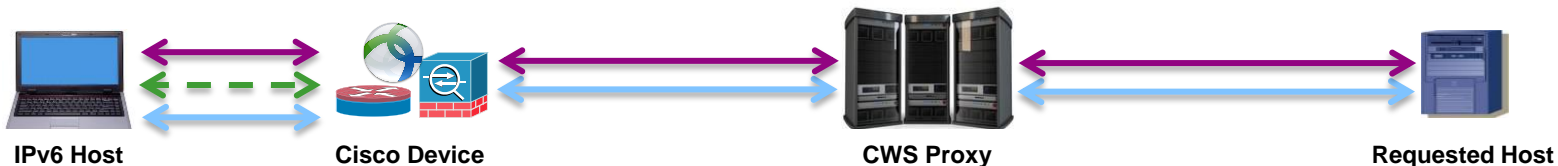
Follow TCP Stream
Stream Content:
GET / HTTP/1.1
X-ScanSafe:
76F4FEE9D21DE262421B85D914750C12337A1C2637BEAC7E5FF7501A651A918C73FF5A7325C45C787678F1A
C9C4F10691E4F149F20C04D003CDCC4CD6AD5F5E5
X-ScanSafe-Data:
243A4BC1C7AAE0E957615F4C9776BCFF28B68682A47161AFA4A0168E4E9BF82A4BEAAAA4E1748A414A672A8
9F2040BF76941BC2E6463B5F230FD38613A32A23371B3B9453D8FC4521B328932576A84FDD6208C4429D5A6
801FCA311346F4C2288D69CB5FE848777C636BDABEB70CC7BA6E20462FCD10D12B195BEE4FC0D3AC76838A
99732AA007B5C060A2CE7ECLA6B
Host: www.google.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
    
```

IPv6 Readiness

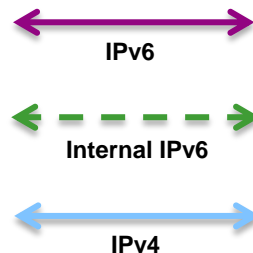
PHASE 1



PHASE 2



Timestamp	Rule Action	Host	Internal IP	Destination IP
22-01-2013 15:14:48	allow	ybb.softbank.jp	2a00:9600:0:182f::18c	d2a9:d348::
22-01-2013 15:14:49	allow	ybb.softbank.jp	2a00:9600:0:182f::18c	d2a9:d348::
22-01-2013 15:14:49	allow	ybb.softbank.jp	2a00:9600:0:182f::18c	d2a9:d348::
22-01-2013 15:14:52	allow	maps.googleapis.com	2a00:9600:0:182f::18c	adc2:435f::
22-01-2013 15:15:10	allow	p.typekit.net	2a00:9600:0:182f::18c	5db8:dc14::
22-01-2013 15:15:10	allow	www.worldipv6launch.org	2a00:9600:0:182f::18c	5c7a:7ff2::
22-01-2013 15:15:10	allow	www.worldipv6launch.org	2a00:9600:0:182f::18c	5c7a:7ff2::
22-01-2013 15:15:14	allow	ipv6launch.ripe.net	2a00:9600:0:182f::18c	4e2e:1104::
22-01-2013 15:15:14	allow	www.worldipv6launch.org	2a00:9600:0:182f::18c	5c7a:7ff2::



Agenda

Security Without Compromise

- What is CWS?
- The Threat Landscape
- Data Flow and Statistics
- Cloud Proxy Architecture

Live Demos

- ASA Connector
- ScanCenter Policies
- Reporting
- User Simulation

Deploying CWS with Your Cisco Infrastructure

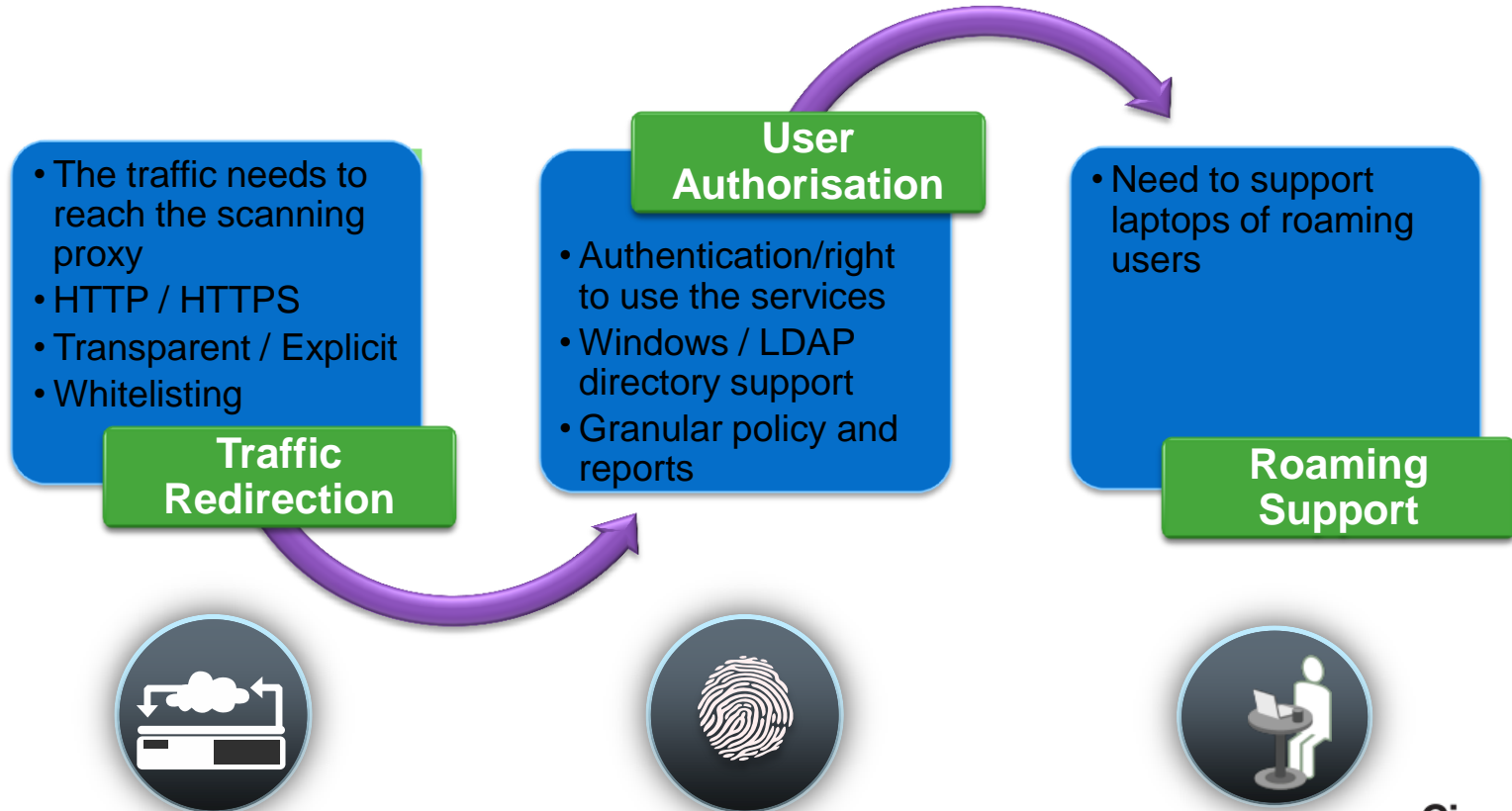
- ASA
- ISR-G2
- WSA Connector
- AnyConnect
- Direct to Cloud



Managing CWS

- Centralised Management
- Web 2.0 Control
- Best of Class Reporting

Key Considerations for Deploying Web Security



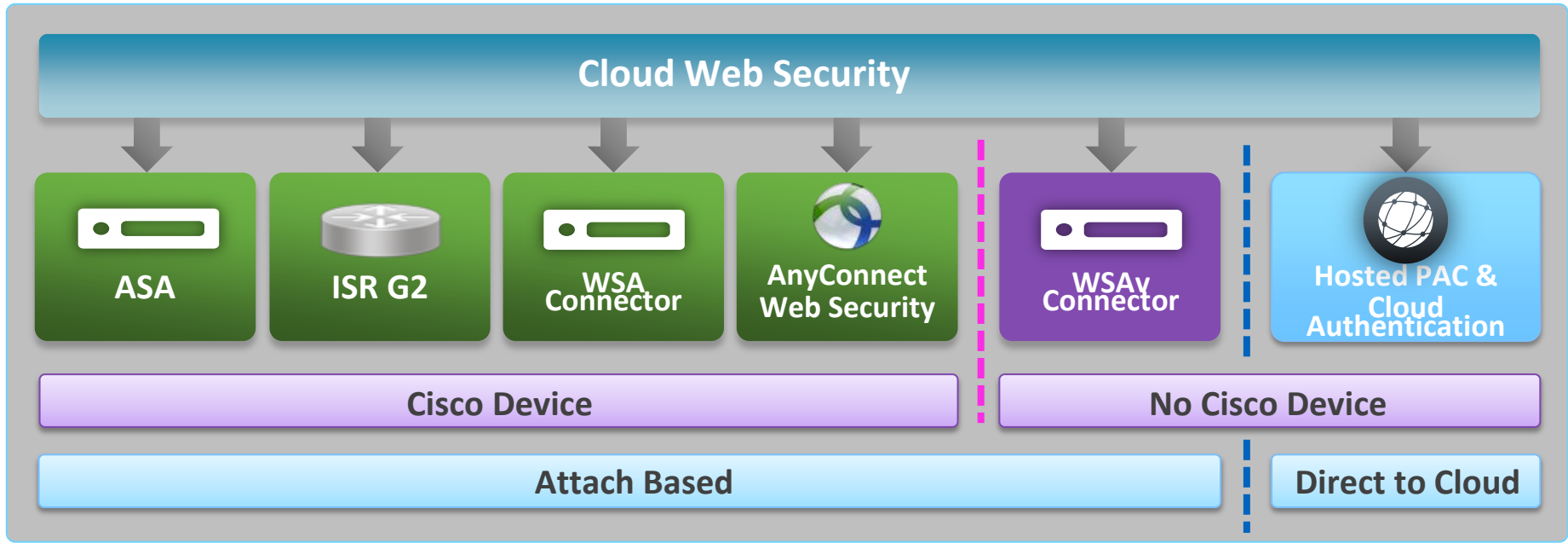
Redirecting to the Cloud

- All browser traffic through HTTP and HTTPS needs to be redirected to cloud proxies
- You can do this in various ways



Cisco Cloud Attach Model

Use your existing Cisco asset to leverage CWS



ASA Connector

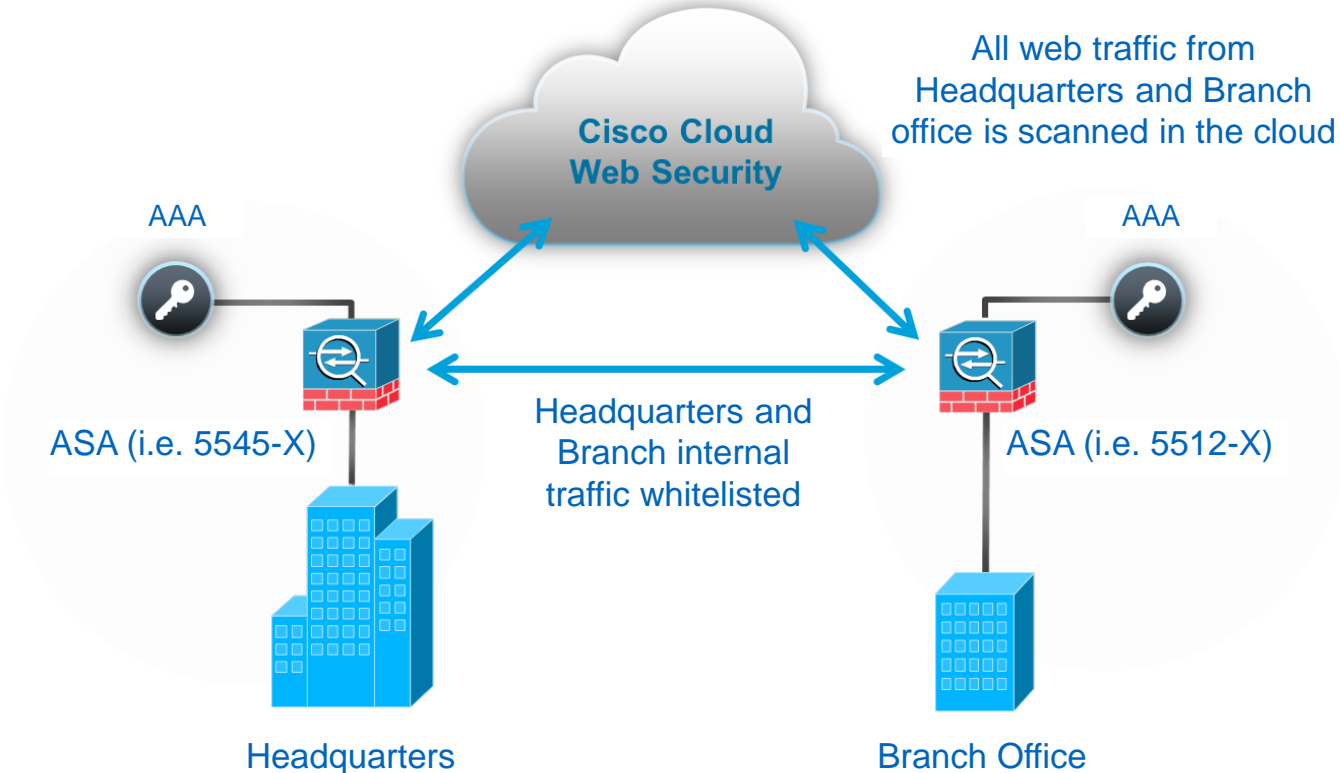


ASA Connector - Main Features

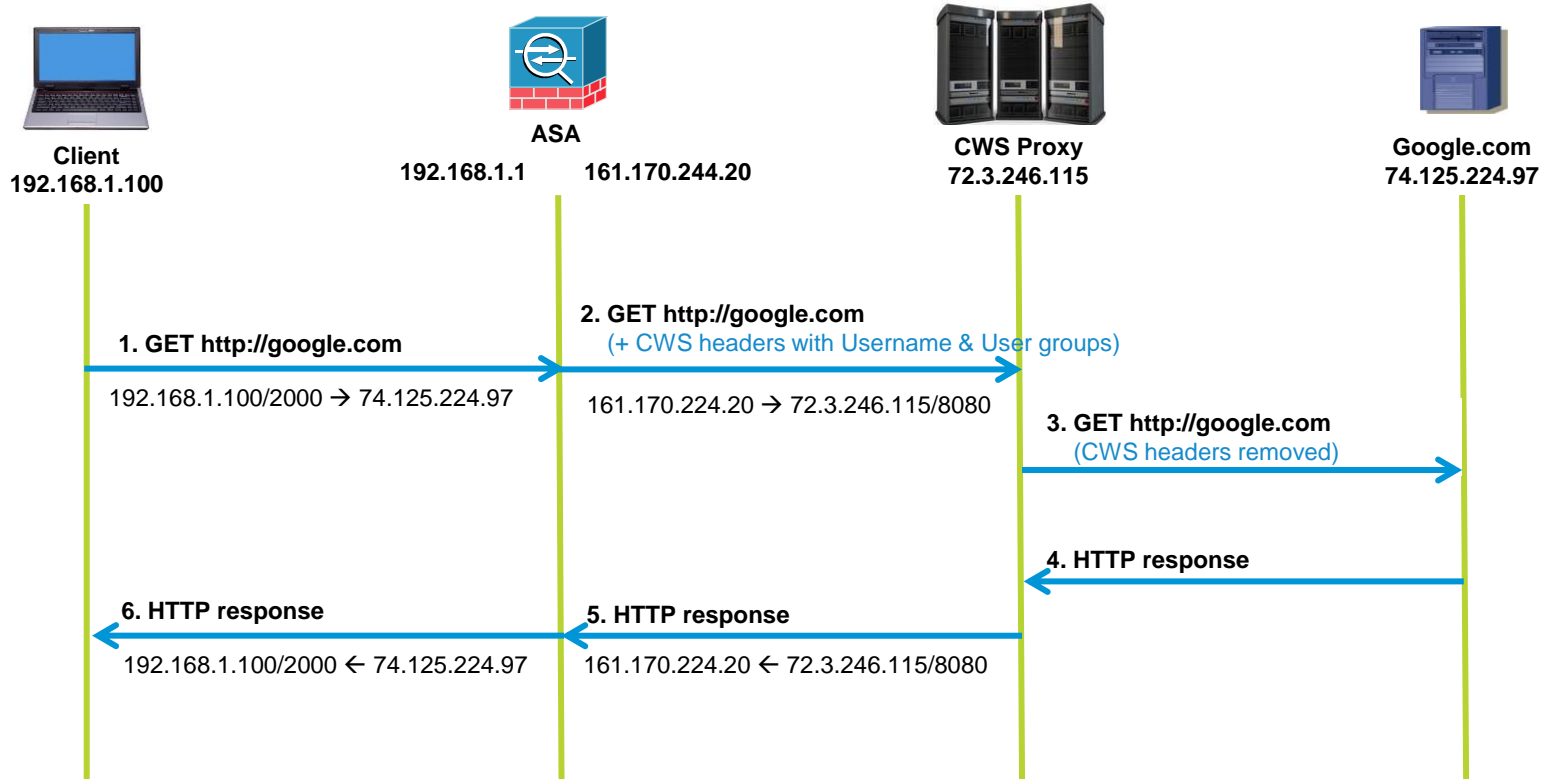
- The ASA Connector is available from v9.0, and runs on all ASA models
- Can be used for transparent deployment in HQ and branch offices
- Single and Multiple Context Modes are supported for HTTP and HTTPS traffic
- No need for special license on ASA (K8 → K9 free upgrade)
- User authorisation provided from AD via IDFW
- Automated fail-over to secondary data centre
- No need to install software on dedicated hardware, or make any browser changes/install a client on end users' machines
- CWS licensing on a per-user basis, so not tied to number of devices

CWS Connector on ASA

Transparent redirection to the cloud with Identity



Packet Flow - ASA

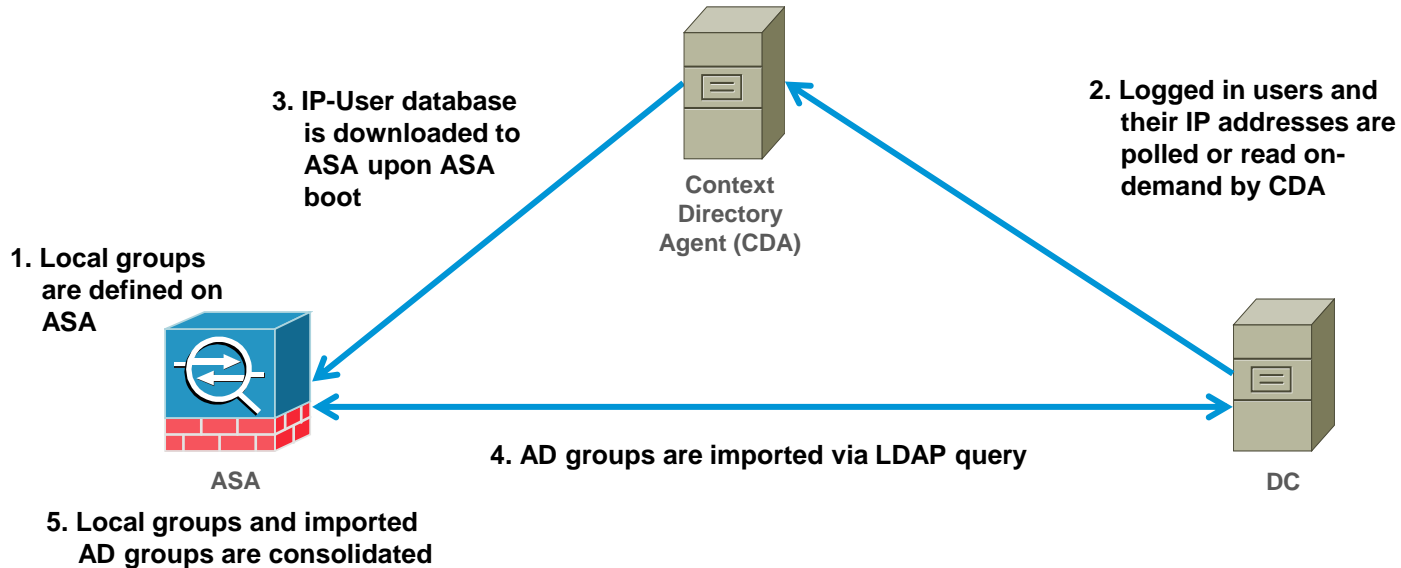


Authentication Process on ASA

IDFW process works with off-box Context Directory Agent (CDA)

- ASA performs a “transparent” auth process via IDFW and CDA
 - The CDA (off-box) communicates with Domain Controllers for user login information and forwards this to ASA
 - CDA reads from the DC’s security event log file for details of user, domain, source IP address and source port
 - Web-Portal and VPN users also supported (VPN ASA reports back to CDA)
 - Local groups are defined on ASA, ASA pulls AD group information directly from DC
 - User and group information is included in CWS headers as they are added to the outbound GET requests

ASA Authentication



6. User and group information is added to CWS headers for any registered IP addresses
7. Non-registered IP addresses will be tagged with 'default' user and group details
8. As additional users log in, CDA polls DC for changes, and updates ASA

ASA Connector

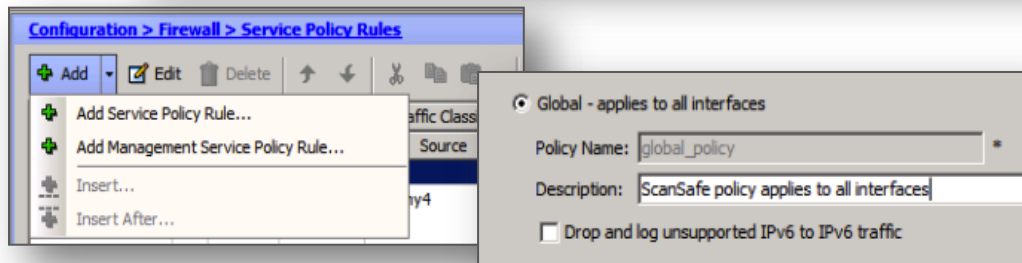
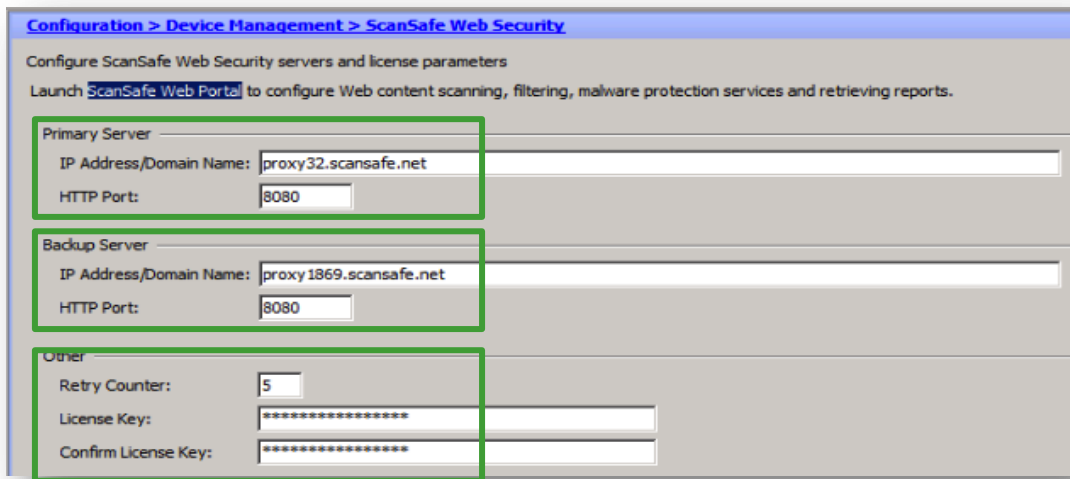


Configuration, diagnostics, troubleshooting



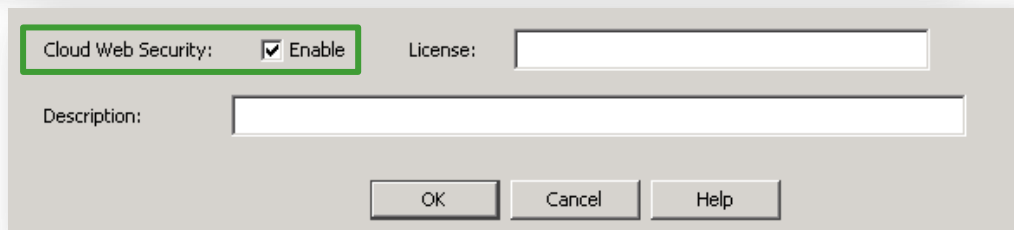
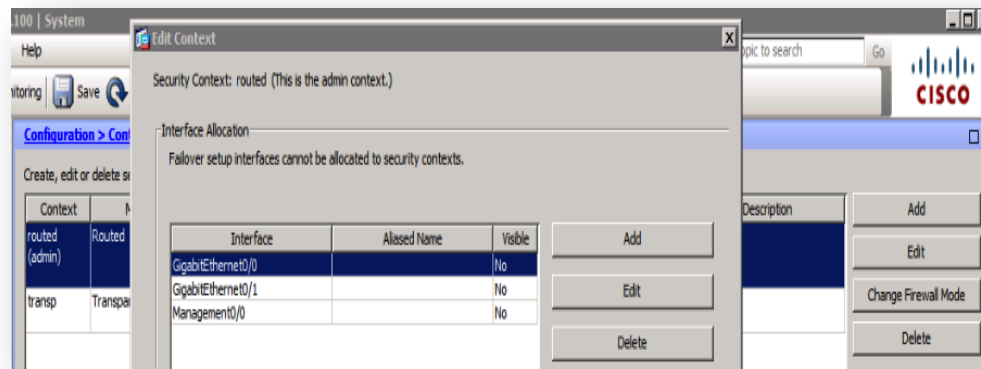
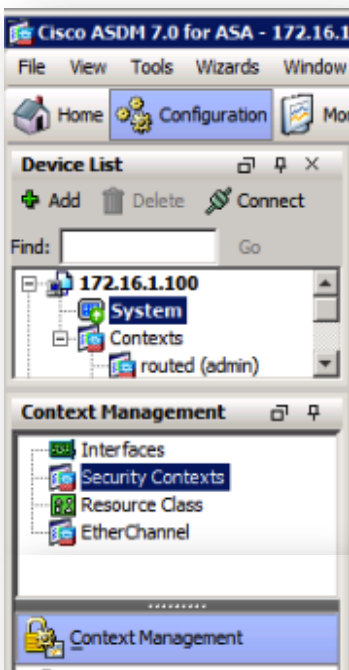
ASA Connector - Proxy and License Configuration

- The ASA Connector is configured via simple configuration steps in the ASDM utility...



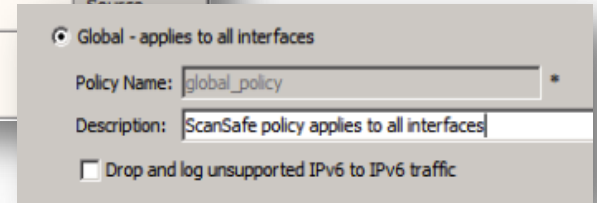
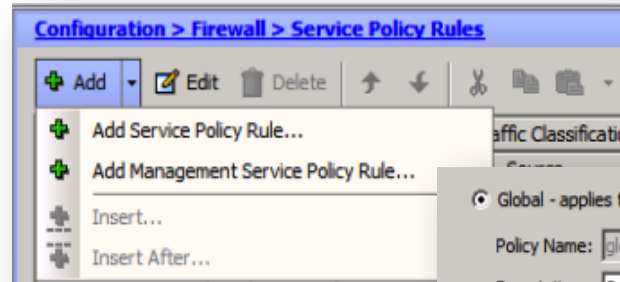
ASA Connector Configuration - Enabling CWS

- Cloud Web Security is enabled in the Security Context

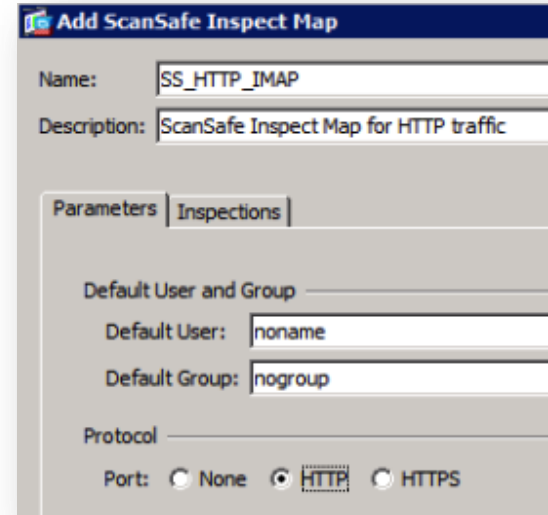
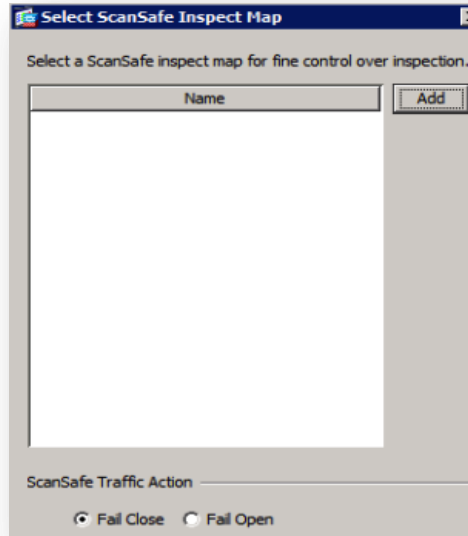


Configuring a Class Map

- Class maps are defined for sending traffic to CWS
 - Example for HTTP traffic:



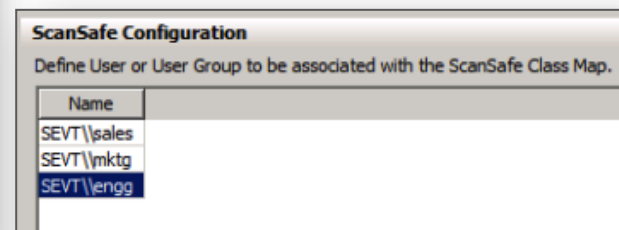
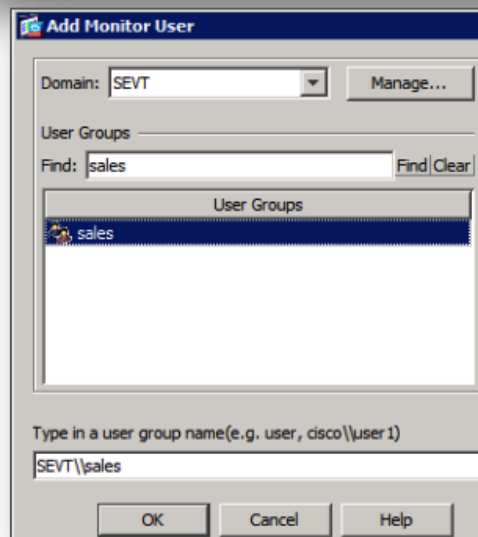
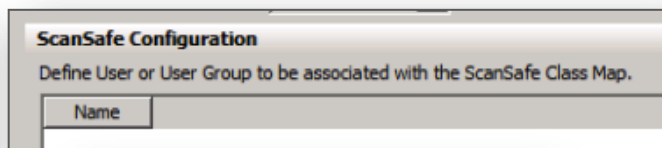
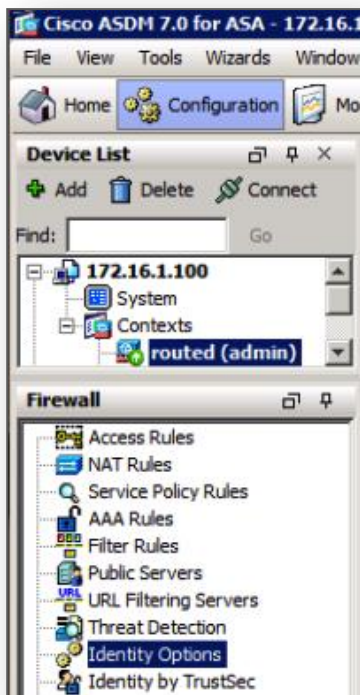
Configuring a Class Map, Cont.



Global; Policy: global_policy							
inspection_default			Match	any4	any4	default-inspec...	Inspect DNS Map preset_dns_map Inspect ESMTP (14 more inspect actions)
SS_HTTP_TRAF_CLASS	1	<input checked="" type="checkbox"/>	Match	any4	any4	http	Inspect ScanSafe Map SS_HTTP_IMAP, fail-dose

User Authorisation with ASA Connector

- The ASA Connector communicates via IDFW with CDA for user and group membership information from the company's AD



Whitelisting Traffic from Redirection to CWS



- Define FQDN Network Objects for URLs that should be exceptioned, and set them in the Service Access Policy to **not match**
 - Recommended for hosts such as software updates, AV signatures, etc.

The screenshot shows the Cisco ASDM 7.0 for ASA - 192.168.2.1 interface. The 'Add Network Object' dialog is open on the left, showing the following fields:

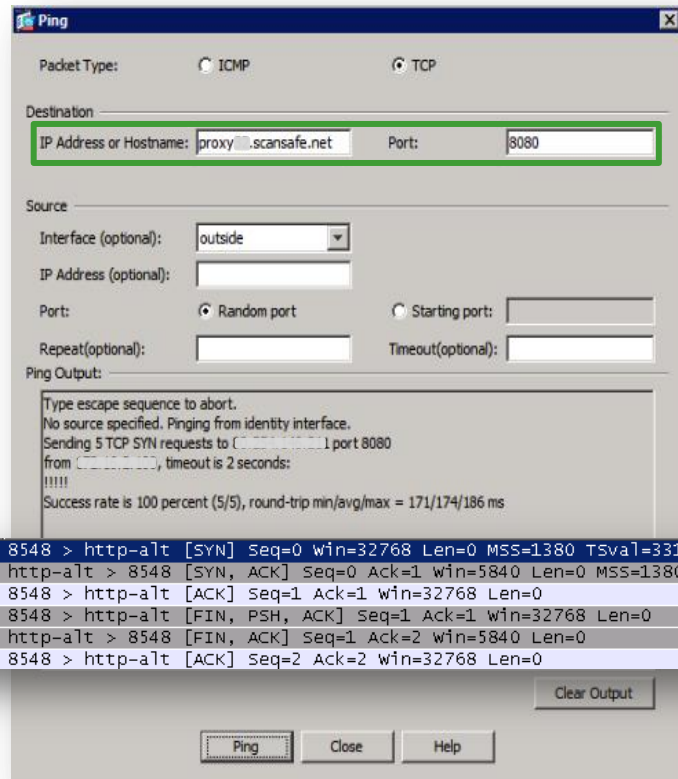
- Name: downloads.ironport.com
- Type: FQDN
- IP Version: IPv4 (selected), IPv6
- FQDN: downloads.ironport.com
- Description: IronPort download site

The main configuration window shows the 'Service Policy Rules' configuration page. The 'Traffic Classification' table is as follows:

Name	#	Enabled	Match	Source	Destination	Service
Global; Policy: global_policy						
inspection_de...			Match	any	any	default-inspec...
cws-http	1	✓	Do not match	any4	Updates.ironport.com	IP ip
	2	✓	Do not match	any4	ironport_downloads	IP ip
	3	✓	Do not match	any4	InternalNetwork	IP ip
	4	☐	Do not match	192.168.2-15	any4	TCP http
	5	✓	Match	any4	any4	TCP http

Verifying Cloud Connectivity from ASA via ASDM

- Use the Ping Tool in ASDM
 - Performed with a 3 way handshake (SYN request)



137	77.945892000	10.49.216.110	7.244.115	TCP	70 8548 > http-alt [SYN] Seq=0 win=32768 Len=0 MSS=1380 TSval=331139729 TSecr=0
139	78.109853000	10.49.216.110	10.49.216.110	TCP	60 http-alt > 8548 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1380
140	78.110002000	10.49.216.110	7.244.115	TCP	60 8548 > http-alt [ACK] Seq=1 Ack=1 win=32768 Len=0
141	78.110048000	10.49.216.110	7.244.115	TCP	60 8548 > http-alt [FIN, PSH, ACK] Seq=1 Ack=1 win=32768 Len=0
142	78.275612000	10.49.216.110	10.49.216.110	TCP	60 http-alt > 8548 [FIN, ACK] Seq=1 Ack=2 win=5840 Len=0
143	78.275730000	10.49.216.110	7.244.115	TCP	60 8548 > http-alt [ACK] Seq=2 Ack=2 win=32768 Len=0

Verifying Cloud Connectivity from ASA via CLI



- To verify connectivity to the CWS proxy, issue the command:
`show scansafe server`
- If the proxy is accessible, **REACHABLE** will be seen:

```
ciscoasa(config)#show scansafe server
Primary: proxy444.scansafe.net (172.37.44.15) (REACHABLE) *
Backup: proxy555.scansafe.net (80.204.15.88)
```

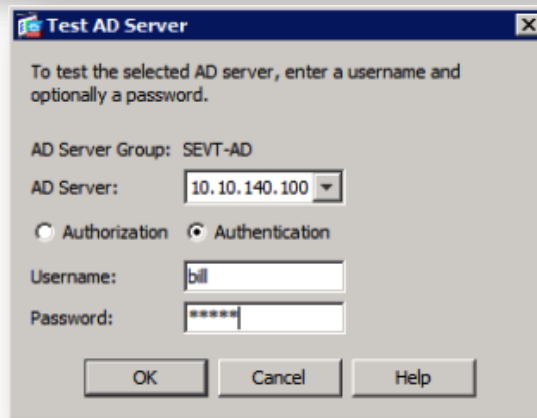
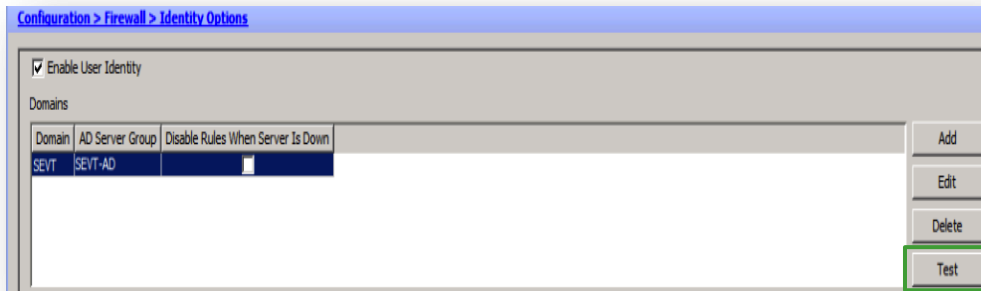
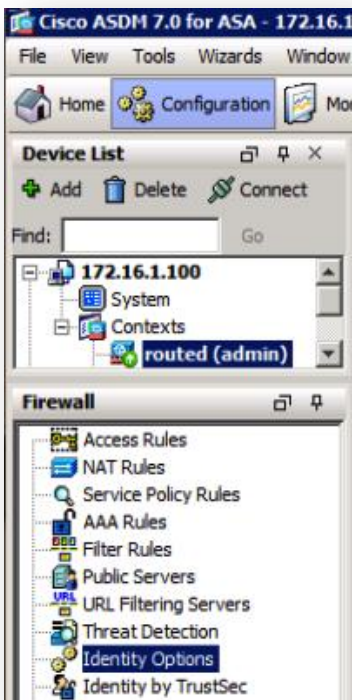
- If there is no connectivity, **UNREACHABLE** will be seen

```
Primary: proxy444.scansafe.net (NOT RESOLVED) (UNREACHABLE) for last
12 secs, tried to connect 0 times
Backup: proxy555.scansafe.net (NOT RESOLVED) (UNREACHABLE) for last
12 secs, tried to connect 0 times
```

Verifying Identity Configuration



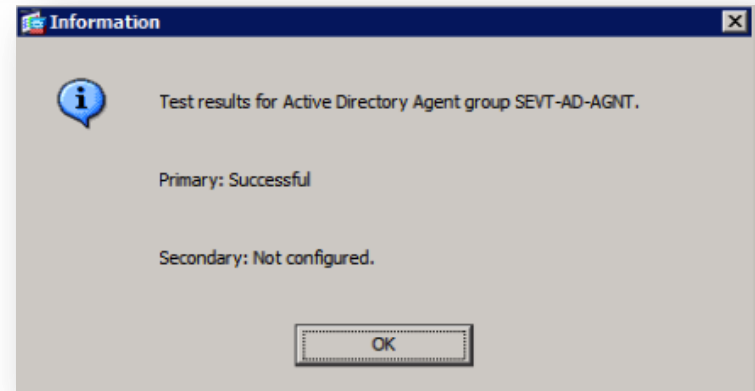
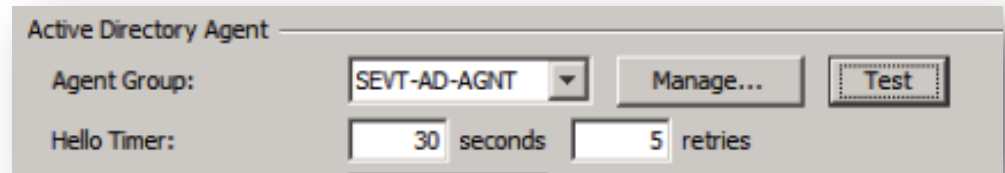
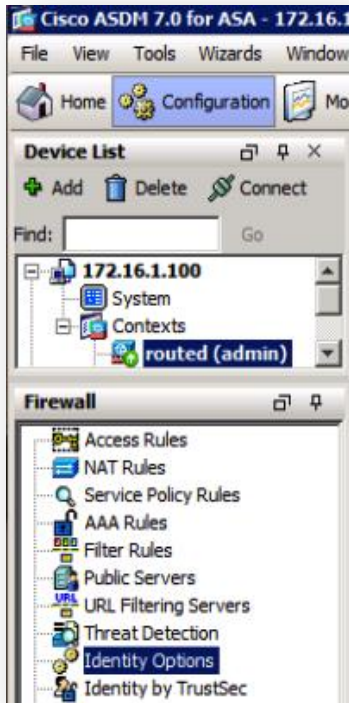
- Dedicated tool in ASDM for testing AD connectivity and user lookup



Verifying AD Agent Connectivity



- Dedicated tool in ASDM for testing connectivity with CDA / AD Agent



Session Flows and Statistics - ASDM

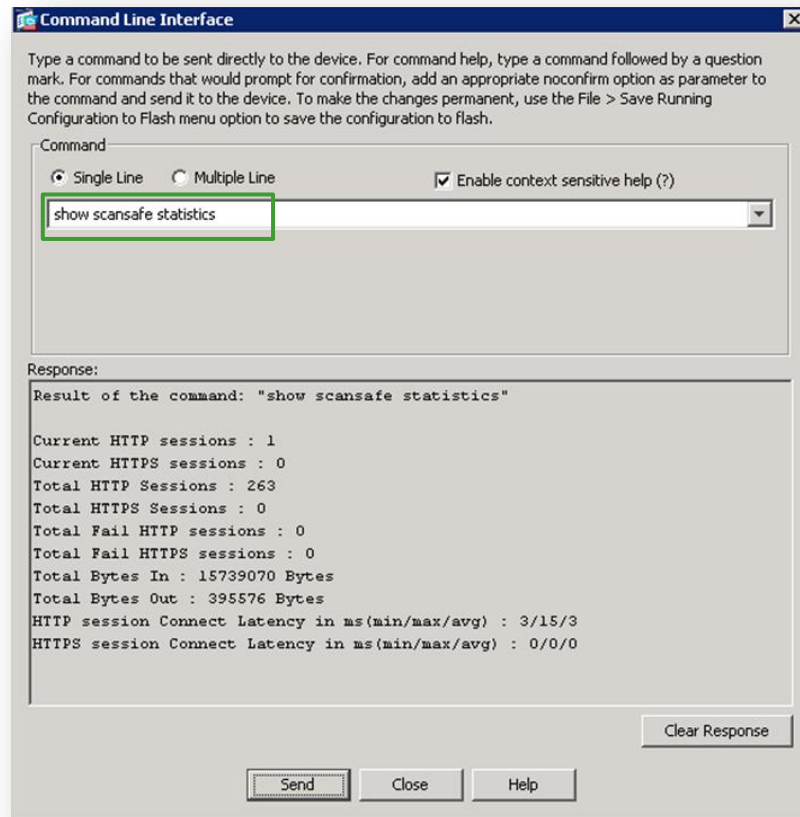
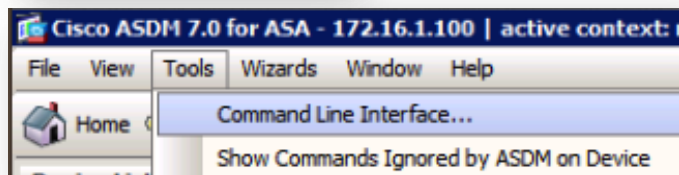
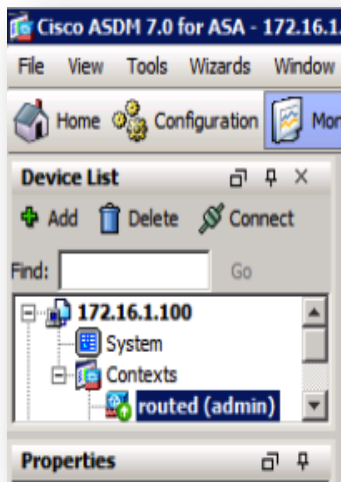


- To see the total number of redirected sessions as well as white-listed sessions (bypassed the connector, going directly to the Internet), use the `show scansafe statistics` command:

```
ciscoasa(config)#show scansafe statistics
Current HTTP sessions : 12
Current HTTPS sessions : 0
Total HTTP Sessions : 102
Total HTTPS Sessions : 0
Total Fail HTTP sessions : 0
Total Fail HTTPS sessions : 0
Total Bytes In : 6532 Bytes
Total Bytes Out : 66622 Bytes
HTTP session Connect Latency in ms(min/max/avg) : 0/0/0
HTTPS session Connect Latency in ms(min/max/avg) : 0/0/0
```

Session Flows and Statistics - CLI

- Various commands can also be run in ASDM



Checking Connections Redirected by a Policy



- `show service-policy inspect scansafe` shows the number of connections redirected or whitelisted by a particular policy:

```
Global policy:
  Service-policy: global_policy
  Class-map: inspection_default
Interface inside:
  Service-policy: scansafe-pmap
  Class-map: scansafe-cmap
    Inspect: scansafe p-scansafe fail-open, packet 0, drop 0,
reset-drop 0, v6-fail-close 0
Number of whitelisted connections: 0
Number of connections allowed without scansafe inspection
because of "fail-open" config: 0
Number of connections dropped because of "fail-close" config: 0
Number of HTTP connections inspected: 0
Number of HTTPS connections inspected: 0
Number of HTTP connections dropped because of errors: 0
Number of HTTPS connections dropped because of errors: 0
```


General Troubleshooting - whoami



- To determine if users or groups are reaching the CWS proxy properly, browse to <http://whoami.scansafe.net> on a browser
- If CWS is working, details of the user, group, and account will be seen, as obtained from the CWS proxy:

```
---
authUserName: 10.55.93.138
authenticated: true
companyName: Internal_UK_PM
countryCode: EU
externalIp: 64.103.25.233
groupNames:
  - King John
internalIp: 10.55.93.138
logicalTowerNumber: 434
staticGroupNames:
  - King John
userName: 10.55.93.138
```

General Troubleshooting - Policy Trace



1. Open a browser on a client that is connected via Cloud Web Security
2. Enter the URL
<http://policytrace.scansafe.net>
3. A page will be displayed prompting you to enter a URL
4. In the URL box, enter the URL for which you want to run a policy trace then click Go
5. The policy actions that are applied to the user for that website will be displayed

```
Identified user '<user name>' from IP address <IP address>
as part of company '<organization>'
User belongs to groups [<list of groups>]
Site categorized as '<category>'
Evaluating # HTTPS rules. HTTPS rule '<rule name>' matches
Using certificate '<certificate name>' to decrypt
Evaluating # rules after reading request headers
Evaluating rule '<rule name>'. Deferring evaluation of rule
'<rule name>'
Headers missing. Skipping quota evaluation
The website reputation is <level>
Evaluating # rules after reading response headers
Evaluating rule '<rule name>'
Deferring evaluation of rule '<rule name>'
Evaluating # rules after reading the first part of the
response body
Evaluating rule '<rule name>'
Taking allow action because of category '<rule name>'
Found virus named '<virus name>'
Blocking connection because of a virus named '<virus name>'
```

ASA Sizing with CWS



Small Office and Branch Office

ASA Platform	5505	5510	5512-X	5515-X
Maximum CWS Users	25	75	2,000	3,000

Internet Edge

ASA Platform	5520	5525-X	5540	5545-X	5550	5555-X
Maximum CWS Users	300	4,000	1,000	5,000	2,000	6,000

Enterprise Data Centre

ASA Platform	5585-X SSP10	5585-X SSP20	5585-X SSP30	5585-X SSP40
Maximum CWS Users	7,500	7,500	7,500	7,500

ISR G2 Connector

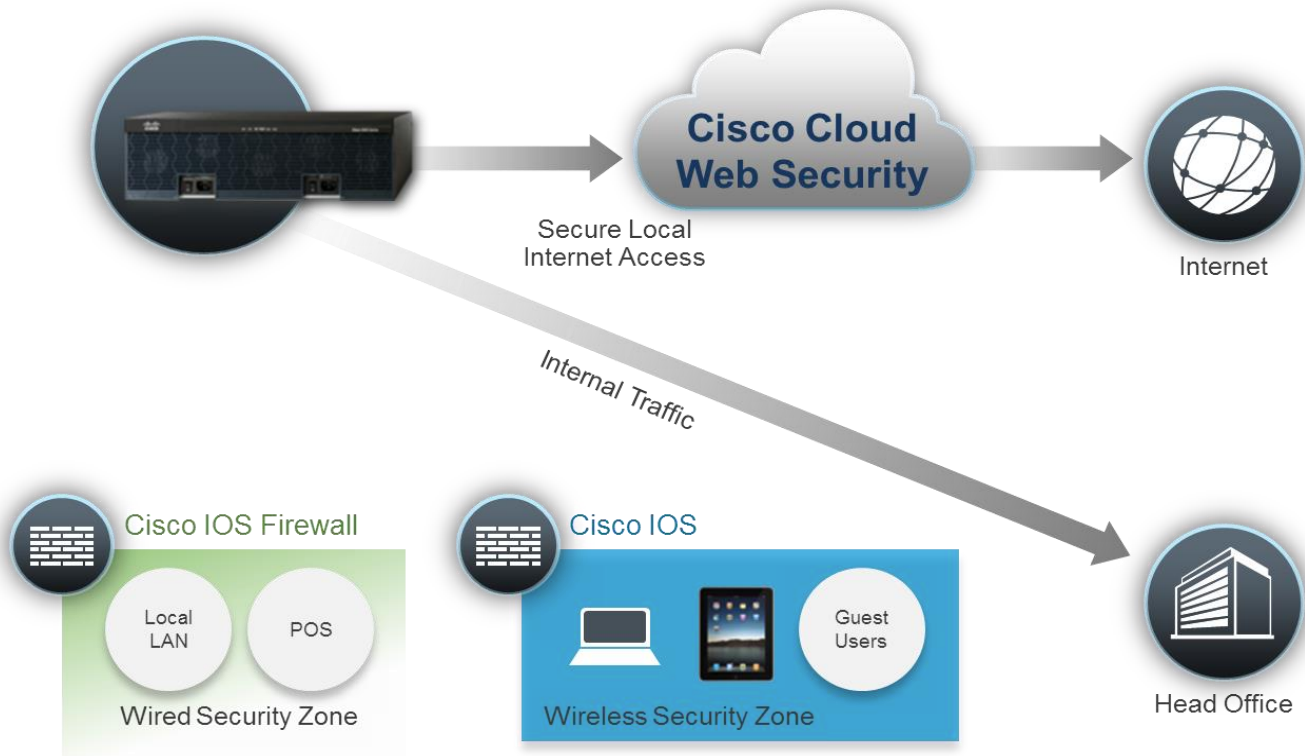


ISR G2 Connector - Main Features

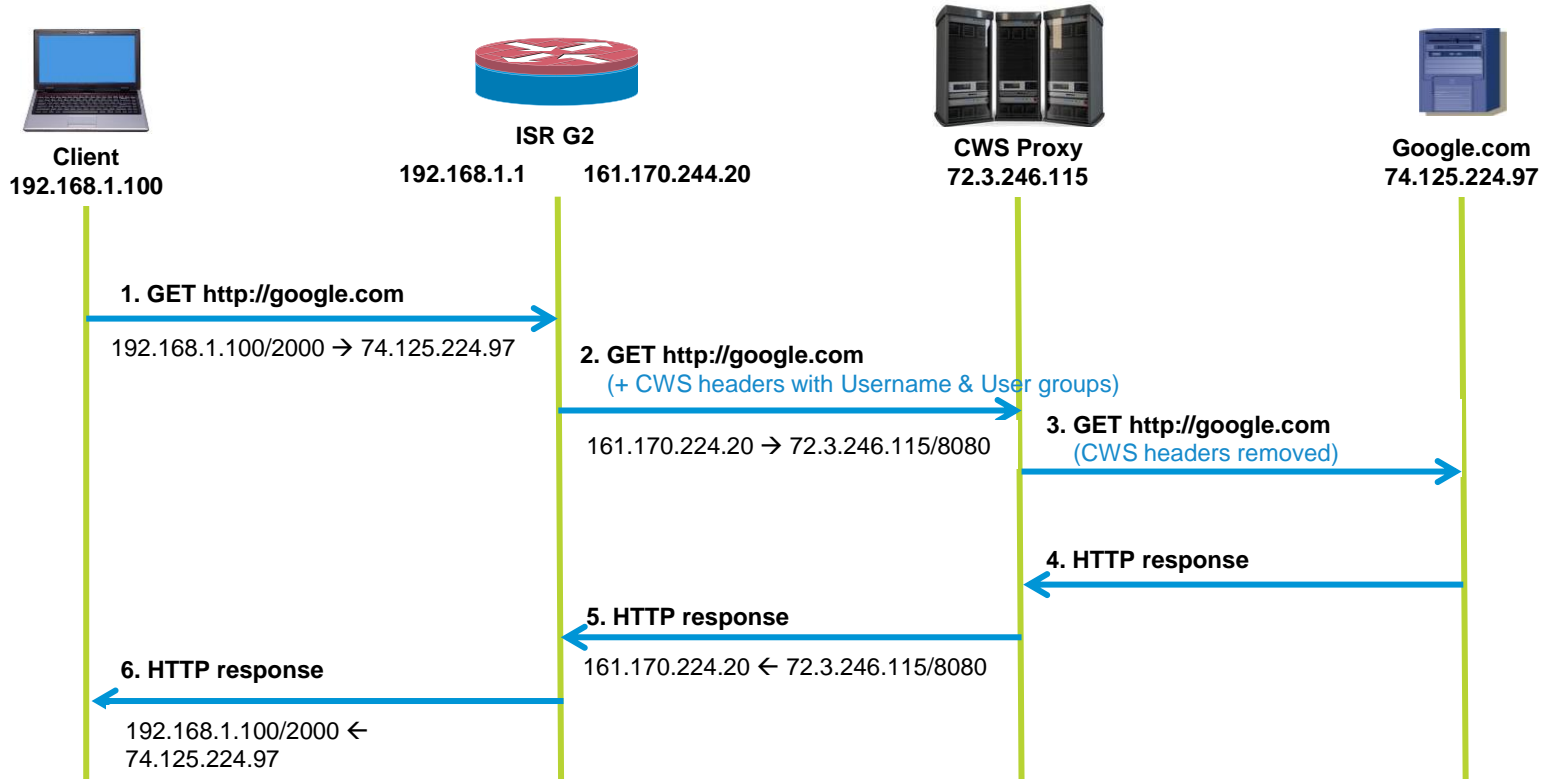
- The Connector is available in IOS (universal) images with the K9 security feature set (SEC) licenses
- Supported on 880, 890, 19xx, 29xx & 39xx/E ISR G2 platforms
- Supports re-direction of HTTP/HTTPS internet traffic directly to the cloud securely without having to backhaul to the corporate network
- User authorisation through AAA service on ISR
- Automated fail-over to secondary data centre
- No need to install software on dedicated hardware, or make any browser changes/install AnyConnect on end users' machines
- CWS licensing on a per-user basis, so not tied to number of devices

Break out Directly to the Internet from Branches

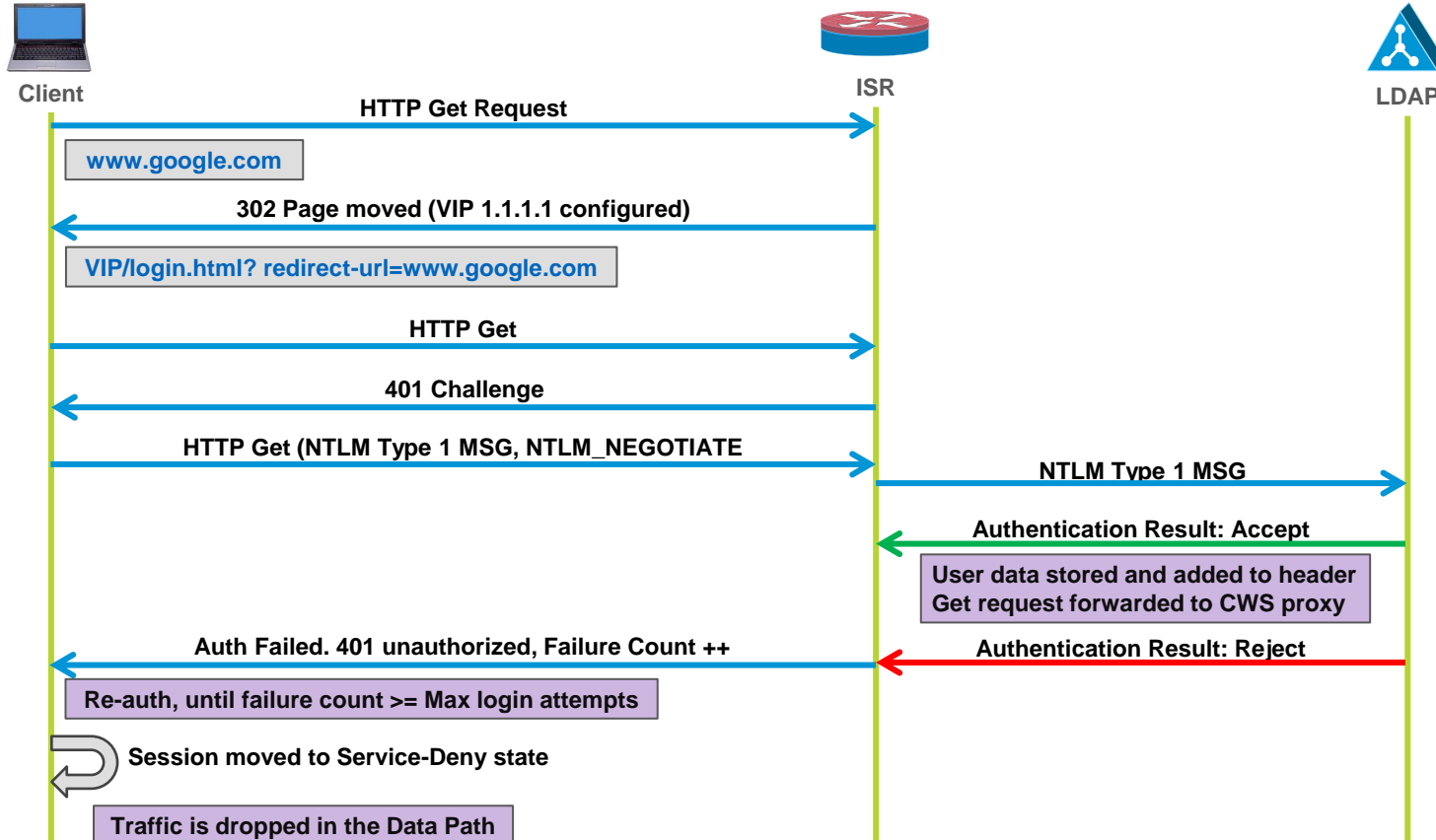
Cloud Redirection for Web Integrated into the ISRG2 Routers



Packet Flow - ISR-G2



Packet Flow Example - NTLM Authentication



ISR G2 Connector

Configuration, diagnostics, troubleshooting



ISR G2 Configuration via CLI - Redirection Example

- The redirection steps are performed simply via CLI using the `parameter-map type content-scan global` command:

```
router#parameter-map type content-scan global
server scansafe primary name proxyXX.scansafe.net port http 8080 https 8080
server scansafe secondary name proxyYY.scansafe.net port http 8080 https 8080
license 0 1234567890ABCDEFGHIJKLMNQRST
source interface GigabitEthernet0/0
timeout server 30
user-group ciscogroup username ciscouser
server scansafe on-failure block-all
```

- Use the `content-scan out` command to enable content scanning on the outbound interface:

```
router#interface GigabitEthernet0/0
content-scan out
```

ISR G2 Configuration - Authorisation Example (NTLM)

- Authorisation is performed via the built-in [aaa services](#) via a few CLI commands:

```
router#aaa new-model
aaa group server ldap ScanSafe
server ss
exit
router#ldap server ss
ipv4 10.10.137.199
transport port 3268
bind authenticate root-dn CN=ldap,CN=Users,DC=lab,DC=com password Pa$$word
base-dn CN=Users,DC=isrvlab,DC=com
authentication bind-first
search-filter user-object-type top
```

- Then the [aaa](#) services are defined, an IP admission rule is defined, and it is applied to the internal facing interface

ISR G2 Configuration - Whitelisting Example



- Whitelisting (exceptions from sending to CWS) can be based on **hosts** or **user agents**:

```
router#parameter-map type regex 888
pattern www.888.com
exit
content-scan whitelisting
whitelist header host regex 888
```

- Any requests to hosts that match those listed in the pattern will be whitelisted, and sent directly to the internet
- This is useful (and recommended) for software update hosts, or specific user agents within the organisation

Diagnostics - Verifying ISR Connectivity to Cloud

- The first step is to verify connectivity to the CWS proxy
- This is tested by issuing the command:
`show content-scan summary`
- If connectivity is established with the proxy, **Up** should be seen in parenthesis:

```
router#show content-scan summary
Primary: 172.75.240.15 (Up) *
Secondary: 87.223.142.99 (Up)
Interfaces: GigabitEthernet0/0
```

- The proxy currently in use will be marked with a *
- If there is no connectivity to the proxy, **Down** will be seen

Testing Telnet to the Cloud Proxy from the ISR



- You can also Telnet to the IP address of the proxy on port 8080:
- An **Open** message means you have connectivity to the proxy:

```
! Connectivity between ISR G2 and ScanSafe Tower
router#telnet 172.75.240.15 8080
Trying 172.75.240.15, 8080 ... Open
```

- If there is no connectivity, the telnet will time out and disconnect:

```
! No connectivity between ISR G2 and ScanSafe Tower
router#telnet 172.75.240.15 8080
Trying 172.75.240.15, 8080 ...
% Connection timed out; remote host not responding
```

Checking Session Flows

- To see the total number of redirected sessions as well as white-listed sessions (bypassed the connector, going directly to the Internet), use the `show content-scan statistics` command:

```
router#show content-scan statistics
Current HTTP sessions: 49
Current HTTPS sessions: 2
Total HTTP sessions: 1486
Total HTTPS sessions: 406
White-listed sessions: 0
Time of last reset: never
```

Session Flows, Cont.

Details:

Max Concurrent Active Sessions: 55

Connection Rate in last minute:

Redirected

HTTP: 64

HTTPS: 2

White-listed

IP-Based: 0

User/User-group: 0

Header-Based: 0

- The active number of redirected HTTP and HTTPS sessions indicates successful redirection to the cloud proxy

Active Sessions Currently Redirected to the Cloud



- To see individual active sessions that are redirected to the cloud proxy, use the `show content-scan session active` command:

```
router#show content-scan session active
```

Protocol	Source	Destination	Bytes	Time
HTTP	10.32.251.117:52790	157.166.226.25:80	(8896:26025)	00:00:12
	URI: www.cnn.com			
	Username/usergroup(s): ciscouser/ ciscogroup			

- URIs are only shown for HTTP requests, not HTTPS requests
- This command may result in numerous entries if many users are connected and actively browsing. It may be beneficial to filter results by URI, username/usergroup or IP address

Checking Entries, Connections, HTTP/S Requests



- The `show content-scan statistics memory-usage` command may be run at the request of Cisco TAC engineers in case of troubleshooting

```
router#show content-scan statistics memory-usage
Chunk Name                Size(bytes)    Chunks in use
Content-Scan entry        4128           23
Content-Scan Connection   904            23
User-Group                 84            23
HTTP Request              7464           0
HTTPS Request             6964           0
HTTPS SSL                  512            0
Buffer Packet              24            0
```

Troubleshooting - Checking if any Failed Requests



- The `show content-scan statistics failures` command is useful to run in cases where pages aren't loading, or loading very slowly
- This won't tell you the reason why there are failed requests, but will indicate a problem that can later be diagnosed by TAC

```
router#show content-scan statistics failures
Reset during proxy Mode:          0
HTTPS reconnect failures:         0
Buffer enqueue failures:         0
Buffer length exceeded:          0
Particle coalesce failures:      0
L4F failures:                     0
Lookup failures:                  0
Memory failures:                  0
Tower unreachable:                0
Resets sent:                       0
```

Testing Users' Authentication Status

- If a user authentication fails more than the maximum allowed login attempts, the user is put in a service-denied state until a configurable watch-list timer has expired (default = 30 minutes)
- To see the status of a user, type `show ip admission cache`
- Authenticated user:

```
router#show ip admission cache
Authentication Proxy Cache
Client Name cisco, Client IP 10.10.10.4, Port 59400,
timeout 1440, Time Remaining 1440, state ESTAB
```


Testing Users' Authentication Status, Cont.

- A user who has been put in the service-denied state after too many incorrect login attempts:

```
router#show ip admission cache
Authentication Proxy Cache
Client Name guest, Client IP 10.10.10.4, Port 59527,
timeout 1440, Time Remaining 2, state SERVICE_DENIED
```

- An admin can then clear the watch-list entry manually by issuing `clear ip admission watch-list [* | ip address]` to allow the user to re-authenticate

Implementation at Various Venue Types



- ISR-G2 integration is useful for retail & commercial enterprises who provide Wifi access to customers, guests and casual users, preventing inappropriate content and risk of malware on their assets



- Hotels
- Airports
- Cafés
- Restaurants



- Retailers



- Guest Access

ISR-G2 Sizing with CWS



Model \ Authentication	3945E	3925E	3945	3925	2951	2921	2911	2901	1941	1921	891
No Authentication	5,000	5,000	1,200	900	600	500	500	350	350	300	120
Web Proxy Authentication	1,200	1,200	1,200	900	600	500	500	350	350	300	120
HTTP Basic Authentication	1,200	1,200	1,200	900	600	500	500	350	350	300	120
NTLM Authentication	1,200	1,200	1,200	900	600	500	500	350	350	300	120

WSA Connector



Embracing the Strength of the Cloud with Local Features



WSA Connector - Main Features

- The Connector is available in AsyncOS ver. 8
- Dedicated Connector configuration via Configuration Wizard
- Supported on S-Series x70 and x80, and WSAv platforms
- Automated fail-over to secondary cloud proxy
- User authorisation through existing WSA mechanism
- CWS licensing on a per-user basis, not per WSA devices
- Common use cases:
 - Connector can be run in a virtual environment when no Cisco appliances available
 - Useful for customers looking for a mix of cloud security with appliance-based features
 - Existing WSA in place, and want to move to CWS to also support roaming users in single policy

WSA Connector

Combine centralised cloud advantages with local features

WSA Connector

- Redirection to CWS
- Primary/Backup proxy failover
- Company, group, and user details in encrypted headers
- Fail-open/fail-closed mechanism

Connector


Cisco Cloud
Web Security

WSA Local Features

- Transparent authentication via on-box NTLM v2
- Transparent or explicit proxy
- Local caching support
- Off-box DLP integration
- Appliance based

WSA

WSA Connector Definitions

 Cisco IronPort S650
Web Security Appliance

1. Start **2. Network** 3. Review

Cloud Web Security Connector Settings

Cloud Web Security Proxy Servers: ?	Server Address <input type="text" value="proxy1731.scansafe.net"/> <input type="text" value="proxy193.scansafe.net"/> <input type="text"/> <small>hostname or IP address</small>
Failure Handling:	<small>Specify how to handle requests if all specified Cloud Web Security Proxy servers fail.</small> <input checked="" type="radio"/> Connect directly <input type="radio"/> Drop requests
Cloud Web Security Authorization Scheme:	<input type="radio"/> Authorize transaction based on IP address <input checked="" type="radio"/> Send authorization key information with transaction Authorization Key: <input type="text" value="1B6FDF:"/> <input type="text" value=":09AD48"/>

WSA Sizing with Connector



Model	User Range
S170	< 1,500
S370	1,500 – 5,999
S670	6,000 – 7,500

- Coming soon... Additional sizing
 - Connector on new X80 platforms
 - Connector on WSAv (virtual) platforms

Roaming Users



Secure Mobility with AnyConnect Web Security



AnyConnect Web Security - Main Features

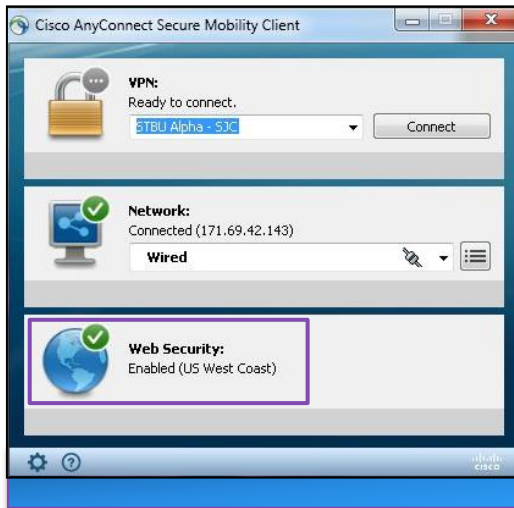


- Full support for Windows (XP, Vista, 7, 8) and Mac OS X (10.5, 10.6, 10.7, 10.8) - 32 and 64 bit versions
- Support for all WWAN (3G modem) network interfaces
- User and group details supported for granular policies and reporting
- Control of direct access to native IPv6 websites (e.g. IPv6.Google.com)
- Lockdown to prevent local Admin users from altering the service
- Hosted configuration to allow the organisation to make changes to their AnyConnect profile and push it to all their roaming clients
- Can be pushed to clients from ASA via ASDM policy settings
- Licenses for roaming users included when ordering through Cisco GPL

What is AnyConnect Web Security?



- Web Security is one of the components of Cisco's AnyConnect VPN client
- Web Security is an additional layer within Any Connect, that works with the driver, alongside the other existing features

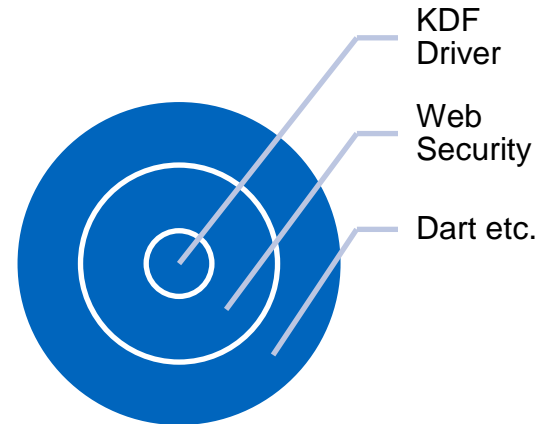


VPN

NAM

Web Security

Driver





What Does Web Security Do?

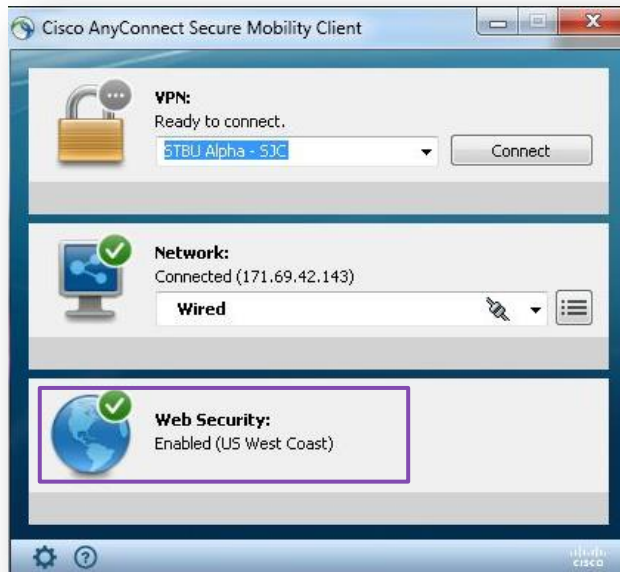
- Intercepts and redirects the user's external web traffic to the cloud proxies
- Automatic peering to the closest data centre for best performance
- Traffic is SSL encrypted for improved security over public networks
- Works with Full or Split Tunnel VPN clients





With or Without the VPN Client

- Web Security can be used as part of Cisco's AnyConnect VPN client, or in standalone mode with any other VPN client



AnyConnect Web Security



Configuration and Deployment



- The admin uses Profile Editor to create the profile which is then obfuscated and deployed together with the AnyConnect client
- The client is installed manually on Windows and OS-X clients, or deployed to users from an ASA upon VPN connection (defined in ASDM)
- The obfuscated profile resides on the client machine:

```
ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Web Security  
/opt/cisco/anyconnect/websecurity
```
- When installed 'locked down', the **Cisco AnyConnect Secure Mobility Agent** service cannot be stopped, even by local admins
- On OS-X, the **acwebsecagent process** cannot be killed
- The agent can be stopped via command line with an admin password



Creating the Profile - Proxies

- All available global proxies are listed here for the client to use
- A default proxy should be selected

The screenshot shows the 'AnyConnect Profile Editor - Web Security' window. The 'Scanning Proxy' section is active, displaying a table of scanning proxies. The table has columns for Scanning Proxy, Host Name, Plain Port, SSL Port, and Display/Hide. The 'UK' proxy is selected as the default. Below the table, there is a 'Default Scanning Proxy' dropdown menu set to 'UK', a 'Traffic Listen Port' input field, and an 'Add' button. A list of ports (80, 8080, 3128) is shown below the input field, with a 'Delete' button next to it. The 'Scanning Proxy list is currently up-to-date.' message is displayed above the table.

Scanning Proxy	Host Name	Plain Port	SSL Port	Display/Hide
UK	80.254.158.219	8080	443	Display
Germany	46.255.40.98	8080	443	Display
France	80.254.150.66	8080	443	Display
Denmark	80.254.154.98	8080	443	Display
Switzerland	80.254.155.66	8080	443	Display
South Africa	196.26.220.66	8080	443	Display

Default Scanning Proxy: UK

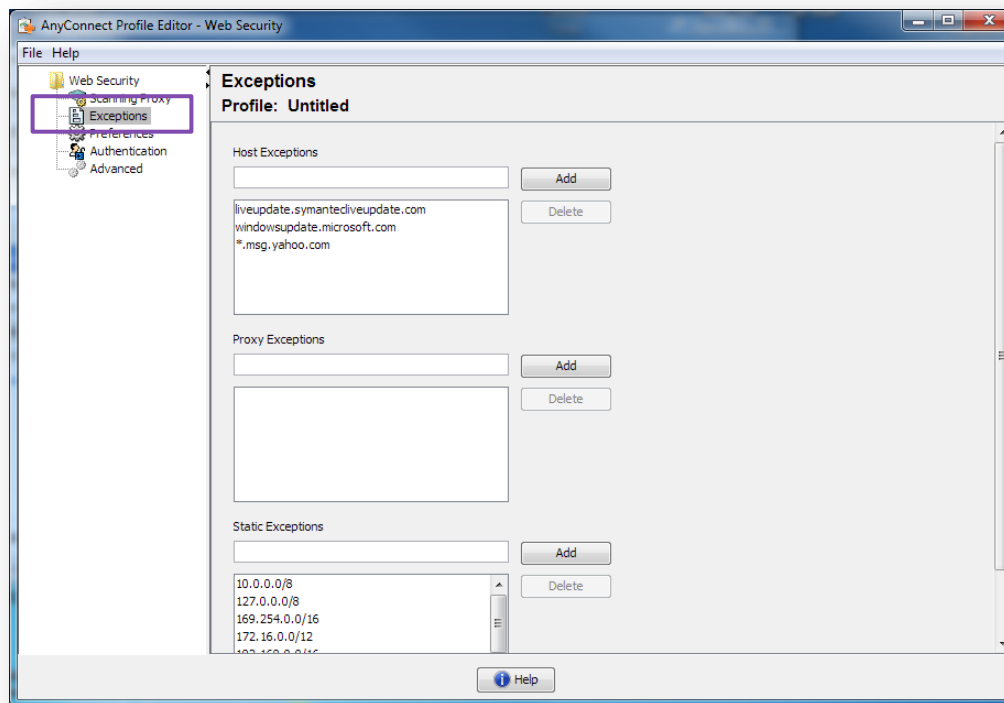
Traffic Listen Port: Add

80
8080
3128 Delete



Creating the Profile - Exceptions

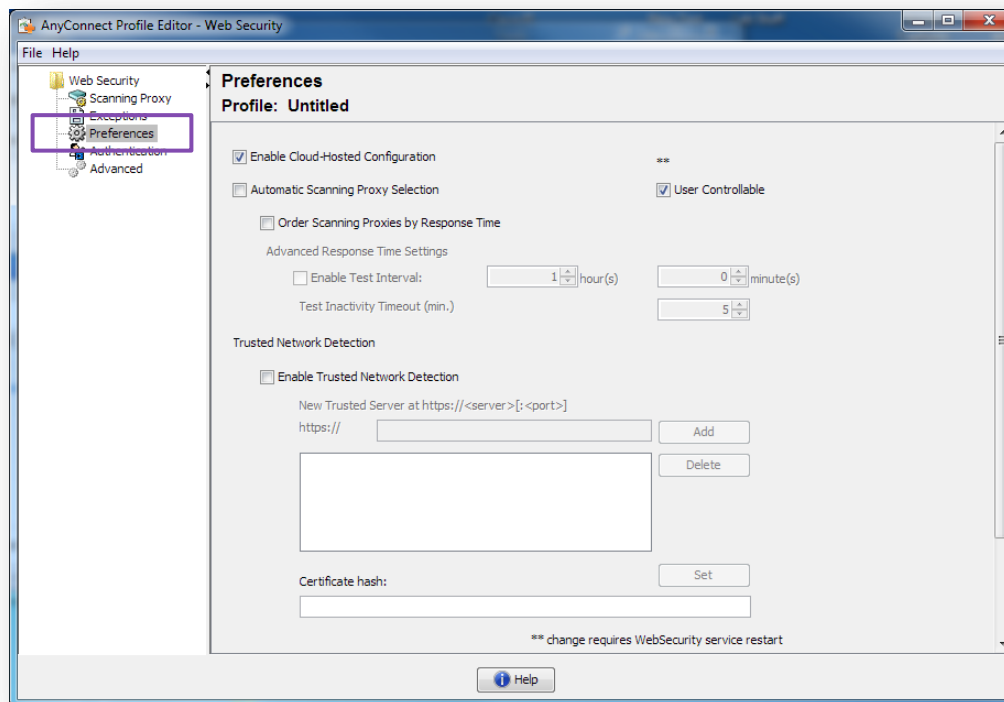
- Host, Proxy, and Static exceptions are configured for bypassing the Web Security agent for certain traffic





Creating the Profile - Preferences

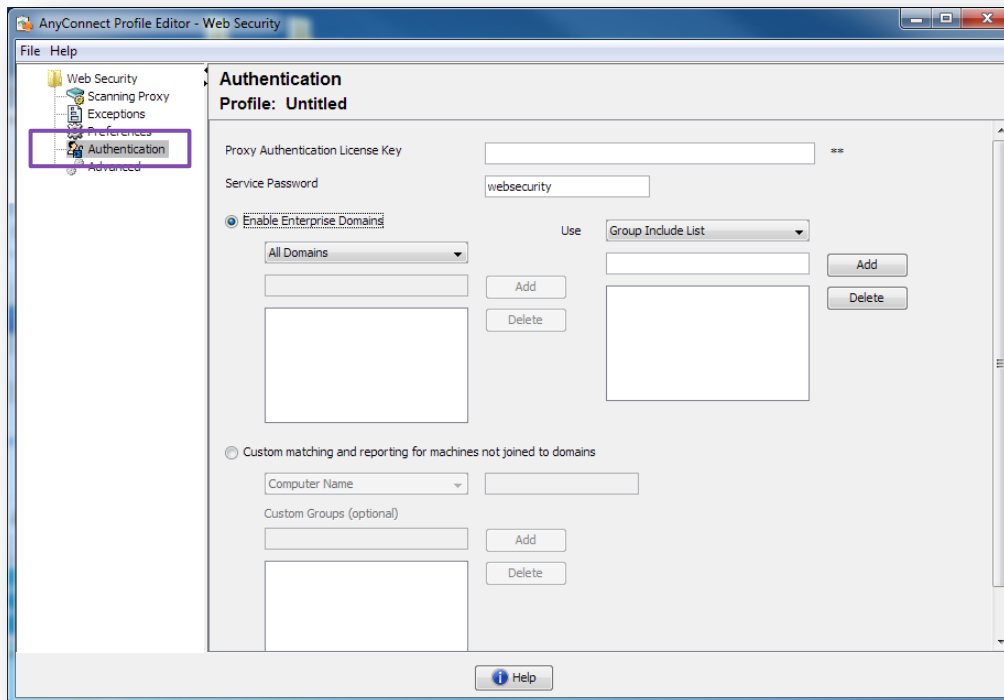
- General settings such as hosted configuration, proxy selection behaviour, and TND (Trusted Network Detection)





Creating the Profile - Authentication

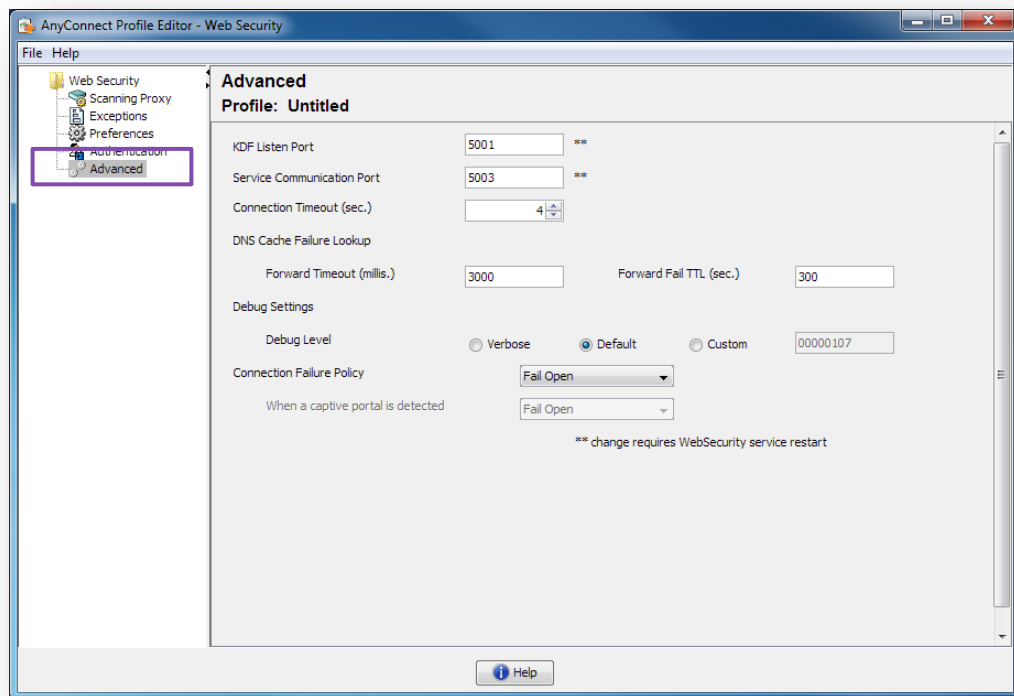
- Company or Group Key, Admin password for disengaging, domain and machine information



Creating the Profile - Advanced



- Advanced values and debug levels should be changed only if instructed to do so by CWS Technical Support (TAC) representatives





Hosted Configuration

Dynamic updates to AnyConnect configuration

- Hosted configuration allows the admin to make changes to the AnyConnect configuration and automatically push it to all roaming clients
 - The configuration files are hosted in the CWS cloud
 - This is especially useful in cases of roaming users who may not connect back to the corporate network for long periods of time
 - The client periodically searches for an updated config with the same license key
 - Multiple files, and versions of each file can be saved

Information	
Active	<input checked="" type="checkbox"/>
Type	Web Security
Created On	8/11/11 3:29 PM
Last Modified	8/11/11 3:29 PM
Note	Jonny test file
Associated Key	B229 (Group) ▼

Save

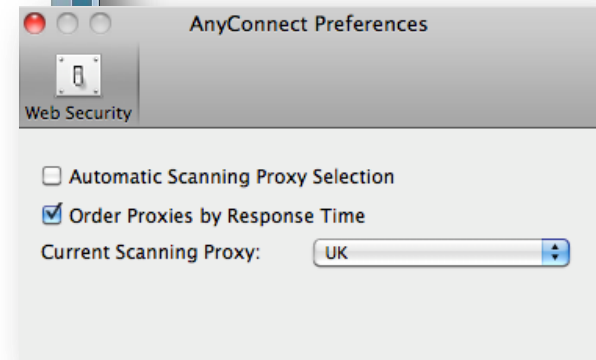
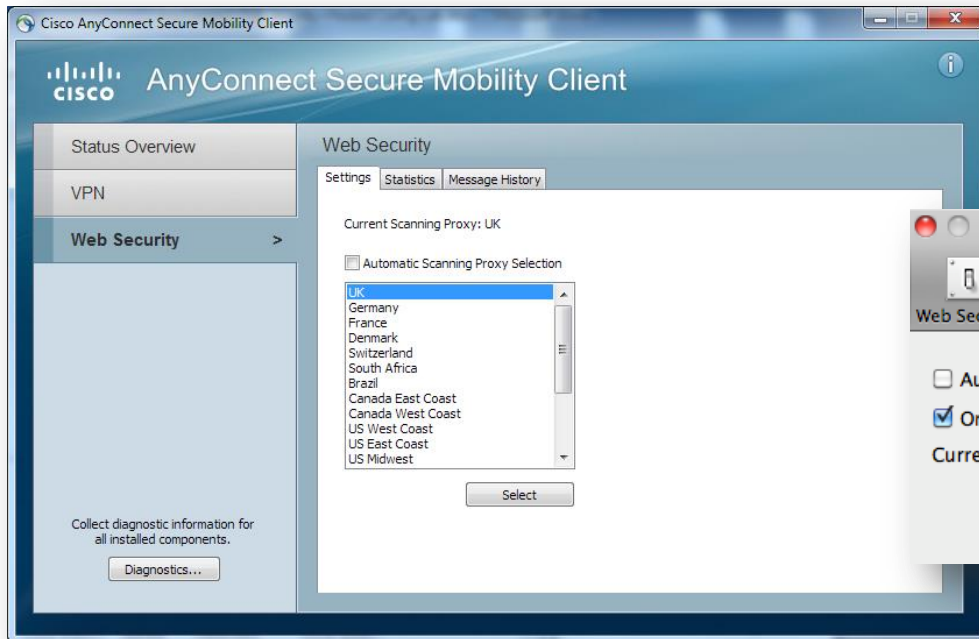




AnyConnect GUI

Giving users some level of control

- The admin can optionally give the user the ability to select proxies



AnyConnect Web Security Messages



- View statistics and messages in the GUI and Windows Event Viewer / Mac system log

The screenshot shows the Cisco AnyConnect Secure Mobility Client interface. The 'Web Security' section is active, displaying a 'Message History' window. The history lists various events such as 'Enabled (UK)', 'Service unavailable', and 'Waiting to contact the Web Security server' with their respective timestamps.

The screenshot shows the Windows Event Viewer with the 'Cisco AnyConnect Web Security Module' selected. A table of events is displayed:

Level	Date and Time	Source	Event ID	Task C
Information	18/02/2011 10:04:21	acwbs...	256	(1)
Information	18/02/2011 10:04:21	acwbs...	256	(1)
Error	18/02/2011 10:04:21	acwbs...	256	(1)
Warning	18/02/2011 10:04:21	acwbs...	256	(1)
Information	18/02/2011 10:04:21	acwbs...	256	(1)

Below the table, the details for 'Event 256, acwbscagent' are shown, including a 'General' tab with a 'TRACE' log snippet.

The screenshot shows a Mac system log window with the search term 'anyconnect'. The log entries detail the startup process of the Cisco AnyConnect Secure Mobility Client, including the loading of modules like 'libvpnipsecdylib' and the initialization of the 'ac06websecurity.log' file.

The screenshot shows the 'Web Security Statistics' dialog box, which is divided into two main sections: 'Scanning Proxy Information' and 'Service Information'. Each section contains a table of active and total connections.

Scanning Proxy Information		Active Connections	
Selection Mode:	Manual	Filtered:	0
Current Proxy:	US West Coast	Bypassed (host or proxy):	0
Last Proxy Switch:	Fri Aug 12 17:18:55	Bypassed (LAN):	0

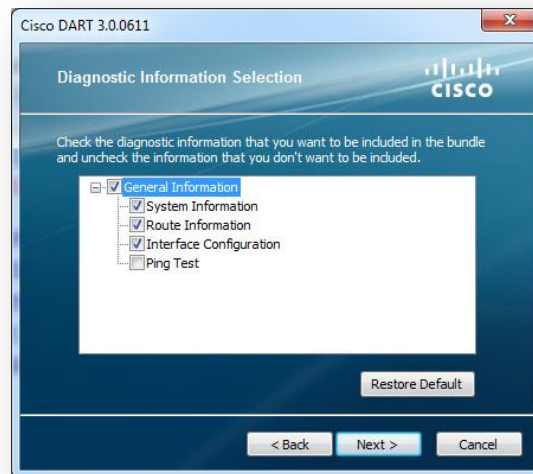
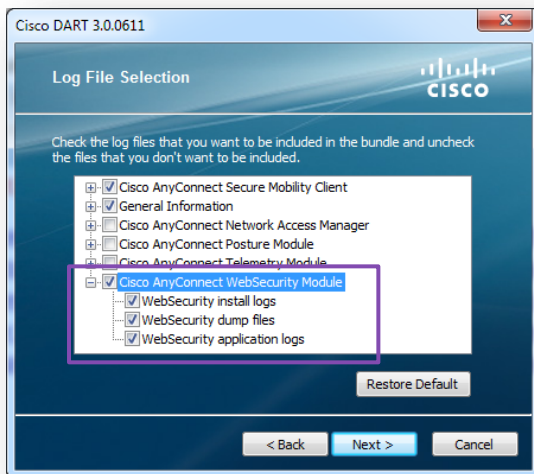
Service Information		Total Connections	
License Key:	Valid	Filtered:	2
Status:	Enabled	Bypassed (host or proxy):	0
Enabled Since:	Fri Aug 12 17:18:54	Bypassed (LAN):	0
Detect on LAN:	Disabled		
On LAN:	N/A		



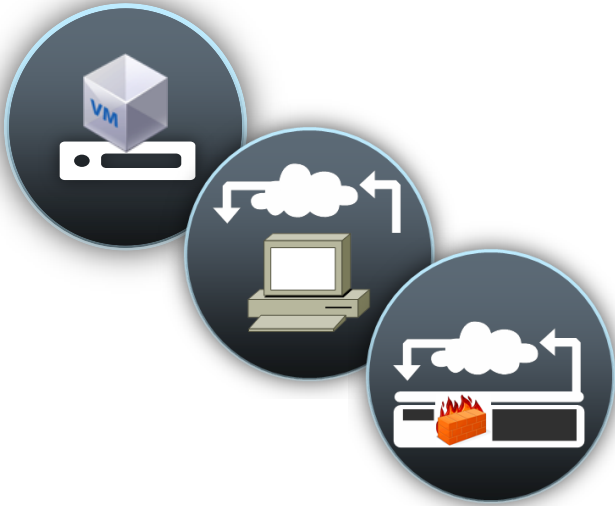
AnyConnect Web Security Debugging



- A DART Package can be created for more advanced debugging scenarios
- All Web Security components should be selected when running the DART wizard
- The DART bundle contains the WebSecurity event log, install and upgrade logs, ipconfig data, route data, and network interfaces data



Direct to Cloud Options - No Cisco Devices



Redirection options



Authentication options



No Cisco Device? No Problem!

- When no Cisco device is available, web traffic can still be redirected to the cloud through one of these methods:
 - WSA Connector on a virtual environment (full connector features + auth)
 - Browser proxy settings/hosted proxy auto configuration (PAC) for browser redirection
 - Traffic forwarding on any other perimeter device that supports forwarding of web traffic via port 8080, failover between two proxies, and exception handling



WSAv Connector



Hosted PAC



Traffic forwarding

Cookie-Based Authentication



- EasyID and SAML are cookie-based client-less authentication methods
- If a cookie is already present, the authenticated user is recognised, and the policy is applied
- If there is no cookie present, a redirect request is sent and the authentication process commences
- Each time a user visits another domain, the cookie gets duplicated so the user doesn't have to authenticate again
- Cookies are session based or persistent and remain as long as the browser is open, or haven't expired
- Perform authentication only, so traffic still needs to be redirected
- Can be used with a Cisco device configured for redirection only



Cisco *live!*






EasyID - Cookie-based Authentication

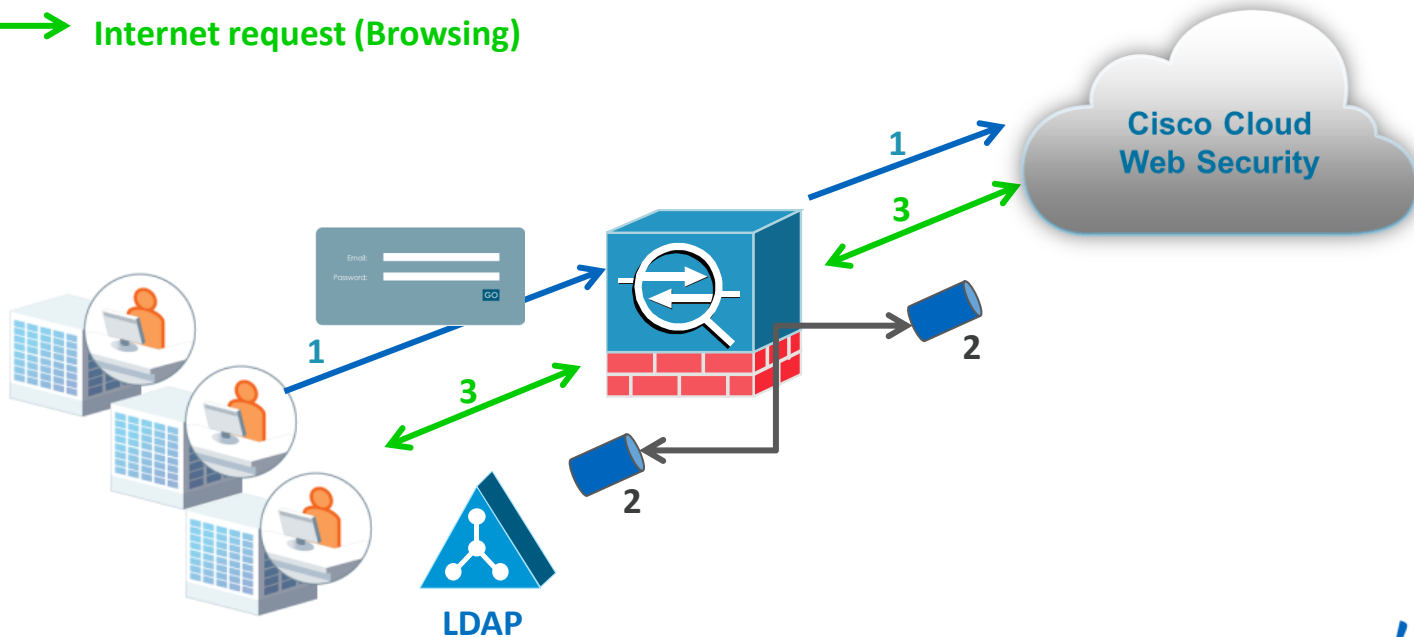
- EasyID is a cookie-based authentication method that authorises from the cloud, therefore does not require anything to be installed on the network
- Specific firewall ports need to be opened to allow requests from specific IP addresses (from the CWS infrastructure), to perform a secure LDAP request
- EasyID is supported on any platform, on any browser that accepts cookies
- EasyID supports the LDAP protocol with standard and secure LDAP authorisation to various LDAP servers such as:
 - MS AD
 - Novell
 - OpenDJ
 - Sun





Authenticating Users with EasyID

- 1  User Information - over HTTPS
- 2  User Information - LDAPS
- 3  Internet request (Browsing)



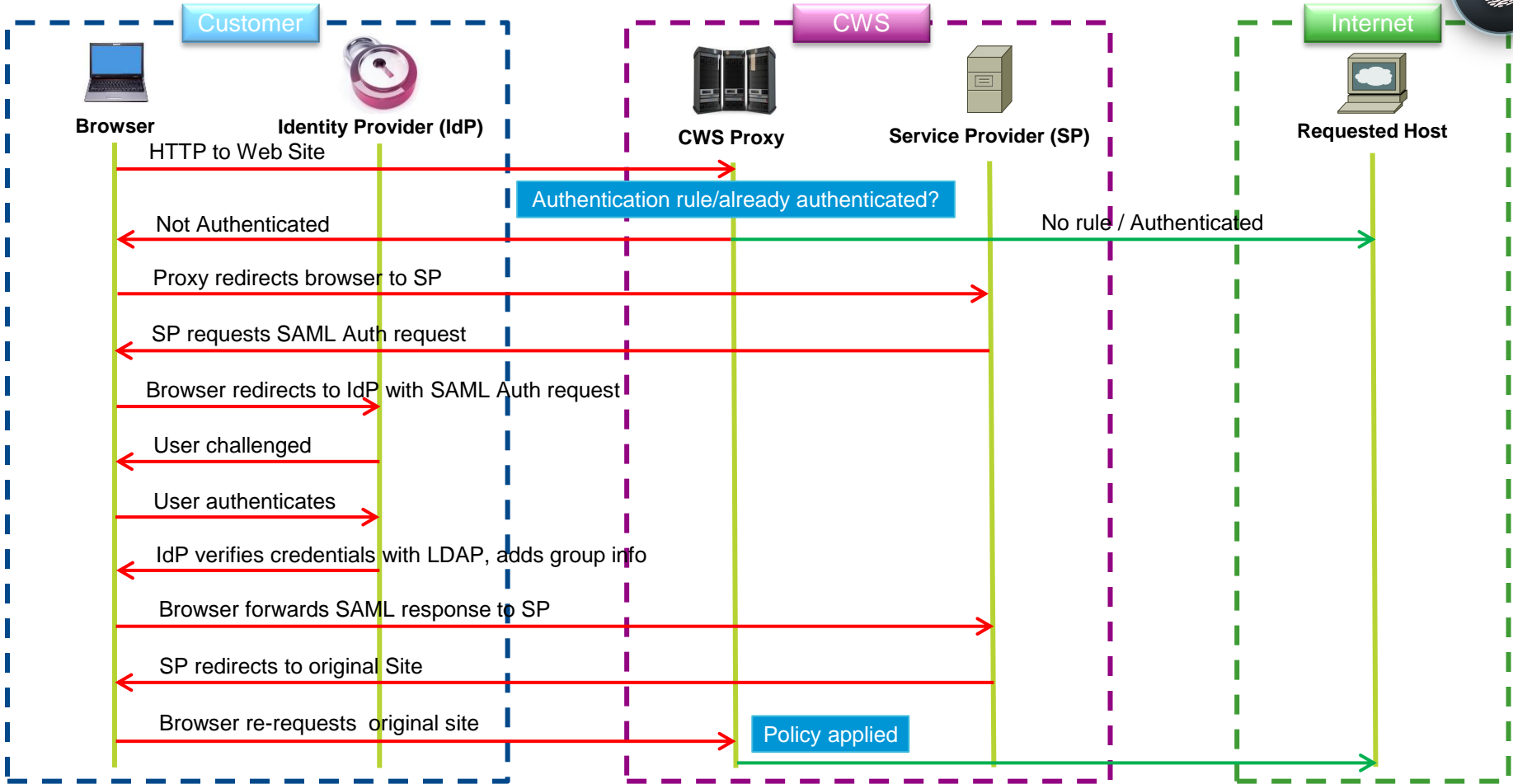
SAML - Cookie-based Authentication



- CWS uses the SAML technology to identify and authenticate users when browsing HTTP and HTTPS sites
- The cloud hosted Service Provider (SP) communicates with a customer managed Identity Provider (IdP) via browser redirections and hidden forms containing SAML messages to authenticate users
- The whole process is performed using the SAML 2.0 protocol, which is all via browser redirects, so therefore does not require the opening of any firewall ports, or any access to an internal LDAP server
- This solution is useful to any organisation already using an IdP for Single Sign On (SSO) purposes
- Supported SAML IdP's:
 - ADFS
 - Pingfederate



Authenticating Users with SAML



Deployment Summary & Feature Guide

	ASA Connector	ISR Connector	WSA Connector	Explicit Proxy	AnyConnect
Cloud Web Security features supported whilst using any platform					
HTTPS Inspection (MITM) ¹			All platforms		
Web Filtering Exceptions			All platforms		
URL Categorization			All platforms		
Application Visibility and Control feature			All platforms		
URL Dynamic Classification			All platforms		
Customizable Notifications			All platforms		
Outbreak Intelligence (Zero Day Malware)			All platforms		
Outbound Content Control			All platforms		
Redirection Capabilities					
Supported user redirection method	Transparent	Transparent / Explicit	WCCP / Explicit	Explicit	Transparent
How devices authenticate to cloud	License Key ²	License Key ²	License Key ²	Egress IP	License Key ²
Tower Failover ³	Failover is determined by lost connection not slow connection. Connection to the towers is checked at regular interval and failover to another tower occurs on the platform if tower does not return a response			Via proxy PAC file	Available in version 3.1 when configured with Detect Closest Tower (DCT)
SSL Tunnelling ⁴	No	No	No	No	Yes (default)
Whitelisting (Exceptions) ⁵ options	IP, IP Ranges	IP,IP Ranges, URL Host (with wildcard), User Agent	IP/CIDR, FQDN, URL (with wildcard), User Agent	IP,IP Ranges, URL Host (with wildcard), User Agent	IP, IP Ranges, Host
Authentication Details					
Mechanism	IDFW	ISR AAA Services	LDAP, NTLM, CDA	N/A	GP result API - Windows
Additional options	EasyID / SAML	EasyID / SAML	EasyID / SAML	EasyID / SAML	EasyID / SAML
Transparent	Yes	Yes	Yes (NTLM, CDA)	No	Yes
Supported browsers	IE, FF, Safari, Chrome	IE, FF, Chrome	IE, FF, Chrome	N/A	IE, FF, Safari, Chrome
Supported Operating Systems	Windows / OS X	Windows	Windows	N/A	Windows / OS X
Non transparent	Yes	Yes	Yes	Yes	No
Supported browsers	All	All	All	All	N/A
Supported Operating Systems	Windows / OS X / iOS devices	Windows / OS X / iOS devices	Windows / OS X / iOS devices	Windows / OS X / iOS devices	N/A
Supported protocols	NTLM (v1,v2),LDAP, Kerberos, TACACS, Radius	NTLM (v1,v2),LDAP, TACACS, Radius	NTLM, Basic (LDAP)	LDAP	NTLM - Windows API
Version that supports CWS Integration	9.0 above	ISR G2 15.3(3)M1 IOS (CA)	8.x	N/A	3.0 above



Agenda

Security Without Compromise

- What is CWS?
- The Threat Landscape
- Data Flow and Statistics
- Cloud Proxy Architecture

Live Demos

- ASA Connector
- ScanCenter Policies
- Reporting
- User Simulation

Deploying CWS with Your Cisco Infrastructure

- ASA
- ISR-G2
- WSA Connector
- AnyConnect
- Direct to Cloud

Managing CWS

- Centralised Management
- Web 2.0 Control
- Best of Class Reporting



Managing Today's Web with CWS

URL Filtering



URL database covering
over 50M sites worldwide

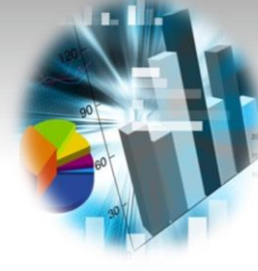
Real-time dynamic
categorisation for
unknown URLs

Application Visibility and Control



Deep application control for
social networking, file
sharing, games, IM,
webmail, media, and more

Reporting



Business intelligence tool
provides best of class
reporting from the cloud

Full flexibility for analysis of
web usage and
investigations

URL Filtering



A blended approach to categorisation

- Unclassified hosts are passed through a dynamic categorisation engine in attempt to provide a real-time categorisation
- Intelligent regex and keyword matching of the URL itself to provide categorisation
- Proactive review of IP addresses in pre-identified IP CIDR ranges to determine a categorisation
- Manual categorisation and recat process of customers' traffic by multilingual team
- SearchAhead utility analyses users' search engine results and provides real-time feedback on categorisation and policy outcome if clicked

✓ [Poker - Wikipedia, the free encyclopedia](#)
Poker is a family of card games involving betting and individualistic play whereby the winner is determined by the ranks and combinations of their cards, some of ...
en.wikipedia.org/wiki/Poker
[More results from en.wikipedia.org »](#)

✗ [Sky Poker - Play Online Poker and Free Poker - £10 ...](#)
For free poker join Sky Poker! Get £10 absolutely free and enter into our £10,000 new player freeroll. Play online poker and compete with players at every level ...
skypoker.com

Powered by SearchAhead

Poker - Wikipedia, the free encyclopedia
<http://en.wikipedia.org/wiki/Poker>

This site is compliant with the web usage policy set by your administrator for the following reason:

Powered by SearchAhead

Sky Poker - Play Online Poker and Free Poker - £10 ...
http://www.skypoker.com/poker/sky_lobby

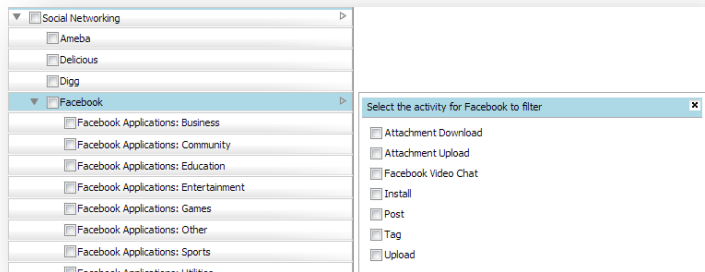
By clicking on this link you will be violating the web usage policy set by your administrator.

Site Content: Gambling

AVC - Application Visibility & Control

Maintaining control over today's web applications

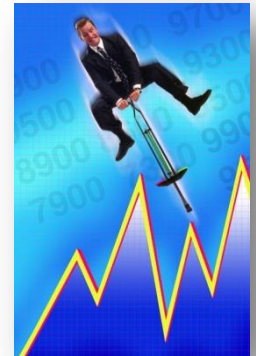
- Granular control over families of web applications
- Individual settings for access levels and control over activities
 - Allow access to Dropbox, but control uploading or downloading activities
 - Block access to certain Facebook Apps such as Games and Sport, but allow access to Business and Education
 - Control activities such as posting, tagging, uploading
- Smart dynamic signatures identify web applications by their behaviour, so any new applications will always be matched (not dependent on recognising URL's)
- Powered by Cisco's Security Applications (SecApps) team, providing AVC cross-platform signatures



Web Intelligence Reporting



- Business Intelligence meets Web Reporting
 - Ultimate flexibility in reporting criteria: 100+ different attributes for each web request
 - Single location in the cloud for all data; availability within 3 minutes
 - Multiple output types, detailed reports, time trending, automated scheduling
- Analysis of Web Usage
 - Complete visibility into web and applications usage, bandwidth, browse time
 - Visibility into Web 2.0 activities
 - User audit reporting
- Enhanced Risk & Resource Management
 - Understand potential exposure to threats and inappropriate content
 - Obtain visibility into how valuable resources are being utilised
 - Enable control over business costs



Simple Yet Granular Reporting



The screenshot shows the 'Reports' section of the ScanSafe interface. At the top, there are buttons for 'Search', 'Time Analysis', and 'Detailed Search'. Below these are settings for 'Time zone' (Europe/London), 'Time period' (Last 24 hours), and date ranges (From: 26-10-2009 to 27-10-2009). A 'Filters' section includes links for 'Add', 'Remove', 'Activate', and 'Deactivate', and a 'Select' dropdown set to 'All'. There are checkboxes for 'Active Traffic Only', 'Category in list' (set to 'online shopping'), and 'User contains' (set to 'stuart'). A 'View' dropdown is set to 'first 10', and the results are sorted by 'Bandwidth (Bytes) (descending)'. A 'Launch search' button is at the bottom right of the filter area. The footer contains contact information for ScanSafe Inc. and ScanSafe EMEA, and a copyright notice for 2009.

Complete control over all filters

Report & filter on up to 80 different attributes

Select volume of results

Sort results

Flexible Report Output - Grid



Reports

Search Time Analysis Detailed Search

Time zone: Europe/London
Time period: Last 24 hours
From: 26-10-2009 21:15 To: 27-10-2009 21:15

Filters:
Add Remove Activate Deactivate
Select: All None
 Active Traffic Only
 Category in list: cinema/tv, music

View first 10 Host sorted by Hits (descending), and their first 5 User sorted by Hits (descending) [checked]

Launch search

What were the Top 10 Sites by Hits for Media Sites?

Show 50 rows per page << first < prev 1 next >> last >> 10 results

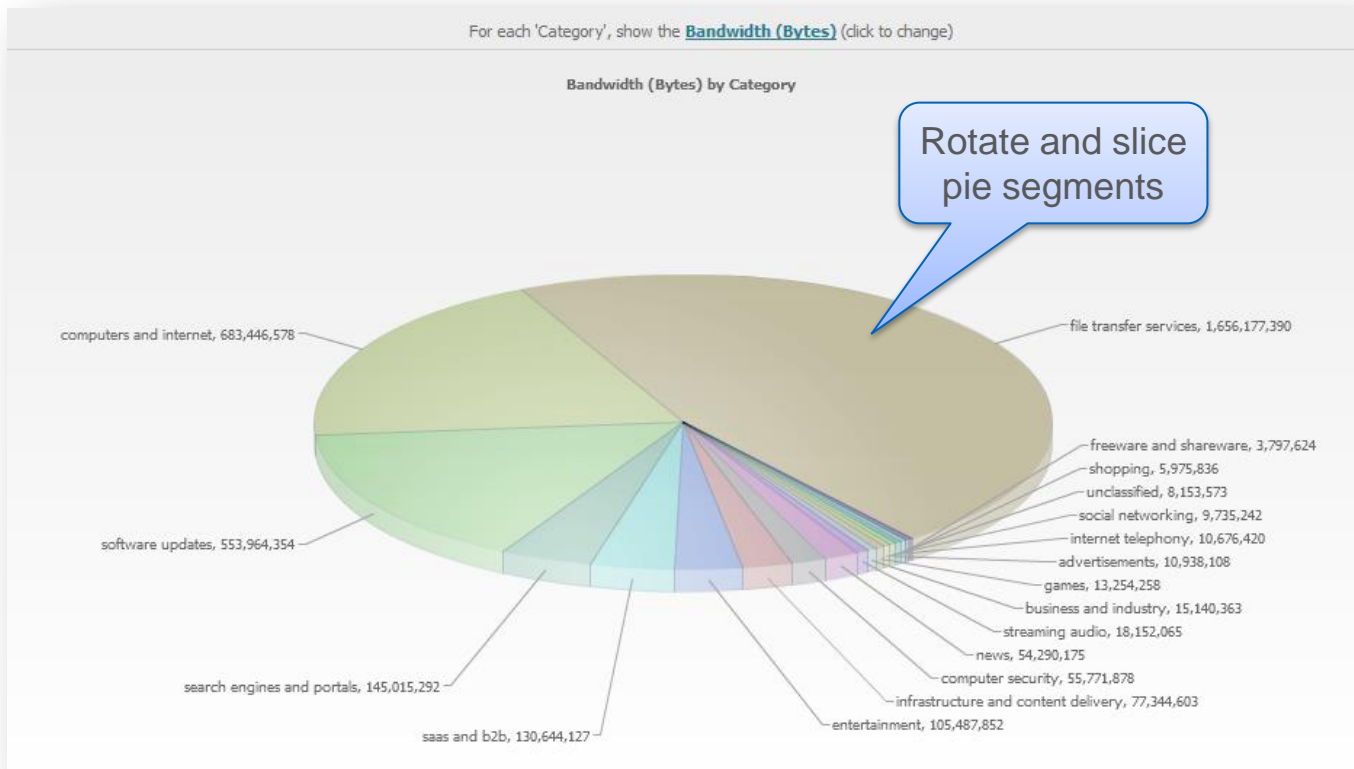
+/-	Host User	Bandwidth (Bytes)	Browse Time (Min)	Bytes Received	Bytes Sent	Hits
	Totals for Host	1,082,270,016	506	1,082,270,016	0	21,744
	www.pep.ph	6,126,048	1	6,126,048	0	144
	L winnt://demo/wayne.parnell	6,126,048	1	6,126,048	0	144
	www.mp3.es	2,947,968	1	2,947,968	0	144
	L winnt://demo/brian.roberts	2,947,968	1	2,947,968	0	144
	www.rhapsody.com	7,234,776	1	7,234,776	0	144
	L winnt://demo/gautam.gambhir	7,234,776	1	7,234,776	0	144
	www.kraftfoods.com	2,102,472	1	2,102,472	0	108
	L winnt://demo/daniel.flynn	2,102,472	1	2,102,472	0	108
	www.webfetti.com	669,456	1	669,456	0	108
	L winnt://demo/travis.dowlin	669,456	1	669,456	0	108

Add in 2nd level detail

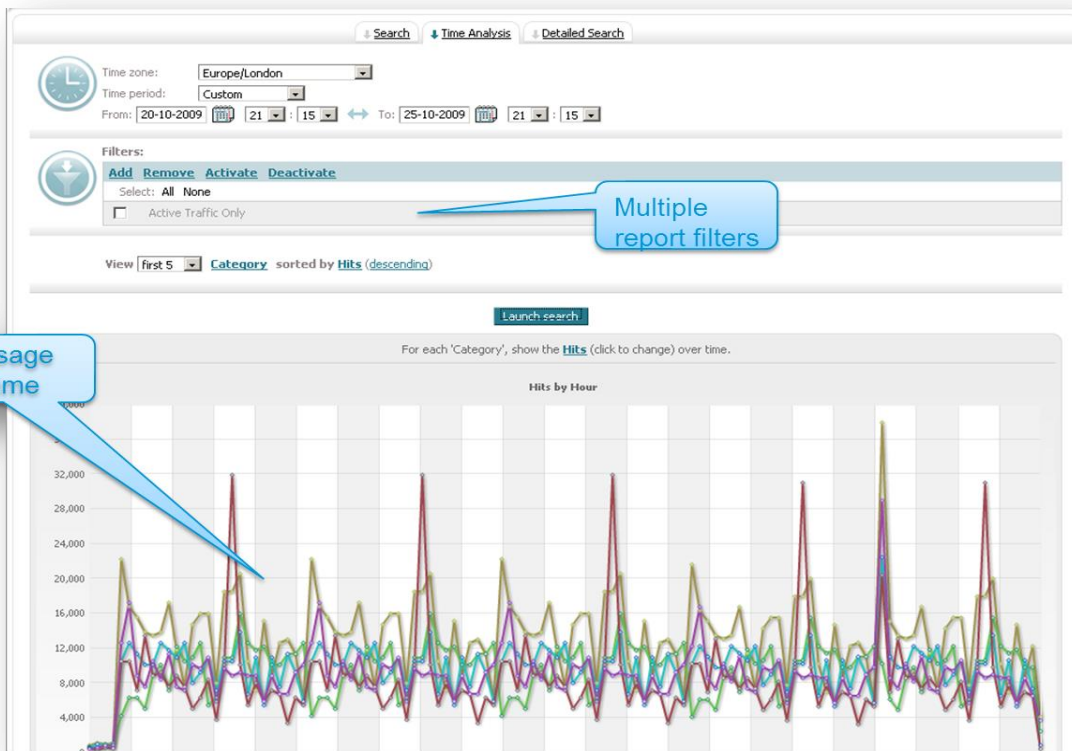
Sort based on column value

Show or hide report columns

Flexible Report Output - Pie Chart



Time Analysis Trending



Multiple report filters

View usage over time

User defined time period

User Audit - Drill Down on a User's Activities



Basic non-technical information shown only

Sessions end if no browsing activity for 5 minutes or more

Session	Host	Category	Rule Action	First Seen	Last Seen	Browse Time (Min)
68 Sessions - Total duration 879 minutes						
Session 1 - Total duration 1 minute				17-01-2012 10:15	17-01-2012 10:15	
1	www.trutv.com	entertainment	warn	17-01-2012 10:15	17-01-2012 10:15	1
Session 2 - Total duration 4 minutes				17-01-2012 10:23	17-01-2012 10:26	
2	pb.ipass.com	computers and internet	block	17-01-2012 10:23	17-01-2012 10:26	3
2	www.inquirer.net	news	block	17-01-2012 10:23	17-01-2012 10:23	1
2	www.bannerbank.ru	finance	allow	17-01-2012 10:25	17-01-2012 10:25	1
Session 3 - Total duration 4 minutes				17-01-2012 10:37	17-01-2012 10:40	
3	ciscosales.webex.com	saas and b2b	block	17-01-2012 10:37	17-01-2012 10:37	1
3	www.ufpr.br	education	allow	17-01-2012 10:38	17-01-2012 10:38	1
3	www.winbuyer.com	shopping	block	17-01-2012 10:38	17-01-2012 10:38	1
3	safebrowsing-cache.google.com	search engines and portals	allow	17-01-2012 10:40	17-01-2012 10:40	1
3	safebrowsing.clients.google.com	business and industry	allow	17-01-2012 10:40	17-01-2012 10:40	1
Session 4 - Total duration 1 minute				17-01-2012 10:52	17-01-2012 10:52	
4	www.stockgroup.com	online trading	warn	17-01-2012 10:52	17-01-2012 10:52	1
Session 5 - Total duration 11 minutes				17-01-2012 11:07	17-01-2012 11:17	
5	ciscosales.webex.com	saas and b2b	block	17-01-2012 11:07	17-01-2012 11:07	1
5	www.dominos.com	business and industry	allow	17-01-2012 11:09	17-01-2012 11:09	1
5	www.dominos.com	dining and drinking	allow	17-01-2012 11:09	17-01-2012 11:09	1
5	www.dominos.com	shopping	allow	17-01-2012 11:09	17-01-2012 11:09	1
5	safebrowsing-cache.google.com	search engines and portals	allow	17-01-2012 11:10	17-01-2012 11:10	1
5	safebrowsing.clients.google.com	business and industry	allow	17-01-2012 11:10	17-01-2012 11:10	1
5	www.zhaopin.com	job search	warn	17-01-2012 11:15	17-01-2012 11:15	1
5	www.trrsf.com	social networking	block	17-01-2012 11:17	17-01-2012 11:17	1

Loss of Productivity is also a Virus

How much time and bandwidth is being wasted on Web 2.0 in a single day?



of Facebook tags and posts: **15,561.**

At ~**10 seconds** a tag/post, that's over **43 hours/day** or almost **2 days** just tagging or posting things!

(and that's only the non-encrypted traffic seen!)



Bytes on Youtube video playback:
7,548,554,900,112,
or **6.87 TB**



Bytes on Pandora:
1,877,303,700,680,
or **1.7 TB**



Total bytes for the day:
170,950,961,023,926
or **155.5 TB**

These statistics were measured over the course of one day on 2 December 2013

Agenda

Security Without Compromise

- What is CWS?
- The Threat Landscape
- Data Flow and Statistics
- Cloud Proxy Architecture

Live Demos

- ASA Connector
- ScanCenter Policies
- Reporting
- User Simulation



Deploying CWS with Your Cisco Infrastructure

- ASA
- ISR-G2
- WSA Connector
- AnyConnect
- Direct to Cloud

Managing CWS

- Centralised Management
- Web 2.0 Control
- Best of Class Reporting

Summary - Fitting your Business Needs

Security Without Compromise

- All users, better security
- Zero hour protection
- Acceptable use policy
- Web 2.0 control



Live Demos

- Try for yourself...



Deploying CWS with Your Cisco Infrastructure

- Leverage of existing infrastructure
- Multiple options
- Fewer parts, one vendor
- Simple deployment



Managing CWS

- Centralised management
- Comprehensive reporting
- No need to manage at branches
- Granular policies and reports



Final Thought

Try it yourself...

- Free evaluations available
 - 45 days
 - Up to 250 users



For More Information...



Additional Resources

- This session's presentation with **footnotes**:
www.tinyurl.com/embracethecloud
- CWS documentation and support on Cisco CCO:
http://www.cisco.com/en/US/products/ps11720/prod_literature.html
- Security sessions on Partner Communities pages:
<https://communities.cisco.com/docs/DOC-30977>
- CWS Case Studies:
http://www.cisco.com/en/US/products/ps11720/prod_case_studies_list.html



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
- 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



CISCO™