Cisco live!

What You Make Possible

TOMORROW
starts here.

CISCO

Deploying Web Security

BRKSEC-2101

TOMORROW
starts here.

For Your Reference

- There are (many...) slides in your print-outs that will not be presented.
- They are there “For your Reference”

For Your Reference

- Some slides have this friendly notice on the corner

15 Billion devices in 2015

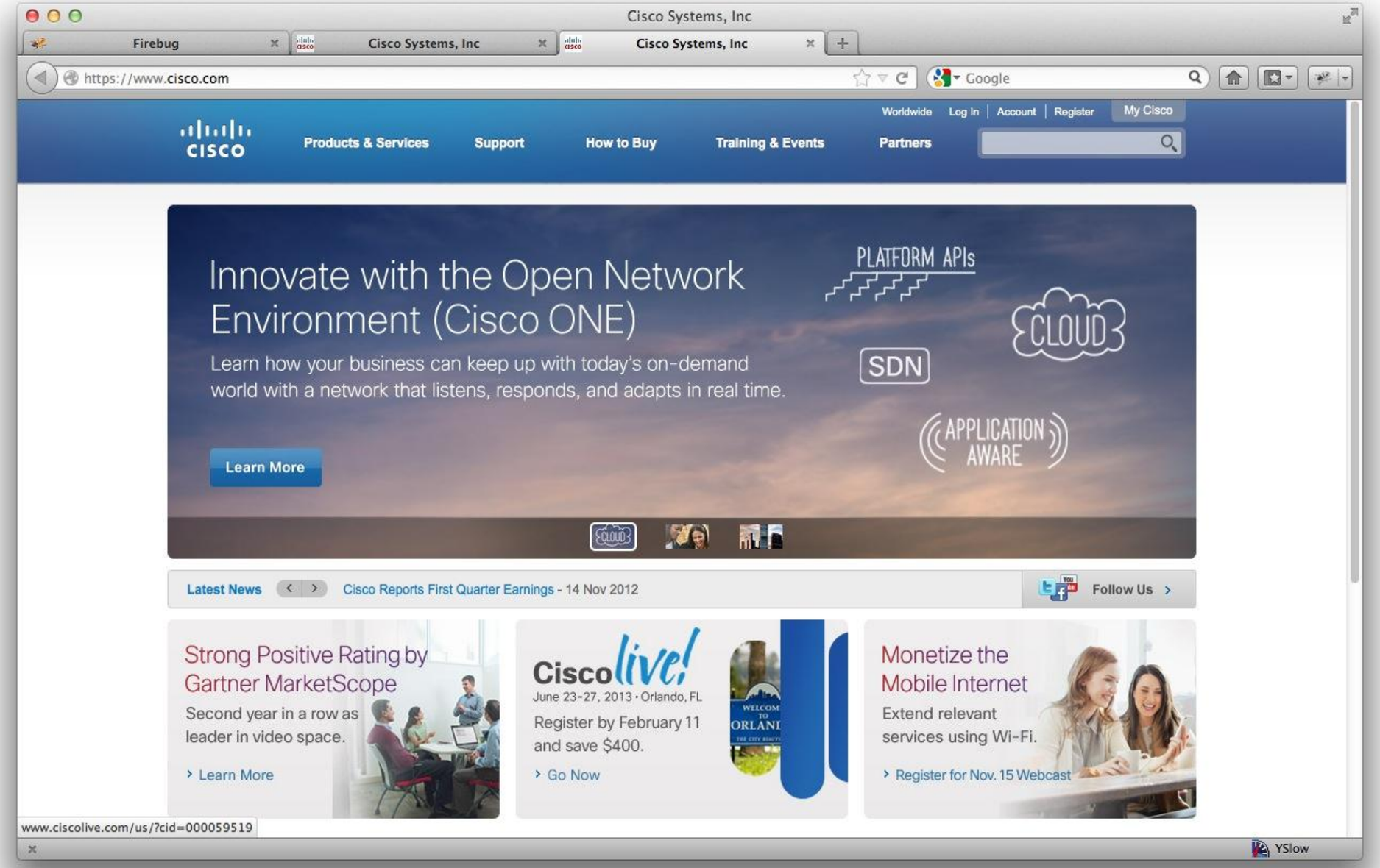
Are you with us or against us?

Agenda

- Web Security Overview
- Cisco Web Security Appliance (IronPort)
- Cisco Cloud Web Security (Scansafe)
- Hybrid Web Security (Appliance + Cloud)

1996

Today's Websites…



Cisco live!

Cisco Systems, Inc

Firebug | Cisco Systems, Inc

https://www.cisco.com

Google

Worldwide | Log In | Account | Register | My Cisco

CISCO | Products & Services | Support | How to Buy | Training & Events | Partners

Innovate with the Open Network Environment (Cisco ONE)

Learn how your business can keep up with today's on-demand world with a network that listens, responds, and adapts in real time.

Learn More

PLATFORM APIs

CLOUD

SDN

APPLICATION AWARE

Console | HTML | CSS | Script | DOM | Net | Cookies | YSlow

Clear | Persist | All | HTML | CSS | JS | XHR | Images | Flash | Media

GET ntpagetag.gif?js=1...=135	200 OK	cisco.com	85 B	198.133.219.25:443	980ms
GET ntpagetag.gif?js=1...=135	200 OK	cisco-tags.cisco.com	85 B	72.163.5.75:443	1.4s
GET mm-icon-lock.gif	200 OK	cisco.com	117 B	198.133.219.25:443	949ms
GET psa_typeahead_common.r	200 OK	cisco.com	3.8 KB	198.133.219.25:443	816ms
GET mm-support_forums.gif	200 OK	cisco.com	1.6 KB	198.133.219.25:443	882ms
GET mm-linksys.png	200 OK	cisco.com	3.3 KB	198.133.219.25:443	914ms
GET mm-flip.png	200 OK	cisco.com	3.2 KB	198.133.219.25:443	945ms
GET mm-valet.png	200 OK	cisco.com	3.2 KB	198.133.219.25:443	999ms
GET mm-umi.png	200 OK	cisco.com	2.6 KB	198.133.219.25:443	1.07s
GET mm-support_contact.gif	200 OK	cisco.com	1.5 KB	198.133.219.25:443	1.09s

75 requests | 649 KB (622.6 KB from cache) | 10.99s (onload: 5s)

B 392.1K 5.004s

Today’s Threats

Sophisticated, Constantly Mutating

Each Attack Instance
can be slightly different

Domains
are rotated in days, even hours

Content
mutates and mimics legitimate traffic

Appliance or Cloud?

Web Security Appliances

S170

S370

S670

Cloud Web Security

Agenda

- Web Security Overview
- Cisco Web Security Appliance (IronPort)
- Cisco Cloud Web Security (Scansafe)
- Hybrid Web Security (Appliance + Cloud)

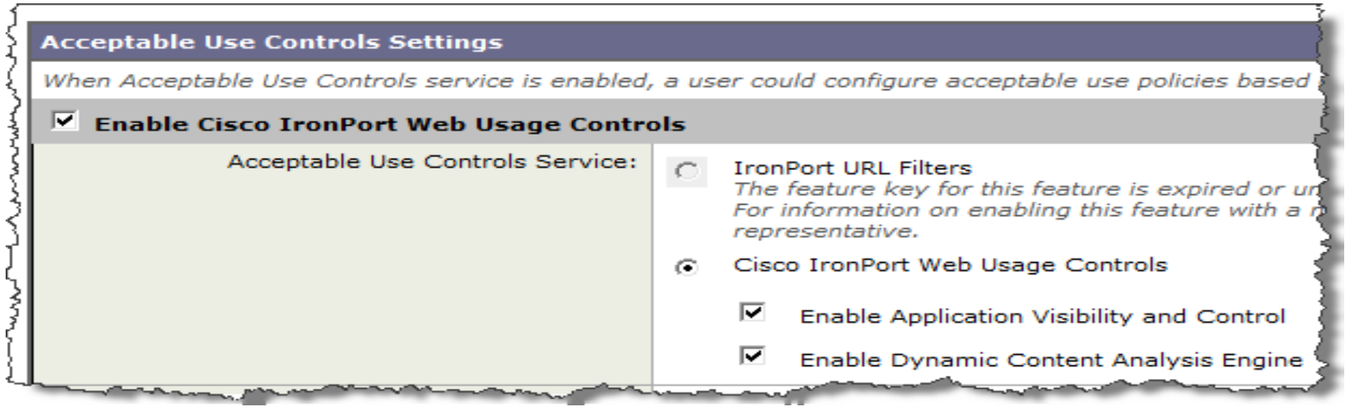
Cisco Web Security Appliance

- Web Proxy incl. Caching (http,https, ftp, ftp over http)

- Rich security functionalities
  - Reputation filtering
  - Malware scanning
  - URL Filtering
  - Application visibility & control
  - HTTPS inspection
  - Authentication
  - Reporting and tracking
  - L4TM
  - ...more to come!

Web Application Control

- Many Applications work on top of HTTP traffic
- Applications are detected and controlled by special Signatures
- Those Signatures are downloaded dynamically via regular Signature Updates from Cisco
- No reboot or manual installation required!



SIO

SensorBase

Threat Operations Centre

Dynamic Updates


CISCO
SIO
75 TB
DATA RECEIVED PER DAY
750,000+
GLOBALLY DEPLOYED DEVICES
30B
WEB REQUESTS
HTTP://
100M
EMAIL MESSAGES
35%
WORLDWIDE TRAFFIC
SensorBase
Threat Operations Centre
Dynamic Updates
live!

3 to 5
MINUTE UPDATES

6,500+
IPS SIGNATURES PRODUCED

20+
PUBLICATIONS PRODUCED

200+
PARAMETERS TRACKED

8M+
RULES per DAY

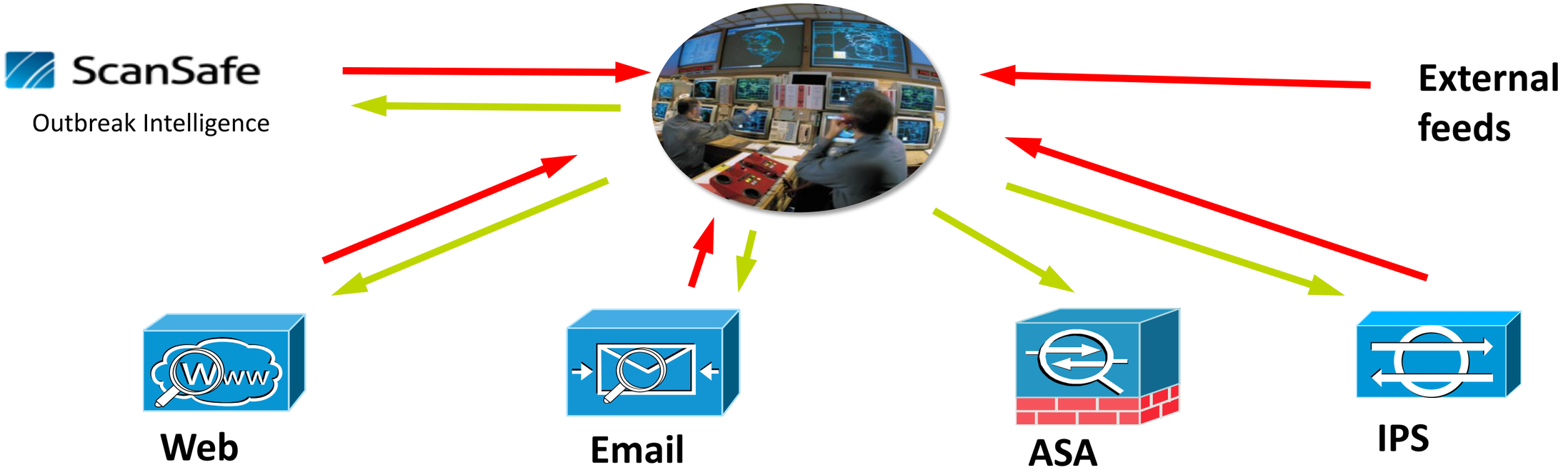
SensorBase

Threat Operations Centre

Dynamic Updates

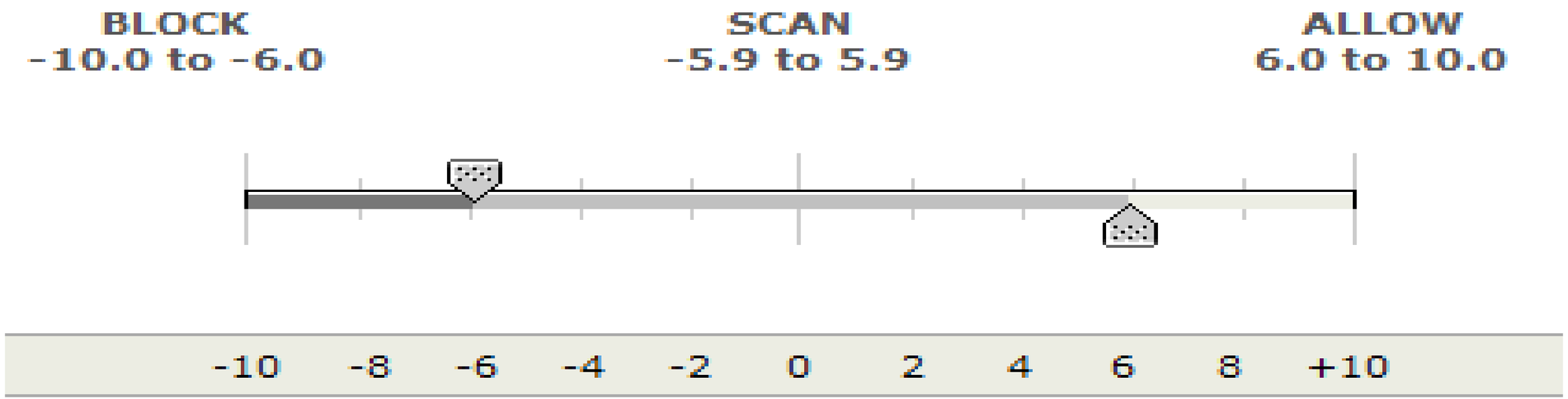
About Reputation

- Cisco SIO gathers statistical informations from Cisco Products and other resources
- Cisco SIO correlates informations
- Updated informations are delivered back to appliances
- Each IP / URL gets a score, ranging from -10 to +10



About Reputation

- Malicious websites are tracked globally through SIO
- WSA evaluates each webrequest against the defined reputation score
- Reputation score and action is configured on WSA



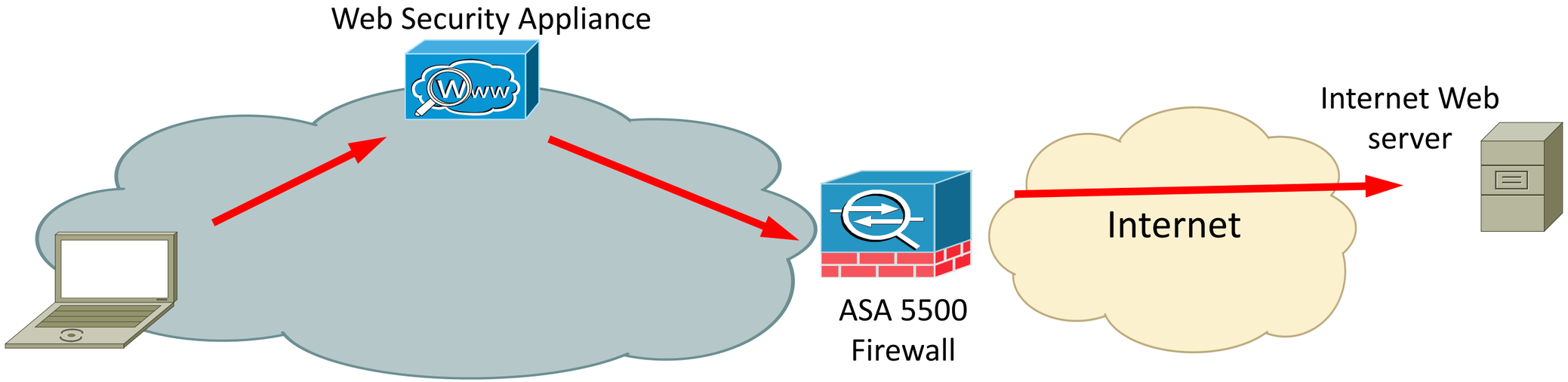
Network Participation

- Admin can define the level of participation
- Requested URL with result is sent back
- User information and internal networks are not sent

Disabled: No information is sent to Cisco SIO Database
Limited: Server URL of request, hash of path segments
Standard: Server URL and all path segments are sent back

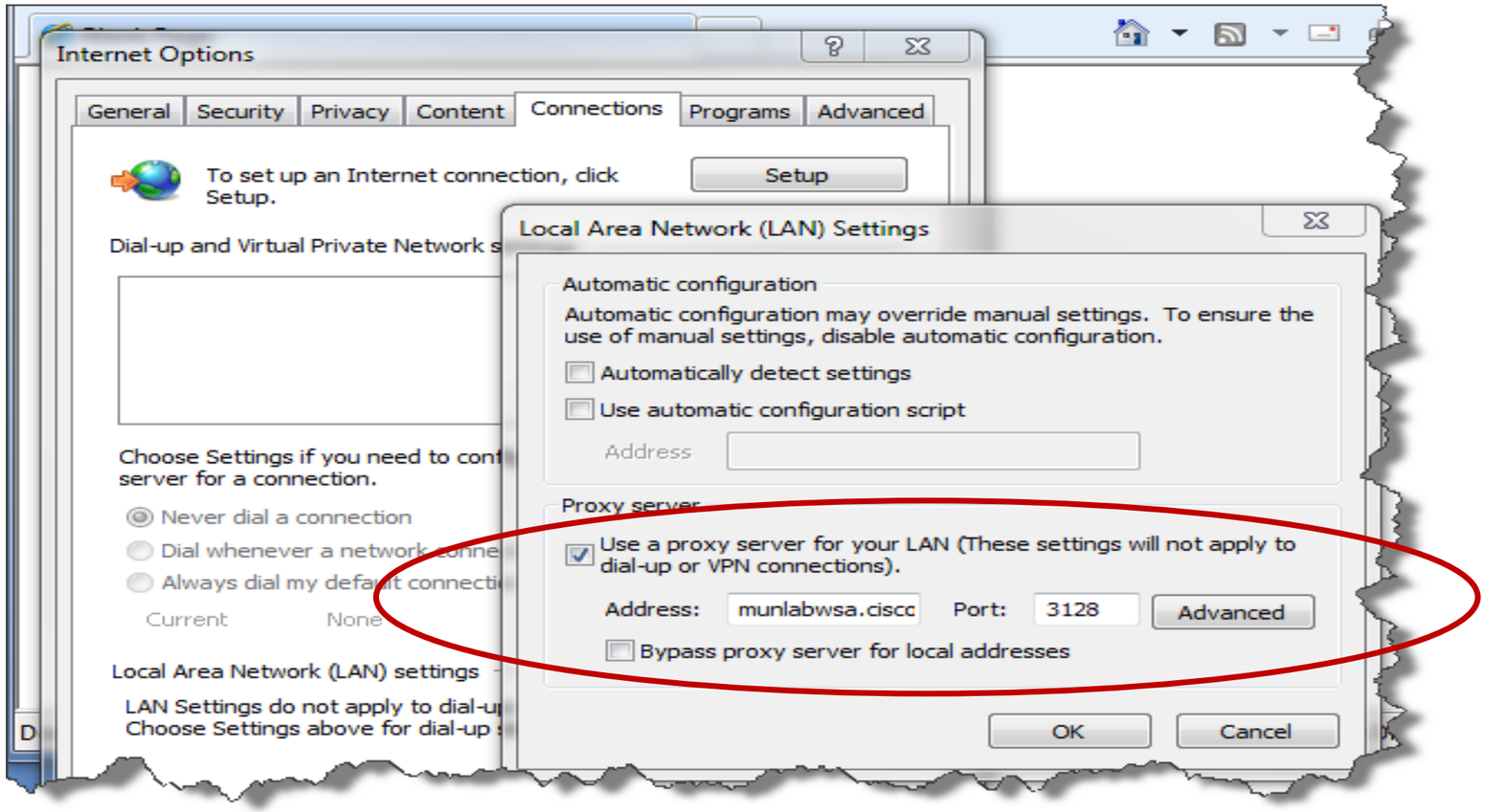
Explicit Proxy

- Client requests a website
- Browser connects first to WSA
- WSA connects to website
- Firewall usually only allows webtraffic from proxy



How does the Browser find the Proxy?

- Proxy setting in the browser
- Static definition with IP/NAME and PORT



How does the Browser find the Proxy?

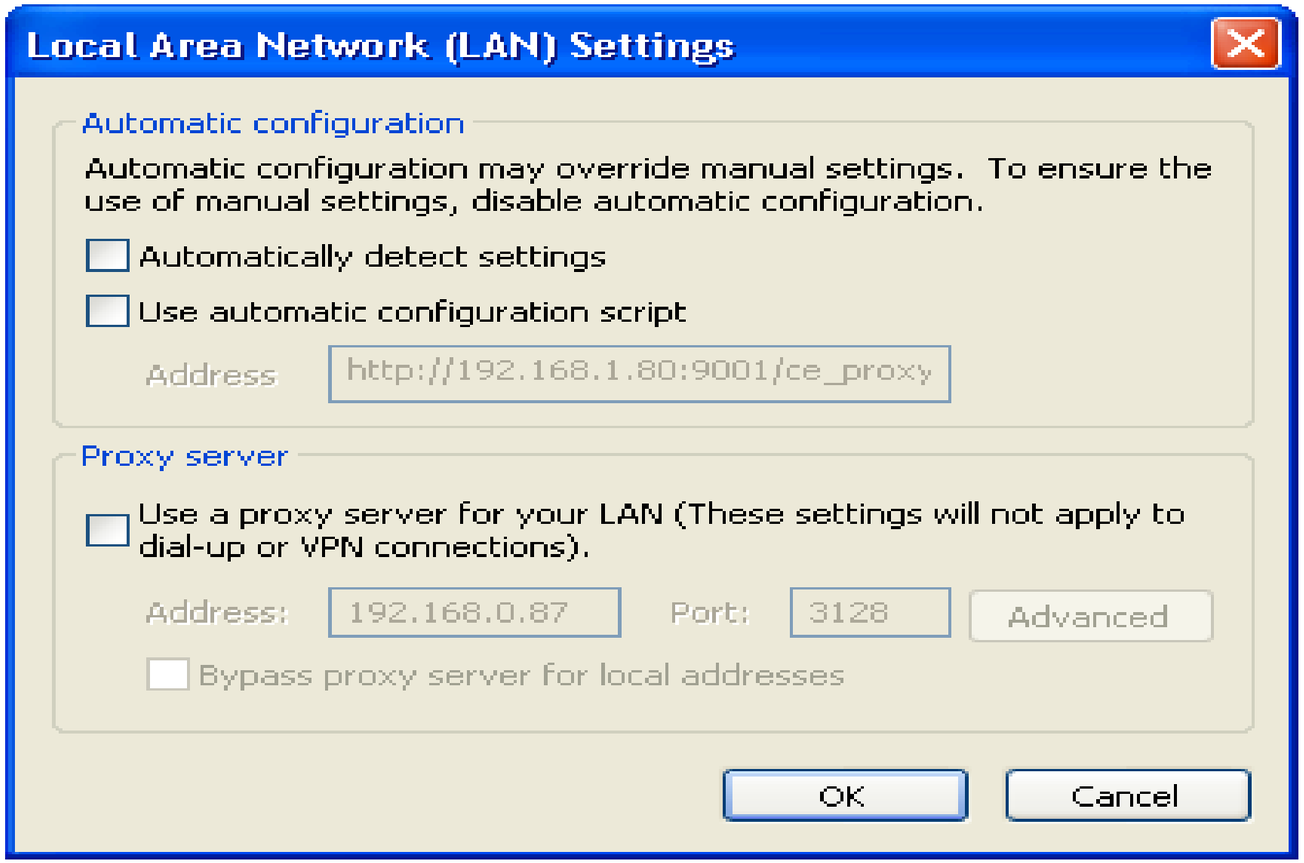
- Automatic Configuration via PAC File

```
function FindProxyForURL(url, host)
 {
   return "PROXY 192.168.1.80:3128";
 }

function FindProxyForURL(url, host)
 {
   return "PROXY 192.168.1.80:3128; 192.168.1.81:3128";
 }
```

http://www.findproxyforurl.com/

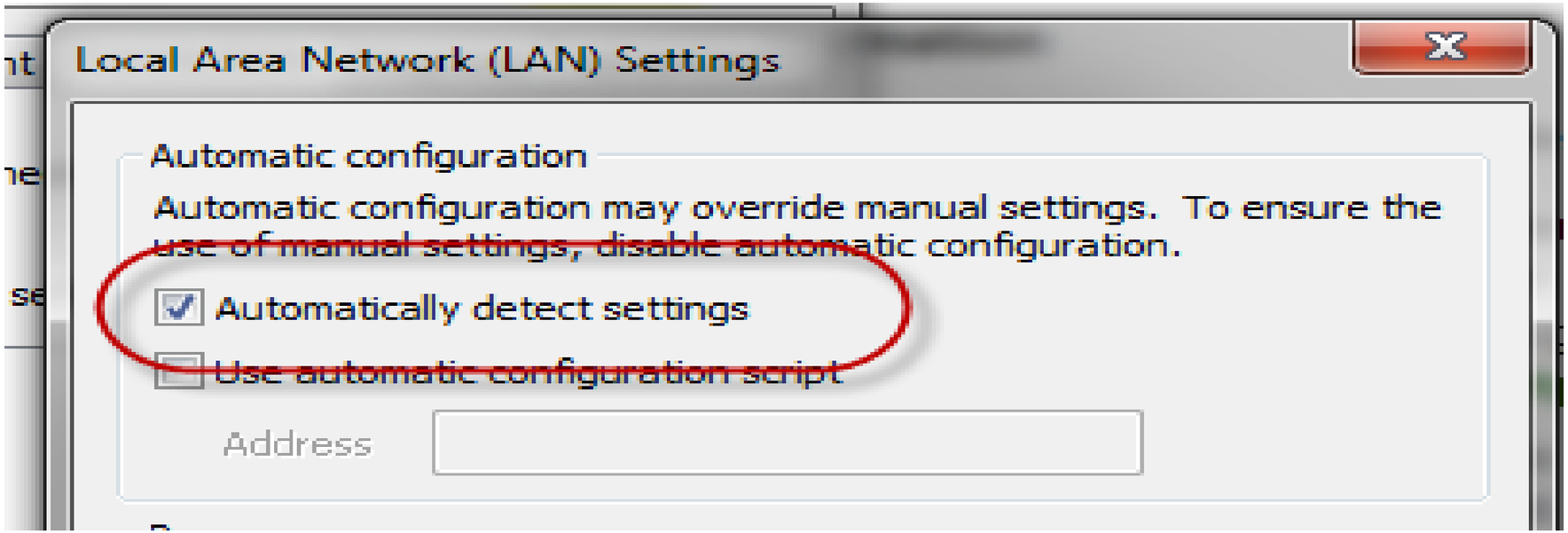
PAC Deployment

- Via AD and GPO
- Via script
- Via manual setting
- Via DHCP
  DHCP Option 252
- Via Wpad Server



WPAD Server

- WPAD Server hosts PAC file as wpad.dat
- File is retrieved via HTTP and Javascript
- „Automatic Settings“ creates a lookup on a server called „wpad“

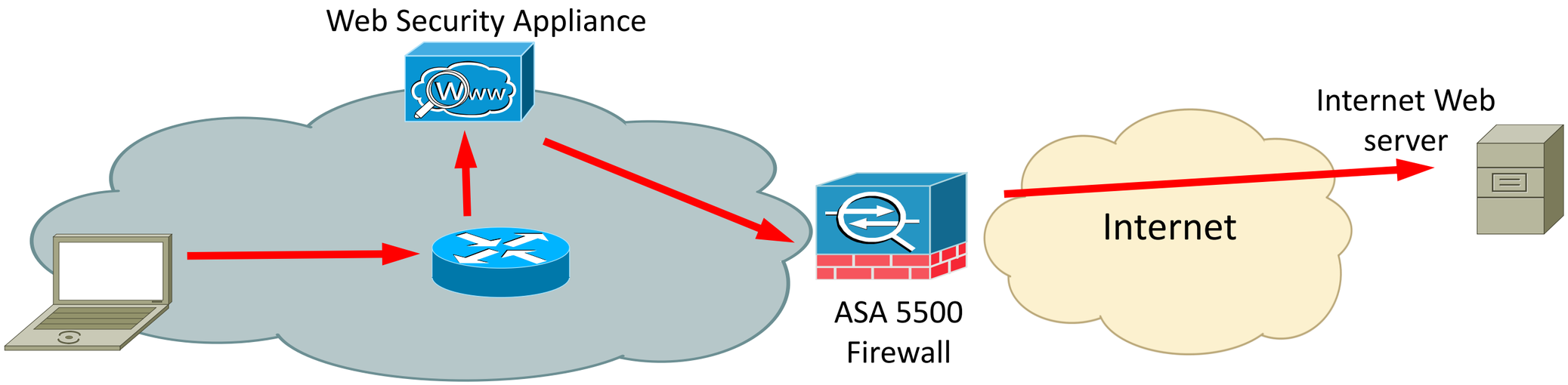


Explicit Deployment - Summary

- Requires Client Settings in the Browser
- Proxy resolves hostname of target web server
- Redundancy can be achieved via PAC files
  - WSA can host PAC files

Transparent Proxy via WCCP

- Client requests a website
- Browser tries to connect to Website
- Network Device redirects traffic to WSA using WCCP
- WSA proxies the request



Background on WCCP

- WCCPv1 developed in 1997 by Cisco Systems and publicly released in July 2000
- WCCPv2 published as an IETF draft in July 2000 to make the specification open and remove the requirement for licensing
  - Enhancements

    Configurable WCCP Router ID

    WCCP Variable Timers – Improved Failover

    Improved Interaction between WCCP and NetFlow

Details

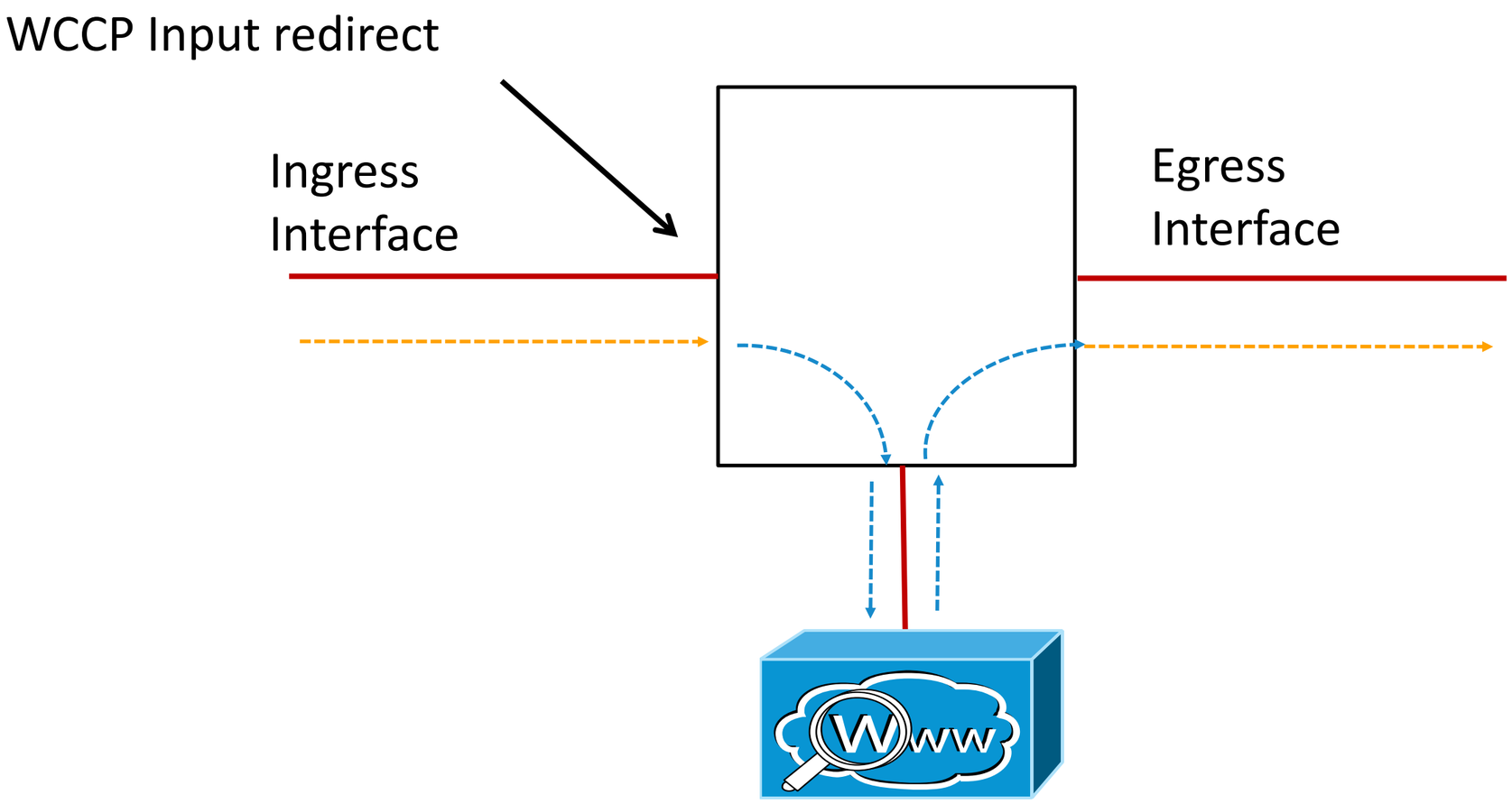
Assignment

The WCCP assignment method is used to determine which WCCP traffic and which WCCP device is chosen for the destination traffic.

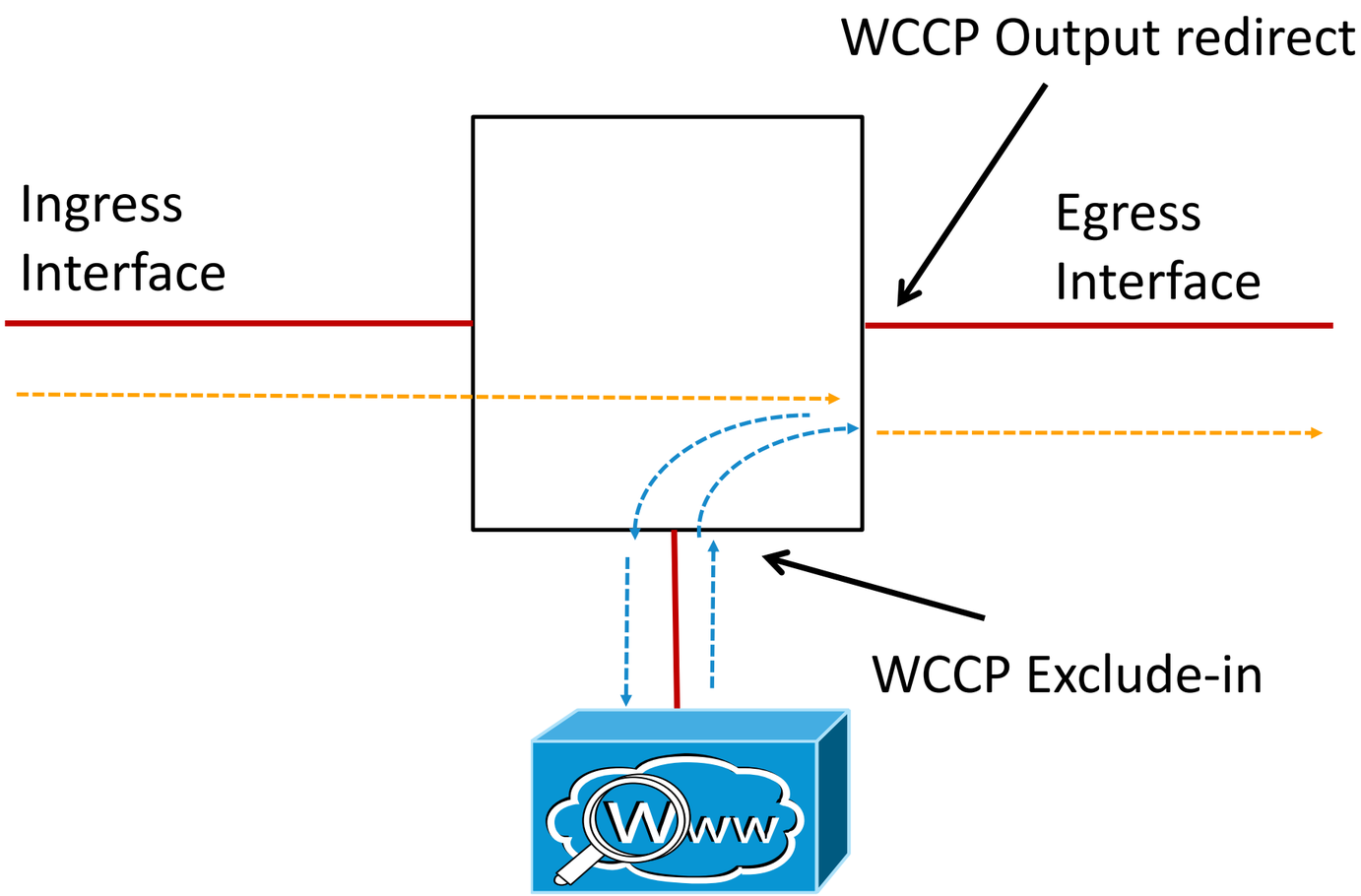
WCCP can use two types of Assignment Methods: Hash and Mask.

- **Hash Based Assignment**
  Uses 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 Assignment**
  Uses the ACL TCAM to assign WCCP entities. This method is fully handled by hardware.

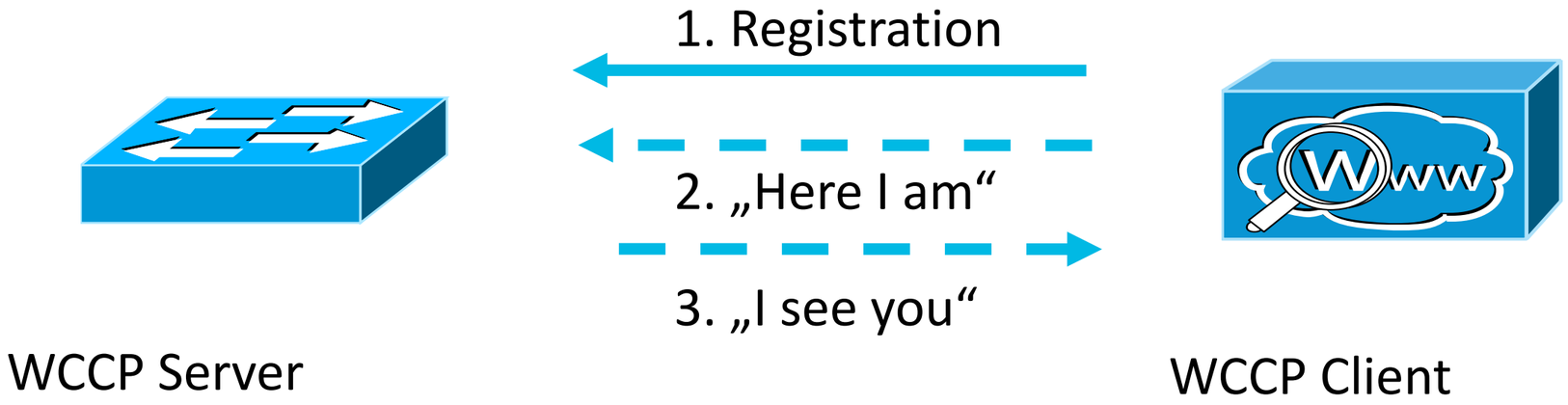
WCCP input redirect



WCCP output redirect and input exclude



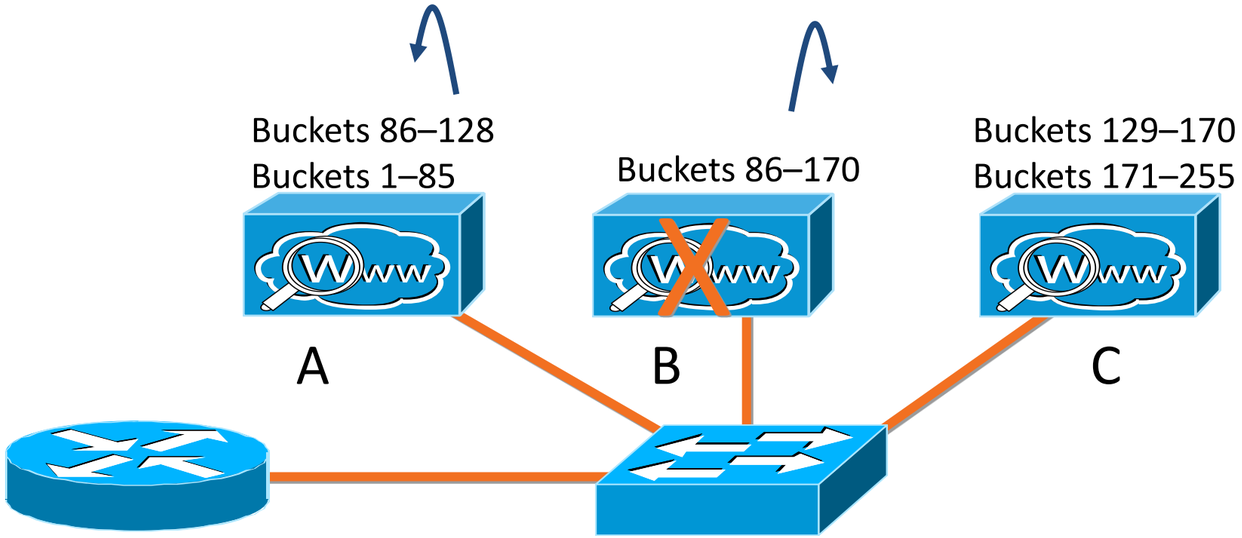
How WCCP registration works



- The WCCP client registers at the WCCP Server
- Both, Server and Client need to use the same WCCP Service Group ID
- One WCCP Server usually can server multiple Clients
- Server and Client exchange „here i am“ and „I see you“ Packets to check availability
  - UDP/2048, unicast
  - Multicast possible
- Traffic is redirected from Server to one or multiple Clients using the „hash“ or „mask“ algorithm

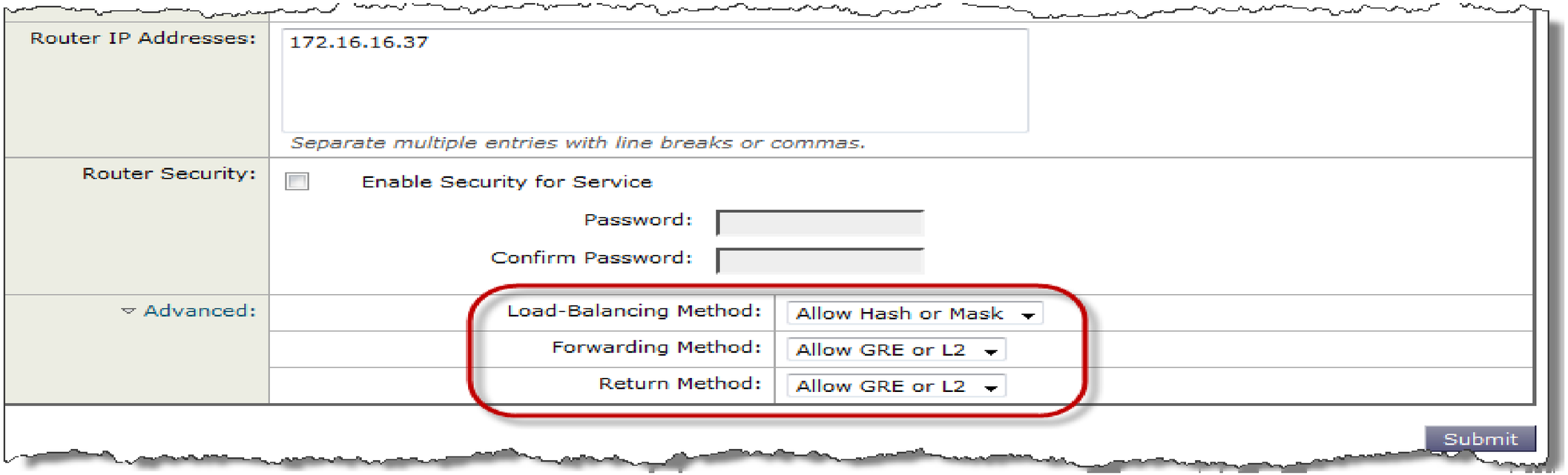
WCCP Protocol

- When a WCCP client fails, the portion of the load handled by that client is automatically redistributed to the remaining WCCP clients in the service group
- If no other WCCP clients are available in the service group, the service group is taken offline and packets are forwarded normally



Using WCCP for Traffic Redirection

- WCCPv2 support is availible on many Cisco Platforms:
  L3 Switches, Routers, ASA 5500 Security Appliance
- Cisco Ironport WSA supports all redirect and assign methods (software implementation)
- Method to use will be negotiated



Using WCCP for Traffic Redirection (2)

Performance Considerations:

- MASK (HW) > HASH (SW)
- L2 (HW) > GRE (SW)
- Use GRE if WSA is located in other subnet

  Check if Device can do GRE in HW
- Use L2 if WSA and WCCP Device are in same subnet

WCCP Protocol

Service Group

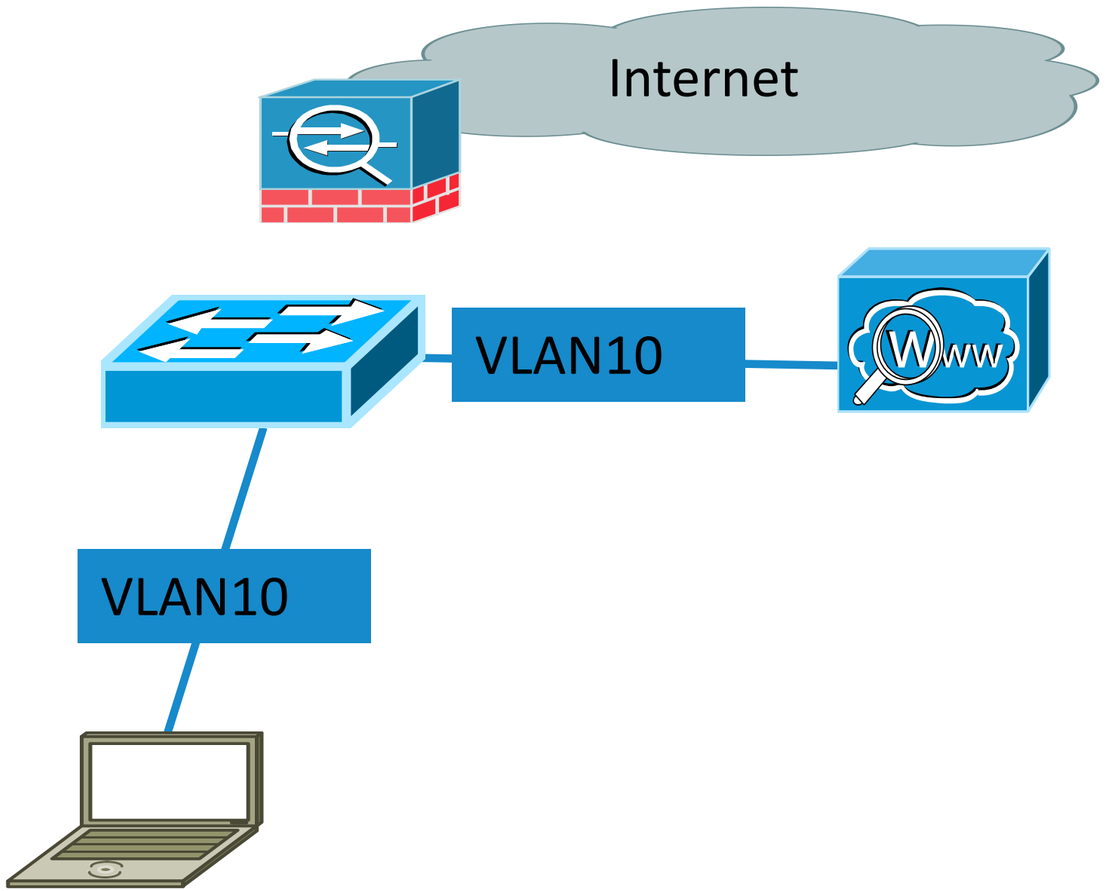
- The routers/switches and WCCP clients participating in a WCCP service constitute a *Service Group*
- Up to 32 routers per service group
- Up to 32 WCCP clients per service group
- Each service group is established and maintained using separate protocol message exchanges
- Service definition must be the same for all members of the service group

Current (Cisco) Service Groups

ID	Product	Name	Protocol	Port
0	ACNS	web-cache	6	80
53	ACNS	DNS	17	53
60	ACNS	ftp	6	21
61	WAAS	tcp-promiscuous	6	0
62	WAAS	tcp-promiscuous	6	0
70	ACNS	https-cache	6	443
80	ACNS	rtsp	6	554
81/82	ACNS	wmt	6 (81), 17(82)	1755
83	ACNS	rtspu	6	554
89	WAFS	cifs-cache	6	139, 445
90-97	ACNS	custom	6	User Defined
98	ACNS	custom-web-cache	6	User Defined
99	ACNS	reverse-proxy	6	80

WCCP with L3 Switch (3560/3750)

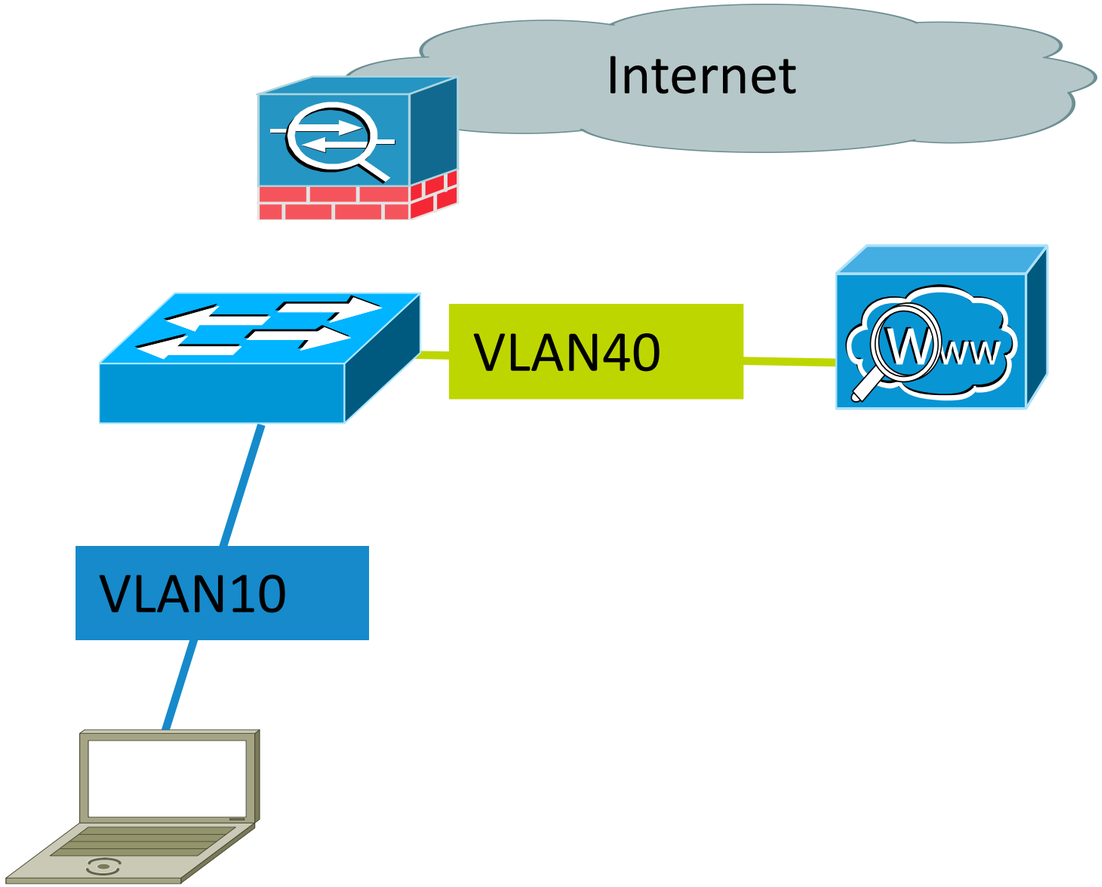
L2 Redirect



```
sdm prefer routing
ip routing
ip wccp 91 redirect-list wsa
ip access-list extended wsa
 permit tcp any any eq www
 permit tcp any any eq 443
!
Interface Vlan10
 ip address 172.16.10.10 255.255.255.0
 ip wccp 91 redirect in
```

WCCP with L3 Switch (3560/3750)

L2 Redirect



- Recommendations:
  Assign seperate VLAN for the connection to the WSA!
- Redirect ACL only allows „permit“ statements on 3560/3750 Series!
  - No easy way to exclude WSA from redirect looping...
- If 3560/3750 is stacked, configure WCCP on the Stack Master!

WCCP with L3 Switch

L2 Redirect - Verification

```
munlab-3560X#show ip wccp 91 detail
WCCP Client information:
        WCCP Client ID:          172.16.10.100
        Protocol Version:        2.0
        State:                   Usable
        Redirection:             L2
        Packet Return:           L2
        Packets Redirected:    0
        Connect Time:          01:02:16
        Assignment:            MASK

        Mask   SrcAddr     DstAddr     SrcPort DstPort
        ----   -------     -------     ------- -------
        0000:  0x00000000  0x00000526  0x0000  0x0000

        Value SrcAddr     DstAddr     SrcPort DstPort CE-IP
        ----- -------     -------     ------- ------- -----
        0000: 0x00000000  0x00000000  0x0000  0x0000  0xAC100A64 (172.16.10.100)
        0001: 0x00000000  0x00000002  0x0000  0x0000  0xAC100A64 (172.16.10.100)
        0002: 0x00000000  0x00000004  0x0000  0x0000  0xAC100A64 (172.16.10.100)
```

Version & State

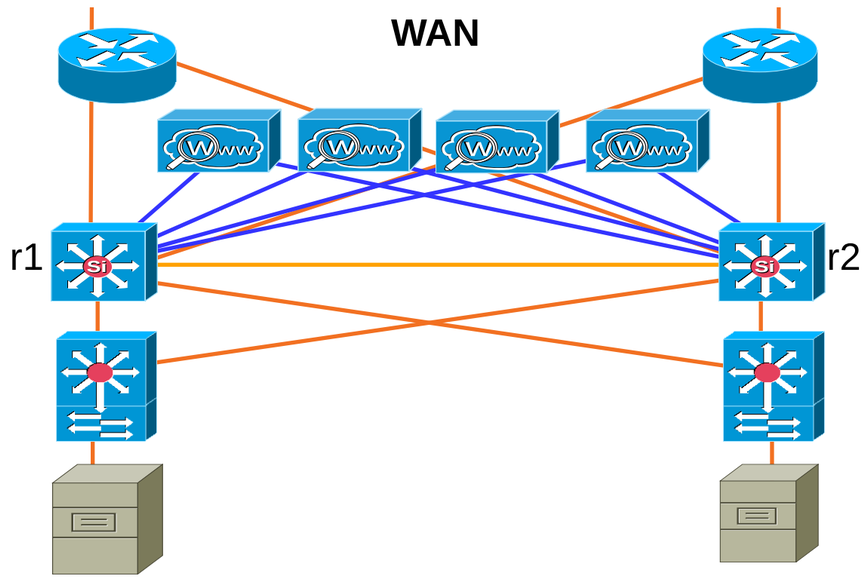
Assignment Method

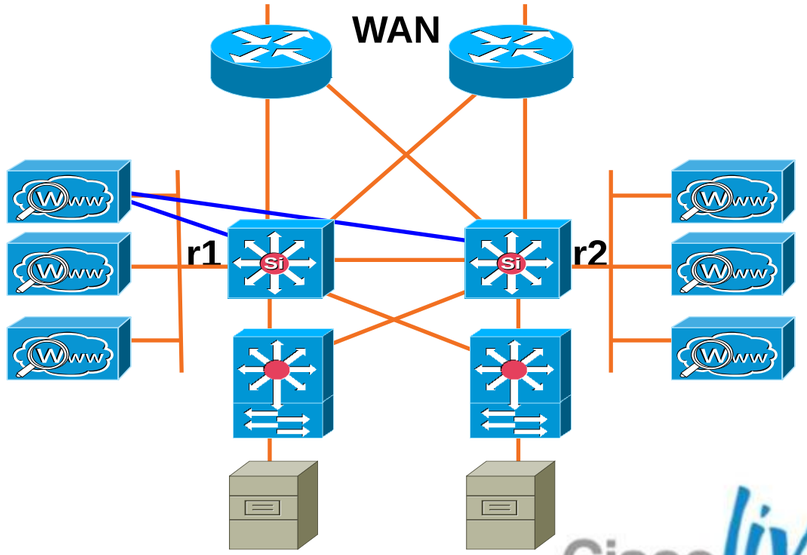
Assignment Method

WCCP with L3 Switch (CAT6500)

L2 or GRE Redirect

- CAT6500 with Sup2T/720/32 and PFC3 allows redirect of L2 and GRE in Hardware
- Redirect-in and Redirect-out is supported
- Permit and Deny ACE is allowed
- Very scalable and flexible





WCCP with L3 Switch (CAT6500)

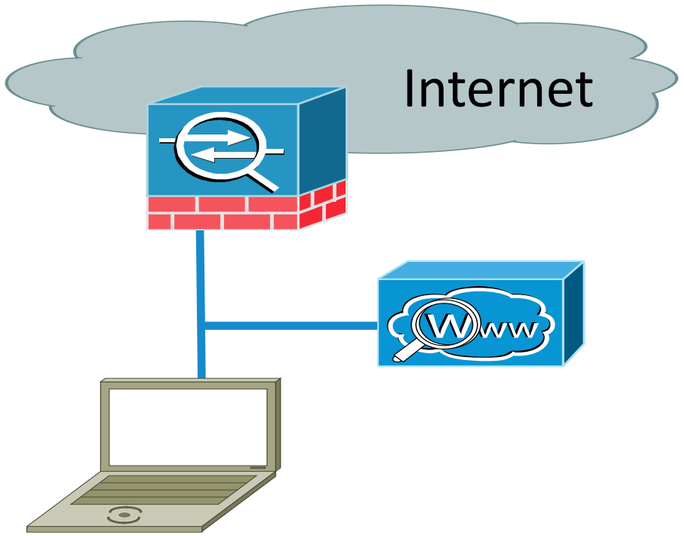
L2 or GRE Redirect

- Ingress - L2 redirection + Hash Assignment (Requires Software Processing)
- Ingress - L2 redirection + Mask Assignment (Full Hardware Processing - recommended)
- Egress - L2 redirection + Hash Assignment (Requires Software Processing)
- Egress - L2 redirection + Mask Assignment (Requires Software Processing)

  First packet is process switched, creates netflow entry. Subsequent packets are HW switched

- Ingress - L3 (GRE) redirection + Hash Assignment (Requires Software Processing)
- Ingress - L3 (GRE) redirection + Mask Assignment (Full HW Processing - Sup32/Sup720 only)
- Egress - L3 (GRE) redirection + Hash Assignment (Requires Software Processing)
- Egress - L3 (GRE) redirection + Mask Assignment (Requires Software Processing)

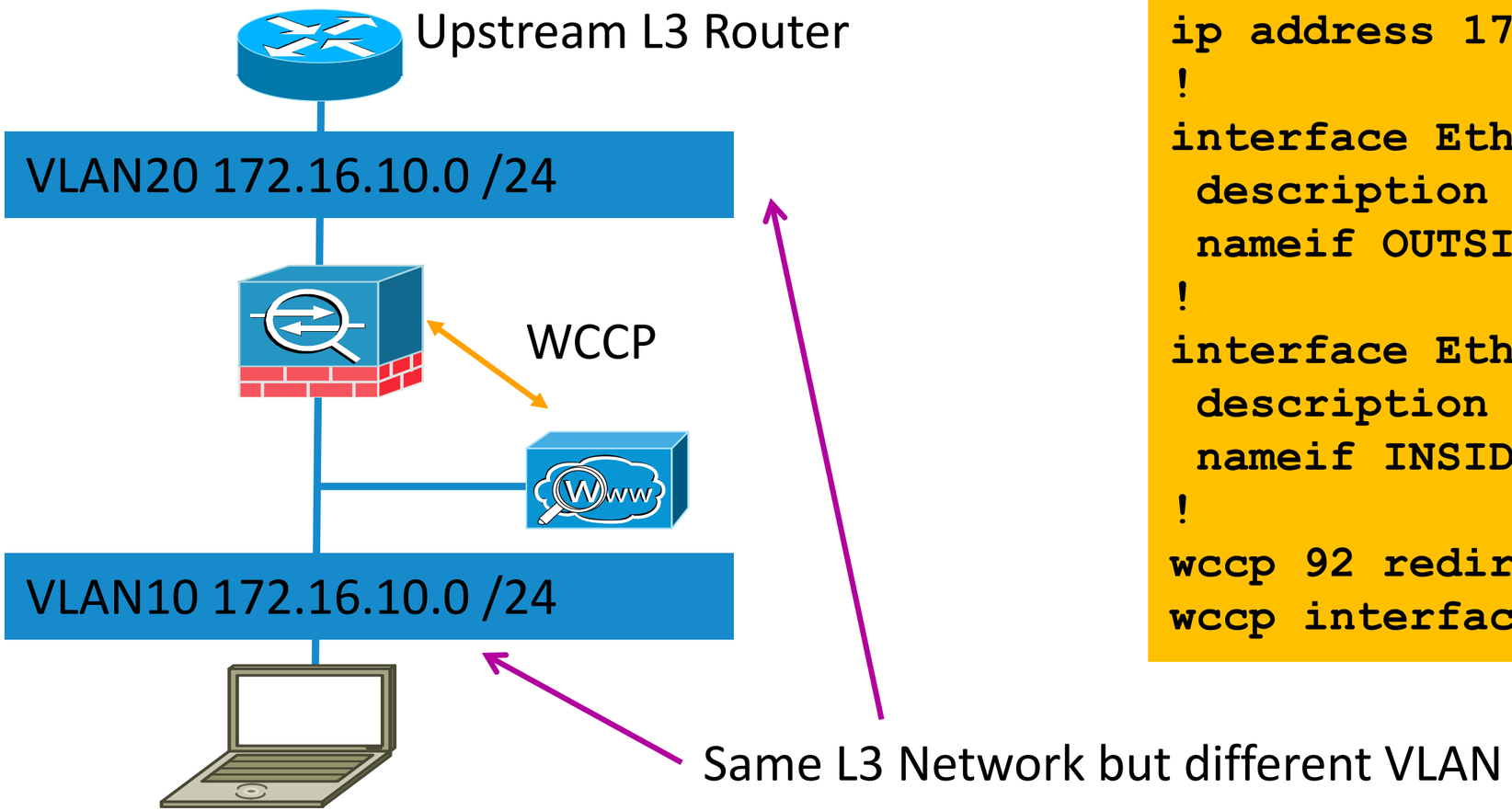
WCCP with ASA



- 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
- No TCP Intercept, Inspect Engine or internal IPS is applied to the redirected flow.
- IPS HW Module however <u>does</u> inspect traffic

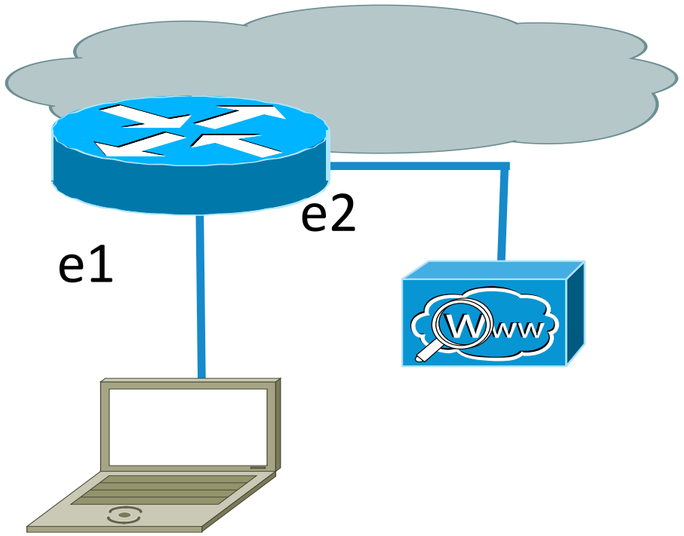
```
access-list WCCPRedirectionList extended deny ip 172.16.10.0
255.255.255.0 172.16.10.0 255.255.255.0
access-list WCCPRedirectionList extended permit tcp any any eq www
access-list WCCPRedirectionList extended permit tcp any any eq https
!
wccp 90 redirect-list WCCPRedirectionList
wccp interface INSIDE 90 redirect in
```

WCCP with ASA in transparent mode




```
firewall transparent
hostname munlab-asa2
ip address 172.16.10.33 255.255.255.0
!
interface Ethernet0/0
 description OUTSIDE INTERFACE
 nameif OUTSIDE security-level 0
!
interface Ethernet0/1
 description INSIDE
 nameif INSIDE security-level 100
!
wccp 92 redirect-list WCCPREDIRECTLIST
wccp interface INSIDE 92 redirect in
```

WCCP with Router – ISR, ISRG2



- Redirect is GRE and Hash
  - Done in SW
- Allows for DMZ-Design
- Supports „permit“ and „deny“ Statements in the redirection ACL

```
ip cef
ip wccp version 2
ip wccp 91 redirect-list <redirect-ACL>
!
interface e1
 ip wccp 91 redirect in
```

WCCP
Router Redirect and Return Support

For Your Reference

	WCCP GRE Redirect	WCCP L2 Redirect
IP Forward Return	Software: 7200, ISR Hardware: 6500/PFC3, 7600(PFC3)	Software: None Hardware: 6500/PFC3, 6500/Sup2 (ODM ACL Merge), 7600/PFC3, ASR, 4500, 3750, 3560
WCCP GRE Return	Software: 7200, ISR Hardware: ASR	Not supported
WCCP L2 Return	Software: 7200, ISR	Software: 7200, ISR Hardware: 6500 (IOS 12.2(33)SXH, ASR, 4500, 3750, 3560) (Not supported by WAAS)
Native GRE Return	Software: 7200, ISR Hardware: 6500/PFC3, 7600/PFC3, ASR	Not supported

WCCP Platform Recommendations

For Your Reference

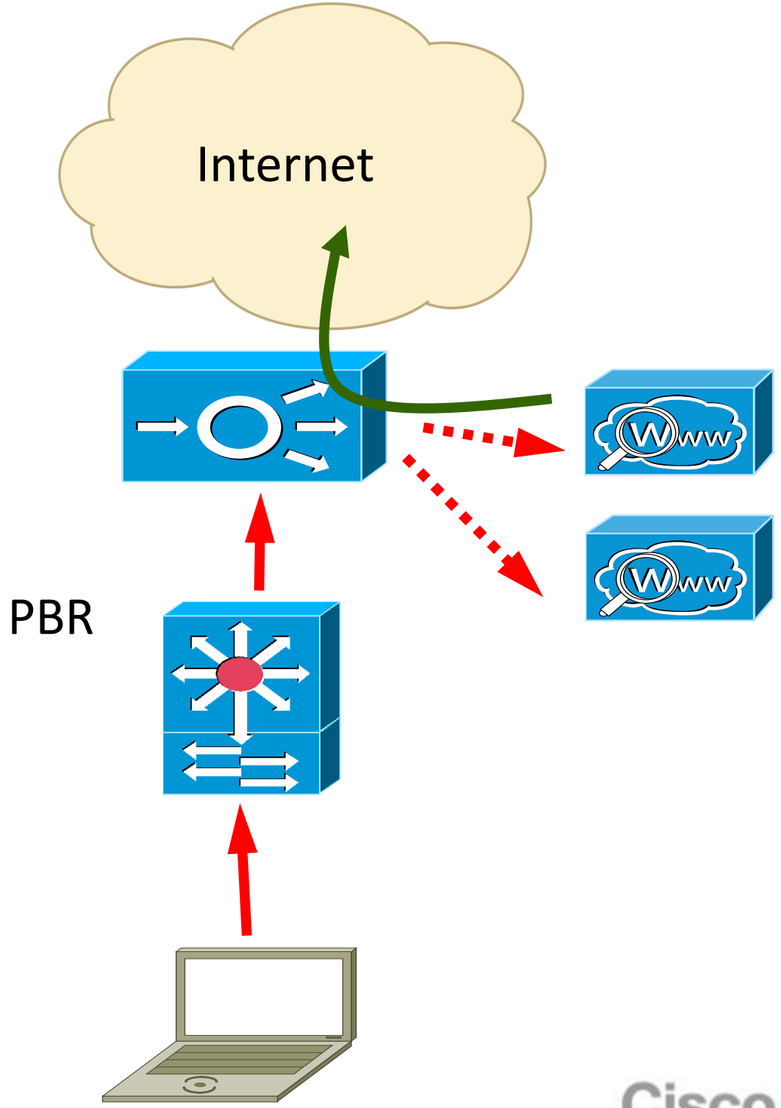
Function Support / Recommend	Software ISR & 7200	ASR 1000	Cat 6500 Sup720 Sup32	Cat 6500 Sup2	Cat 4500	Cat 3750	ASA 5500
Assignment	Hash Only	Mask Only	Mask or Hash / Mask	Mask or Hash / Mask	Mask only	Mask only	Hash only
Forwarding	GRE Only	L2 or GRE / L2 or GRE	L2 or GRE / L2 or GRE	L2 or GRE / L2	L2 only	L2 only	GRE Only
Forwarding Redirect List	Full extended ACL	Full extended ACL	Full extended ACL	Full extended ACL	No Redirect List Support	Extended ACL (no deny)	Full extended ACL
Direction	In or Out / In	In only	In or Out / In	In or Out / In	In only	In only	In only
Return	IP Forward , L2 or GRE	IP Forward, L2, WCCP GRE, or generic GRE	GRE, nGRE, L2, & IP Forward / No GRE	IP Forward or L2 / IP Forward	IP Forward or L2 / IP Forward	IP Forward or L2 / IP Forward	GRE

Transparent Deployment - Summary

- No client settings necessary
- Client resolves hostname of target web server -> improved performance!
- Traffic gets redirected by the network
- Requires involvement of the network department
- Requires HTTPS Proxy activation for HTTPS requests
- Allows for redundancy by defining multiple WSA to redirect
- Selection of the right device to redirect is critical

Deploying using external Loadbalancer

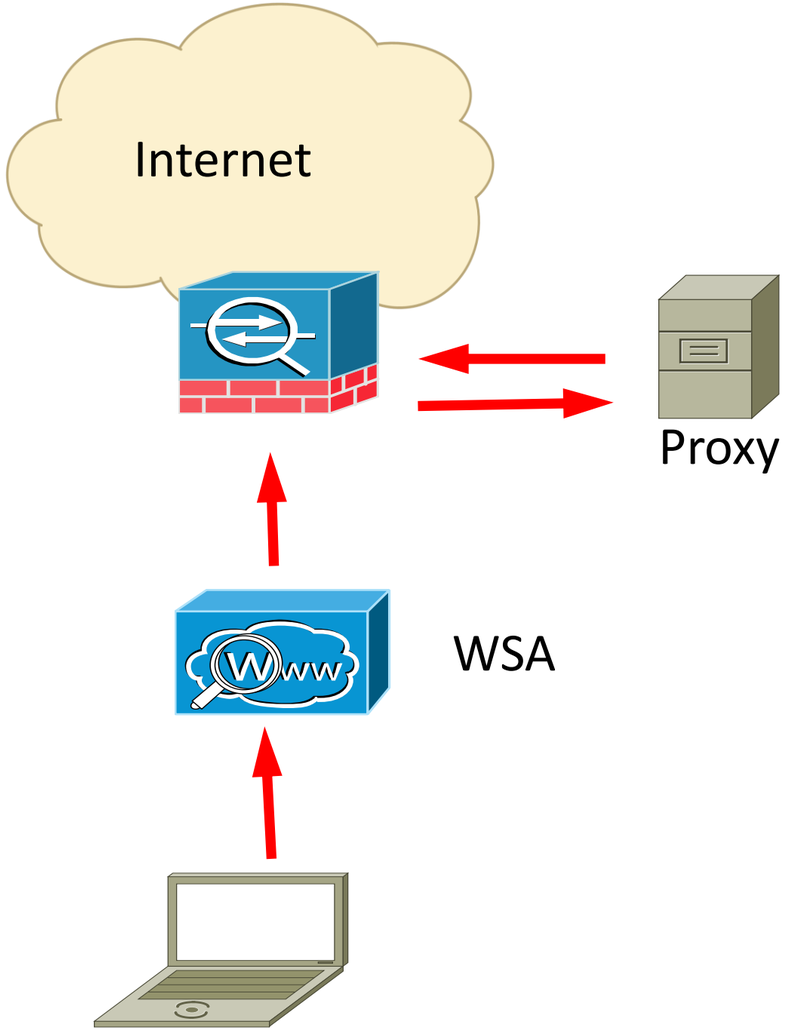
- Scalable up to 16 Gig Throughput in a single ACE Appliance / Module and beyond the limitations of WCCP (32 WCCP Clients max)
- Provides intelligent L7 loadbalancing (i.e. URL based decission)
  - Use CMD :“predictor hash url“ on ACE
- Can be deployed transparently with Policy based Routing (PBR)
- If WSA is using IP-Spoofing, enable MAC-sticky on ACE
- Enable HTTP Probes on ACE



General Consideration - Upstream Proxy

Advice ??

- WSA can be deployed behind an existing Proxy
- To get the value of webreputation, WSA should be placed behind an existing proxy (close to the client...)
- Depending on the upstream proxy, check connection limits!



Policy - Authentication

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Web Reputation and Anti-Malware Filtering	Delete
1	**PO.MUNLABNOAUTH** Identity: ID.MUNLABNOAUTH	(global policy)	(global policy)	(global policy)	(global policy)	(global policy)	🗑
2	**MunlabIP Policy VPN** Identity: ID.MunlabIPVPN	(global policy)	Block: 7 Warn: 3 Monitor: 56 Safe Search: Enforce on Supported Engines Site Content Rating: Block	Block: 1 Monitor: 33 (Bandwidth Limit: 11)	(global policy)	(global policy)	🗑
3	**MunlabIP Policy** Identity: ID.MunlabIP	(global policy)	Block: 6 Monitor: 60 Allow: 2 Safe Search: Enforce on Supported Engines Site Content Rating: Block	Monitor: 34	(global policy)	(global policy)	🗑

- Policy objects can be managed from central access policy screen
- First step is to define the Identity:
  ”For whom does this policy apply?”

Authentication

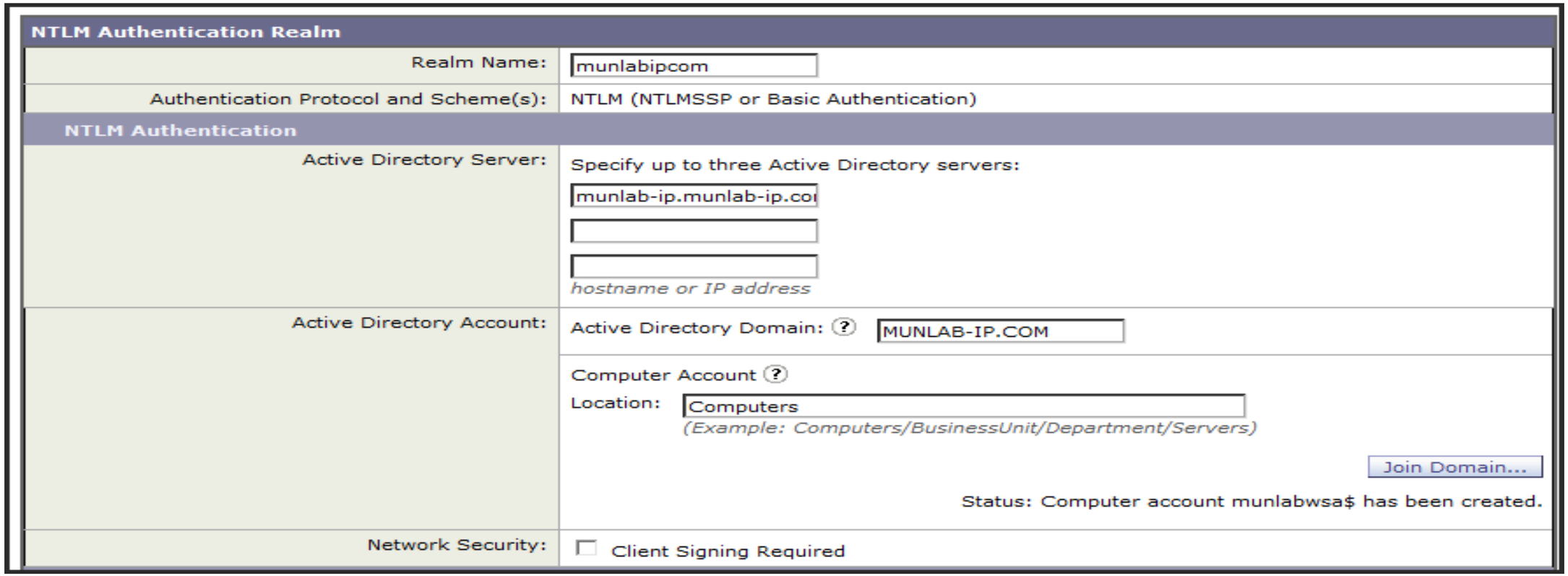
- Authentication Protocols
  - Directory:
    - LDAP or NTLM
  - Method:
    - Basic: Credentials are sent unencrypted
    - NTLMSSP: Challenge-Response
- Tracking the User
  - IP based Surrogates
  - Cookie based Surrogates

Proxy and Authentication Types

For Your Reference

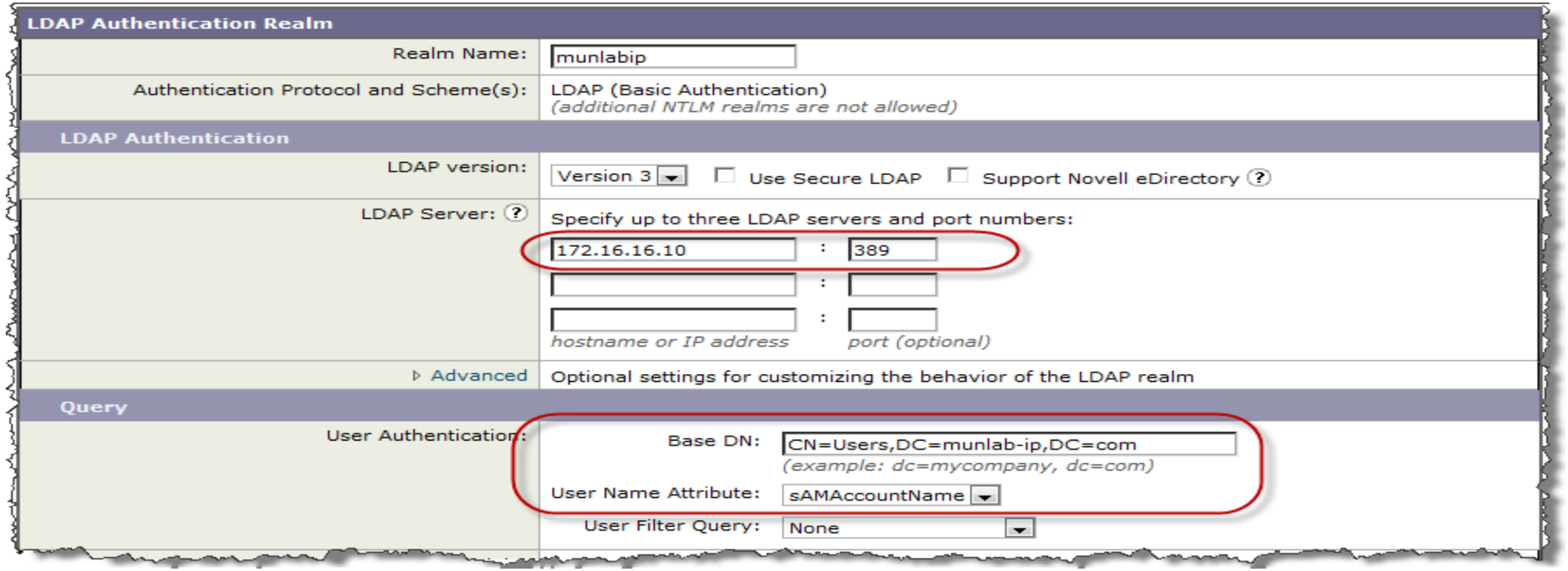
Proxy Type	Authentication	
	Browser to WSA	WSA to Auth Server
Explicit	Basic	LDAP (or NTLM Basic)
Transparent	Basic	LDAP (or NTLM Basic)
Explicit	NTLM	NTLMSSP (Active Directory)
Transparent	NTLM	NTLMSSP (Active Directory)

NTLM Authentication



- NTLM requires Account in the AD Domain
- Credentials to create a computer account are used only once, not stored on appliance
- Currently only one domain is supported via NTLM

LDAP Authentication

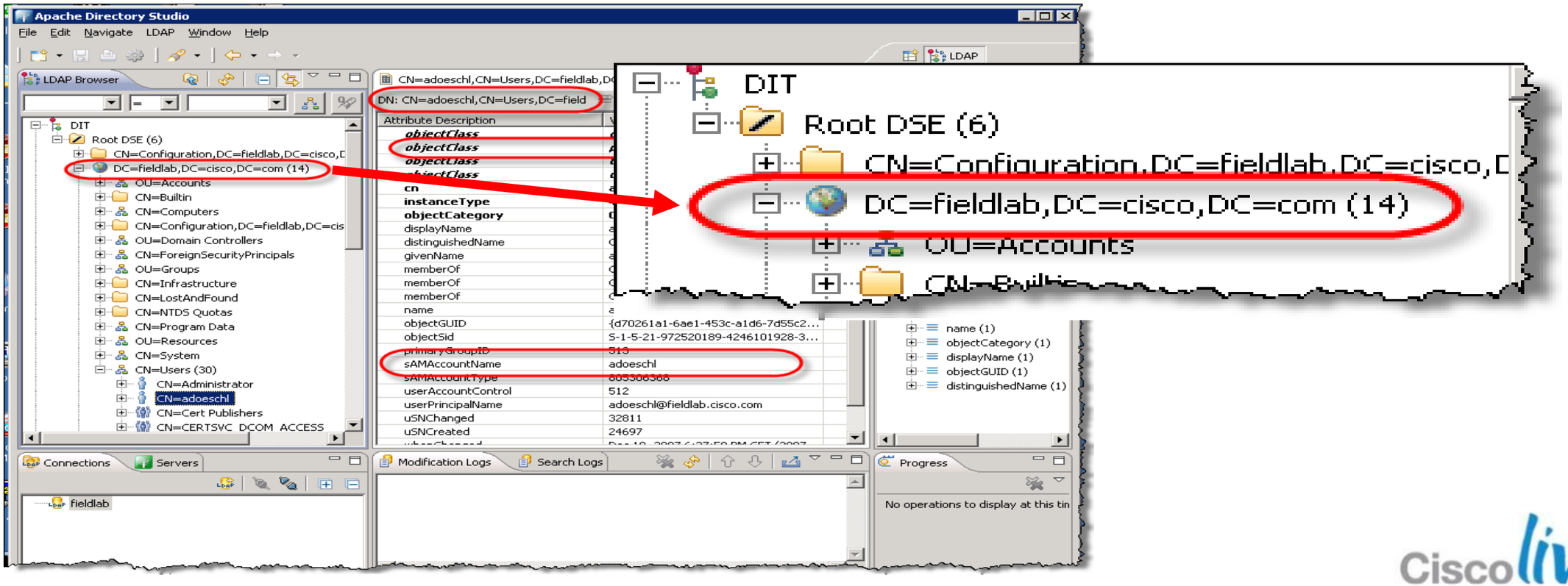


- LDAP queries on port 389 or 636 (Secure LDAP), 3268 (AD GC Server)
- Need to know the Base DN Name Parameter
- Can connect to multiple different domains

Authentication against LDAP

Advi$^{c}_{s}$e ??

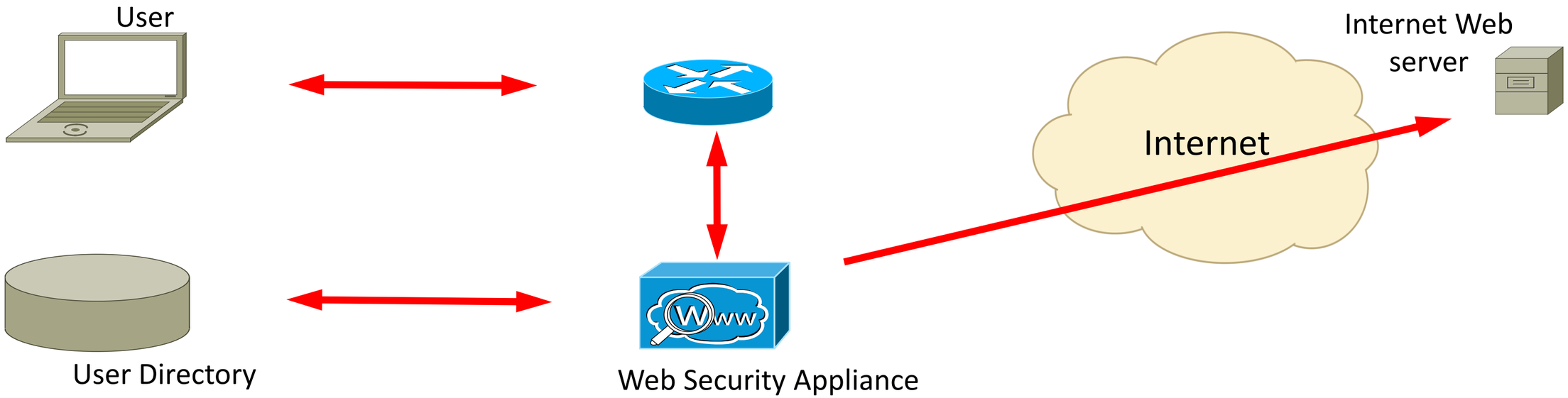
- Knowing the LDAP Base DN is fundamental
- Use an LDAP Browser to find out
  - Recommendation: Apache Directory Studio/Softerra



Authentication in Explicit Deployment

- Proxy sends http response 407 (proxy auth. request)
  - Client recognises the proxy
  - Client will then accept a http response 407 from the proxy
- Works for HTTPS
  - Client sends a CONNECT request to the proxy
  - Client will then accept a 407 response from the proxy

Authentication in Transparent Deployment



- Client is not aware of a proxy -> http response 407 cannot be used
- Need to use http response 401 – basic authentication

  Client needs to be first redirected to the wsa

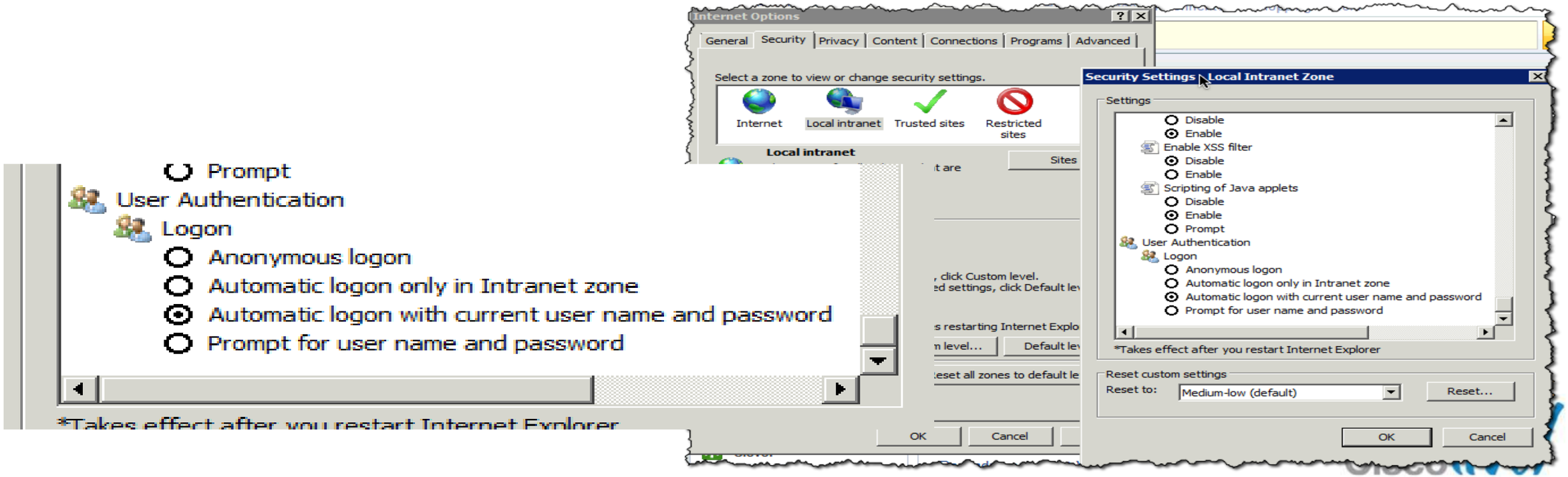
Authentication in Transparent Deployment

	What the client thinks	What is really happening
1	The client sends a request to the remote HTTP server	The client **request is rerouted** to the WSA
2	The client receives a “307” from the remote server redirecting the client to the WSA	The client receives a “307” from the WSA, **spoofing the remote server**, redirecting the client to the WSA
3	The client connects to the WSA	The client connects to the WSA
4	The client receive a “401” authentication request from the WSA	The client receive a “401” authentication request from the WSA
5	The client authenticates with the WSA	The client authenticates with the WSA
6	The client receive a 307 from WSA, redirecting it back to the remote server	The client receive a 307 from WSA, redirecting it back to the remote server
7	The client connects back to the remote server	The client **continues to use the WSA** as a transparent proxy

IE8/IE9 with Single-Sign On

Advice ??

- SSO on WSA correctly configured but Clients still get prompted
- Check if WSA Redirect Name is listed in „Trusted Sites“
- Check „Security Settings“ on Trusted Sites and set to „Automatic Logon with current user name and password“

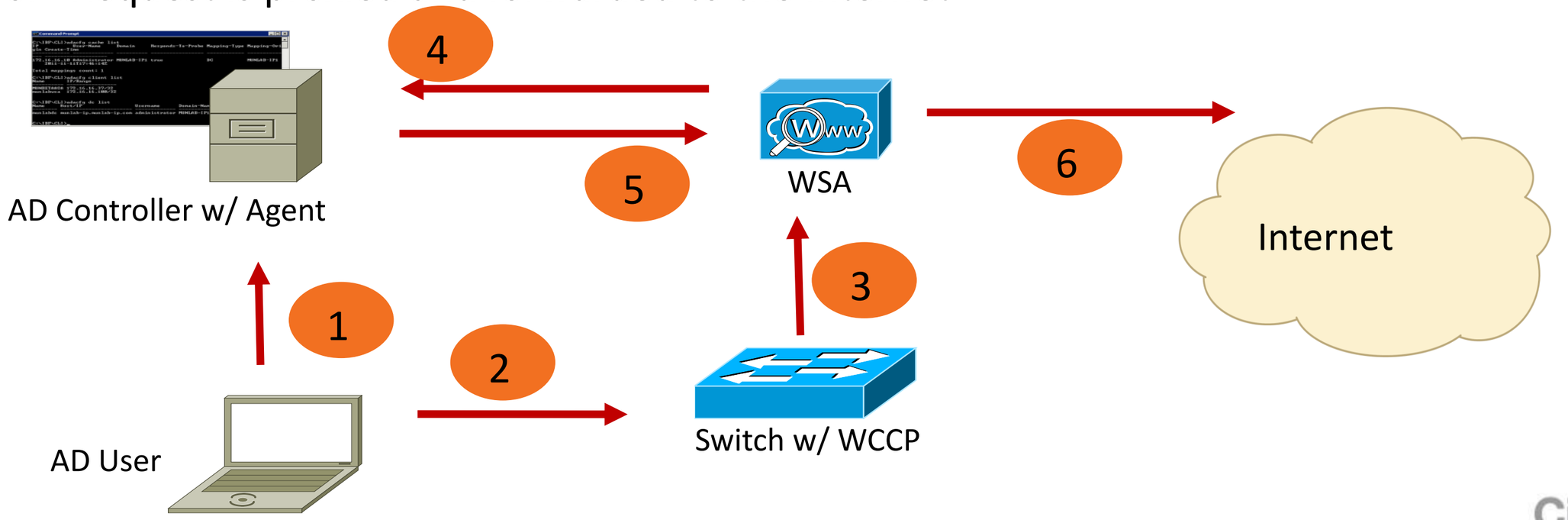


WSA with Transparent User Identification

Transparent User Identification (TUI)

Web Security Release 7.5

1. Client logs on to the AD Domain
2. Client request a Web Site
3. Traffic is transparently redirected to the WSA
4. WSA needs to authenticate and queries the AD Agent for the User/Group
5. AD Agent looks up the IP and delivers User/Group
6. Request is proxied and forwarded to the Internet



Transparent User Identification (TU

For Your Reference

- Web Security Release 7.5 – Config AD Agent

```
Command Prompt

C:\IBF\CLI>adacfg cache list
IP            User-Name      Domain      Responds-To-Probe Mapping-Type Mapping-Ori
gin Create-Time
------------- -------------- ----------- ----------------- ------------ -----------
--- --------------------
172.16.16.10 Administrator MUNLAB-IP1 true                DC           MUNLAB-IP1
    2011-11-11T17:46:14Z

Total mappings count: 1

C:\IBF\CLI>adacfg client list
Name        IP/Range
----------- ----------------
MUNBETAASA 172.16.16.37/32
munlabwsa  172.16.16.100/32


C:\IBF\CLI>adacfg dc list
Name     Host/IP                    Username      Domain-Name Latest Status
-------- ------------------------- ------------- ----------- -------------
munlabdc munlab-ip.munlab-ip.com administrator MUNLAB-IP1  up


C:\IBF\CLI>_
```

```
adacfg client create -name adagent -ip 127.0.0.1 -secret mysecret
adacfg client create -name mywsa -ip 172.16.16.100/32 -secret
mysecret
adacfg dc create -name mydc -domain mydomain.com -host
      dc11.mydomain.com -user admin -password password
```

Transparent User Identification (TUI)

For Your Reference

Web Security Release 7.5 - Config

Active Directory Agent: Enable Transparent User Identification using Active Directory

Primary Active Directory Agent:

Server: munlab-ip.munlab-ip.com Shared Secret: ••••••••

Backup Active Directory Agent (Optional):

Server: Shared Secret:

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

Network Security: Client Signing Required

Define Members by Authentication: Identify Users Transparently

No Authentication
Require Authentication
Identify Users Transparently

munlabipcom

If transparent user identification fails: Support Guest privileges / Enforce authentication prompt

Select a Scheme: Use NTLMSSP

Scheme setting applies to HTTP/HTTPS only.

If a user fails authentication: Support Guest privileges

Authorization of specific users and groups is defined in subsequent policy layers (see Web Security Manager > Decryption Policies, Routing Policies and Access Policies).

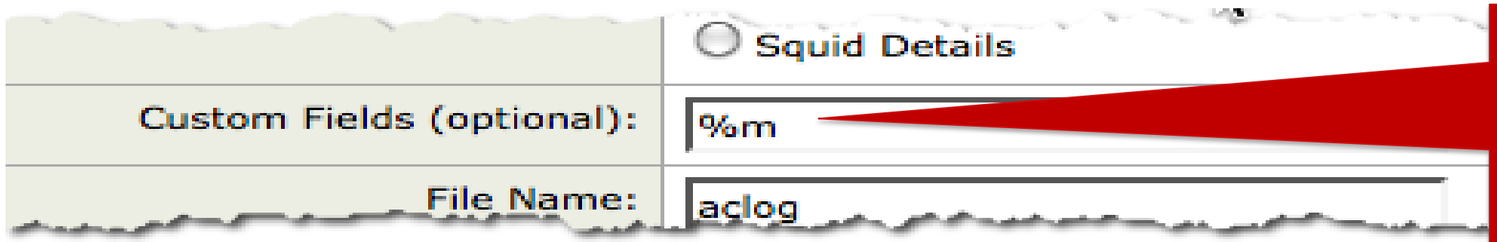
Enable TUI in the Authentication Realm

Specify the Agent via Radius

Edit the Identity to activate TUI

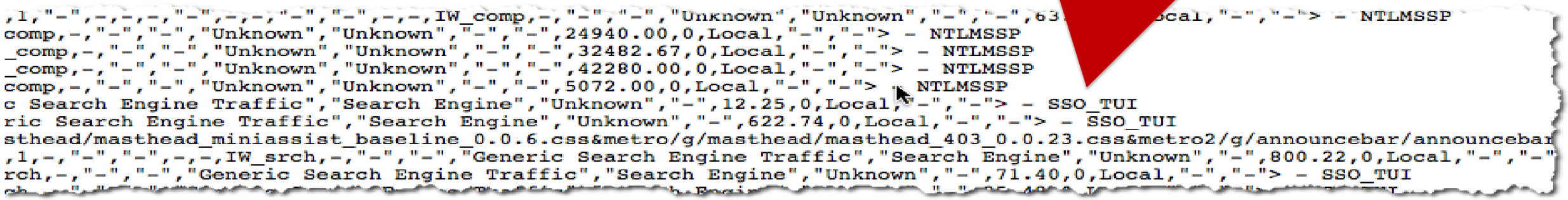
Transparent User Identification (TUI)

Web Security Release 7.5 – Verification accesslogs



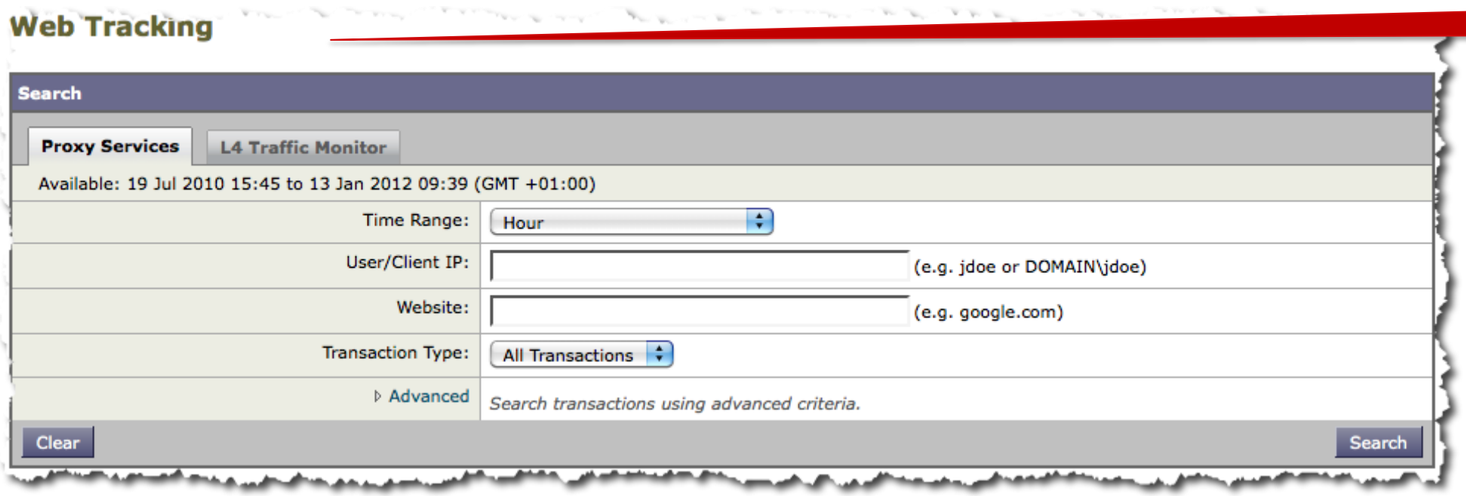
Add custom field “%m” (=Authentication Method) to the access_log

In the Access_logs:
Check for SSO_TUI



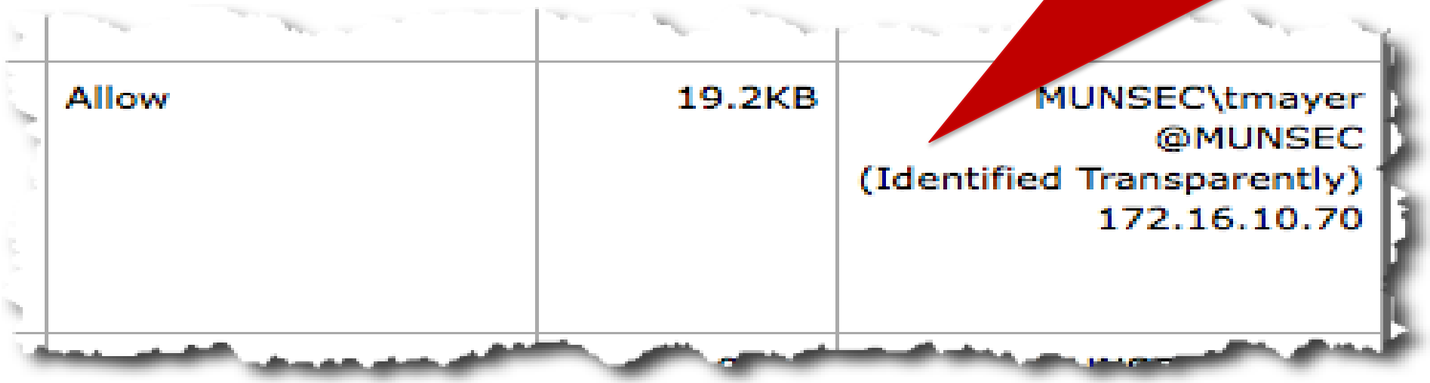
Transparent User Identification (TUI)

Web Security Release 7.5 – Verification GUI



Go to Webtracking

User was identified transparently



TUI – Summary & Caveats

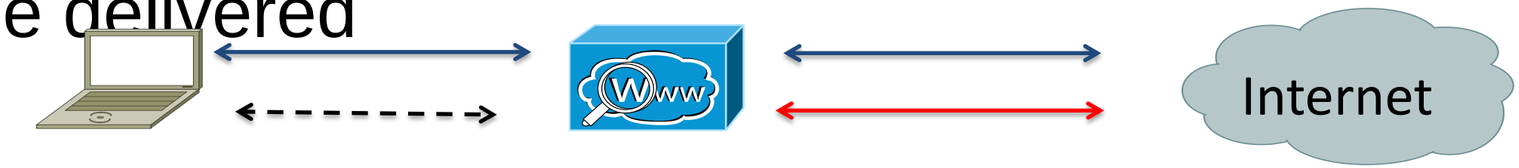
- Uses an Agent running on a Server in the AD Domain
- Same Agent is also used for Identity based Firewalling on the ASA
- Allow all applications on the client to work with authentication without starting a browser first
- Does support IPv6 for Client registration and RADIUS messages

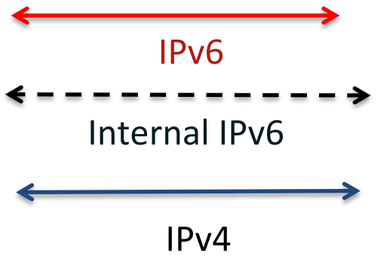
```
Administrator: Command Prompt

C:\IBF\CLI>adacfg cache list
IP                                      User-Name  Domain  Responds-To-Probe  Mapping-Typ
e  Mapping-Origin  Create-Time
_______________________________________  _________  ______  _________________  ___________
_  ______________  ____________________
2001:db8:1:10:526e:766a:a260:d816  tmayer     MUNSEC  true               DC
  MUNSEC          2012-01-13T10:06:00Z

Total mappings count: 1

C:\IBF\CLI>_
```

- Does not work if Client is NATed after AD Authentication but before reaching the WSA
- If Client cannot be identified, fallback to previous authentication mechanism like Basic or NTLM

Cisco Ironport WSA & IPv6 Support

- Current version of WSA does not yet support IPv6
- Support is planned for Q2CY2013
  IPv6 Support for explicit mode
  WCCP depends on implementation of ISR, ASA and Switches, will be done in a later release
- WSA will listen for connections both on IPv4 and IPv6
- Admin can configure, if IPv4 or IPv6 should be preferred
- Depending on Configuration, A-record or AAAA-record will be delivered





Sizing for WSA

- Main Parameters for sizing are “requests per second” and “ # HTTP Requests”
- Rule of thumb:
  Each request/s is approx. 80-90 Kbps of HTTP traffic
  Each Mbps of HTTP translates to approx. 10 requests/s
  100 Mbps of sustained HTTP traffic is approx. 1000 requests/s
- To find out the request rate on a WSA: use the “rate” CLI command

```
^Cmunlab-wsa01.munsec.com> rate

Press Ctrl-C to stop.
    %CPU  reqs                          client    server    %bw  disk  disk
    used  /sec   hits blocks misses     kb/sec    kb/sec  saved   wrs   rds
    15     6      1      0     65       196       192     1.6     57     1
    18    21      4      0    215       787       787     0.0    164     2
    15    17      0      0    171       835       835     0.0    150     0
```

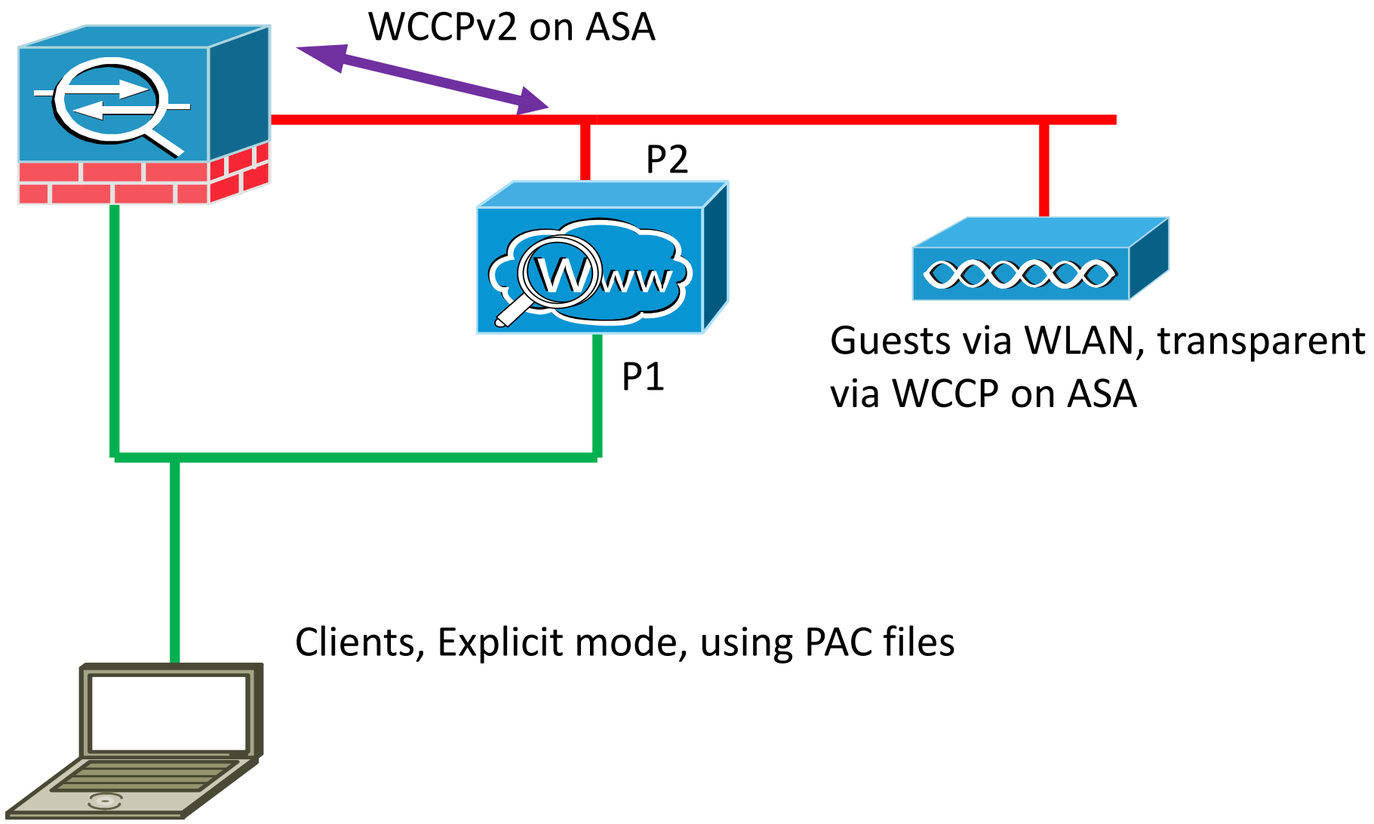
Those parameters allows a quite correct sizing depending on features together with the Cisco SE

WSA 7.5 Sustained System Capacity (RPS)
(along with Peak RPS)

Features	S670	S370	S170
Proxy	1200 (3500)	650 (3300)	150 (310)
Proxy, CIWUC, AVC	800 (3100)	650 (2100)	150 (310)
Proxy, CIWUC, AVC, WBRS	800 (3100)	650 (2100)	150 (310)
Proxy, CIWUC, AVC, WBRS, NTLM, Webroot, Sophos,	700 (1050)	400 (490)	100 (230)
Proxy, CIWUC, AVC, WBRS, NTLM, Webroot, Sophos, Adaptive Scanning	700 (940)	400 (440)	100 (210)
Proxy, CIWUC, AVC, WBRS, NTLM, Webroot, McAfee	600 (850)	290 (300)	90 (100)
Proxy, CIWUC, AVC, WBRS, NTLM, Webroot, McAfee, Adaptive Scanning	600 (770)	290 (270)	90[b] (90)

Sample Design using WSA with Explicit and Transparent mode

- Clients connect via PAC-File to P1 Interface
- Guests are connecting via WLAN in DMZ transparently
- Interface P2 is used for WCCP with ASA
- Interface P2 has by default ACL configured
  - Needs to be adjusted via „advancedproxyconfig“ on WSA



Summary – Cisco Ironport Web Security Appliance

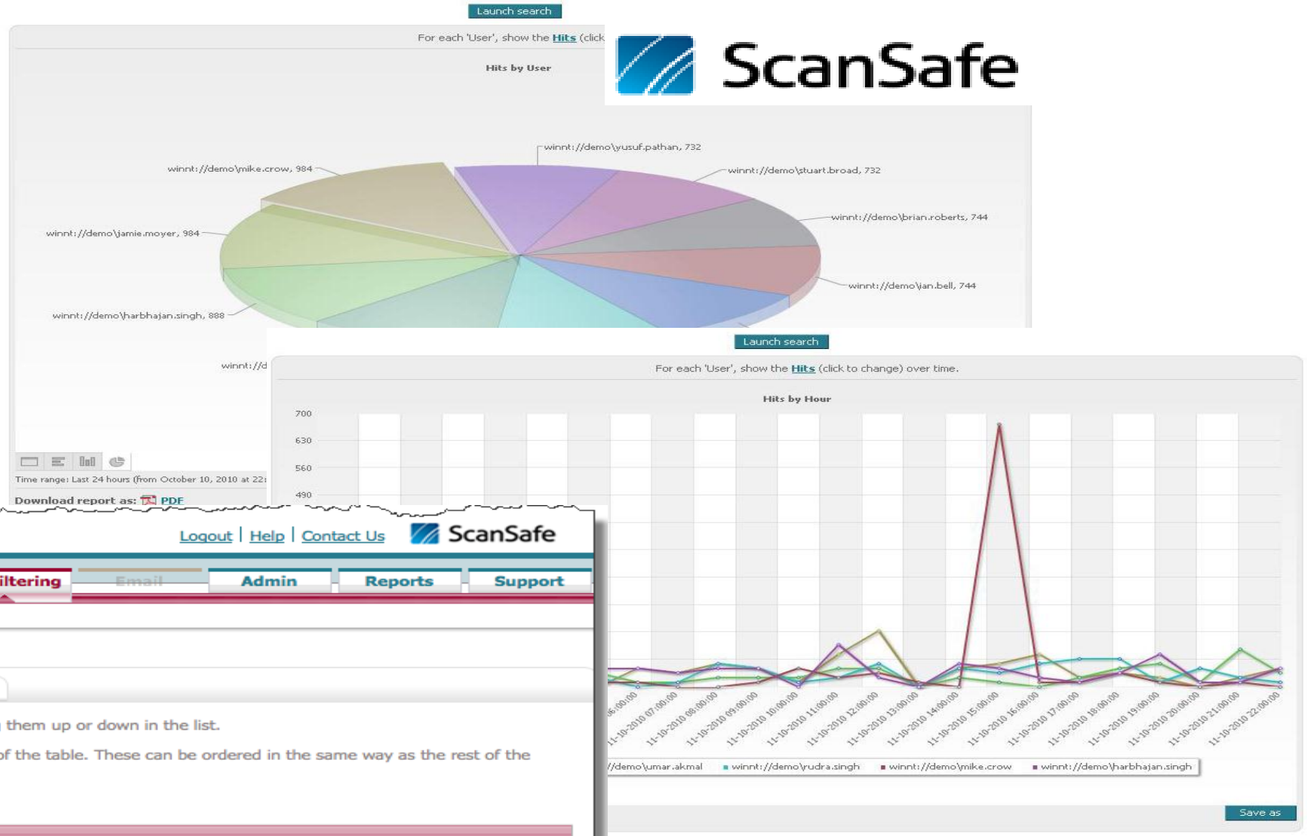
- Scalable On-premise Solution
  - S170 : up to 1000 Users, S370: up to 10000 Users, S670: more than 10000 Users
- Many functionalities in one single appliance
  - Reputation, malware filtering, SSL decryption, URL Filtering
- Can be deployed explicit or transparent mode (WCCP)
  - Transparent:
    right sizing of network hardware
    no client settings necessary
    high scalability
    careful with non-browser Web applications that require authentication (TUI might help)
  - Explicit:
    requires client settings
    High Availability with PAC files or Loadbalancer

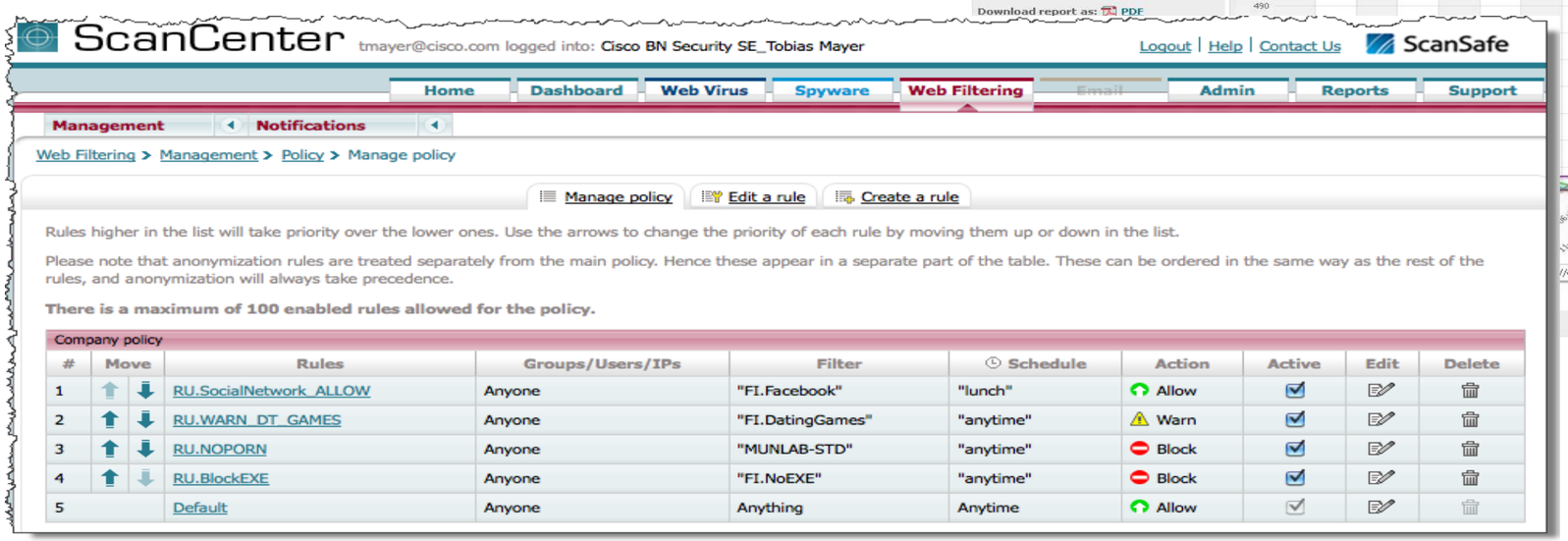
Agenda

- Web Security Overview
- Cisco Web Security Appliance (IronPort)
- Cisco Cloud Web Security (Scansafe)
- Hybrid Web Security (Appliance + Cloud)

Websecurity through Cloudservice

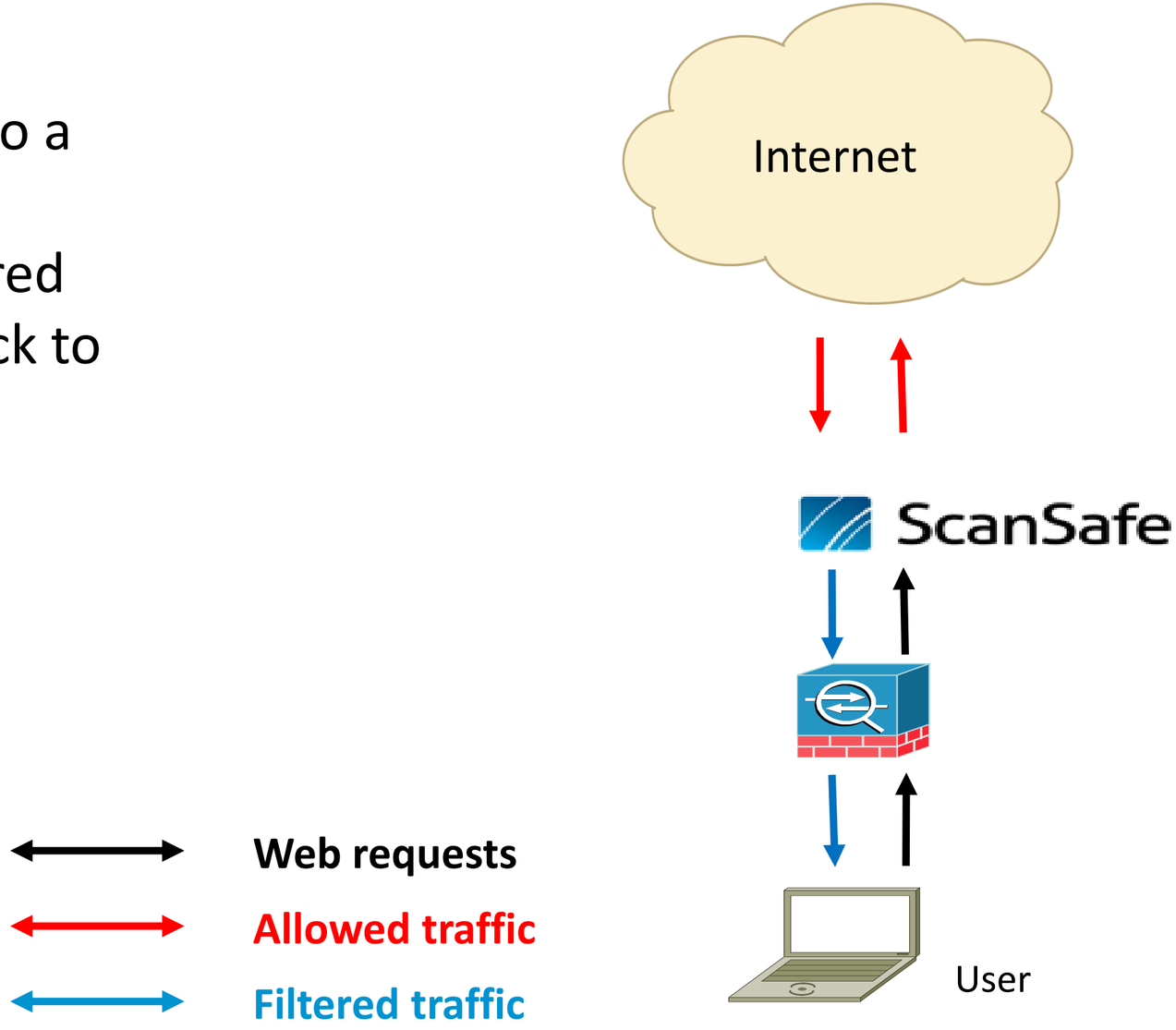
- Hosted Websecurity through Cisco Scansafe Cloud Service
- Central reporting and administration through Scancenter Portal





Data Flow with ScanSafe

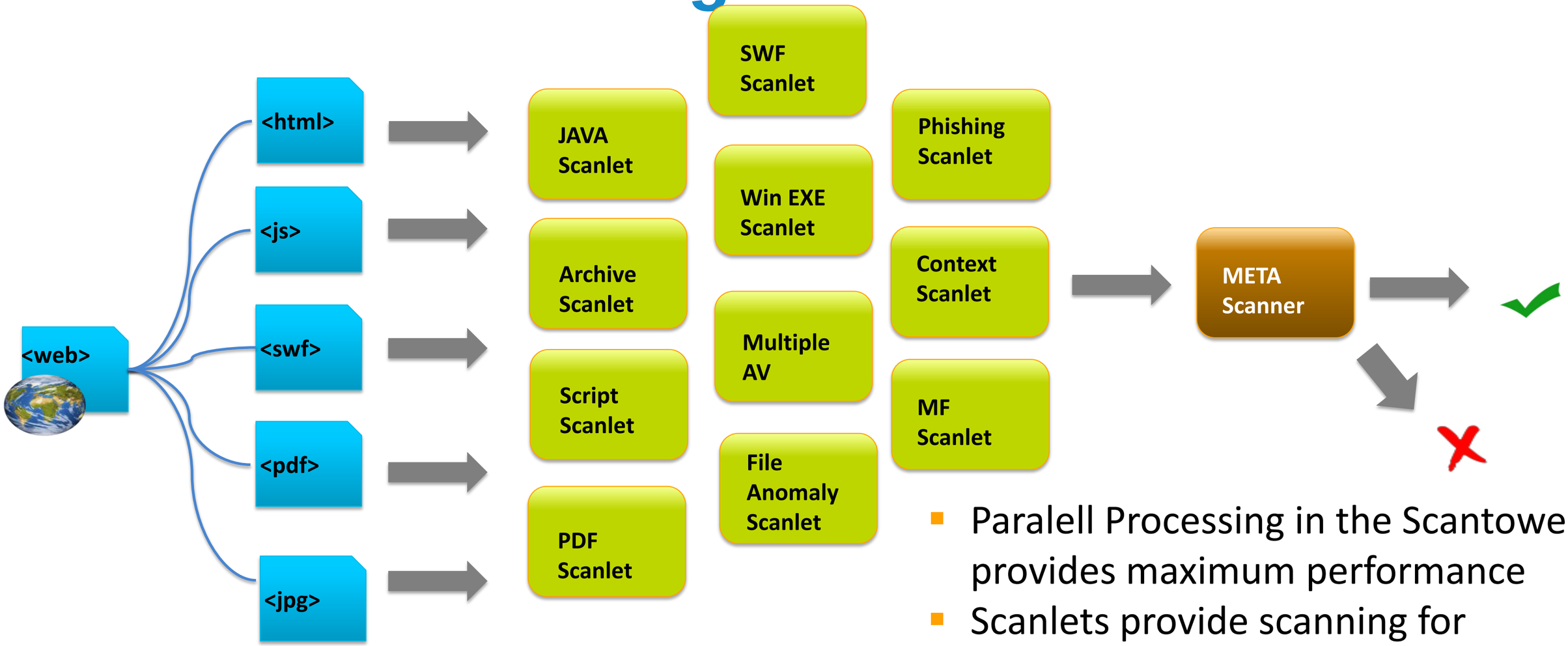
- Client requests are redirected to a proxy in the cloud
- Requests are checked and filtered
- Clean requests are directed back to the client



Scalability & Reliability

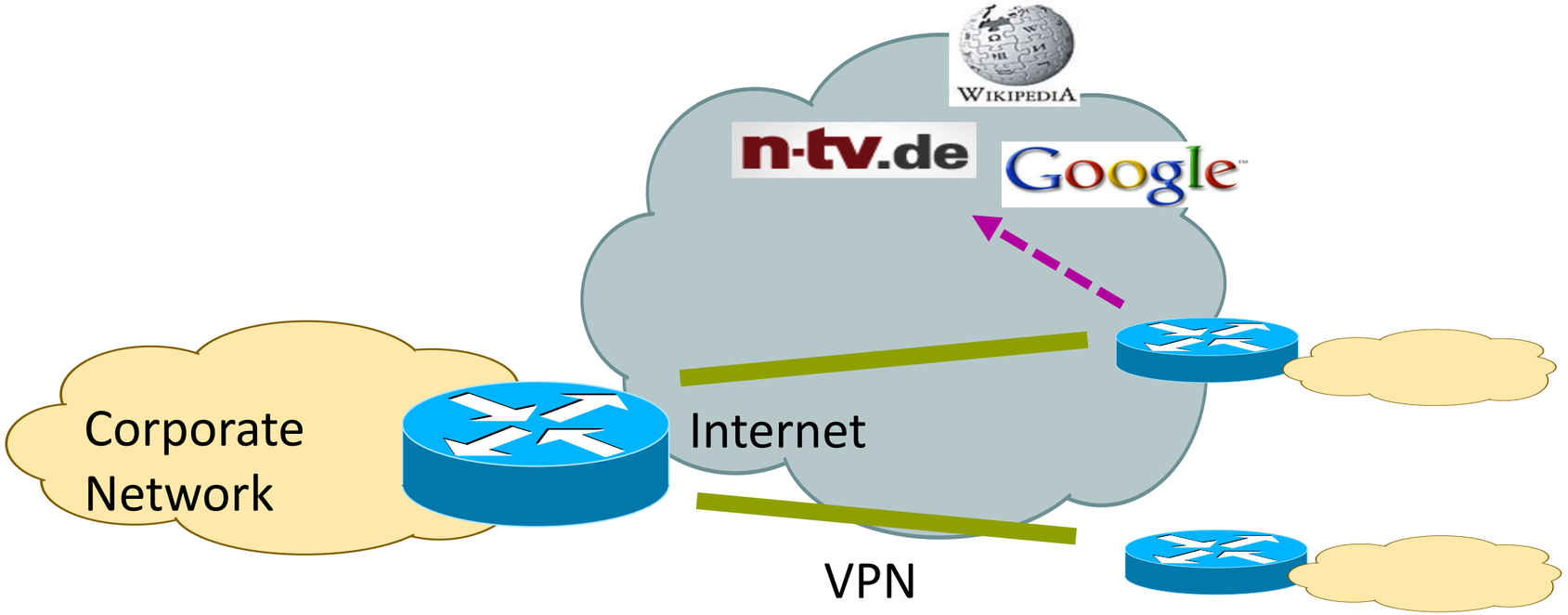
- Billions of web requests per day
- <50 ms latency
- High-Availability Infrastructure
- Parallel Processing

Outbreak Intelligence



- Paralell Processing in the Scantower provides maximum performance
- Scanlets provide scanning for malware through code anomaly analysis

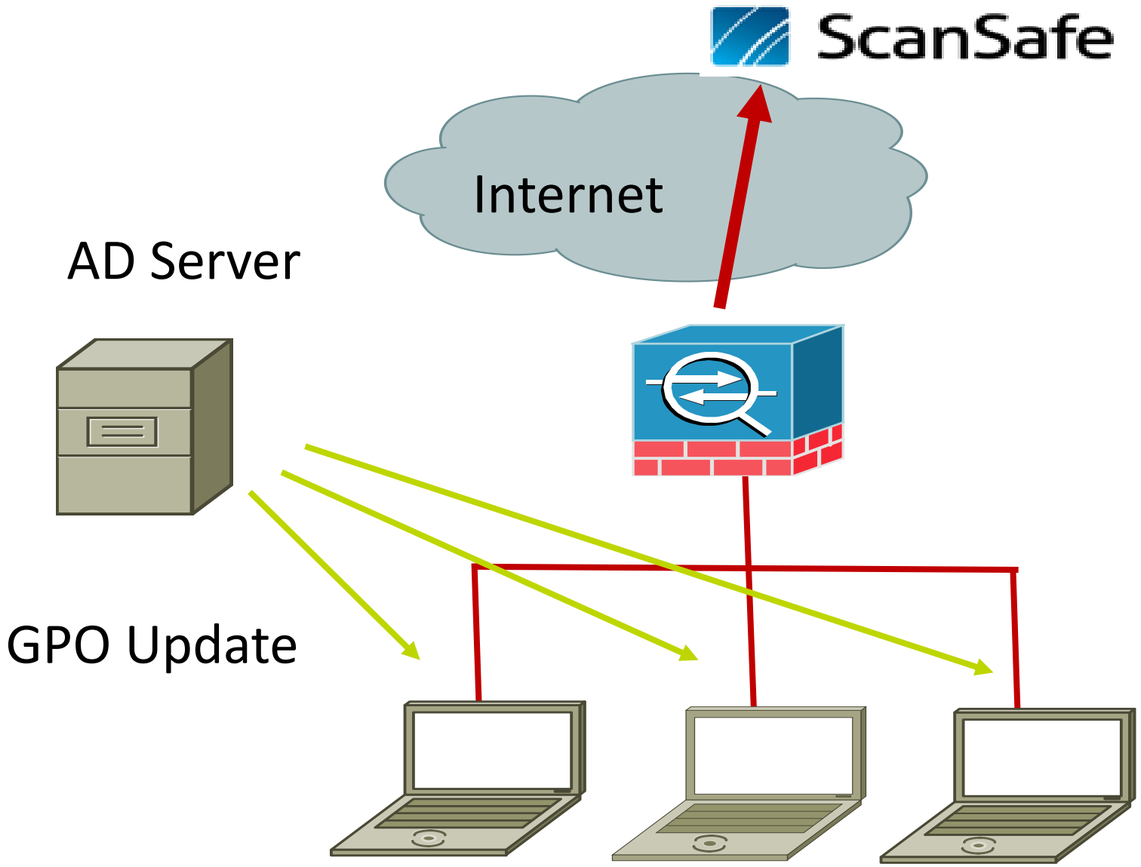
Challenge:
Branch Office with local Breakout



- Webtraffic destined for the central DC is sent via VPN Tunnel
- Normal Webtraffic goes directly to the Internet
  bandwidth saving in the central site
- But how to secure the webtraffic?

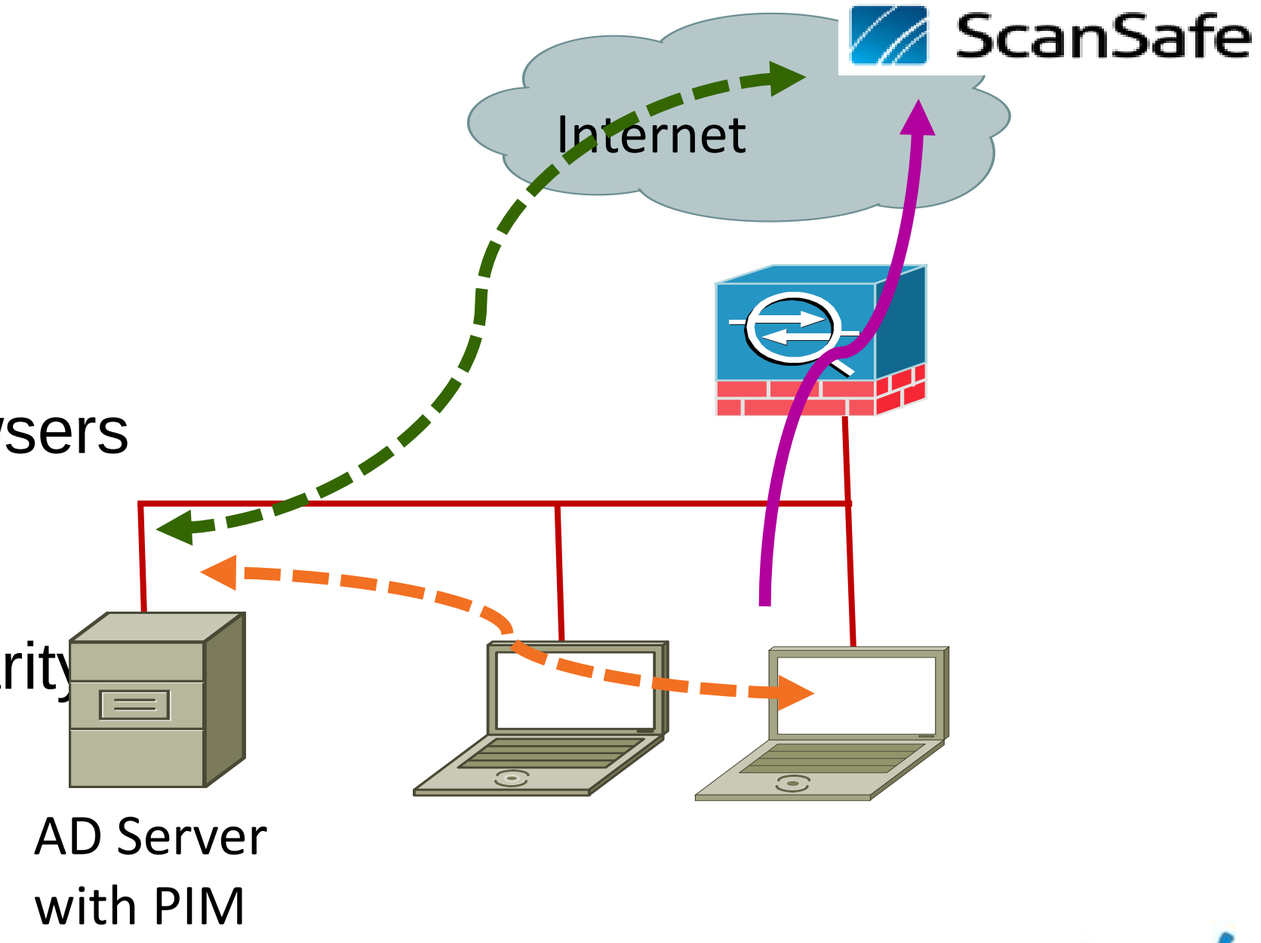
Browser Redirection via GPO / PAC

- Proxy Settings are pushed to browsers via Active Directory GPO
- Browsers connect through Firewall on port 8080 to Web Security Service
- Firewall blocks all other GET requests
- Provides Site/External IP granularity



PIM – Passive Identity Management

- PIM is a small EXECUTABLE, run by **Login Script or GPO**
- Runs GPRESULT API to get identity Information, **contacts ScanSafe and downloads Identifier**
- Does not work for Opera or other Browsers
- Requires no client installation
- Provides only End User/Group granularity
- Provides no traffic redirection



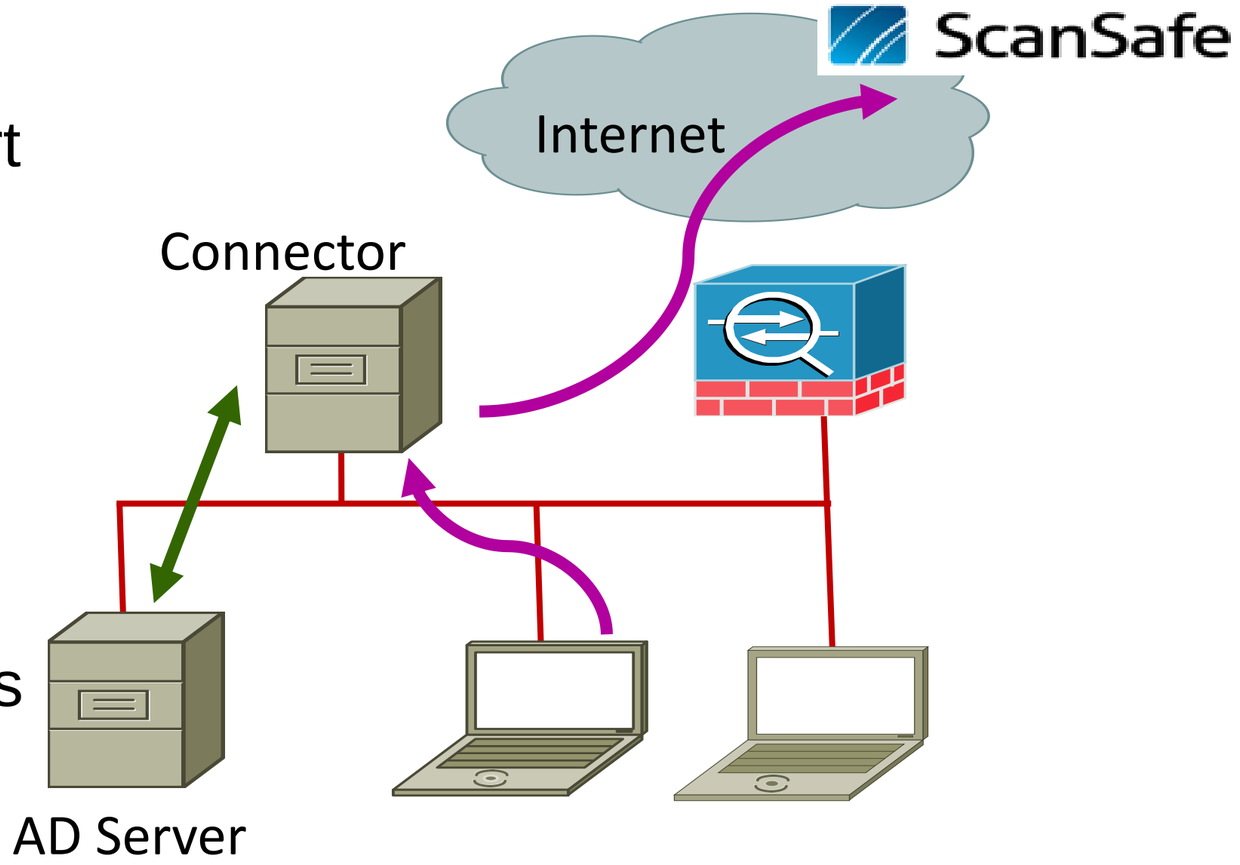
How Does PIM Work in Detail?

For Your Reference

- PIM adds -XS headers to the browser's user agent string
- Included in this string is a unique hash that identifies the user in our Scanning tower
- This detail is encrypted
- Upon logon, PIM sends an out-of-bound request to the scanning tower and uploads the group information for that user
- These groups are automatically created in ScanCenter
- Following registration, each time a request to the Web is made, only the hash is sent to us along with the request and we can indentify the user and apply the correct policy according to the relevant group/s

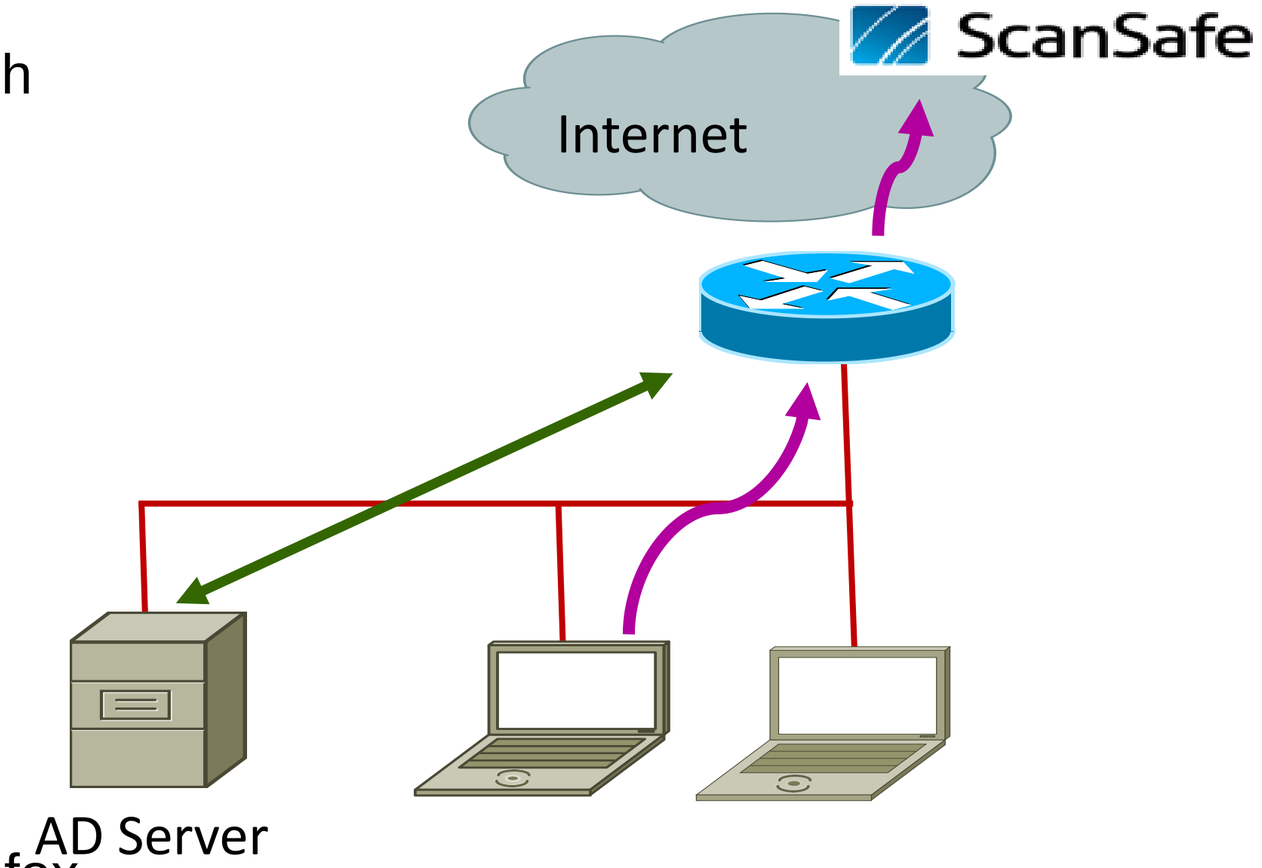
Standalone Connector

- Proxy Settings are pushed to browsers via AD,GPO or PAC file
- **Forwards web traffic** to ScanSafe on port 8080/443 to the Cloud based Tower
- Connector receives Client info and queries Active Directory Server for **Group Information**, then proxies to ScanSafe upstream
- Set Firewall to block all other GET requests
- Provides IP/End User/Group granularity
- Scalable up to 10000 Users per Connector, depending on which HW it is installed



ISR G2 with integrated Connector

- Connector is integrated into Cisco ISR G2 Router Platforms
- No need to install Connector seperatly in branch networks
- Redirect of the webtraffic is happening transparently for the user on the router
- Provides Scantower redundancy
- Provides User granularity
  - Authenticate User via NTLM (transparent authentication) or Basic (Prompt for Credentials)
  - NTLM works without prompting for IE, Firefox and Google Chrome



ISR G2 with integrated Connector

Simple Config

```
parameter-map type content-scan global
 server scansafe primary name proxy100.scansafe.net port http 8080 https
8080
 license 0 686684863893669869869686896986 68
 source interface FastEthernet8
 timeout server 60
 timeout session-inactivity 120
 user-group munlab username tmayer
 server scansafe on-failure block-all

interface FastEthernet8
 description $WAN-Interface$
 ip address dhcp client-id FastEthernet8
 ip nat outside
 content-scan out
```

Sizing and Scalability for ISR with Connector

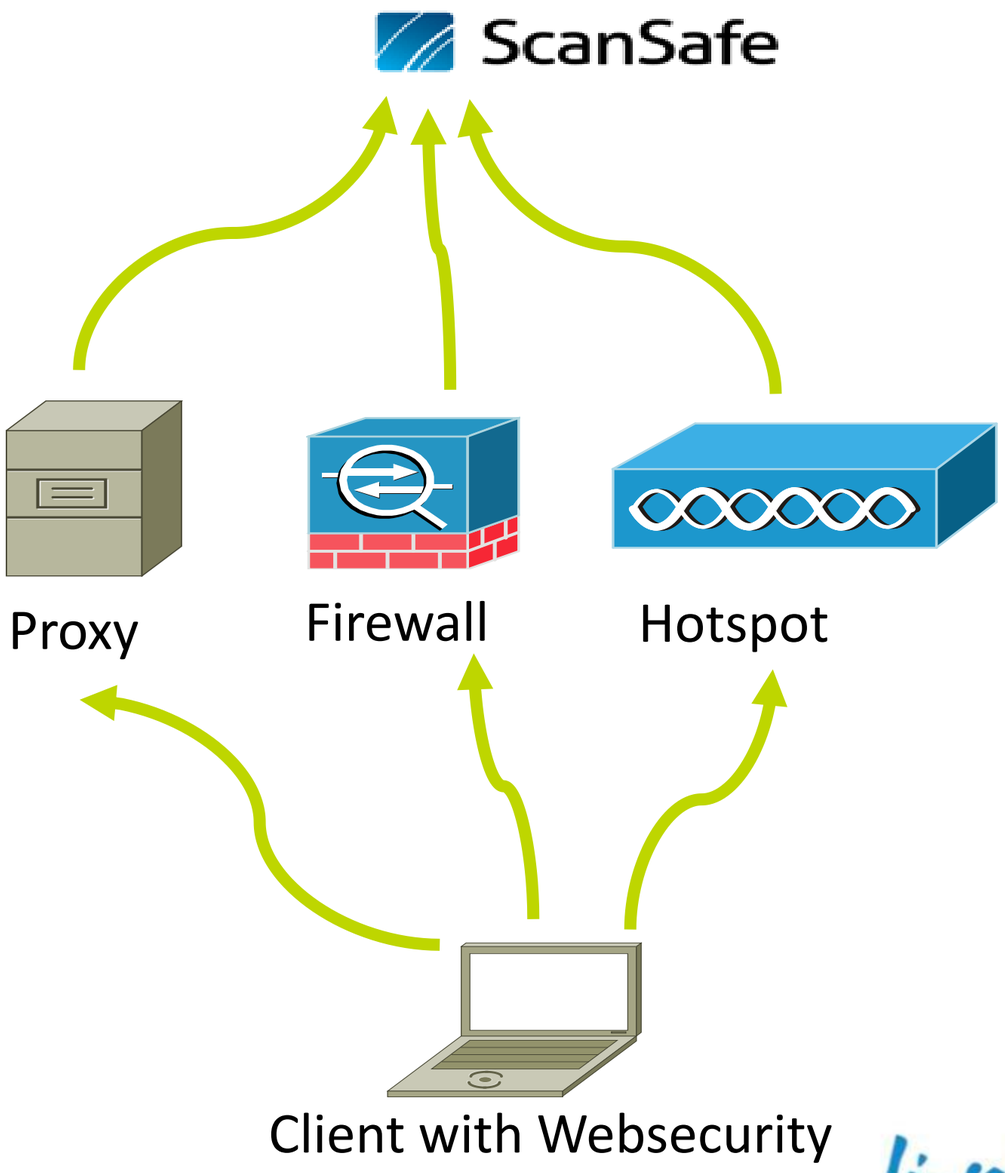
For Your Reference

ScanSafe Users Supported per ISR G2 Platform

		3945E	3925E	3945	3925	2951	2921	2911	2901	1941	1921	891
Phase I	No Auth	5000	5000	1200	900	600	500	400	350	350	300	120
Phase I	Web Proxy	1200	1200	1200	900	600	500	400	350	350	300	120
Phase II	HTTP Basic	1200	1200	1200	900	600	500	400	350	350	300	120
Phase II	NTLM	1200	1200	1200	900	600	500	400	350	350	300	120

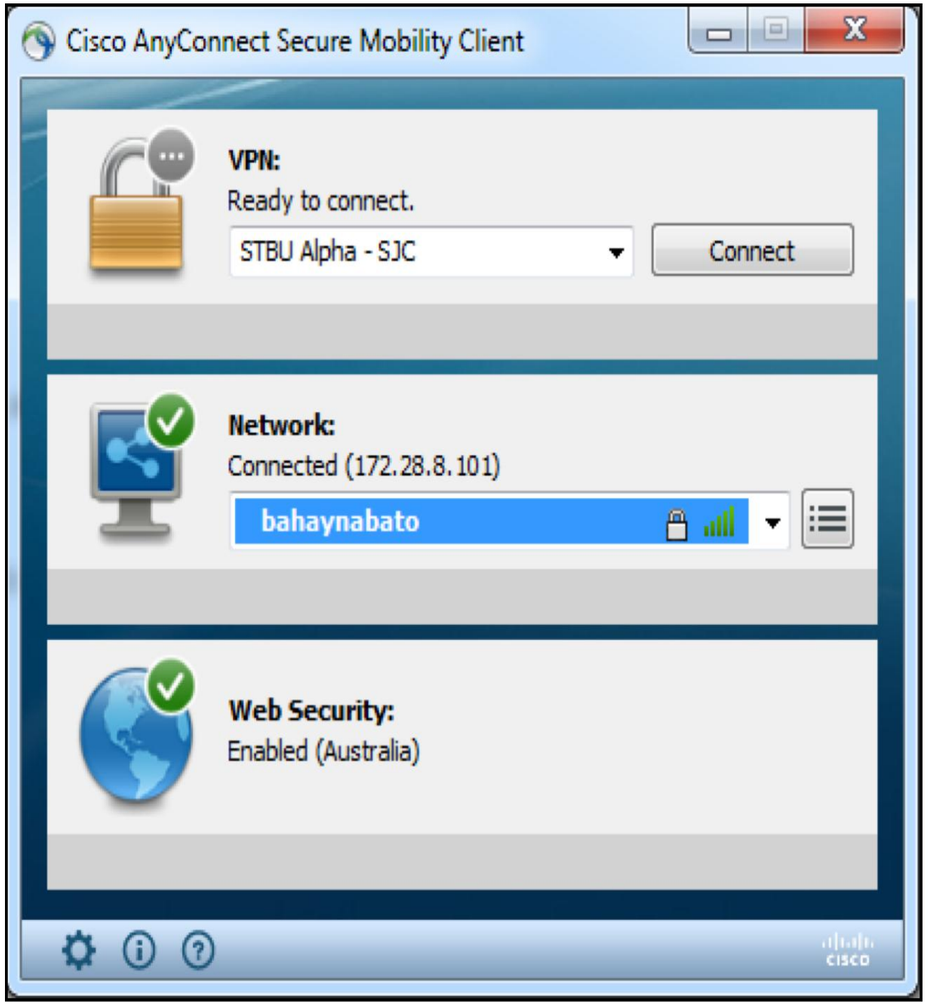
Roaming User

- Installs a Network Driver which binds to all connections (LAN, Wireless , 3G)
- Automatic Peering Identifies nearest ScanSafe Data Centre and whether a connection is possible.
- AD information can be remembered from when the user was last on the corporate network using the GPRESULT API (group policy)



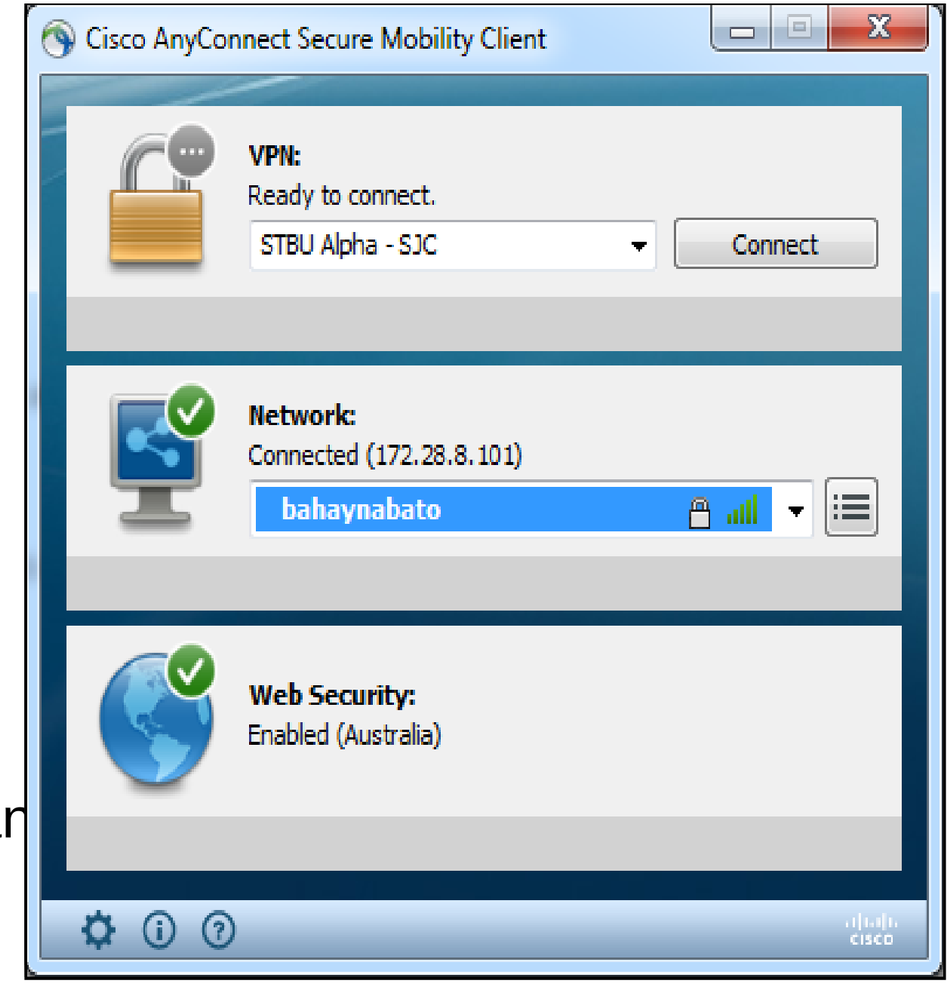
Web Security & AnyConnect

- Supported on Windows & MAC OS X
- Client settings are controlled via Profile
- Profile can be centrally distributed via the Scancenter Portal



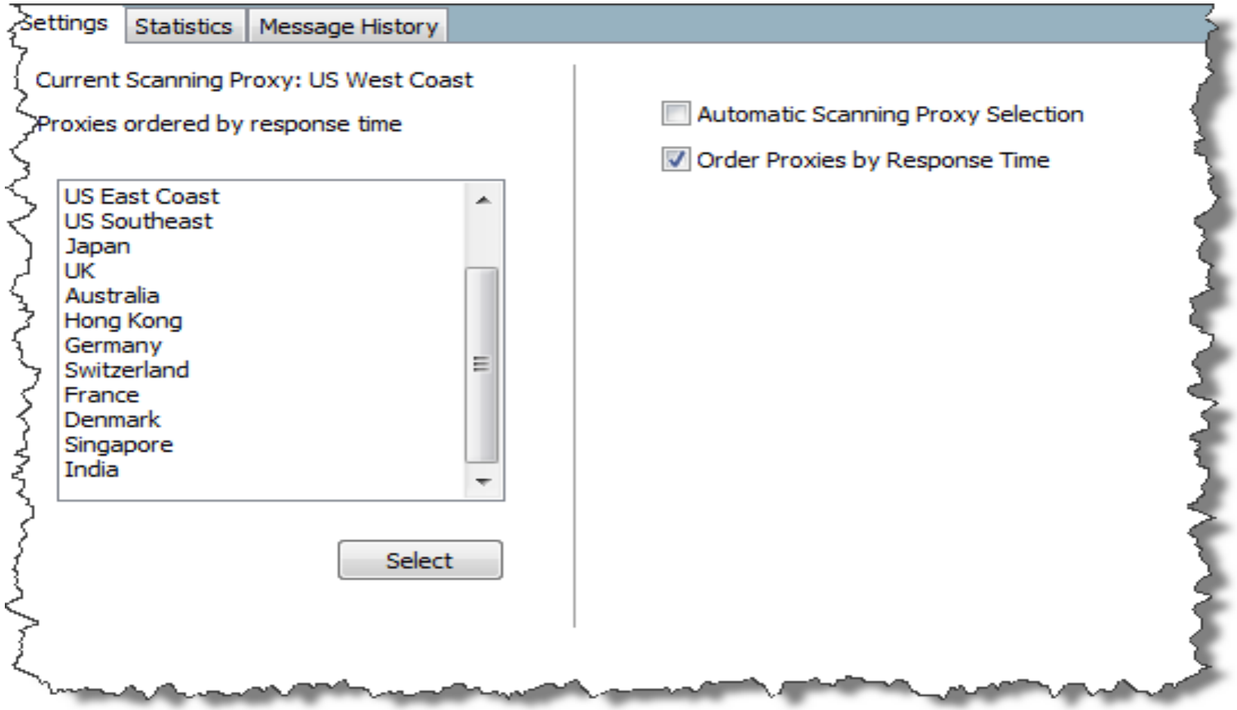
Web Security & AnyConnect

- Single and modular client
  - VPN (SSL, IKEv2, Always-On,...)
  - 802.1x (Wired, Wireless, MACSEC...)
  - Websecurity
  - Posture for VPN
  - Telemetry (SIO)
- All modules can be used independently or all together
- If VPN Module is used, profile management can be done centrally through ASA



How Does it Work?

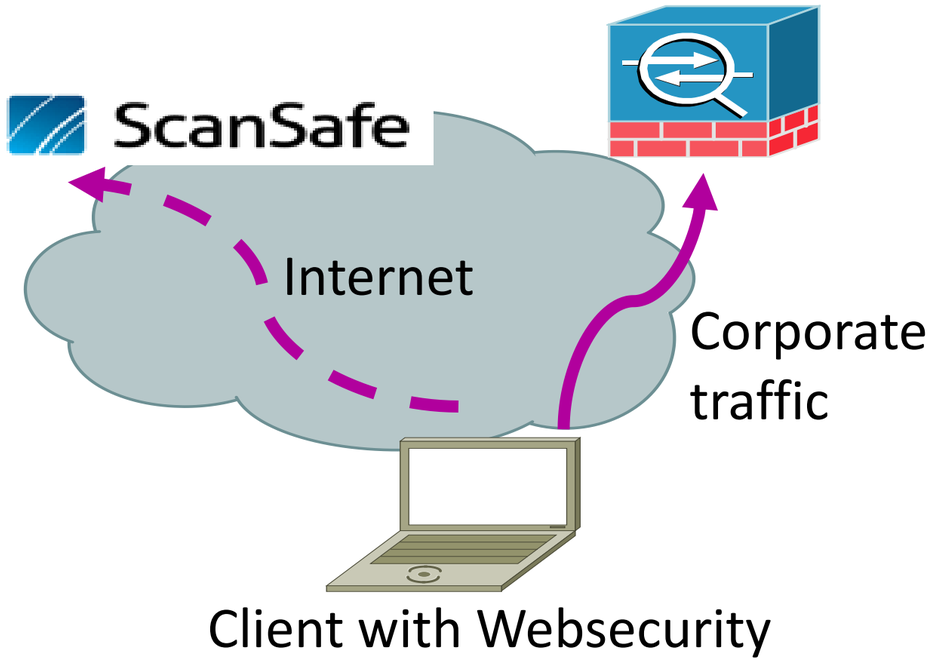
- Authenticates and directs your external client Web traffic to our scanning infrastructure
- Automatically connect to nearest Scantower
- SSL encryption of all Web traffic sent improves security over public networks (example: Firesheep Plugin for FF)



Web Security & AnyConnect

Configuration for Web Security with VPN

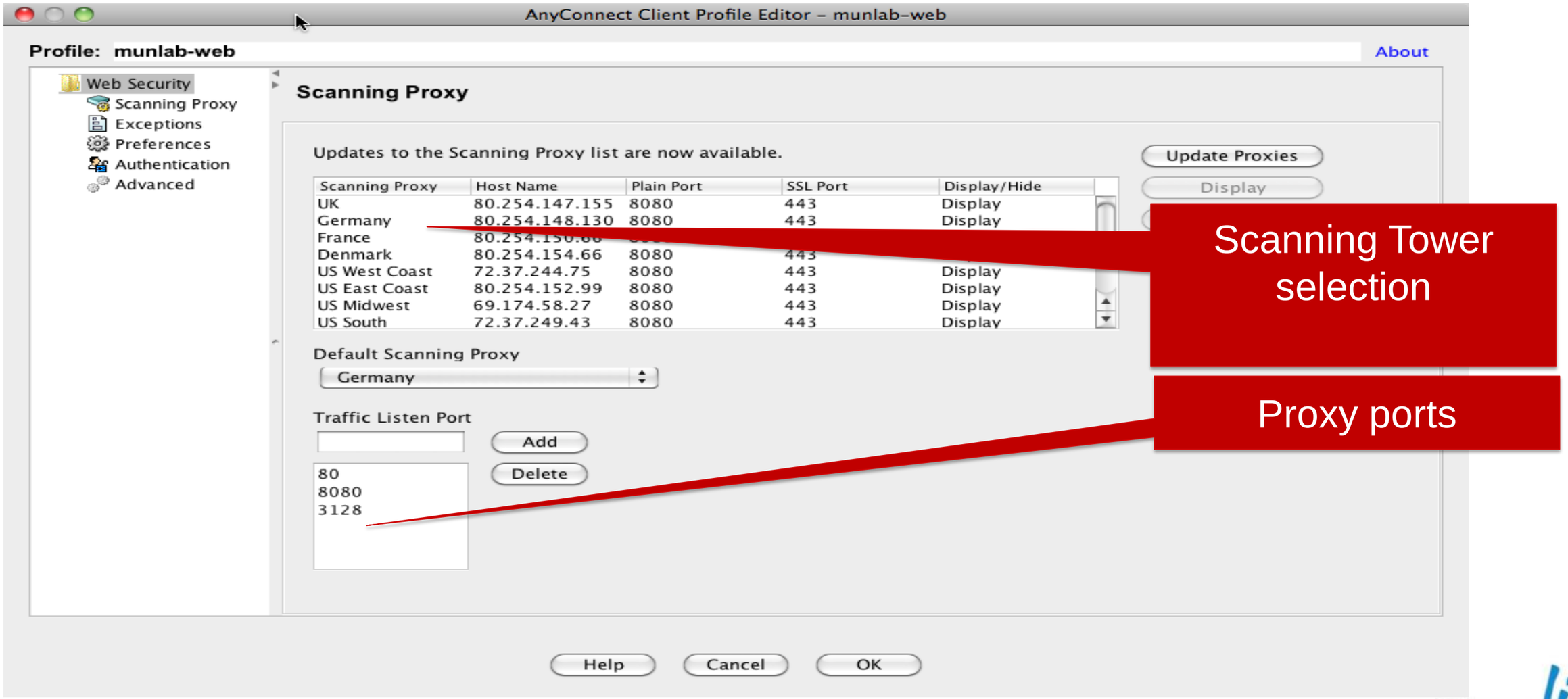
- Configured through a profile, downloaded from ASA at connect
- VPN is lower in the stack than the Websecurity Module
- Split tunnel Scansafe gateways in the VPN Config (on the ASA)
- Exclude Corporate adresses from being forwarded to the scansafe towers



AnyConnect with Web Security

AnyConnect Profile Configuration

For Your Reference

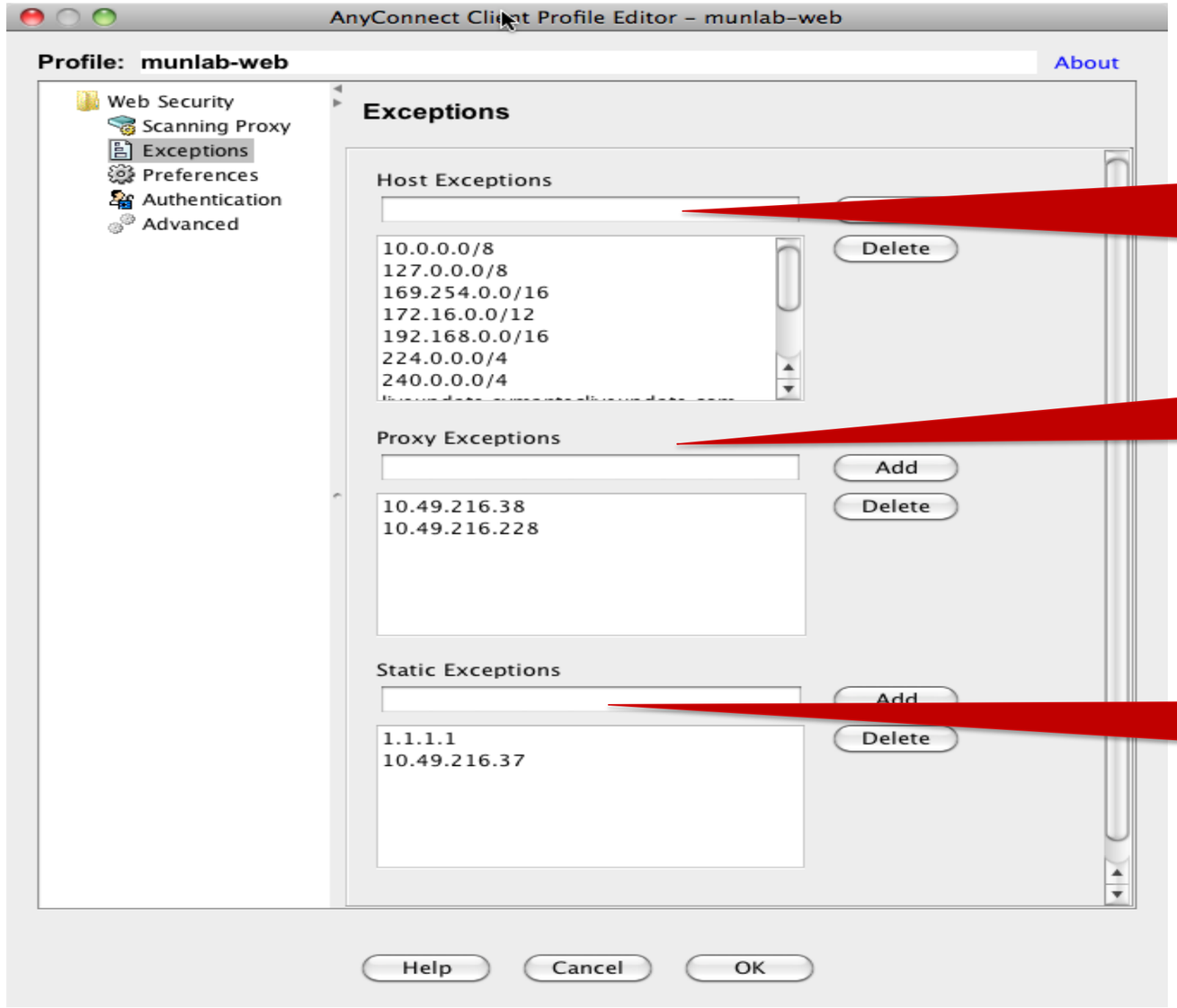


Scanning Tower selection

Proxy ports

AnyConnect Profile Configuration

For Your Reference



Exceptions for internal networks & public websites to be excluded from scanning

Exceptions for authorised internal proxies

Static Exceptions like VPN Gateways

AnyConnect Profile Configuration

For Your Reference

AnyConnect Profile Editor - Web Security

File Help

- Web Security
  - Scanning Proxy
  - Exceptions
  - Preferences
  - Authentication
  - Advanced

Preferences

Profile: Untitled

Enable Cloud-Hosted Configuration **

Automatic Scanning Proxy Selection User Controllable

Order Scanning Proxies by Response Time

Advanced Response Time Settings

Enable Test Interval: 1 hour(s) 0 minute(s)

Test Inactivity Timeout (min.) 5

Trusted Network Detection

Enable Trusted Network Detection

New Trusted Server at https://<server>[:<port>]

https:// Add

Delete

Certificate hash: Set

** change requires WebSecurity service restart

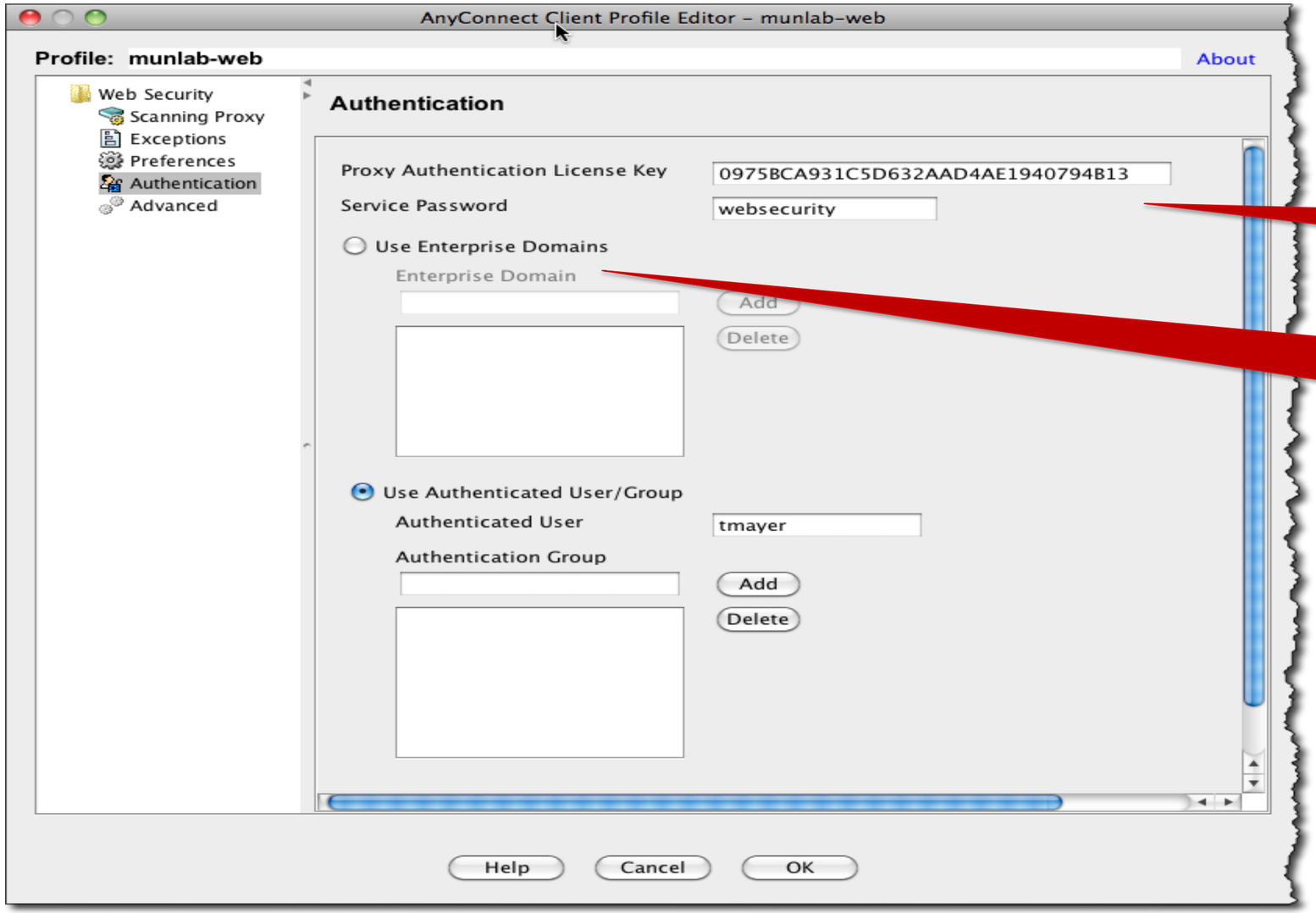
Help

Automatic selection of nearest Scantower

Trusted Network Detection

AnyConnect Profile Configuration

For Your Reference



License Key

Authentication Settings

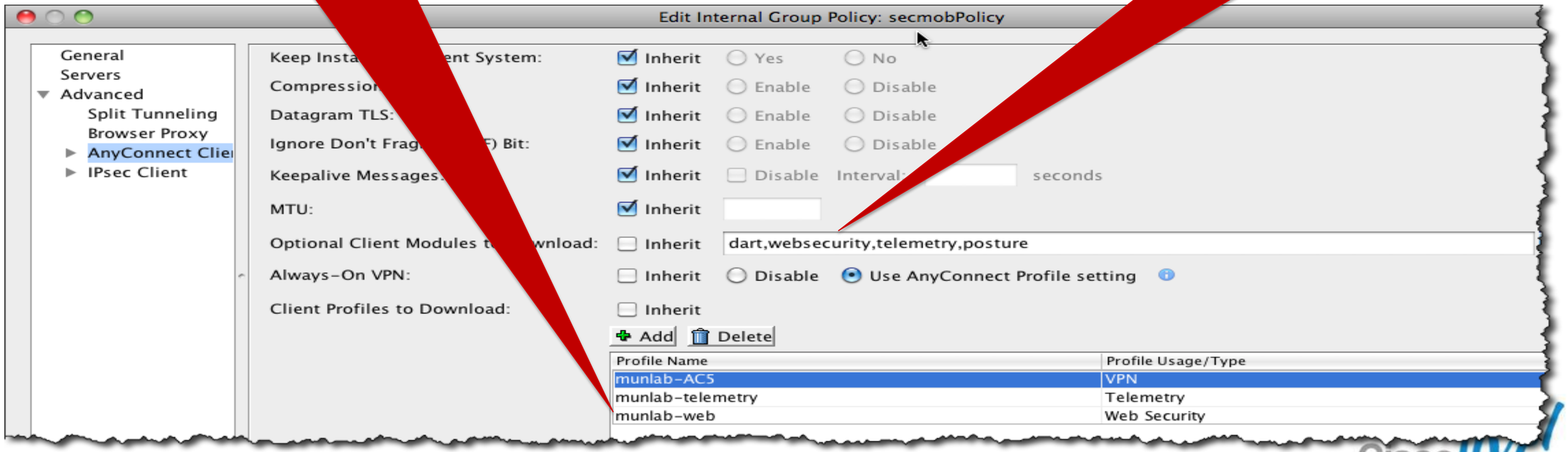
Web Security Config on ASA

using AnyConnect with VPN

For Your Reference

Assign Profile

Define Module to download

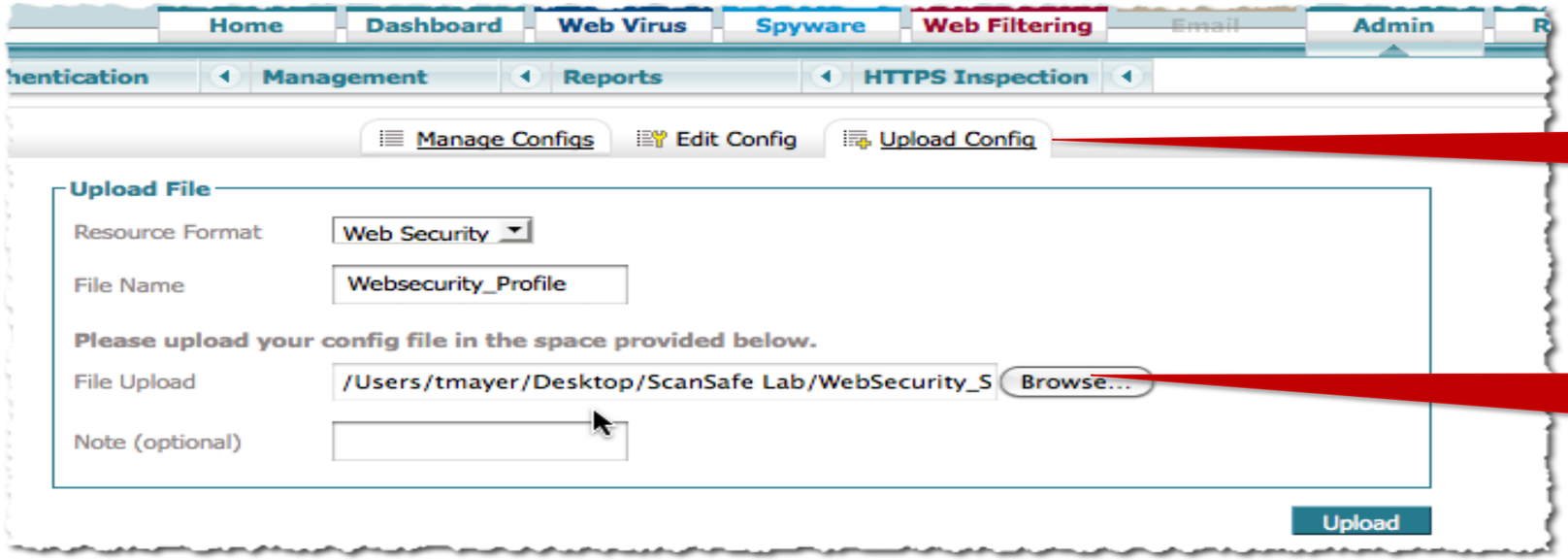


Web Security Config on Scansafe Portal

Using AnyConnect without VPN

For Your Reference

- Scancenter Portal provides hosting of PAC file and / or Client Profile
- Differentiate Usergroups due to usage of group keys



Upload Client Profile

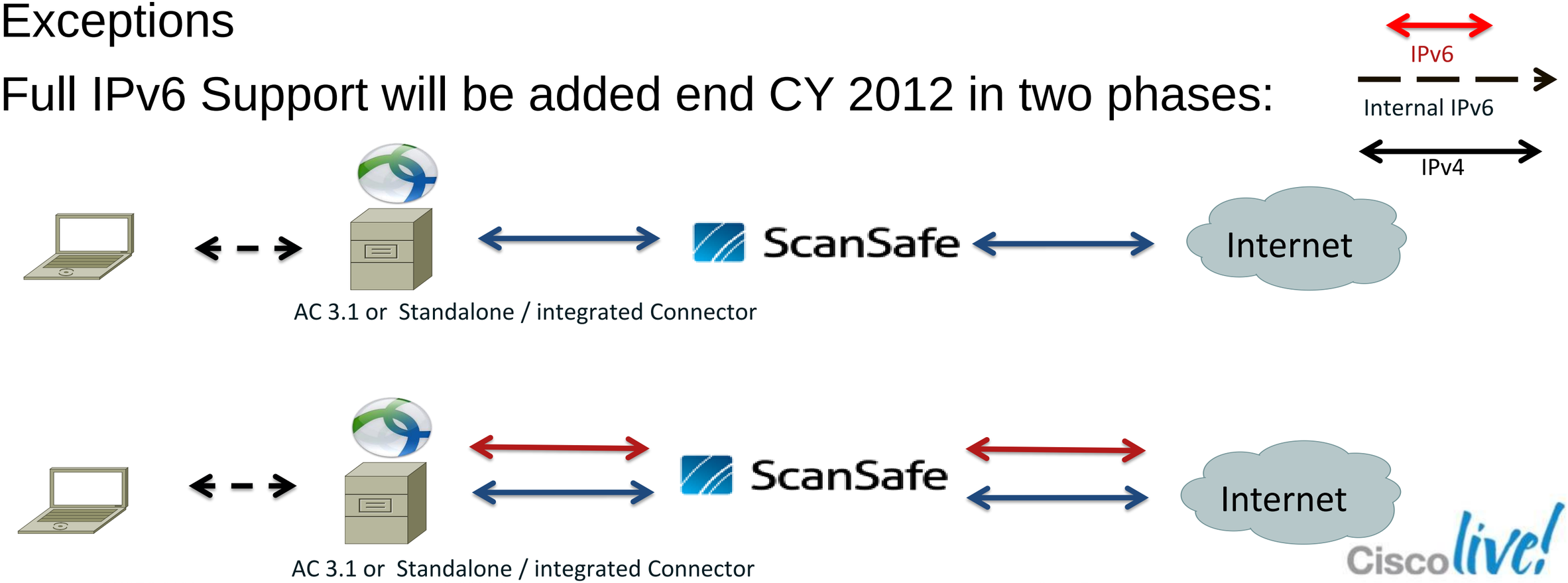
Specify Client Profile

Key for Authentication

File Name	Type	URL/Associated Key	Active	Created On	Last Modified	Note	Edit	Delete
WebsecurityProfile	Web Security	4B13 (Group)		11/26/11 11:17 AM	11/26/11 11:17 AM			

Scansafe & IPv6 Support

- Current version of ScanSafe does not yet support IPv6
- IPv6 traffic scanning can be excluded by adding “::/0” to Static Exceptions
- Full IPv6 Support will be added end CY 2012 in two phases:



Easy ID

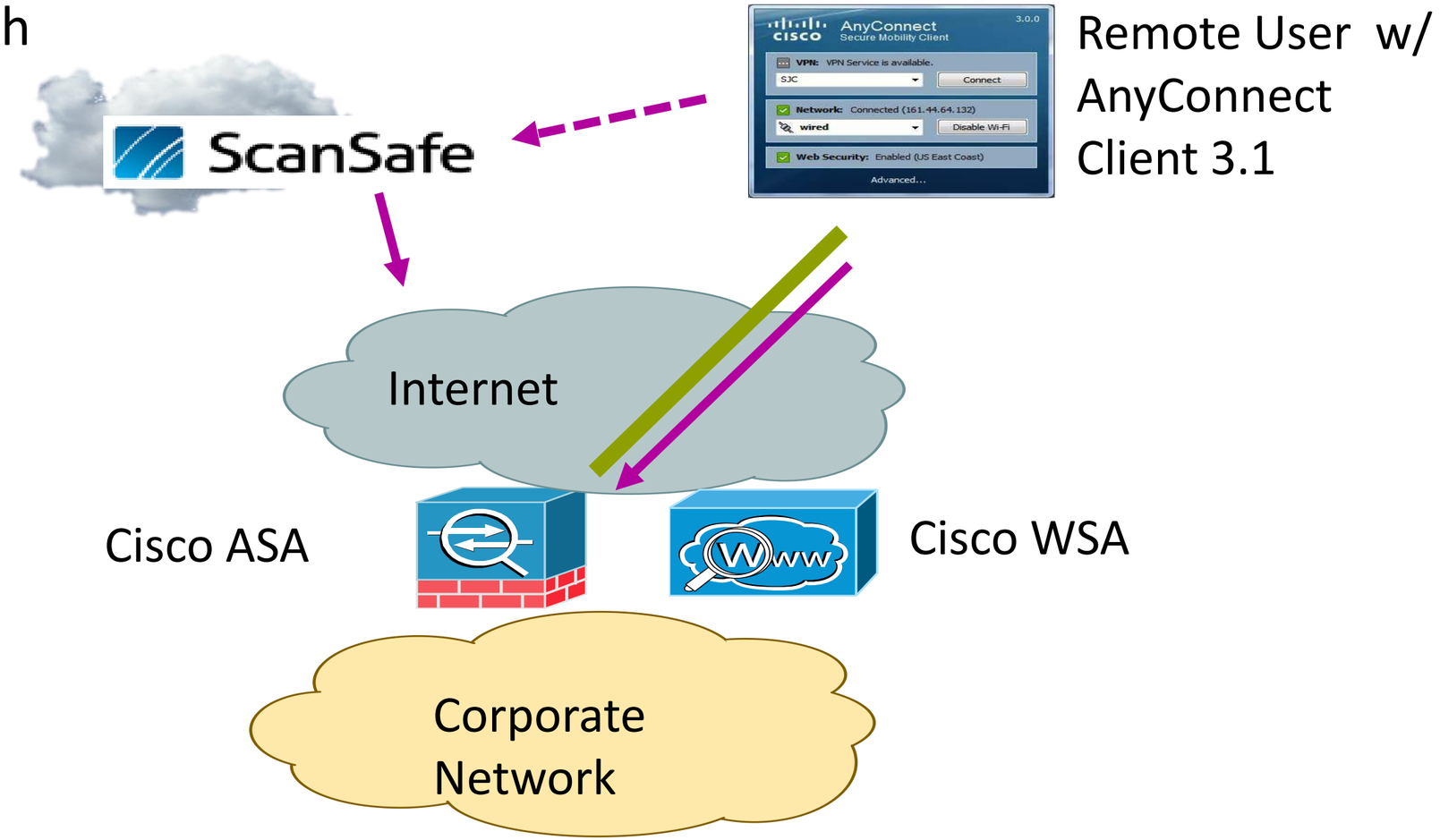
- Clientless User authentication via webbrowser
- User authenticates via Webportal
- Policies are applied from Scancenter Portal verifying User Name and Group through AD Connection
- AD Connection is done via LDAPS query from Scancenter to the LDAP Directory at customer site
- Scancenter is sending a cookie that is used for subsequent authentication

Agenda

- Web Security Overview
- Cisco Web Security Appliance (IronPort)
- Cisco Cloud Web Security (Scansafe)
- Hybrid Web Security (Appliance + Cloud)

Secure Mobility Future – Hybrid Security

- Internet traffic secure through web security cloud service
- Corporate traffic secure through tunnel and WSA
- Consistent Policy and Monitoring



Hybrid Security –

What has been done and what lies ahead

- Unification of URL Databases ✓
- Connector Integration in ISR G2 Router ✓
- Unification of features – Q1/Q2 CY2012 ✓
  - Application visibility and control ✓
- Connector Integration in ASA – ✓
- Connector Integration in WSA
- Provide common management
- Provide common logging and reporting

Hybrid Web Security:

Form Factor Choice

Corporate Office

On-Premise

IronPort WSA

ASA

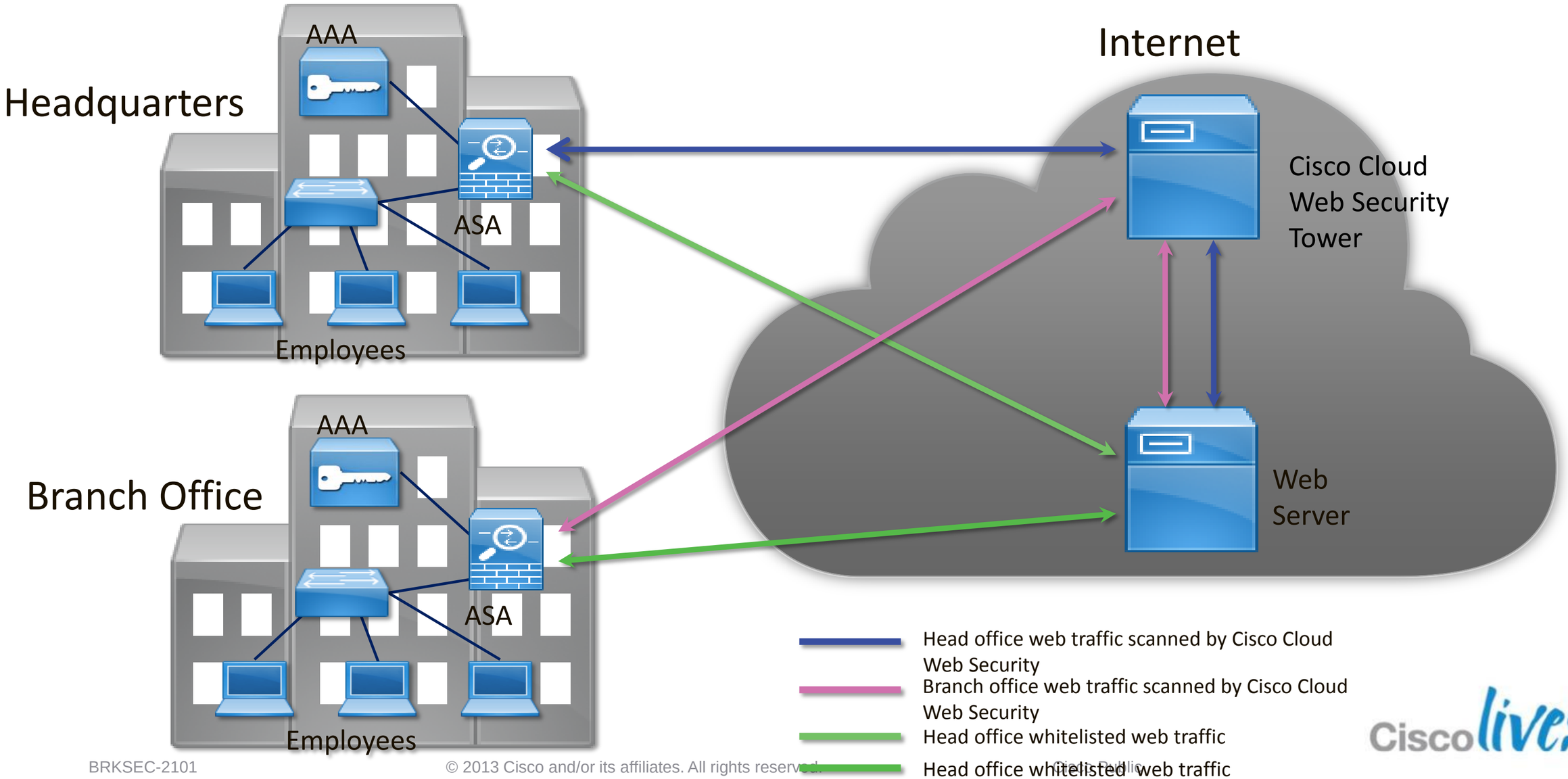
ScanSafe

Data Centre

Mobile User

ASA with integrated Connector

ASA with Cloud Web Security Integration



Configuration Parameters

- **Cisco Cloud Web Security General Options**

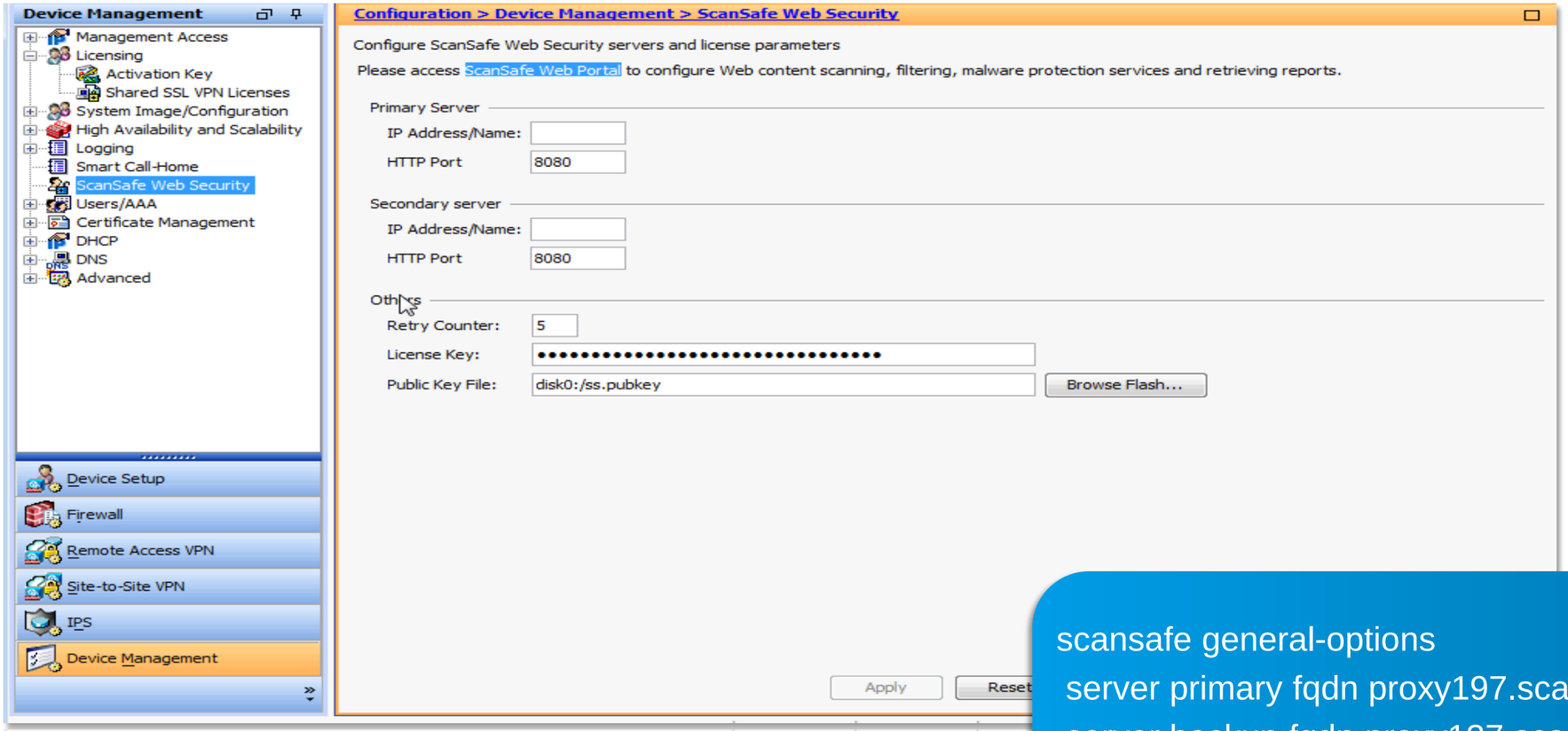
  [no] server {primary | backup} {ip <ip-address> | fqdn <fqdn>} [port <port-no>]

  [no] retry-count <2 - 100>

  [no] license <16 byte Hex key>

- **Configured in system context when the ASA is running in multiple context mode**

Configuration of Server and License




```
scansafe general-options
 server primary fqdn proxy197.scansafe.net port 8080
 server backup fqdn proxy137.scansafe.net port 8080
 retry-count 5
 license xxxxxxxxxxxxxxxxxxxxxxxxx
 publickey disk0:/ss.pubkey
```

Cloud Uplink Status and Statistics

Home | Configuration | Monitoring | Save | Refresh | Back | Forward | Help

Properties

- AAA Servers
- Device Access
- Connection Graphs
- CRL
- DNS Cache
- Failover
- Identity
- Identity by TrustSec
- ScanSafe
- IP Audit
- System Resources Graphs
- WCCP
- Connections
- Per-Process CPU Usage

Interfaces
VPN
Botnet Traffic Filter
IPS
Routing
Properties
Logging

Monitoring > Properties > ScanSafe

ScanSafe Status and Statistics

Server Status:

Server	IP Address/FQDN	Status	Active
Primary	proxy197.scansafe.net(72.37.244.115)	REACHABLE	Active
Backup	proxy137.scansafe.net	80.254.152.99	Standyby

Server Connection Statistics:

Server Connection	Value
Current HTTP sessions	0
Current HTTPS sessions	0
Total HTTP Sessions	4217
Total HTTPS Sessions	861
Total Fail HTTP sessions	0
Total Fail HTTPS sessions	0
Total Bytes In	253426068
Total Bytes Out	8439619
HTTP session Connect Latency in ms(min/max/avg)	4/59/4
HTTPS session Connect Latency in ms(min/max/avg)	4/16/4

Refresh

Last Updated: 3/13/12 7:36:41 PM

Identity Firewall Security Policy

Configuration > Firewall > Access Rules

Add | Edit | Delete | Find | Diagram | Export | Clear Hits | Show Log | Packet Trace

#	Enabled	Source Criteria: Source	User	Security Group	Destination Criteria: Destination	Security Group	Service
DMZ (3 incoming rules)							
1	✓	Engineering_Net	THREATDLABS\\Engg		DataCenter-1		ip
2	✓	Engineering_Net	THREATDLABS\\Engg		DataCenter-2		ip
3	✓	Engineering_Net	THREATDLABS\\Engg		DataCenter-3		ip
Global (21 rules)							
1	✓	any	THREATDLABS\\Mktg		any		ip
2	✓	any	THREATDLABS\\Sales		any		ip
3	✓	any	THREATDLABS\\Engg				ip

Configuration > Firewall > Identity Options

☑ Enable User Identity

Domains

Domain	AD Server Group	Disable Rules When Server Is Down
THREATDLABS	MS-AD_1	☑

Default Domain: THREATDLABS

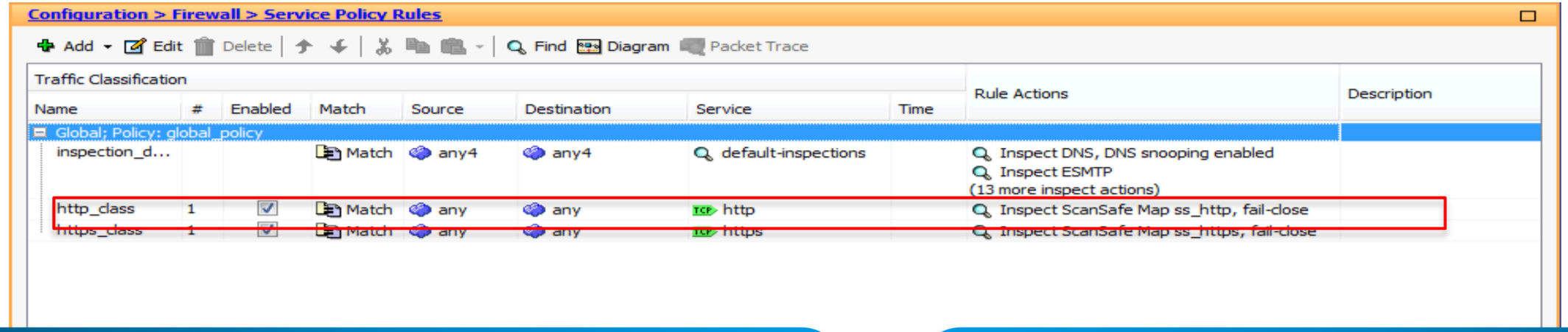
Active Directory Agent

Agent Group: MY-DC_1 | Manage... | Test

Hello Timer: 30 seconds | 5 retries

Retrieve User Information: Full Download

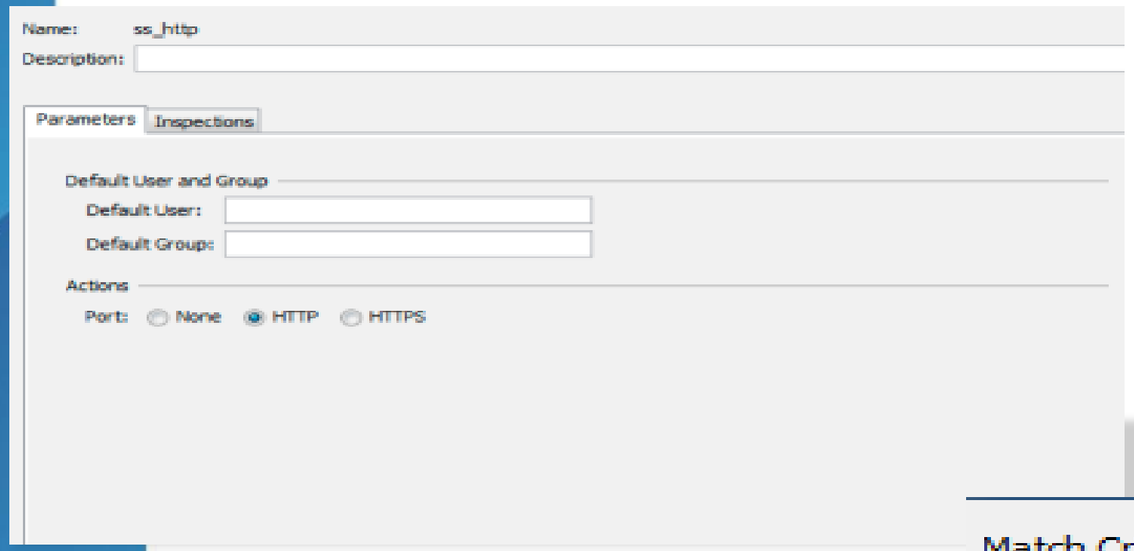
Configuration of Service Policy

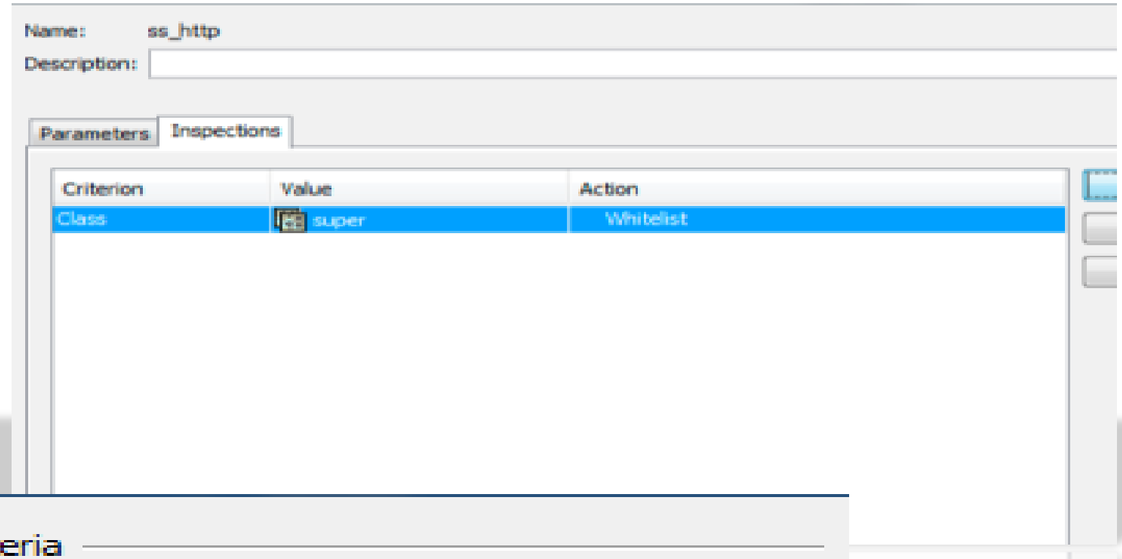


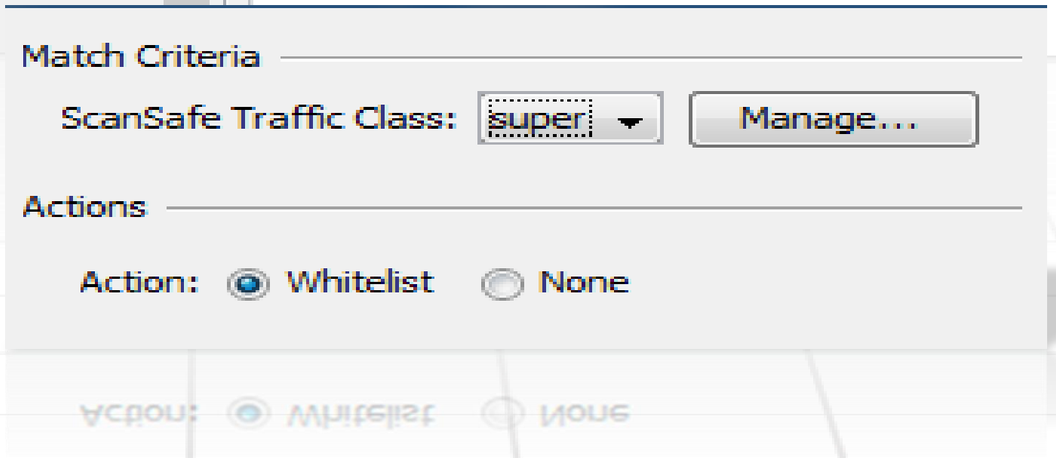

```
access-list all_http_traffic
    permit tcp any any eq www
!
class-map http_class
 match access-list all_http_traffic

class-map type inspect scansafe match-all super
 match user superuser
```

```
policy-map type inspect scansafe ss_http
 parameters
  http
 class super
  whitelist
!
policy-map global_policy
 class http_class
  inspect scansafe ss_http fail-close
!
 class https_class
  inspect scansafe ss_https fail-close
```

White Listing configuration







Security Policies Within Cisco Cloud Web Security SaaS Service

ScanCenter saib@cisco.com logged into: Cisco BN Security SE_Ku Cheng

Logout | Help | Guides | Contact Us ScanSafe

Home | Dashboard | Web Virus | Spyware | Web Filtering | Admin | Reports

Management | Notifications

Web Filtering > Management > Policy > Manage policy

Manage policy | Edit a rule | Create a rule

Rules higher in the list will take priority over the lower ones. Use the arrows to change the priority of each rule by moving them up or down in the list.

Please note that anonymization rules are treated separately from the main policy. Hence these appear in a separate part of the table. These can be ordered in the same way as the rest of the rules, and anonymization will always take precedence.

There is a maximum of 100 enabled rules allowed for the policy.

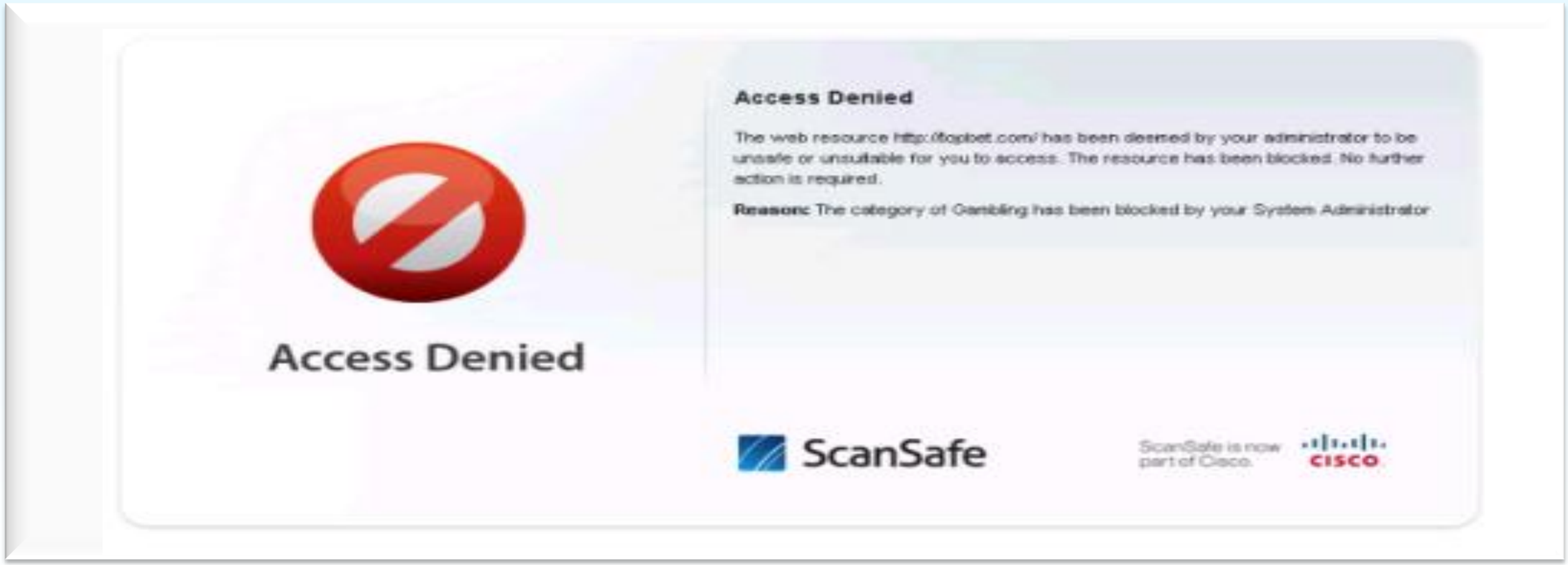
Company policy

#	Move	Rules	Groups/Users/IPs	Filter	Schedule	Action	Active	Edit	Delete
1		Facebook App Control	"THREATDLABS\Sales" or "THREATDLABS \Engg"	"Facebook Controls"	"anytime"	Block			
2		THREATDLABS_AUP_Policy	"THREATDLABS\Mktg" or "THREATDLABS\ Sales" or "THREATDLABS\Engg"	"AUP Non-Compliance URL Filter"	"anytime"	Block			
3		Default	Anyone	Anything	Anytime	Allow			

ScanSafe Inc - 950 Elm Avenue, San Bruno, CA 94066
Tel: +1 877 472 2680 - Email: support@scansafe.com

ScanSafe EMEA - Qube, 90 Whitfield Street, London W1T 4EZ, United Kingdom
Tel: +44 (0) 207 034 9400 - Fax: +44 (0) 207 034 9301 - Email: support@scansafe.com

© ScanSafe 2011 | Contact Us | Privacy Policy | Disclaimer



Summary

- Cisco Web Security Solution leverages a comprehensive architected featurelist to protect the dynamic environment from the ubiquitios web 2.0 world.....

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2013 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 8 March 12:00pm-2:00pm

Cisco live! 365

Don't forget to activate your Cisco Live 365 account for access to all session material, communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button.
www.ciscoliveaustralia.com/portal/login.ww