



Cisco Expo 2009

Deployment of Cisco IronPort Web Security Appliance



Petr Růžička, CSE

CCIE #20166

Session Abstract

Web security proxy is a must for world full of Web 2.0 threats.

Focus of our session will be placement of Web Security Appliance (WSA) in the network, real world deployment scenarios, tips and tricks related to authentication of users, load balancing and scalability.

We would provide many answers to typical “how” and “why”. We assume knowledge of networking and basics of security concepts.

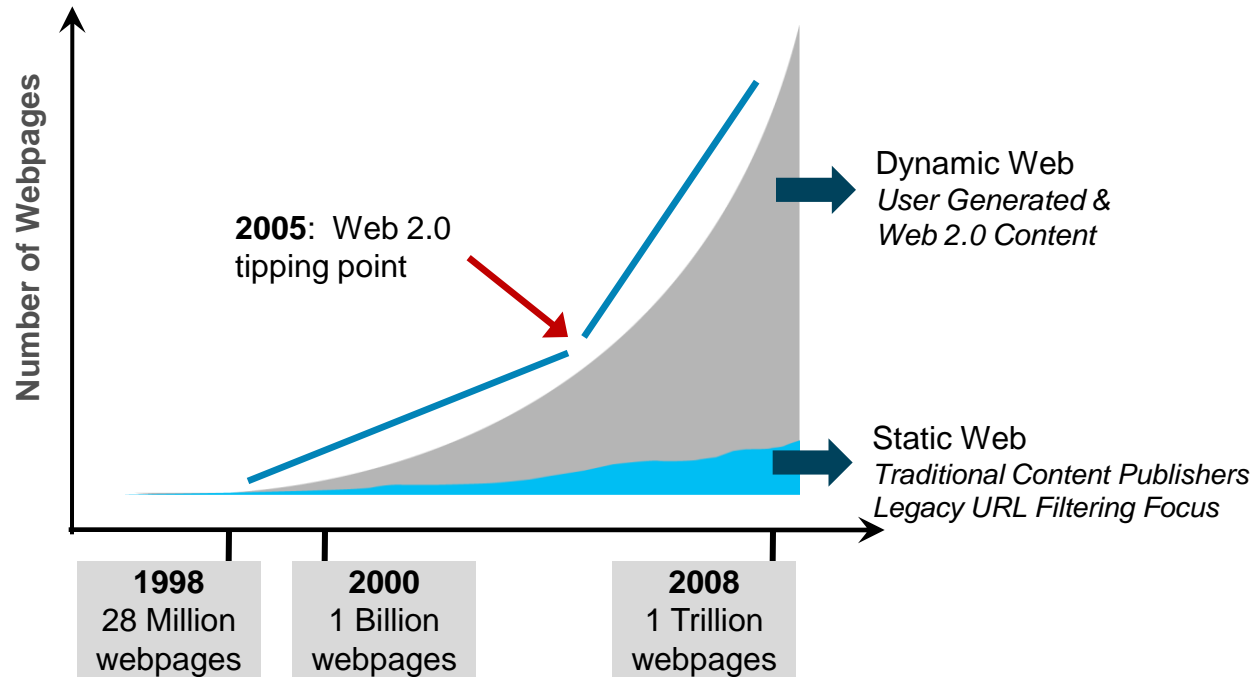
Agenda

1. Why
2. Testing
3. Deployment Options
4. Web Usage Controls
5. Q & A

Why



Web: Huge, Growing and Transient



Huge

1 Trillion
unique URLs

Growing

1 Billion
new pages added
every day

Transient

30%
domain-level churn
every year

Traditional Firewall

1. ACL for L3/L4 filtering

```
access-list inside permit udp DNS any eq 53
```

```
access-list inside permit tcp LAN any eq 80
```

```
access-list inside permit tcp LAN any eq 443
```



Page Sample

Home Page | Today's Paper | Video | Most Popular | Times Topics | Most Recent | Try Times Reader 2.0 | Log In | Register Now

BETTER TOGETHER
NOVEMBER 2-4 ONLINE ONLY
Neiman Marcus Click for details ▶

The New York Times

Tuesday, November 3, 2009 Last Update: 9:48 AM ET

BETTER TOGETHER
NOVEMBER 2-4 ONLINE ONLY
Neiman Marcus Click for details ▶

Switch to the [Global Edition](#) for an international perspective on news, business, sports and more.

Try Our **EXTRA** Home Page | Try Times Reader 2.0 | Personalize Your Weather

Search 

Switch to [Global Edition](#) ▶

JOB
REAL ESTATE
AUTOS
ALL CLASSIFIEDS

WORLD
U.S.
POLITICS
N.Y./REGION
BUSINESS
TECHNOLOGY
SPORTS
SCIENCE
HEALTH
OPINION
ARTS
Books
Movies
Music
Television
Theater
STYLE

3 Contests on Election Day Could Signal Political Winds

By ADAM NAGOURNEY

In this supposedly quiet off-year election, what to look for Tuesday as results come in from New Jersey, New York and Virginia.

- [Interactive: Who's Who on Tuesday's Ballot](#)
- [The Caucus: Races to Watch Across the Nation](#)
- [New York Mayoral Race Focuses on Economy at End](#)
- [Suburbs Key in New Jersey](#)



Moises Saman for The New York Times

A Vow to Fight Corruption, but No Details

By ALISSA J. RUBIN and HELENE COOPER 7:59 AM ET

President Hamid Karzai of Afghanistan, in his first speech since he was declared the winner of a disputed election, made no specific commitments for tackling corruption.

- [Video \(Reuters\) | Room for Debate: U.S. and the Karzai Brothers](#)

OPINION »
HAPPY DAYS
Happy Ending
This series's last essay of 2009 discusses how death makes us take life seriously.



- [Herbert: Glimpse of the Future?](#) | [Comments \(51\)](#)
- [Brooks: Texts and Lovers](#)
- [Cohen: Hinge of History](#)
- [Editorial: Karzai](#)
- [Op-Ed: Buying New York](#)
- [Op-Ed: Job Machines](#)

SCIENCE TIMES »
How Mean Can Office Gossip Be?
A study at an elementary school found the insults subtle and the conversations unpredictable.



- [Post a Comment](#)

MARKETS » [10:08 AM ET](#)

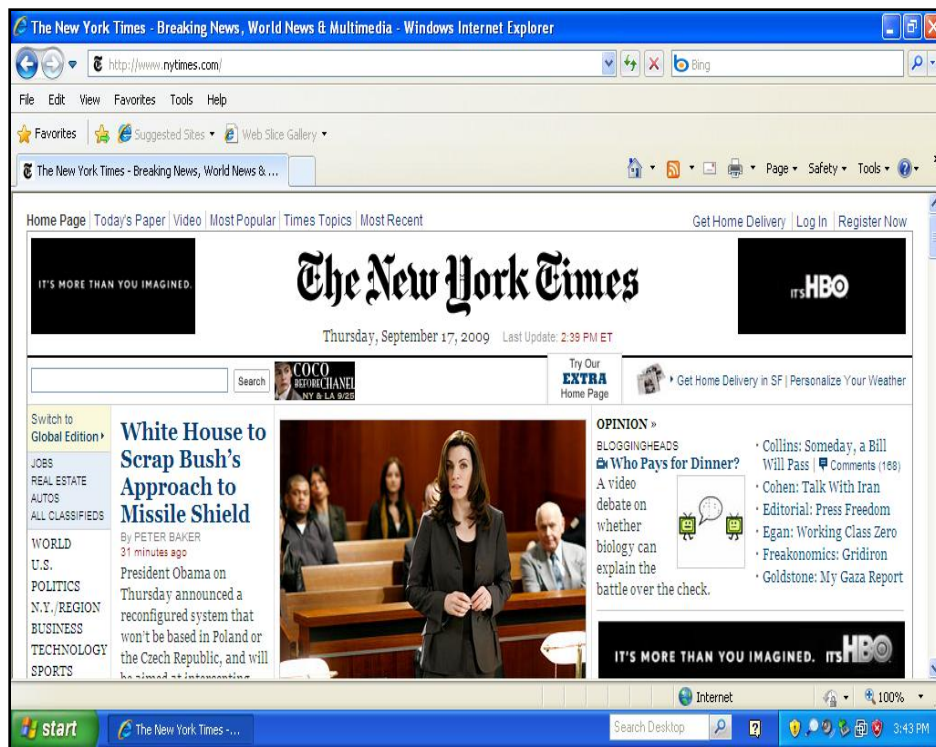
S.&P. 500	Dow	Nasdaq
1,042.43	9,771.31	2,045.26
-0.45	-17.53	-3.94
-0.04%	-0.18%	-0.19%

[GET QUOTES](#) | [My Portfolios](#) ▶



- 8 HTMLs
- 23 CSS
- 33 JS
- 56 images
- 3 Flash
- 11 cookies
- 123 GETs

The New York Times: *Victim of an advertiser attack!*



1. **Seemingly legitimate** ad changed after NYT accepted it
2. **3 malicious redirections** before malware reaches user
3. **Ultimate destination:** protection-check07.com

America's Newspaper of Record

Testing





TESTING

I FIND YOUR LACK OF TESTS DISTURBING.

What we are after ?

1. We are interested in requests per seconds
2. Secondary in throughput
3. Features of course are important

Following performance details are
really **VERY ROUGH** estimates.

Suggested Positioning

S660



10,000 – 30,000 users

S360



1000 – 10,000 users

S160



0 – 1000 users

Why ?

1. User's browsing habits could be very different
2. Traffic profile could be different
3. Configuration and activated features could differ a lot
4. Some traffic could be denied

HTTP Performance

Requests/second & Throughput

- Key metric: Requests/second or Transactions/second
- The larger the object size, the higher the throughput
 - Throughput (Mbps) = Object size (bytes) × Request rate (req/s)



Throughput gets big...



...as object size gets bigger...



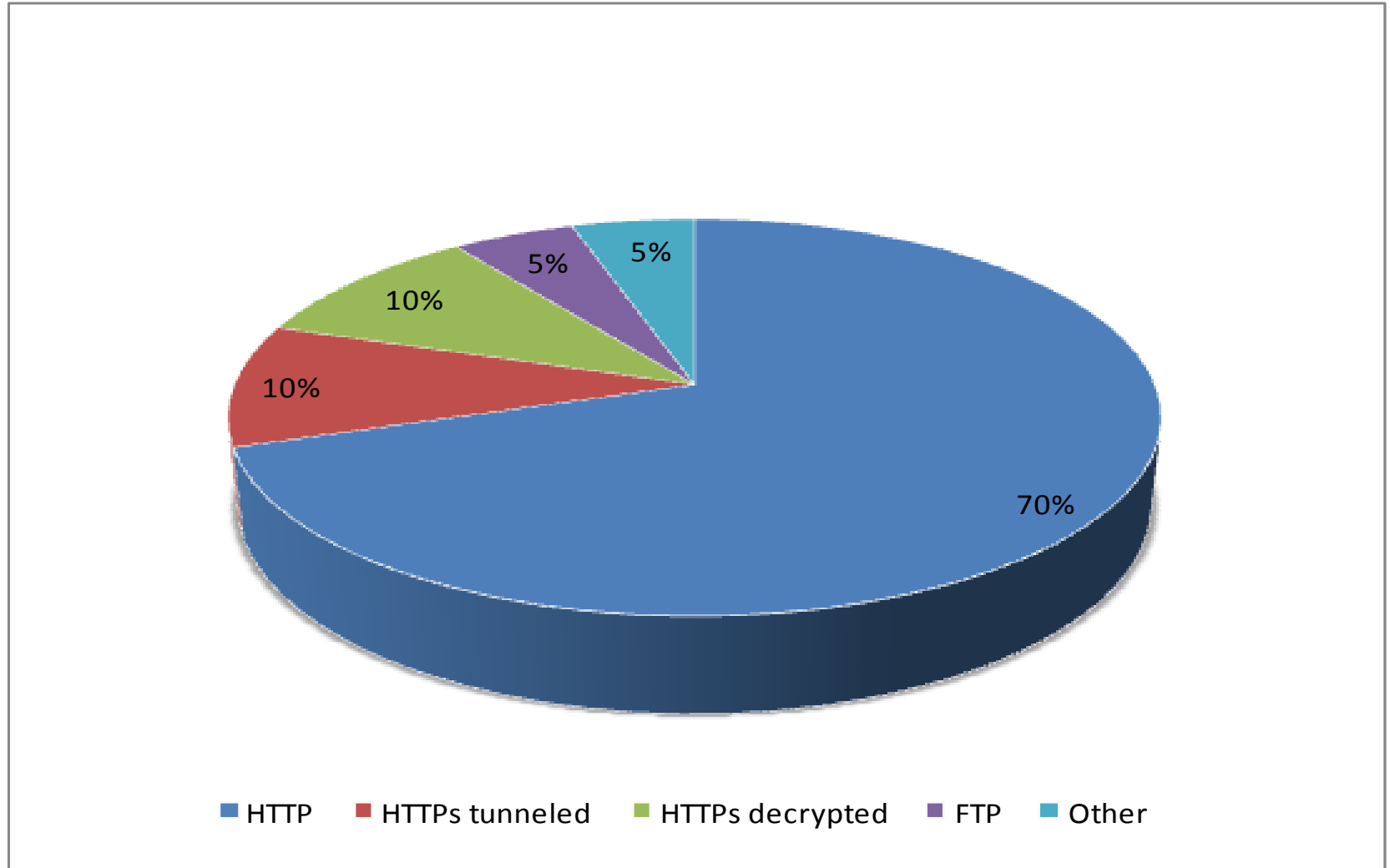
... even if the request rate stays constantly low.

Mbit/sec = Transactions Per Second (TPS) x Average HTTP object size (bytes) x bits in a byte (8) bits x in a megabit (1,000,000)

Rules of thumb:

- Each Request/second is approx. 80-90 Kbps of HTTP traffic
- Each Mbps of HTTP traffic translates to ~10 requests/second
- 100 Mbps of sustained HTTP traffic translates to ~1000 requests/second

Typical Traffic Profile



Performance testing

1. Nothing beats real life traffic
2. Almost any tool that is used to test HTTP servers could be used here
3. Have a bunch of powerful servers ready
4. Test features relevant to your deployment
Antimalware, HTTPs decryption, IP Spoofing...



Tools One Could Use

1. Wget

```
wget -l 3 -r --proxy=on --delete-after
```

```
http://guide.opendns.com/s?service=web&q=music&search\_type=guide
```

```
wget --proxy=on --delete-after -i list_of_sites.txt
```

2. Httpperf

```
http://sourceforge.net/projects/httpperf/
```

3. Curl-loader

```
http://curl-loader.sourceforge.net/
```

4. Pylot

```
http://www.pylot.org/
```

5. Siege

```
http://www.joedog.org/index/siege-home
```

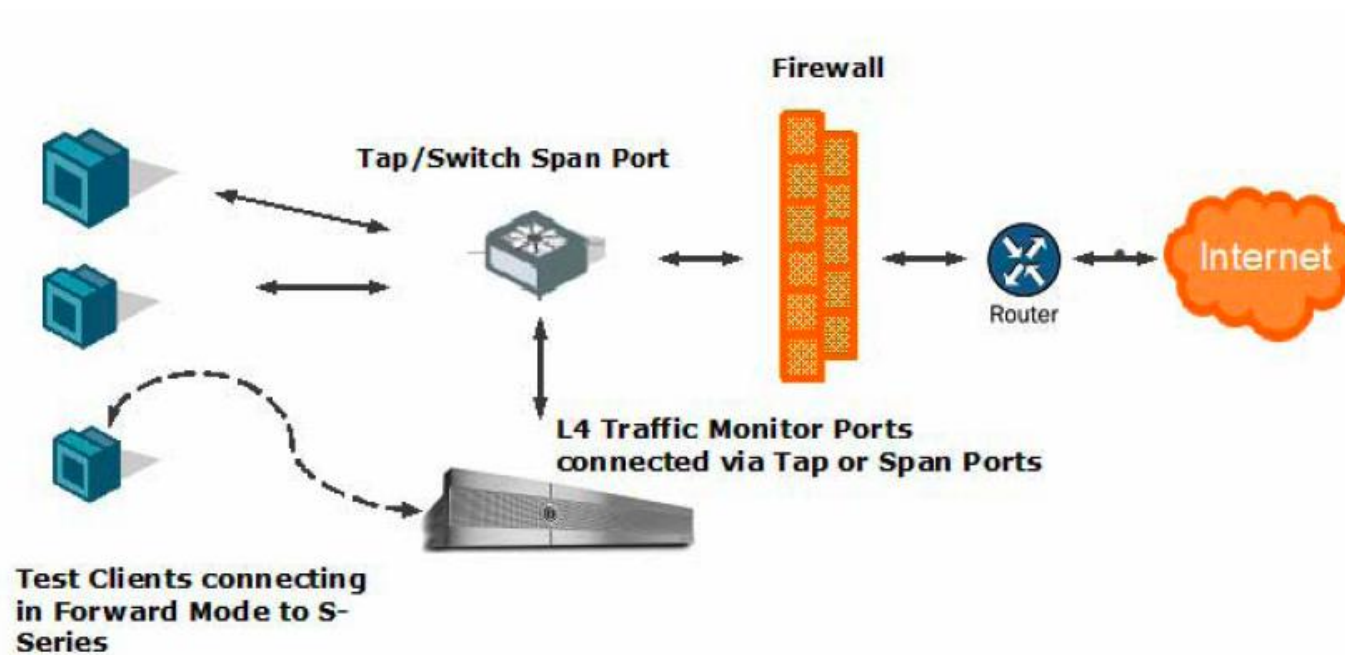
6. Virus site of your choice :o)

Deployment



Web proxy modes

1. Explicit forward mode
Use for evaluation
2. Transparent mode
3. Multiple upstream proxies mode



Proxy Selection Method

1. Deployment of Explicit Forward Proxy uniformly on many clients (Manual)

Avoid Configuration at the Desktop

Failover and/or Load Balancing

Performance

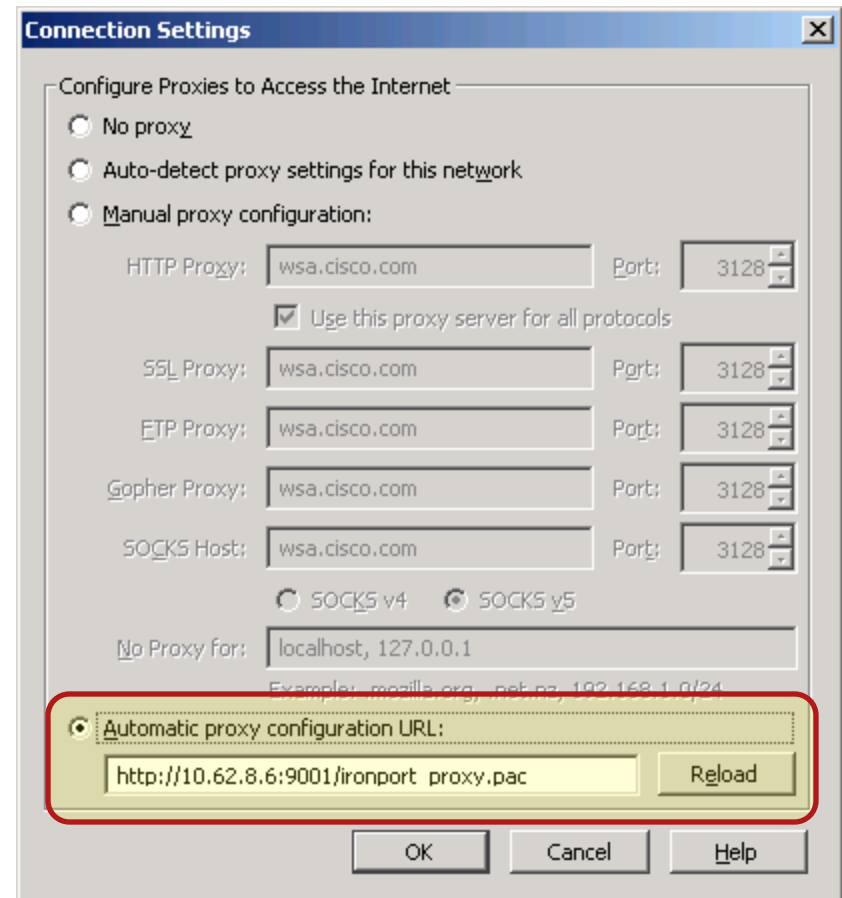
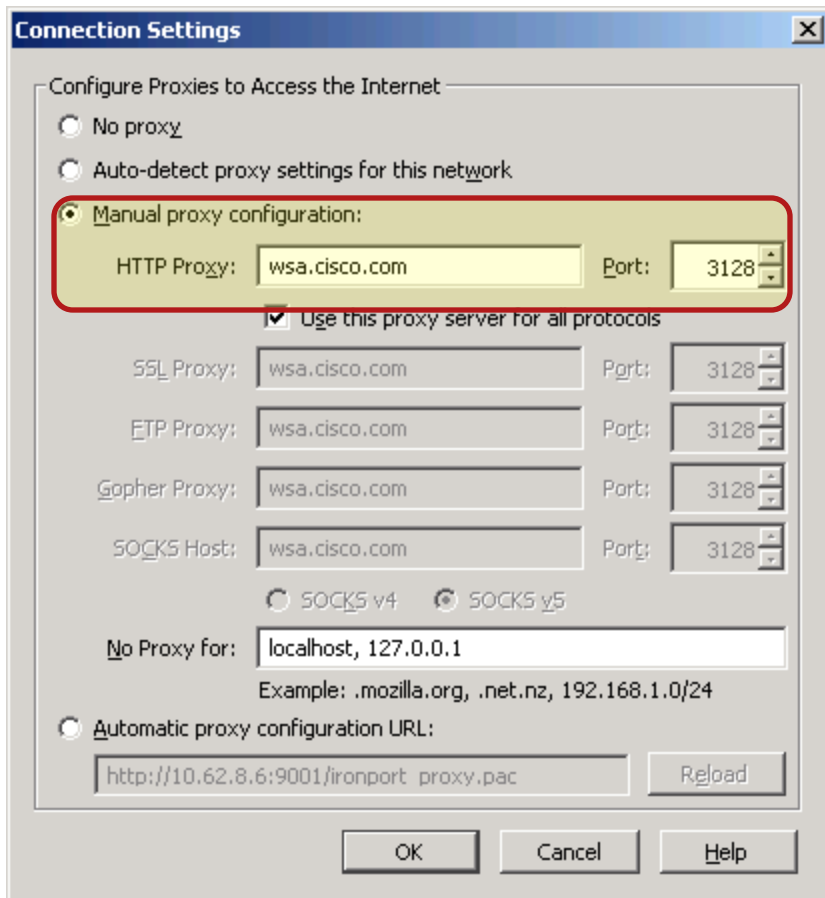
2. PAC file hosting

Locally on the desktop, on the server, or on the S-Series

3. WPAD

Explicit forward mode

1. Manual
2. PAC File



Creating the PAC file

1. Based on JavaScript

Main function “FindProxyForURL(url, host)”

12 PAC functions with return: DIRECT or PROXY

2. Different browsers behavior

PAC file location

IE limitations

3. Google PAC tester

Test your PAC file if working properly

<http://code.google.com/p/pactester/>

4. PAC file example

Creating the PAC file

```
function FindProxyForURL(url, host) {  
  // If IP address is internal or hostname resolves to internal IP, send direct.  
  var resolved_ip = dnsResolve(host);  
  if (isInNet(resolved_ip, "10.0.0.0", "255.0.0.0") ||  
      isInNet(resolved_ip, "172.16.0.0", "255.240.0.0") ||  
      isInNet(resolved_ip, "192.168.0.0", "255.255.0.0") ||  
      isInNet(resolved_ip, "127.0.0.0", "255.255.255.0"))  
    return "DIRECT";  
  // Use a different proxy for each protocol.  
  if (shExpMatch(url, "http:*")) return "PROXY proxy1.domain.com:3128";  
  if (shExpMatch(url, "https:*")) return "PROXY proxy2.domain.com:3128";  
  if (shExpMatch(url, "ftp:*")) return "PROXY proxy3.domain.com:3128";  
  // If I'm not in corporate network, send direct  
  if (!isInNet(myIpAddress(), "144.254.0.0", "255.255.0.0"))  
    { return "DIRECT"; }  
  // URL based load balancing  
  function FindProxyForURL(url, host) {switch(URLHash(url)%2){  
    case 1: return "PROXY proxy1.domain.com:3128";  
    default: return "PROXY proxy2.domain.com:3128";}}  
  function URLHash(url) {server_name=url.split("/")[2]  
    if(!server_name) {return url.length;}return server_name.length;}  
  // All other traffic uses below proxies, in fail-over order.  
  return "PROXY 1.2.3.4:8080; PROXY 4.5.6.7:8080; DIRECT";  
}
```


WPAD Web Proxy Autodiscovery Protocol (WPAD)

1. Using DHCP

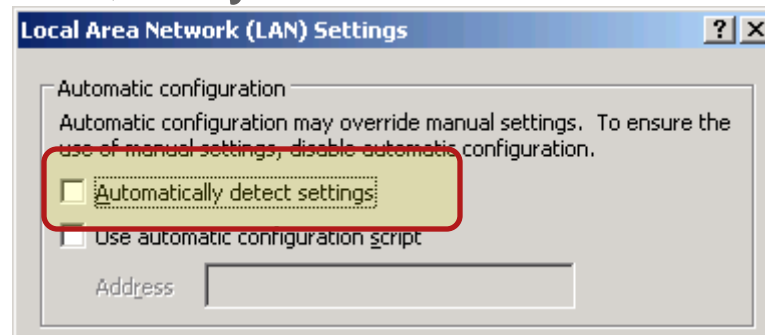
- Specification of PAC's URLfile using DHCP
- In DHCP environment uses option 252 "auto-proxy-config"
- **Be aware of security when in use**

2. Using DNS via A or CNAME

host wpad

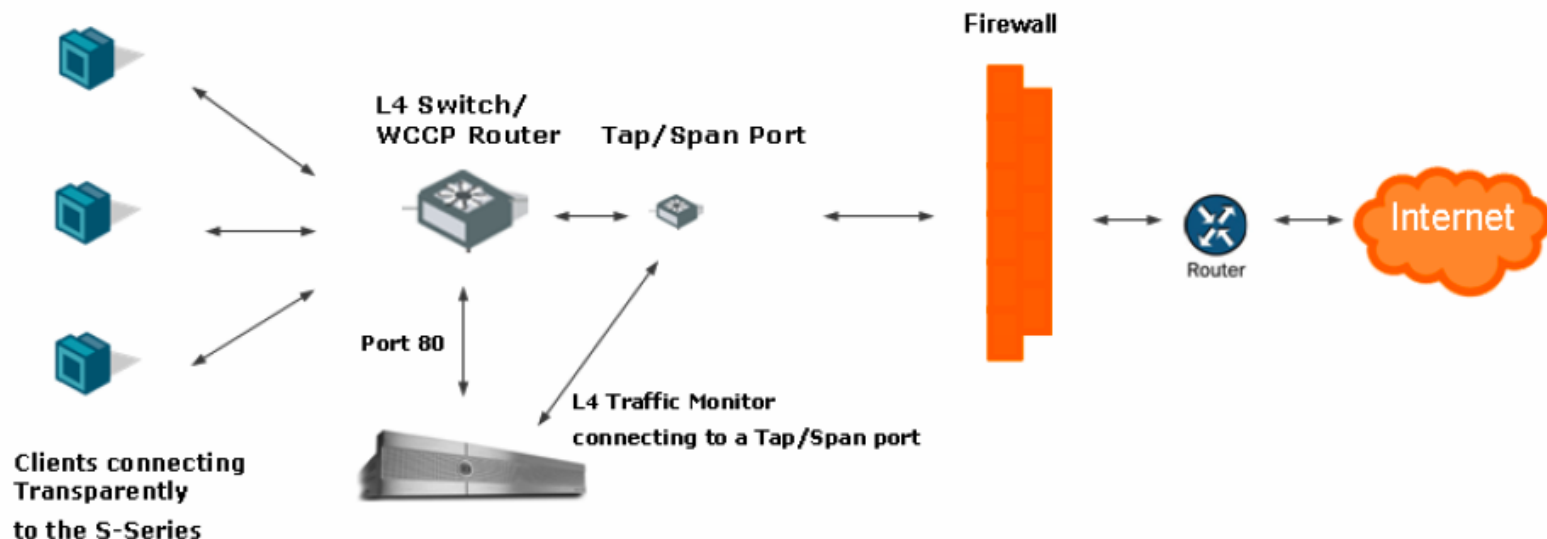
PAC file should be then located on <http://wpad.<domain>/wpad.dat>

3. FF doesn't support DHCP option, only DNS



Transparent Mode

1. User (browser, process...) doesn't know it's traffic is being proxied
2. Could be challenging sometimes, let's say while having needs to authenticate users
3. Nothing needs to be done on users desktops



Transparent Proxy deployment

1. Configure transparent redirection

PBR – L4 Switch, simple usage

WCCP – WCCPv2 router, more complex, but more flexible

2. Configure the return method

Layer 2 or GRE

3. Configure IP Spoofing or X-Forwarded-For Headers

When upstream proxies requires to identify the client

Via Headers

IP Spoofing in Forward mode

4. Configure Transparent Bypass List

To exclude any special HTTP application servers or clients

WCCP

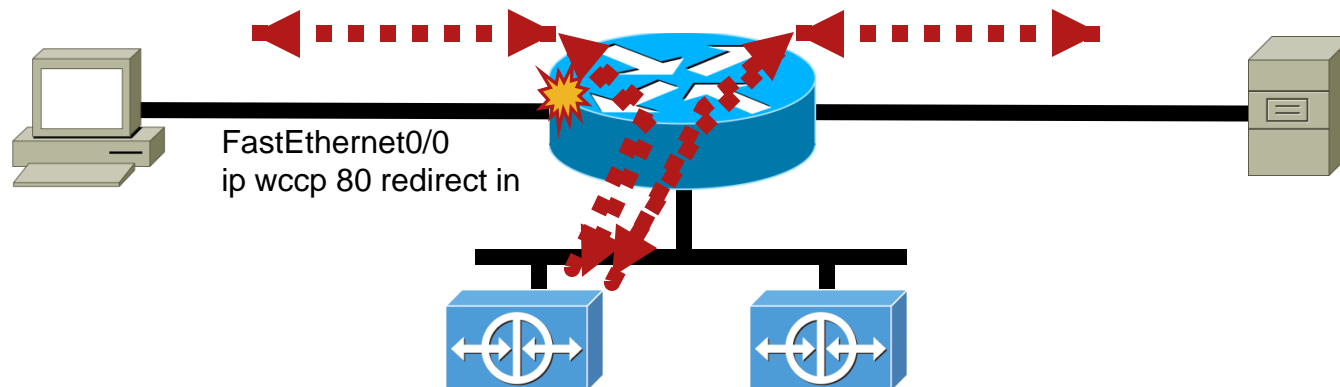
1. Identify traffic

Ingress redirection (preferred)

Egress redirection

2. WSA failure results in redistribution of load to remaining WSAs in 30 sec

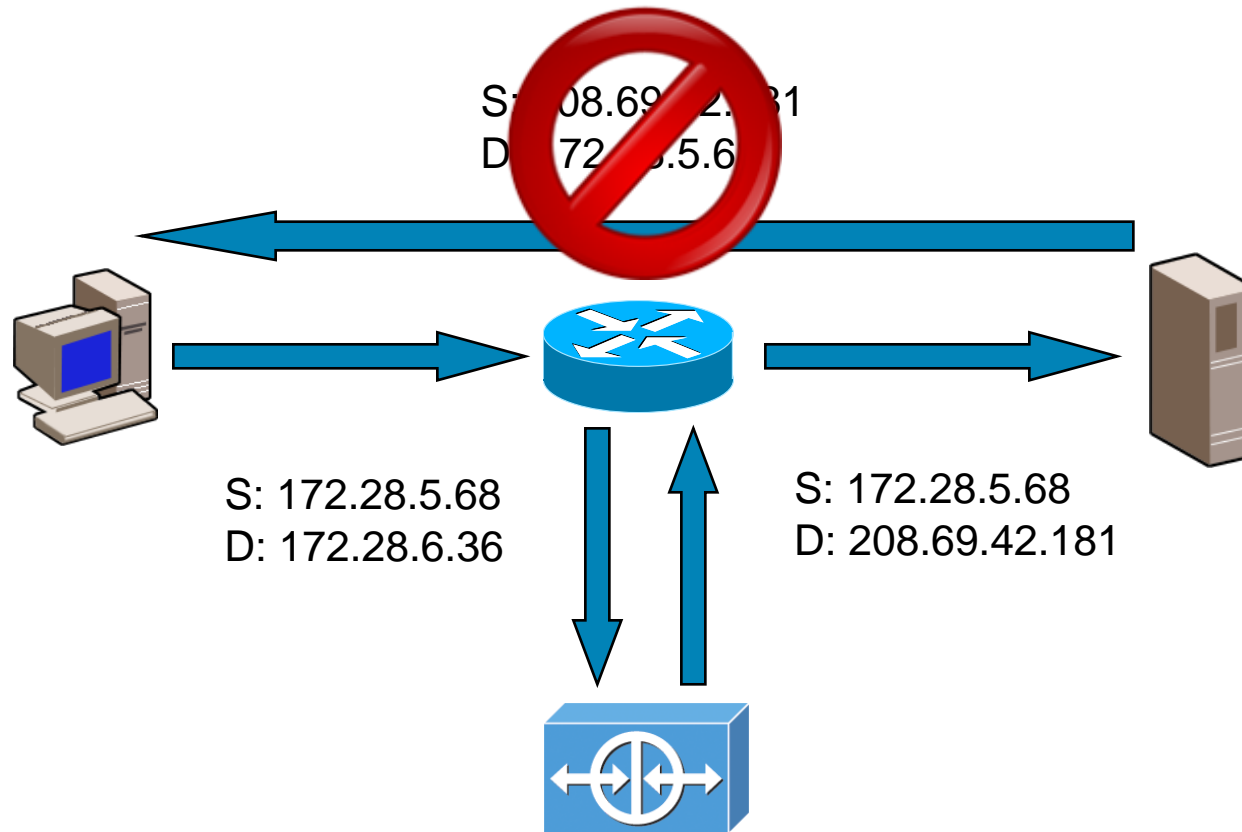
3. If no remaining WSA's service group is taken offline and packets are not redirected (fail-open)



IP Spoofing Explained

1. Using proxy means connection to server would come from proxy address
2. Sometimes we need to identify client/subnet after proxy (think firewall, QoS, NAT, malicious requests detection)
3. Using spoofing we could, well, spoof 😊 source IP address
4. We would use original (clients) IP address

IP Spoofing in Forward Mode



Without redirection, the packets go straight back to the client!

Headers for Identification

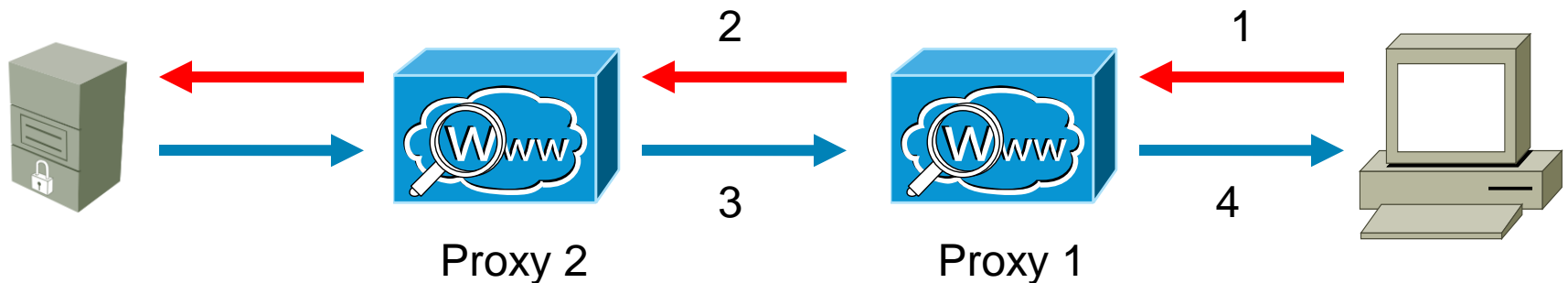
1. XFF (not sent by default)

X-Forwarded-For: client1, proxy1, proxy2

2. Via (sent by default)

Used for identification of gateway or proxy server

VIA: http protocol-version, host



From Client & To Client (request, answer)

Follow TCP Stream

Stream Content

```
GET http://www.cisco.com/ HTTP/1.1
Host: www.cisco.com
User-Agent: Mozilla/5.0 (windows; U; windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3
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
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Proxy-Connection: keep-alive

HTTP/1.1 200 OK
Date: Sat, 07 Nov 2009 13:52:06 GMT
Server: Apache/2.2
Last-Modified: Fri, 06 Nov 2009 03:55:03 GMT
ETag: "59d4"
Accept-Ranges: bytes
CDCHOST: cdcxweb-prod1-02
Content-Type: text/html
Set-Cookie: CP_GUTC=144.254.252.68.1257601926808328; path=/; expires=wed, 01-Nov-34 13:52:06 GMT; domain=.cisco.com
Content-Length: 22996
Via: 1.1 Application and Content Networking System Software 5.5.13, 1.1 s650.prglab.cisco.com:80 (IronPort-WSA/6.3.0-604)
Connection: keep-alive
Proxy-Connection: keep-alive
X-Junk: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<!-- $Revision: 1.17 $ -->
<html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en">
<head>
```

1

4

Find Save As Print Entire conversation (30020 bytes) ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close

From Proxy & To Proxy (request, answer)

The screenshot shows a 'Follow TCP Stream' window with the following content:

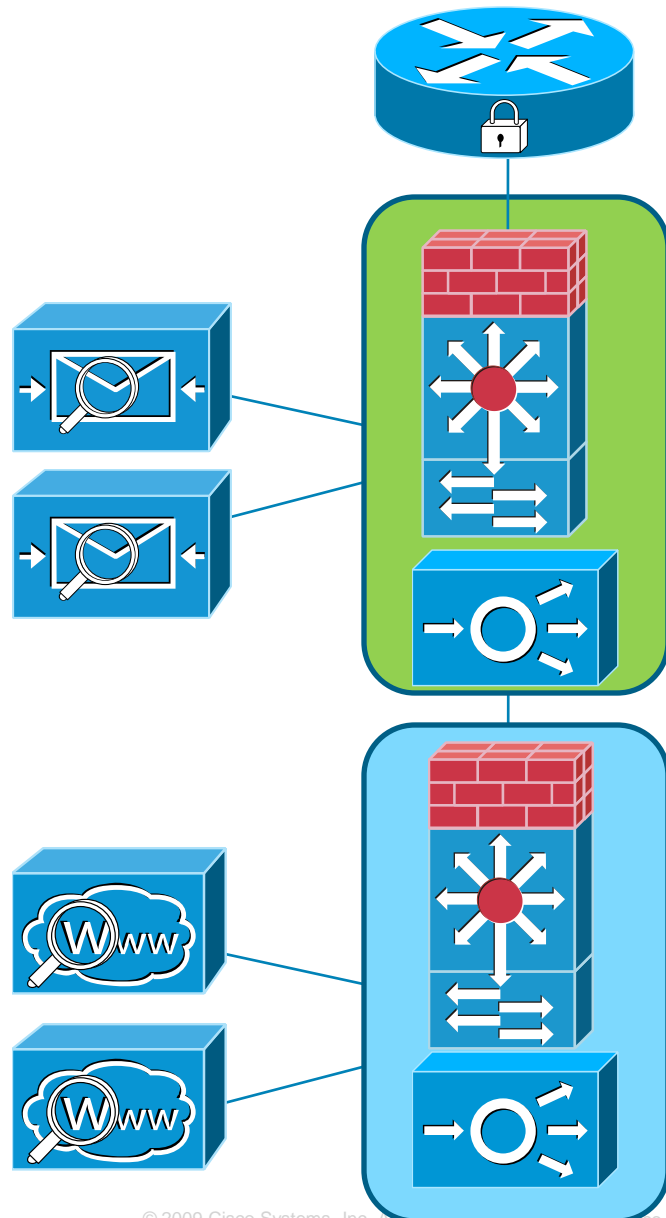
```
Stream Content
GET http://www.cisco.com/ HTTP/1.1
Connection: keep-alive
User-Agent: Mozilla/5.0 (windows; U; windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Host: www.cisco.com
X-IMForwards: 20
Via: 1.1 s650.prglab.cisco.com:80 (IronPort-WSA/6.3.0-604)
X-Forwarded-For: 10.21.107.164

HTTP/1.1 200 OK
Date: Sat, 07 Nov 2009 13:52:06 GMT
Server: Apache/2.2
Last-Modified: Fri, 06 Nov 2009 03:55:03 GMT
ETag: "59d4"
Accept-Ranges: bytes
Content-Length: 22996
CDCHOST: cdCxweb-prod1-02
Content-Type: text/html
Set-Cookie: CP_GUTC=144.254.252.68.1257601926808328; path=/; expires=wed, 01-Nov-34 13:52:06 GMT;
domain=cisco.com
Via: 1.1 Application and Content Networking System Software 5.5.13
Connection: Close

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-
transitional.dtd">
<!-- $Revision: 1.17 $ -->
<html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en">
<head>
  <title>Cisco systems, Inc</title>
  <meta http-equiv="Content-type" content="text/html; charset=UTF-8"/><meta name="doctype">
```

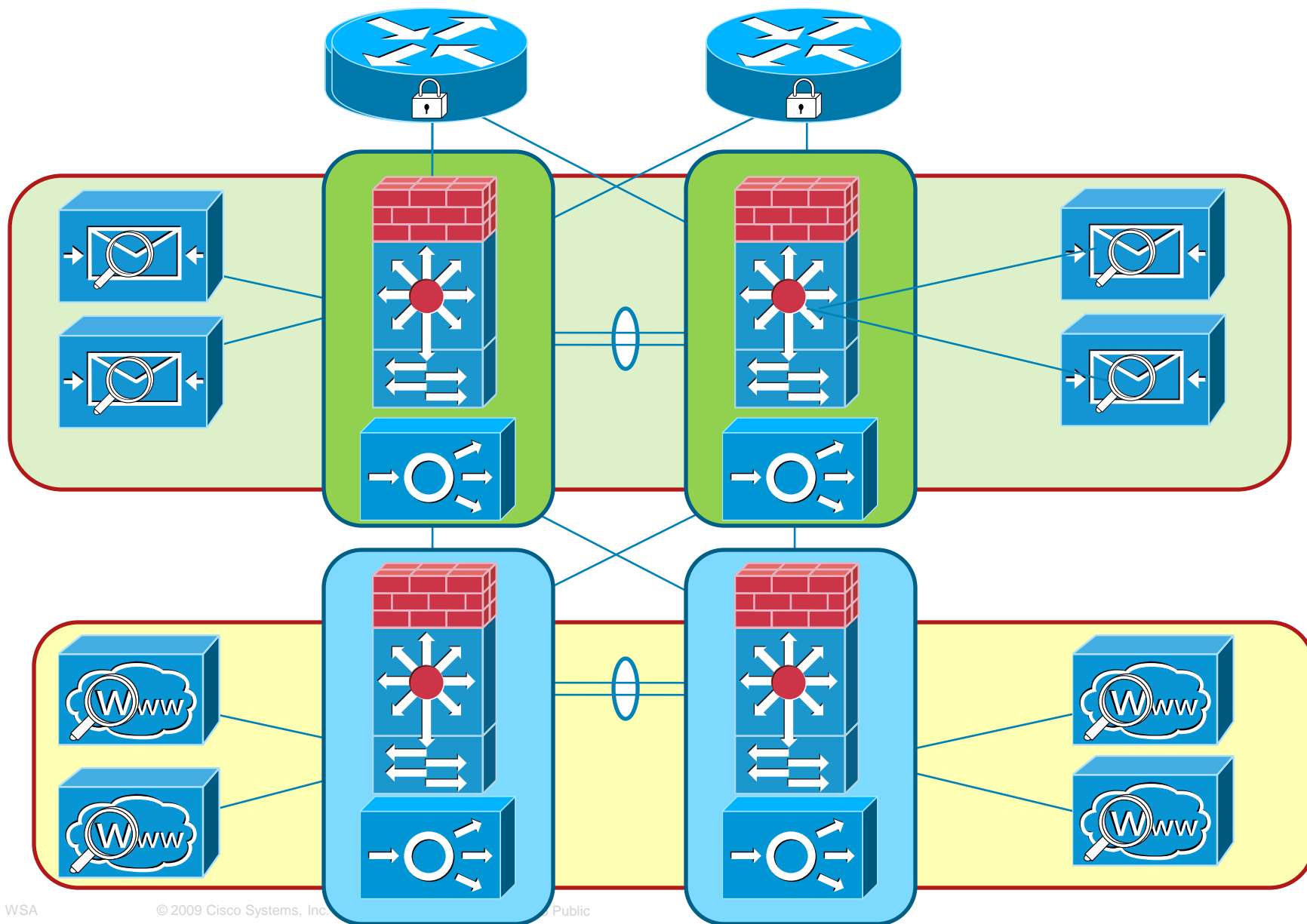
The request lines (from 'Via: 1.1 s650.prglab.cisco.com:80' to 'X-Forwarded-For: 10.21.107.164') are highlighted in yellow and labeled with a large black '2'. The response lines (from 'Via: 1.1 Application and Content Networking System Software 5.5.13' to 'Connection: Close') are highlighted in yellow and labeled with a large black '3'. The status bar at the bottom shows 'Entire conversation (23913 bytes)' and 'Raw' is selected.

ACE Loadbalancing Example



1. Using VIP (virtual IP address) for WSA cluster
2. ACE would provide HA and loadbalancing for both ESA and WSA
3. Could (and does) work for both transparent and explicit deployment
4. Using “IP Spoofing” gives us a option to identify traffic later in “green zone”

ACE Loadbalancing Bigger Picture



Cisco Web Usage Controls



Customer Problem

**The Categorized
Web**

20% covered by URL lists

The Dark Web

*80% of the web is uncategorized,
highly dynamic or unreachable*

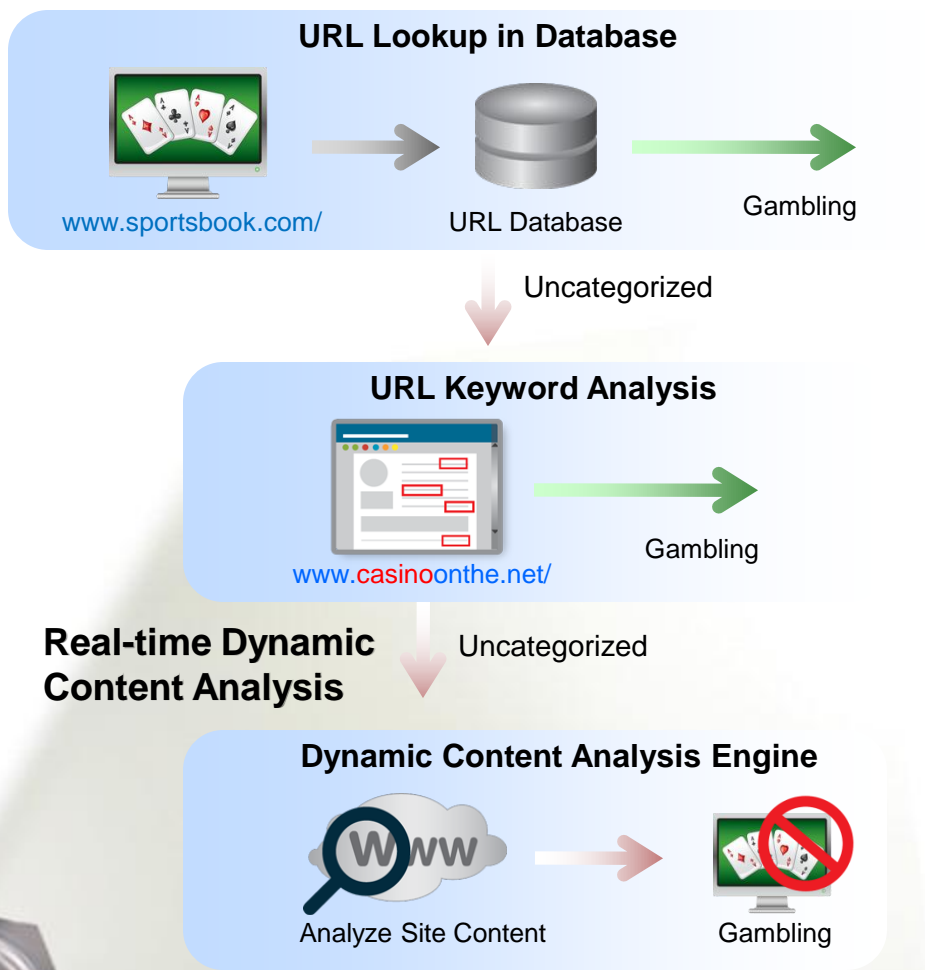
- Dynamic content*
- Password protected sites*
- User generated content*
- Short life sites*

The Categorized Web

20% covered by URL lists

Introducing Cisco IronPort Web Usage Controls

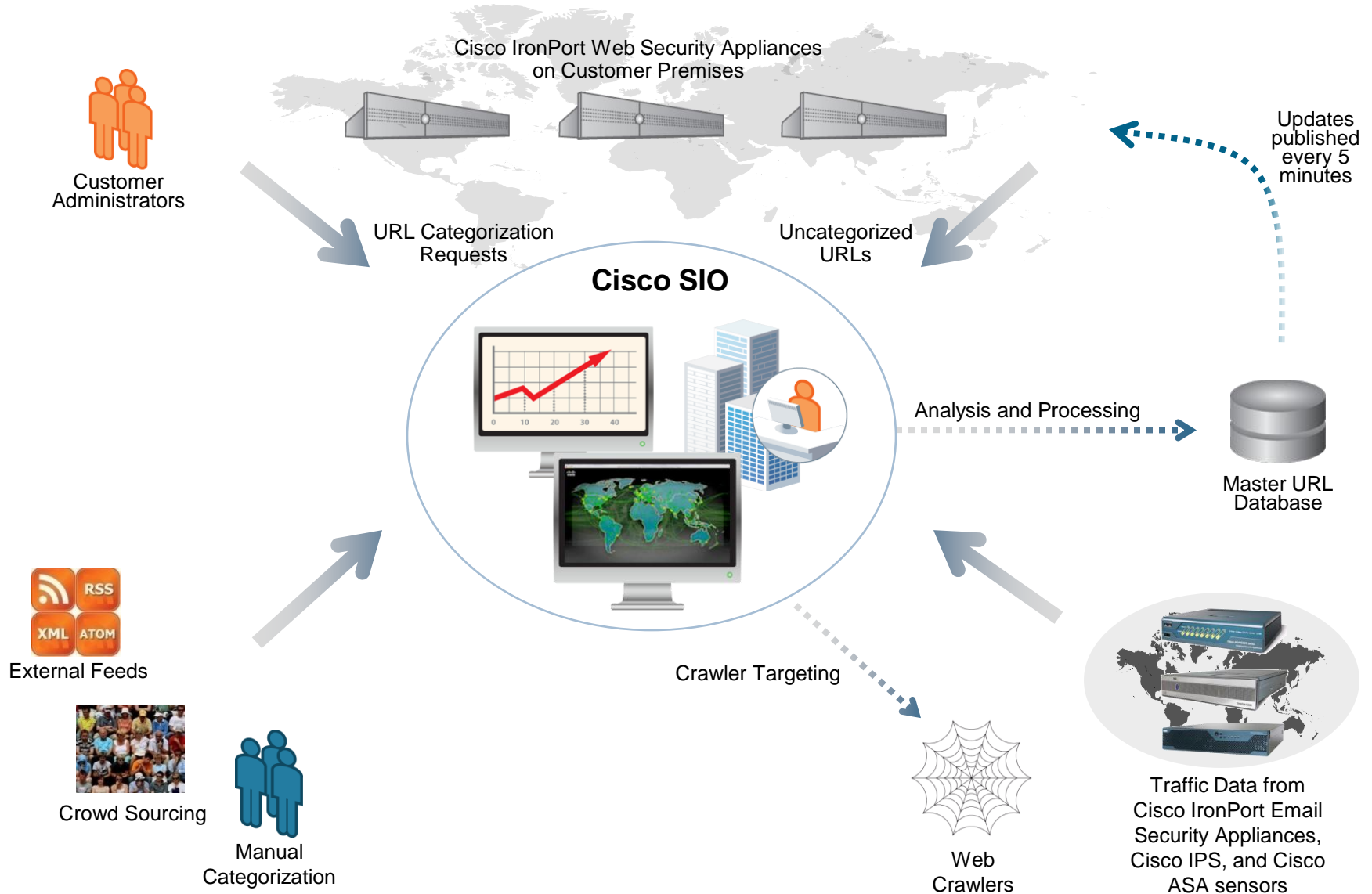
A Spotlight for the Dark Web



1. Industry-leading URL database efficacy
 - 65 categories
 - Updated every 5 minutes
 - Powered by Cisco SIO
2. Real-time Dynamic Content Analysis Engine accurately identifies over 90% of Dark Web content in commonly blocked categories

Cisco Security Intelligence Operations (SIO)

Unmatched Visibility Drives Unparalleled Efficacy



Agenda

1. Why
2. Testing
3. Deployment Options
4. Web Usage Controls
5. Q & A



Registrujte se za Cisco Networkers

25-28. januar 2010. Barsekona
28-31. mart 2010. Bahrein





CISCO