

v7.5 Jump Start Part 3: Filtering with the V-Series proxy

Webinar December 2010



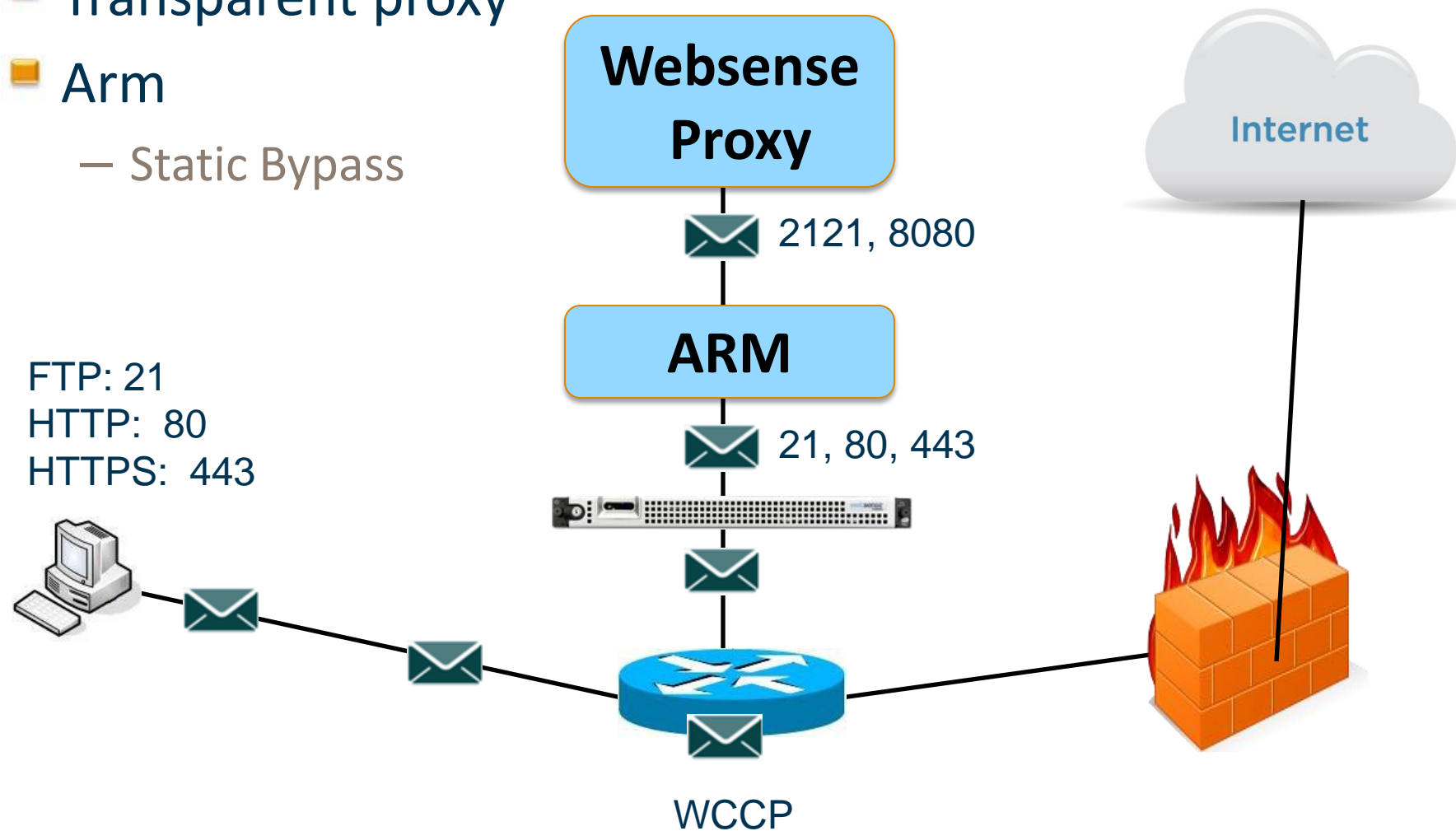
Greg Didier

- **Title:** Support Specialist
- **Accomplishments:**
 - 7 years supporting Websense products
- **Qualifications:**
 - Technical Support Mentor
 - Product Trainer

- How packets reach the Content Gateway proxy
 - Explicit proxy
 - Transparent Proxy
 - Adaptive Redirection module (ARM)
- Scanning
 - Analytic engines
 - Bypass and exceptions
- Common proxy dilemmas
- Best practice tips

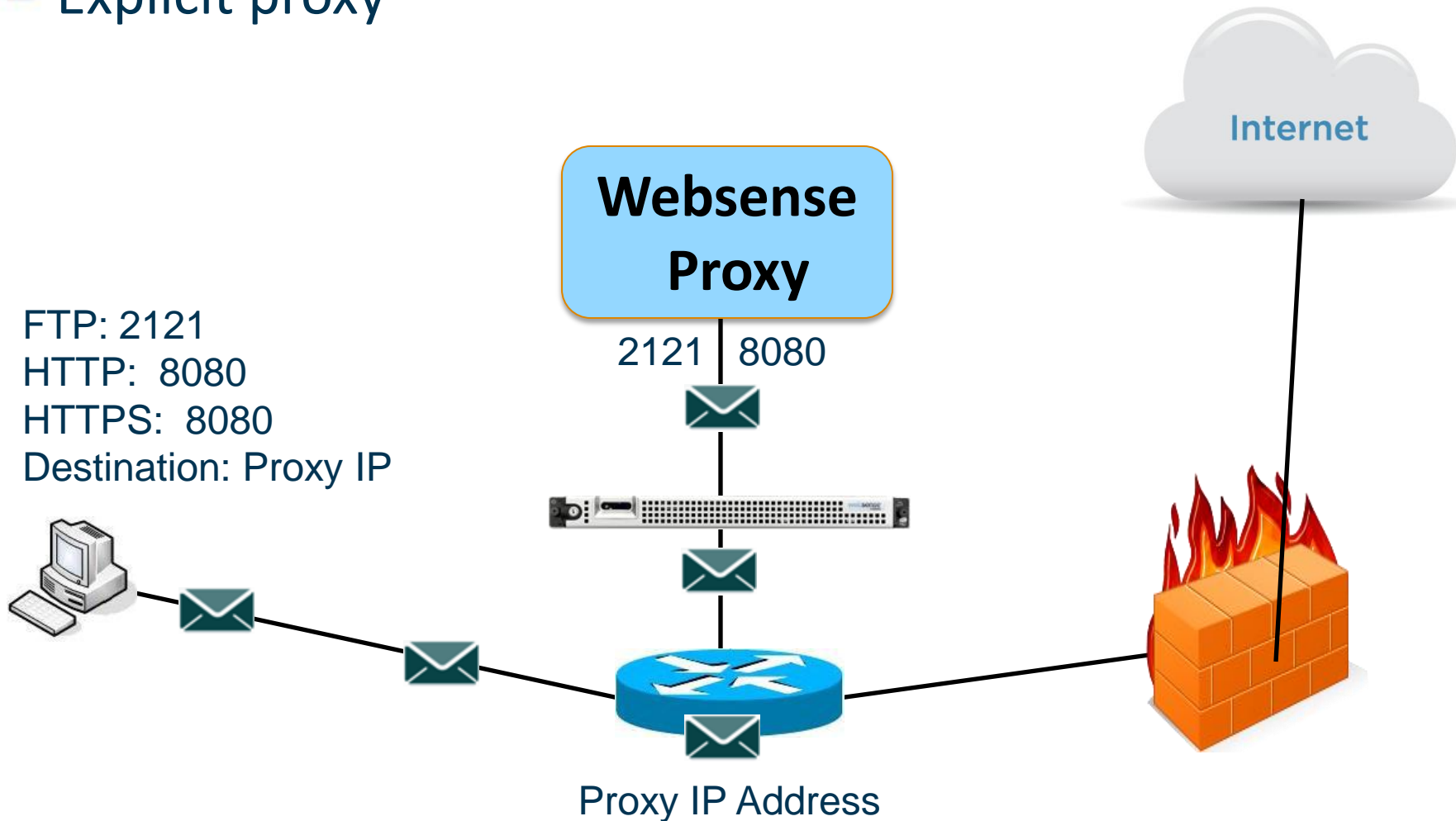
Directing traffic to the proxy

- Transparent proxy
- Arm
 - Static Bypass



Directing traffic to the proxy

■ Explicit proxy



■ Transparent proxy

- ARM module for bypassing traffic
- Static Bypass works only when proxying transparently
- When bypass does not help, use your ACL

■ Explicit proxy

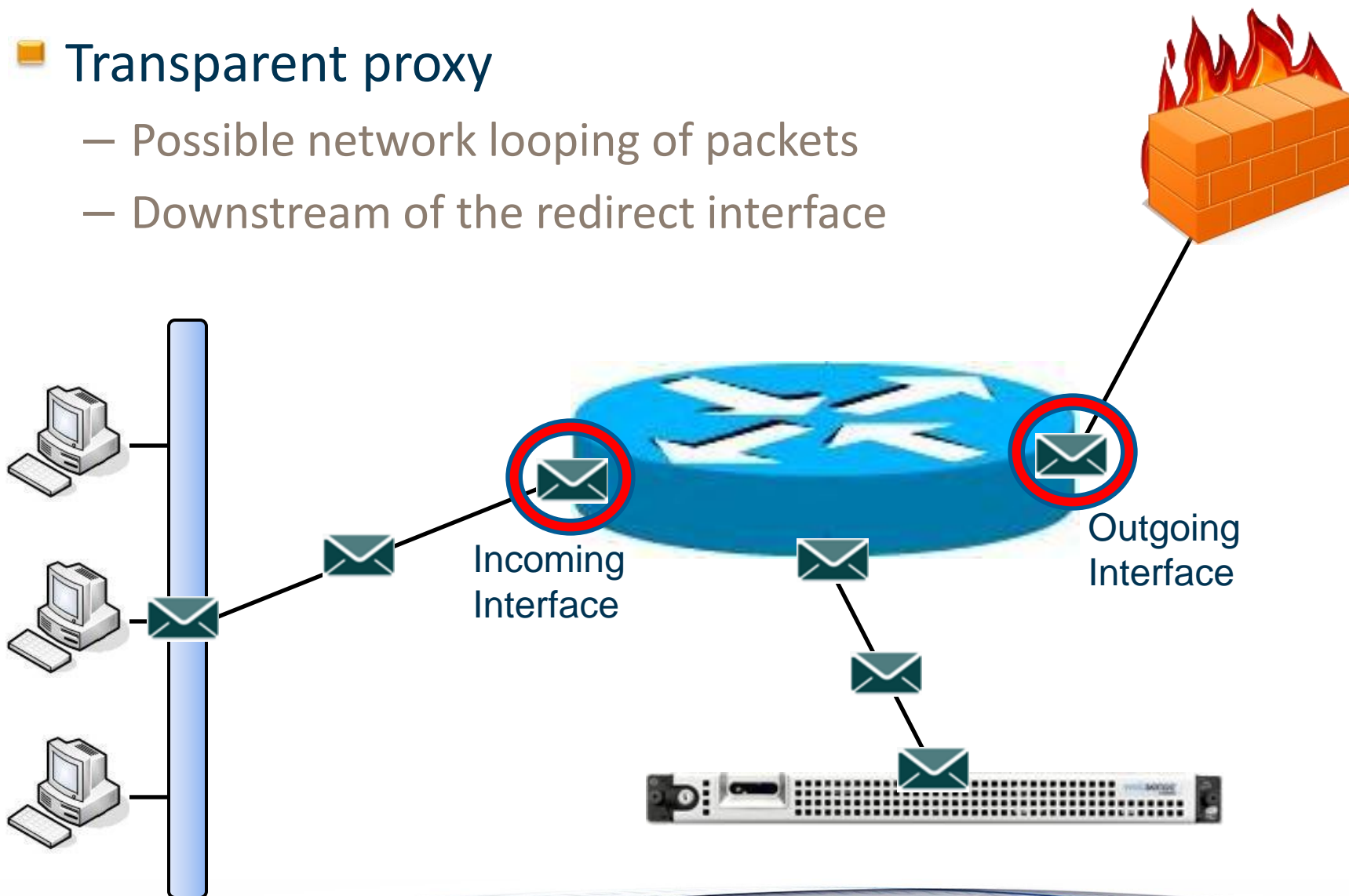
- Exceptions are external to the proxy
 - Client Web browser
 - WPAD
 - PAC file

- Test external proxy connectivity
 - `wget` command
- SSL - tunneling certificates
 - Incident list
 - Add sites manually
- Static bypass – ARM
 - List site by destination IP address
 - Used primarily with transparent proxy
 - Add sites manually

- Demonstration

■ Transparent proxy

- Possible network looping of packets
- Downstream of the redirect interface



- **NTLM bypass**
 - Is NTLM enabled
 - Ignoring an authentication request
- **Caching**
 - Expectations in today's dynamic world
 - Flushing the cache
 - Never-cache rule
 - Optimize settings
 - Disable caching
- **Demonstration**

■ Timeout & Keep-Alive settings

- Sites may stall
- Sites may not respond

■ Concurrent connections

- 5000 to 6000 is acceptable

■ Demonstration

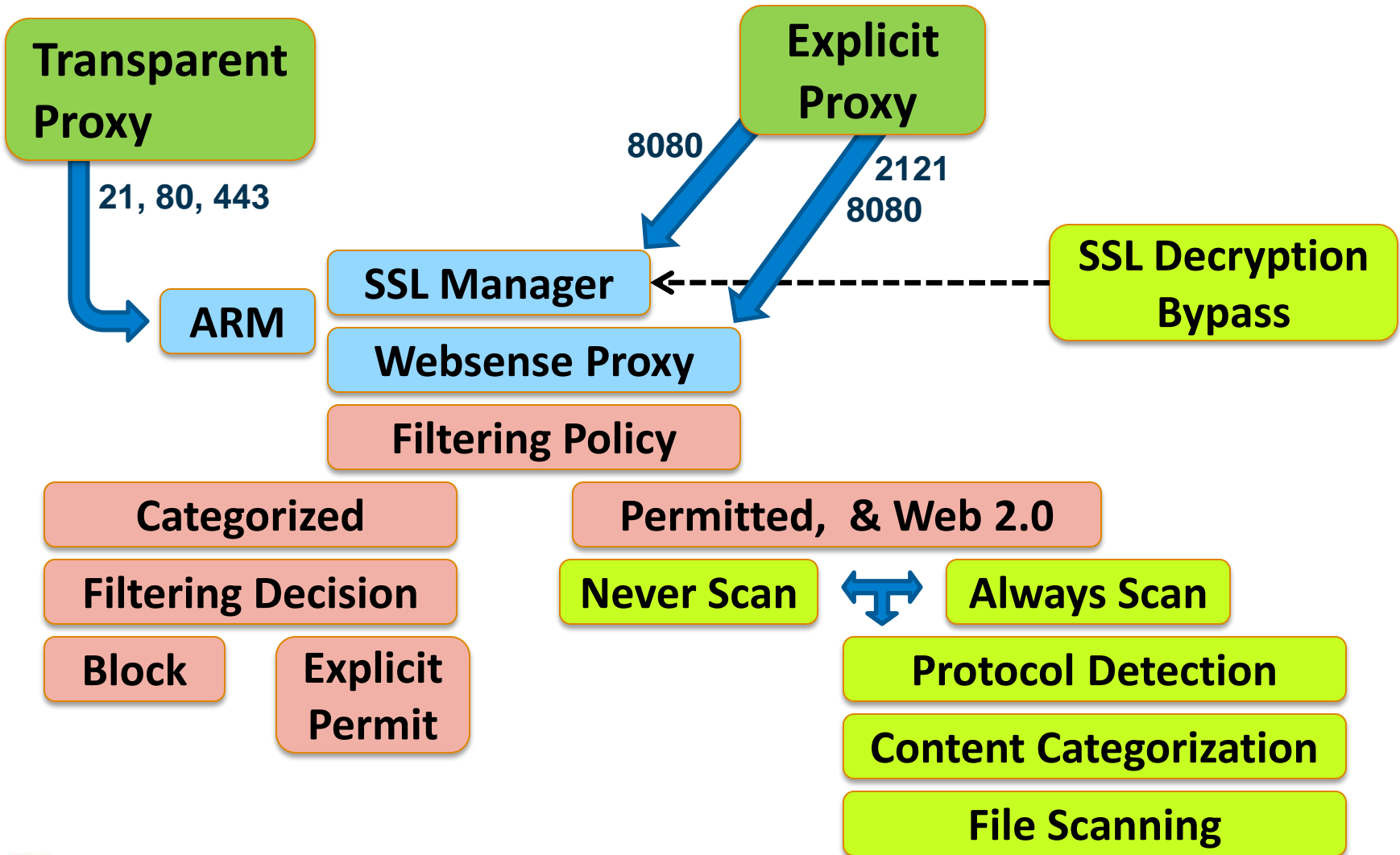
- HTTP timeouts
- FTP timeouts
- HTTPS timeouts

- Protocol tunneling
 - New feature for v7.5
 - May need to allow protocols
- URL Expandomatic
 - Do not disable
- Demonstration

■ Management

- Scanning options
 - Tunneled Protocol Scanning
 - Content Categorization
 - Security Threats: Content Scanning
 - Security Threats: File Detection
- Scanning Exceptions
 - To scan or not scan is the question...
- SSL Decryption Bypass
 - Disable decrypting an entire category of URLs

TRITON Unified Security Center



■ Demonstration

- Scanning options
 - Offers several security inspections
 - Method for exceptions
 - Bypass decryption
- User reports help identify scanning issues

■ Backup

- Appliance Manager
- Not an automatic feature
- Move backup files off-box

■ Some sites should not be proxied

- Internal web sites & web applications
- Trusted client updates
 - Anti-virus
 - Operating system patches
 - Etc.

■ Update to the latest version

- Apply all patches

■ Slow sites – proxy caching

– Update records.config file

- proxy.config.http.cache.max_open_read_retries -v 0
- proxy.config.http.cache.max_open_write_retries -v 0
- proxy.config.cache.threads_per_disk -v 12

■ General proxy tuning for latency

– Update records.config file

- proxy.config.http.down_server.cache_time -v 0
- proxy.config.http.connect_attempts_timeout -v 60
- proxy.config.http.send_http11_requests -v 1
- proxy.config.http.chunking_enabled -v 0
- proxy.config.http.insert_request_via_str -v 0

■ KB Article

- [How Do I Remove External Header Information In Websense Proxy?](#)

■ Applying configuration changes

- Prior Webinar
 - Example starts 20 minutes into the presentation
 - Title: [*Troubleshooting and Debugging Issues for V-Series v7.5*](#)
 - Date: July 21, 2010

■ KB Article

- [Site Access Issues With WCG Or V-Series Appliance](#)

Knowledge Base

- Search or browse the knowledge base for documentation, downloads, top knowledge base articles, and solutions specific to your product.

Support Forums

- Share questions, offer solutions and suggestions with experienced Websense Customers regarding product Best Practices, Deployment, Installation, Configuration, and other product topics.

Tech Alerts

- Subscribe to receive product specific alerts that automatically notify you anytime Websense issues new releases, critical hot-fixes, or other technical information.

ask.websense.com

- Create and manage support service requests using our online portal.

Customer Training Options

- To find Websense classes offered by Authorized Training Partners in your area, visit:
<http://www.websense.com/findaclass>
- Websense Training Partners also offer classes online and onsite at your location.
- For more information, please send email to:
readiness@websense.com

WEBSense®
**Authorized Training
Partner**

WEBSense®
Certified Instructor



Webinar Update

Title: Jump Start Part 4: Using Reports to Strengthen Filtering Policies

Date: January 19th, 2010

Time: 8:30 AM PDT (GMT -8)

How to register:

[http://www.websense.com/content/
SupportWebinars.aspx](http://www.websense.com/content/SupportWebinars.aspx)

Questions?



■ Origin server blacklisting

- There will always be servers that do not perform correctly, and because of this there is a blacklisting function in the WCG to ban origin servers if they constantly return errors.
- However this may occur in unexpected ways so in general it can be disabled by doing:
 - `proxy.config.http.down_server.cache_time -v 0`
- This has no known impact.

■ Origin server timeout

- If an origin server does not respond to the initial request within 30 seconds it will be disconnected (and may be blacklisted), this can be too low for some highly stressed sites and so it can be increased to 60 seconds by doing:
 - `proxy.config.http.connect_attempts_timeout -v 60`
- This does not have a negative impact.
- There are also some timers exposed in the WCG GUI that can help with some non-standard applications using HTTP, these again with moderate modification do not cause problems, particularly the idle timer can be increased.
- Excessive increase of the timers will result in the proxy using more resources, but increasing the origin server inactivity timer to 250 seconds or so has no discernable effect and makes some applications work.

■ HTTP 1.1 support

- In all cases the proxy should force the use of HTTP 1.1 over 1.0 or 0.9 by doing:
 - `proxy.config.http.send_http11_requests -v 1`
- This is because there are some origin servers capable of both HTTP 1.1 and 1.0 but when HTTP 1.0 requests are made they fail to close the connection properly. With the change the proxy will use HTTP 1.1 and so the origin server will close the connection correctly.
- This has no negative implications.

■ Client chunking support

- In all cases the proxy should disable the use of HTTP chunking by doing:
 - `proxy.config.http.chunking_enabled -v 0`
- Chunking is used to optimize connections to origin servers to pull content more efficiently, however in some cases when the proxy starts to use chunking the browser does not properly handle the subsequent http data sent to it, so when it is disabled then there is better client compatibility.
- This has no negative implications.

■ Via headers

- In all cases the Via headers should be disabled both to clients and to origin servers.
- This is accessed via the WCG GUI in HTTP->Privacy.
- If the proxy sends Via headers this is both a security issue and causes problems with various web sites.
- In particular when the origin server uses Apache mod_security then it is possible that the Via string will be misinterpreted as a HTTP protocol header and so blocked.
- There is a possible negative impact in proxy chaining where the upstream proxy can need Via headers for rule determination etc. but this is very uncommon.