# Configuring WCCP v2 with Websense Content Gateway – the Web proxy for Web Security Gateway

## Webinar December 2011

web security | data security | email security

# Webinar Presenter

**Greg Didier**

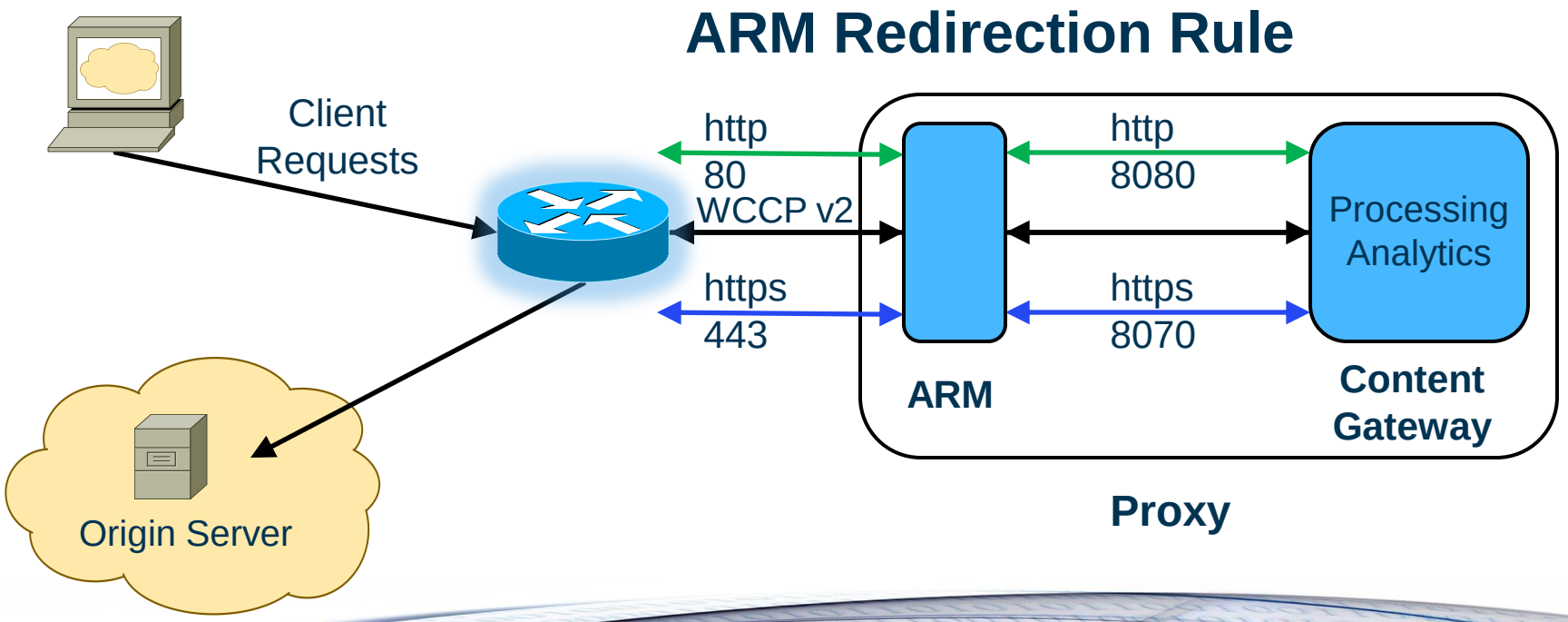
- Title: Support Specialist
- Accomplishments:
  - 9 years supporting Websense products
- Qualifications:
  - Technical Support Mentor
  - Product Trainer

# Goals and Objectives

- Why WCCP
- WCCP features
- Router configuration
- Content Gateway configuration
- Router demonstrations
- Troubleshooting tips
- Best practices

# WCCP v2 Interception

- WCCP v2 devices intercept traffic, usually on ports 80 and 443, and redirect it to the proxy
- ARM module receives the traffic and readdresses it to Content Gateway, which performs security functions
- Acting on behalf of the client now, the traffic is readdressed by ARM, restoring the origin server IP address and port number
- Traffic exits network with proxy as source IP address



# WCCP v2 Features

websense
ESSENTIAL INFORMATION PROTECTION™

- Multiple routers in a proxy cluster
- Multiple ports per service group
- Multiple service groups per protocol
- Dynamic load distribution in a proxy cluster through assignment method HASH or MASK, and weight
- Packet Return Method and Packet Forward Method negotiation
  - Only negotiates when method is not stipulated by router
- MD5 password security per service group
- Multicast mode

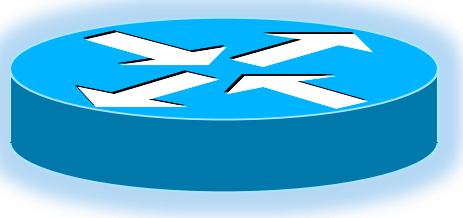
# Transparent Interception Strategies

websense
ESSENTIAL INFORMATION PROTECTION™

- Employing transparent proxies:
  - A Layer 4 switch
  - Policy-Based Routing (PBR)
  - Software Routing
  - A router or switch that supports WCCP v2
    - Cisco IOS-based routers are the most common
- Terms
  - *WCCP Server,* the WCCP redirection device
  - *WCCP Client,* the Content Gateway proxy
  - *Service Group,* defines the type of traffic to be intercepted
  - *ARM,* Adaptive Redirection Module modifies packet header

# WCCP v2 Setup Overview

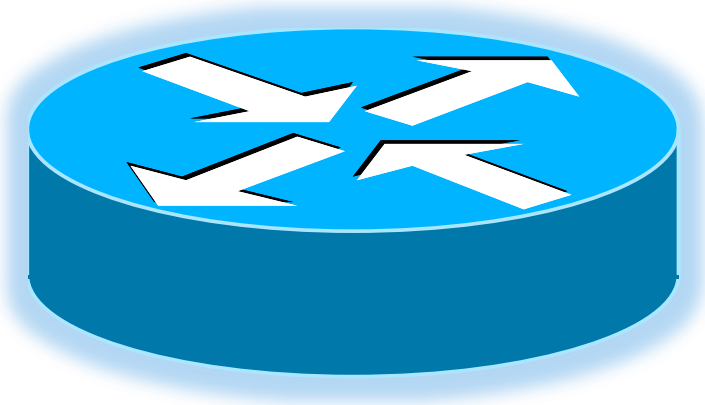
- Configure the WCCP Server



- Configure the WCCP Client (Content Gateway) to work with WCCP Server
  - Service groups must match exactly
- Validate configuration

# WCCP v2 Setup

- Step one
  - Configure the WCCP Server



# Configure the WCCP Server

- Set WCCP version 2
- Create a standard ACL for the Group List
  - Specifies what WCCP Clients are allowed to participate in a given service group
  - Increases security
- Create an extended ACL for the Redirect List
  - Identifies the interesting traffic to be redirected
- Enable WCCP globally
  - Set Service Group ID
  - Establish password for security
    - Must match corresponding password on the Content Gateway
- Enable WCCP on the appropriate interface
  - Interface where WCCP redirection is applied

# Configure the WCCP Server

- Telnet demonstration
  1. Set WCCP version 2
     - `ip wccp version 2`
  2. Standard ACL for the Group List
     - `ip access-list standard`
  3. Extended ACL for Redirect List
     - `ip access-list extended`
  4. Enable WCCP globally
     - `ip wccp <#> redirect-list <name> group-list <name> password <pwd>`
  5. Enable interface
     - `int vlan <#>`
     - `ip wccp <#> redirect in`
- Demonstration

# Configure the WCCP Server

- WCCP Server is now configured and waiting…
  - A WCCP Client to advertizing with “Here_I_Am” packets
  - The WCCP Server will respond with “I_See_You” packets
  - The WCCP Client sends its configured Service Group data
  - Negotiation starts
    - Service Group ID
    - Password check
    - Only allows proxies identified in the group-list
    - Determines data exchange method (L2 or GRE)
    - Etc.
- A successful negotiation results in a Service Group

# WCCP v2 Setup

- Step two
  - Configure Content Gateway to work with WCCP Server

# Configure Content Gateway

- Enable ARM
- Enable WCCP v2
- Define the WCCP service group
- Restart Content Gateway proxy

# Enable ARM

- ARM inspects incoming packets and readdresses them to Content Gateway for processing
  - Must be enabled
  - **Configure > My Proxy > Basic > General**
- For WCCP, there must be a redirection rule for every port in every active service group
  - **Configure > Networking > ARM > General**
- If prompted, do **not** restart proxy
- Demonstration

# Enable WCCP v2

- WCCP must be enabled
  - Must be enabled
  - **Configure > My Proxy > Basic > General**
  - If prompted, do **not** restart proxy
- Specify the WCCP network interface
  - **Configure > Networking > WCCP > General**
  - This interface communicates with the WCCP routers
    - Used by all service groups
    - Must be set on each node in the cluster – the value is not propagated
- Demonstration

# Define WCCP Service Group

- Every WCCP service group redirecting traffic must have a corresponding service group defined for it in Content Gateway
  - Service groups need only be configured once within the cluster
  - Except the **enabled/disabled** setting and the **weight** setting, if used, which must be set on each node
- Service Group information
- Router information
- Mode negotiation
- Advanced settings -parameters used to distribute intercepted traffic among multiple nodes in a cluster
  - Assignment method, Weight, and Reverse Service Group ID
- Restart Content Gateway
  - **Configure > My Proxy > Basic > General > Restart**
- Demonstration

# WCCP v2 Setup Overview

- Step three
  - Validate configuration

# Validate Configuration

- Is the Service Group formed?
  - sh ip wccp 0
  - sh ip wccp 0 detail
  - sh ip wccp 0 view

Telnet 10.212.0.3

```
1711Router#sh ip wccp 0
Global WCCP information:
    Router information:
        Router Identifier:                  10.212.0.3
        Protocol Version:                   2.0

    Service Identifier: 0
        Number of Cache Engines:            1
        Number of routers:                  1
        Total Packets Redirected:           2633
        Redirect access-list:               R_TST
        Total Packets Denied Redirect:      0
        Total Packets Unassigned:           7
        Group access-list:                  TST
        Total Messages Denied to Group:     0
        Total Authentication failures:      0
        Total Bypassed Packets Received:    0
```

Telnet 10.212.0.3

```
1711Router#sh ip wccp 0 detail
WCCP Cache-Engine information:
        Web Cache ID:           10.212.1.52
        Protocol Version:       2.0
        State:                  Usable
        Initial Hash Info:      00000000000000000000000000000000
                                00000000000000000000000000000000
        Assigned Hash Info:     FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                                FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
        Hash Allotment:         256 (100.00%)
        Packets Redirected:     2633
        Connect Time:           03:59:28
        Bypassed Packets
          Process:              0
          Fast:                 0
          CEF:                  0
```

Telnet 10.212.0.3

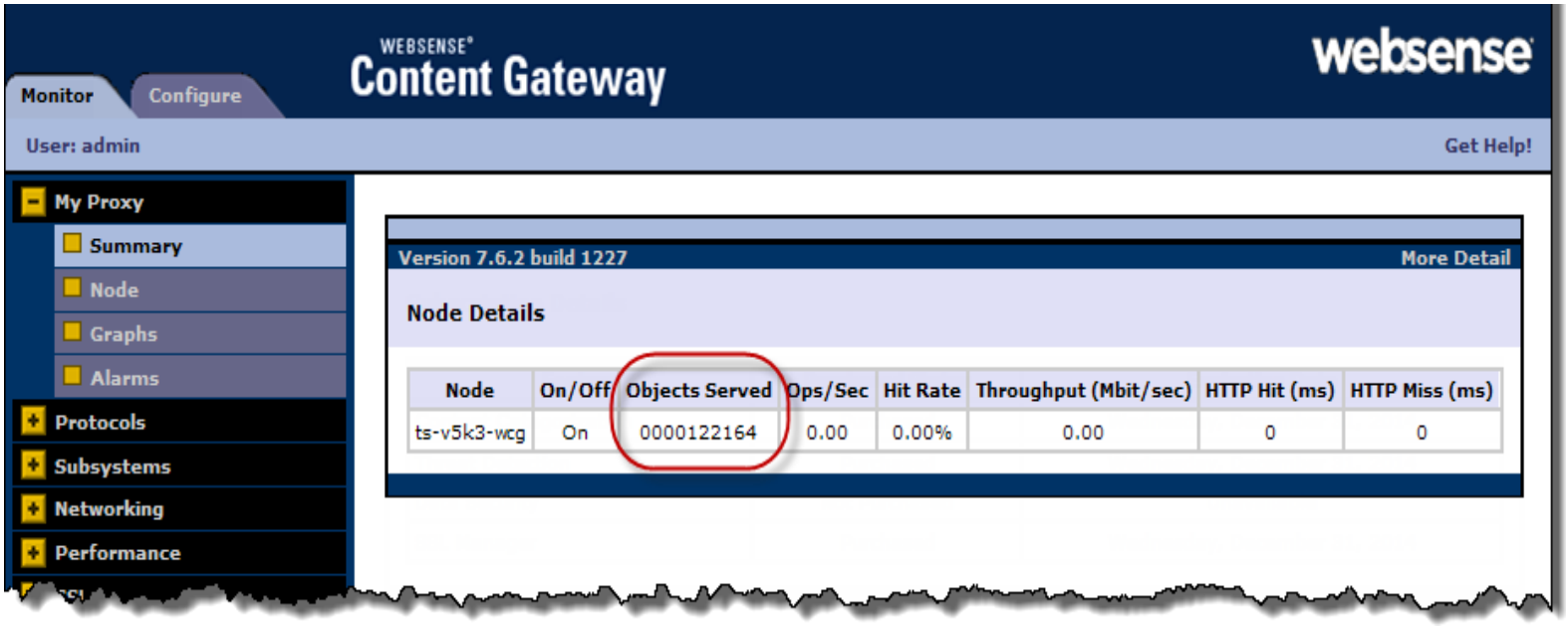
```
1711Router#sh ip wccp 0 view
    WCCP Routers Informed of:
        10.212.0.3

    WCCP Cache Engines Visible:
        10.212.1.52

    WCCP Cache Engines NOT Visible:
        -none-
```

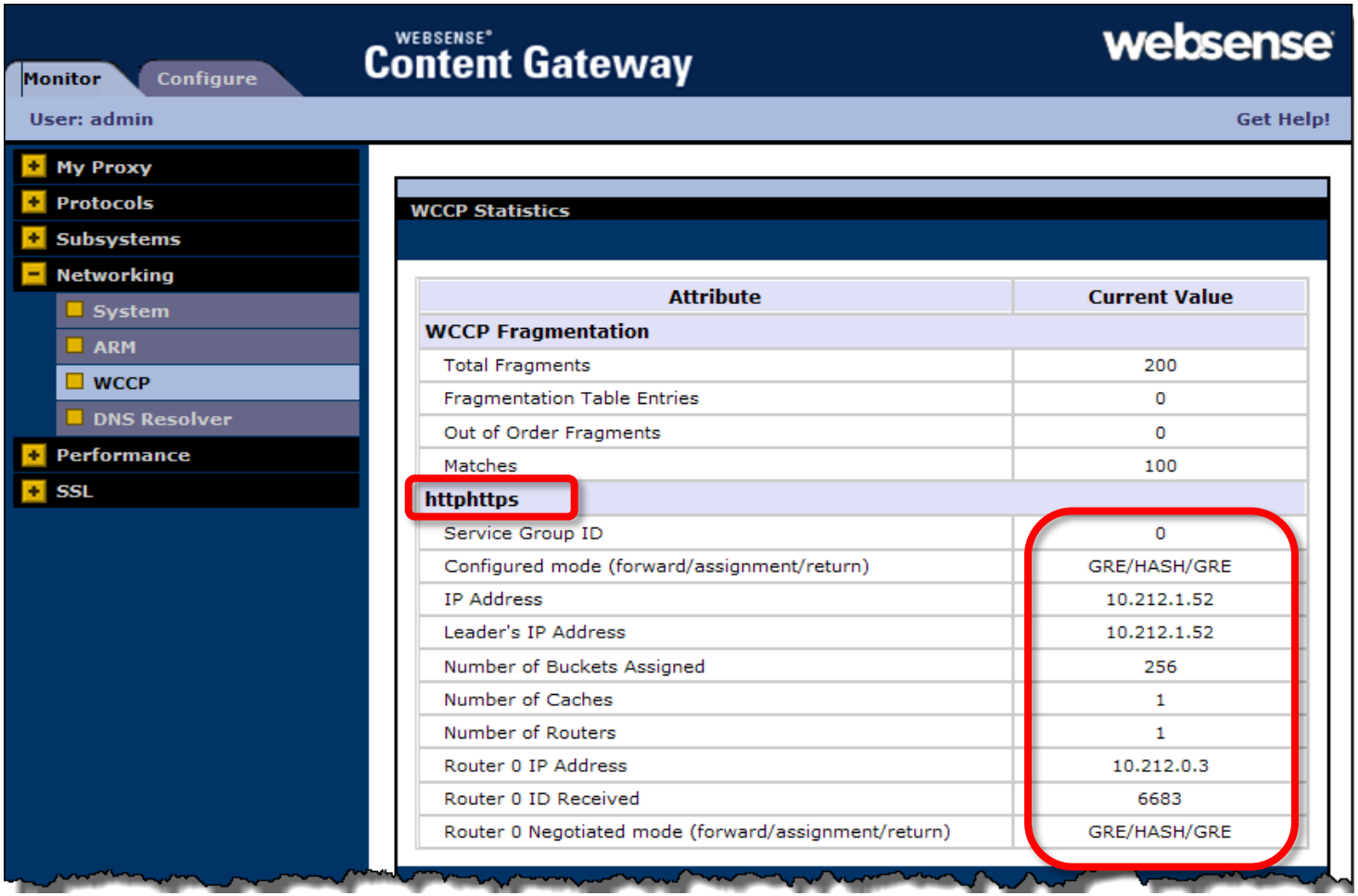
# Validate Configuration

- Examine statistics
  - It may take up to a minute for the router to report that a new proxy server has joined a service group
  - In **Monitor > My Proxy > Summary**, check that **Objects Served** is increasing



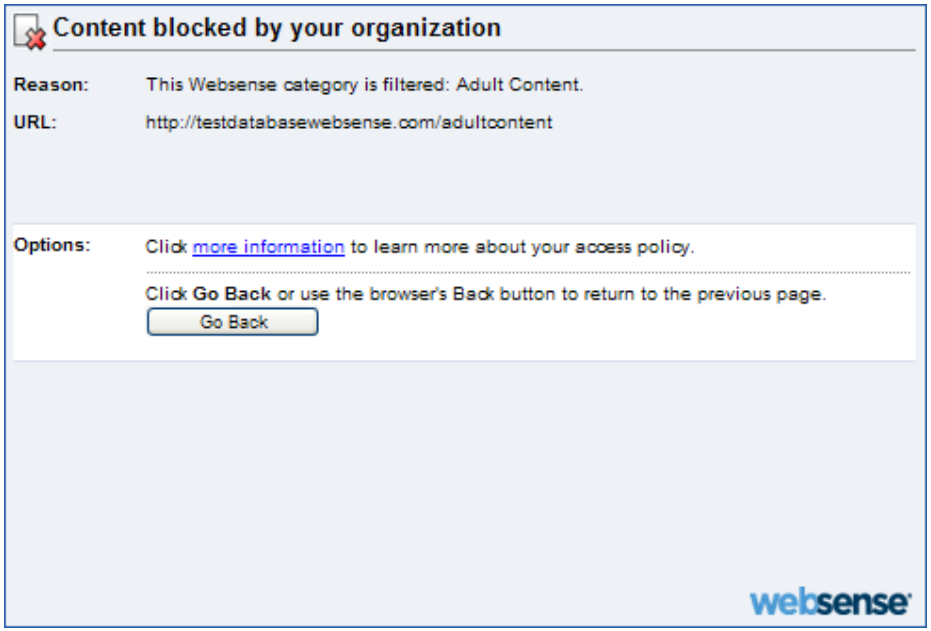
# Validate Configuration

- WCCP v2 statistics



# Validate Configuration

- Are reports showing new user activity?
- Test client workstation
  - Is traffic blocked?
    - http://testdatabasewebsense.com




- Demonstration

# Router Troubleshooting

- Informational commands
  - `sh ip wccp <#> <detail or view>`
  - `sh ip access-list <name>`
  - `sh run`
  - `sh run | include wccp`
  - `sh run int vlan 10`
  - `sh logging`
  - `sh debugging`
- Enable WCCP debugging
  - `terminal monitor`
  - `debug ip wccp packets`
  - `debug ip wccp events`
- Disable WCCP debugging
  - `no debug ip wccp packets`
  - `no debug ip wccp events`
  - `terminal no monitor`

# Best Practice Tips

websense
ESSENTIAL INFORMATION PROTECTION™

- Standard service group ‘web-cache’ not supported
  - Characteristics of the web cache service are known by both the router and cache engines
- Websense only supports dynamic service groups
  - Dynamic services are defined by the first web cache to join the service group
  - The cache instructs the router which protocol or ports to intercept, and how to distribute the traffic
- WCCP command options
  - ip wccp {web-cache | service-number} [group-list access-list] [redirect-list access-list] [group-address groupaddress] [password [0-7] password]

# Best Practice Tips

- Changing established service groups
  1. Disable WCCP on all Content Gateway nodes
  2. Remove interface configuration
  3. Remove or change the global configuration
     - Redirect/Group Lists on WCCP Server
     - Forward/Return/Assignment Method on Content Gateway
  4. Reapply new global and interface configurations
  5. Re-register Content Gateway nodes

# Best Practice Tips

websense
ESSENTIAL INFORMATION PROTECTION™

- Inbound redirections should be used whenever possible to reduce CPU overhead
- For Routers:
  - Use GRE Forward/Return
  - Use HASH assignment
- For Switches:
  - Use L2 Forward/Return Method when possible
  - Use MASK assignment

# Best Practice Tips

- Difference with a Cisco switch
  - Not much difference in configuration syntax
  - Leverage hardware use as much as possible
    - Use inbound redirection
    - Use Mask assignment
    - User L2 Forward/Return methods
      - L2 requires layer-2 adjacency between WCCP Client and WCCP Server

# Best Practice Tips

- Difference with a Cisco ASA
  - Quite different, if possible leverage WCCP elsewhere
  - Limitations:
    - Cannot use IP Spoofing
    - Cannot redirect traffic from one security zone to another
    - Cannot employ ARM bypass in WCG
      - Causes a WCCP redirect loop
  - For configuration:
    - Use GRE Forward/Return methods
    - Use Hash assignment
    - Use 'specific' Layer 4 statements in the redirect list ACL
      - **Good:** `permit tcp 10.212.8.8 255.255.255.248 any eq www`
      - **Bad:** `permit ip 10.212.8.8 255.255.255.248 any`

# Router Telnet Commands

- Redirect workstation (10.212.2.215)
  - Enable
  - config t
  - ip wccp version 2
  - ip access-list standard TST
  - permit host 10.212.1.52
  - ip access-list extended R_TST
  - deny ip host 10.212.1.52 any
  - deny ip any 10.0.0.0 0.255.255.255
  - deny ip any 172.16.0.0 0.15.255.255
  - deny ip any 192.168.0.0 0.0.255.255
  - Permit ip host 10.212.2.215 any
  - ip wccp 0 group-list TST redirect-list R_TST password tst
  - int vlan 10
  - ip wccp 0 redirect in
  - end

# Router Telnet Commands

websense
ESSENTIAL INFORMATION PROTECTION™

- Redirect network range and proxy range
  - Enable
  - config t
  - ip wccp version 2
  - ip access-list standard TST
  - permit ip 10.212.8.8 0.0.0.7
  - ip access-list extended R_TST
  - deny ip host 10.212.1.52 any
  - deny ip any 10.0.0.0 0.255.255.255
  - deny ip any 172.16.0.0 0.15.255.255
  - deny ip any 192.168.0.0 0.0.255.255
  - permit ip 10.212.0.0 0.0.255.255 any
  - ip wccp 0 group-list TST redirect-list R_TST password tst
  - int vlan 10
  - ip wccp 0 redirect in
  - end

# Best Practice Tips

websense
ESSENTIAL INFORMATION PROTECTION™

- Negotiation Mode
  - The WCCP Client advertizes to the WCCP Server
  - Router should stipulate the data exchange method
  - *Packet Forward / Return Methods:*
    - The mode selected should match the capabilities of the WCCP Server
    - *L2*– Requires the router or switch be Layer 2-adjacent
      - In the same subnet as Content Gateway
    - *GRE– Overcomes L2 obstacle by adding a second Layer 3 header*
      - Routers typically support only one method
      - Typically, forward and return methods should match
    - *Packet Forward– from redirection device to proxy*
    - *Packet Return– from proxy to redirection device*
  - Hash and Mask Assignment Method:
    - *Parameters used to distribute intercepted traffic among multiple proxies*

# Presentation References

websense
ESSENTIAL INFORMATION PROTECTION™

- These links correlate to the presentation outline
  - How WCCP v2 interception works (slide 5)
  - WCCP v2 supported features (slide 6)
  - Transparent interception strategies (slide 7)
  - Transparent interception with WCCP v2 devices (slide 8)
  - Install and configure your WCCP v2 devices (slide 8)
  - Configuring WCCP v2 routers (slide 10)
  - Configuring service groups on the WCCP device (slides 11-12)
  - Enabling WCCP processing for a service group (slides 11-12)
  - Enabling WCCP v2 security on the router (slides 11-12)

# Presentation References

websense
ESSENTIAL INFORMATION PROTECTION™

- These links correlate to the presentation outline
  - Configure Content Gateway to work with WCCP devices (13-14)
  - Enabling the ARM (slide 15)
  - Enabling WCCP v2 in Content Gateway (slide 16)
  - Enabling WCCP in Content Gateway Manager (slide 16)
  - Specifying the WCCP network interface (slide 16)
  - Configuring service groups in Content Gateway Manager (17)
  - Restarting Content Gateway (see step 9) (slide 17)
  - Validate the configuration with test traffic (slide 18)

# WCCP References

- Web Cache Control Protocol (WCCP), Version 2 (V1.7.6)
- Websense Content Gateway v7.6 Help document
- Configuring WCCP v2 for Websense Content Gateway
- Past Webinar: Common Configuration Methods for the Websense Content Gateway
  - WCCP configuration starts 28 minutes into this webinar
- Past Webinar: Achieving rapid success with WCCP and Web Security Gateway
- IP spoofing

# Support Online Resources

websense
ESSENTIAL INFORMATION PROTECTION™

## 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.

# Webinar Announcement

websense
ESSENTIAL INFORMATION PROTECTION™

**Webinar Update**

Title: **Identifying and resolving logging issues when reports are blank**

Date: **January 18th, 2012**

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

How to register: http://www.websense.com/content/SupportWebinars.aspx

# Customer Training Options

websense®
ESSENTIAL INFORMATION PROTECTION™

- 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