Scaling Your Cisco IronPort Web Security Appliance Using Cisco Application Control Engine

Executive Summary

This guide discusses a validated scalable deployment option for the Cisco IronPort™ Web Security Appliance (Cisco IronPort WSA) S-Series as a transparent proxy using the Cisco® Application Control Engine (ACE).

Because of its proxy architecture, Cisco IronPort Cisco IronPort WSA is commonly deployed using transparent redirection through the Web Cache Control Protocol (WCCP). Although WCCP is a very capable interception engine, the combination of Cisco IronPort Cisco IronPort WSA and Cisco ACE creates a solution architecture that provides a more robust, scalable, and flexible solution than is possible using WCCP. In certain network environments, WCCP is not feasible and is incompatible with preexisting features such as Virtual Routing and Forwarding (VRF), Cisco IOS® Software version requirements, and complex configurations, and Cisco IOS Software products and third-party products offer varying degrees of WCCP support. Cisco ACE provides an alternative means of transparently intercepting outgoing web traffic and intelligently directing it to a group of Cisco IronPort Cisco IronPort WSA devices. This approach mitigates the dependencies of the WCCP solution and significantly increases scalability, extending the number of Cisco IronPort Cisco IronPort WSA devices beyond the 32-device limit of WCCP. The virtualization capabilities of the Cisco ACE allow it to be securely used as a server load balancer as well, combining multiple application functions in a single platform.

Introduction

Cisco ACE can transparently redirect Internet traffic to a cluster of Cisco IronPort WSA proxy servers. The transparent proxy solution allows network administrators to quickly deploy proxies anywhere in the network with no modification to end-user browsers or other software. The Cisco IronPort WSA S-Series provides a scalable proxy platform architecture to protect and accelerate the delivery of business applications.

Cisco ACE offers enterprises and service providers a highly resilient server load-balancing solution. Cisco ACE is available in two form factors: a standalone appliance and a module for Cisco Catalyst® 6500 Series Switches and Cisco 7600 Series Routers. The Cisco ACE transparent mode capability offers client protection, improves Internet response time, and reduces WAN operating costs by redirecting web traffic destined for remote Internet sites to a group of local proxy cache servers.

The Cisco IronPort WSA S-Series delivers a scalable proxy platform architecture to protect web traffic and accelerate the delivery of business applications. Figure 1 shows the main components of the Cisco IronPort WSA S-Series solution.

© 2010 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 1. Main Components of Cisco IronPort WSA S-Series

	Cisco IronPort WSA S-Series Components
Web Security	▪ Web Reputation Filters ▪ Antimalware Filters ▪ Layer 4 Traffic Monitor
Web Traffic Control	▪ URL Filters ▪ Web Security Manager (for Policy Management) ▪ Web Security Monitor (for Reporting and Visibility)
High-Performance Web Gateway	▪ Integrated Proxying, Caching, and Content Acceleration ▪ Authentication, Logging, and Alerting ▪ Integrated Scanning Engine ▪ Network-Layer Monitoring

Challenges

Proxy technology inherently relies on interception technologies to deliver traffic to the proxy server group for protection and acceleration. These methods include explicit proxy (inline), proxy automatic configuration (PAC) file distribution (through direct upload, Dynamic Host Configuration Protocol [DHCP], or Domain Name System [DNS]), WCCP, and Cisco ACE technology. Explicit proxy requires massive resources to manually configure every client system. PAC files also present deployment challenges. WCCP, which provides Layer 2 transparent cache switching, has been the most commonly used redirection mechanism in the data center to date. However, the Cisco ACE, which provides a Layer 7 intelligent Layer 2–style transparent cache switching service, can be deployed as a Layer 2 redirection engine offering many benefits over the traditional WCCP engine, including scalability (16-Gbps throughput and 4 million connections), high availability and robustness (uninterrupted Internet access in high-availability mode) Layer 7 awareness, and advanced monitoring of Cisco IronPort WSA services.

In a traditional proxy deployment, the client's IP address is replaced with that of the proxy or cache server. Although this approach provides inherent security by masking the address of the end user, in some cases certain web applications require access to the originating client's IP address.

In many cases in which the client IP address must be preserved when it reaches the originating server, the Cisco ACE can easily be deployed because its default behavior is to preserve client IP addresses. In addition, the Cisco ACE supports 5-tuple flow matching and source MAC address matching to help ensure proper flow paths through the design. The Cisco ACE feature known as MAC-sticky helps ensure that the response traffic is given to the device that originated the connection, instead of the traffic's being routed as would happen in traditional proxy environments. To help ensure that only traffic destined for Cisco IronPort WSA is sent through the Cisco ACE and Cisco IronPort WSA solution, the router (a Cisco Catalyst 6500 Series Multilayer Switch Feature Card [MSFC] in this case) uses policy-based routing to force traffic to the Cisco ACE to be processed and forwarded to the Cisco IronPort WSAs.

In many cases, the Cisco IronPort WSA performs better when traffic is sent to it based on Layer 7 information. This approach is problematic for traditional proxy solutions such as WCCP, in which flow decisions are made at the connection level. The Cisco ACE offers a rich set of Layer 7 classifications that allow it to easily make per-request decisions to distribute traffic optimally to each Cisco IronPort WSA device.

© 2010 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Cisco ACE Solution

Cisco ACE supports load balancing of transparent and conventional proxy servers. Cisco ACE provides several load-balancing methods, which you can apply depending on how you want to distribute data over the proxy farm (for example, using the entire URL, a URL string, the entire domain name, or a domain string).

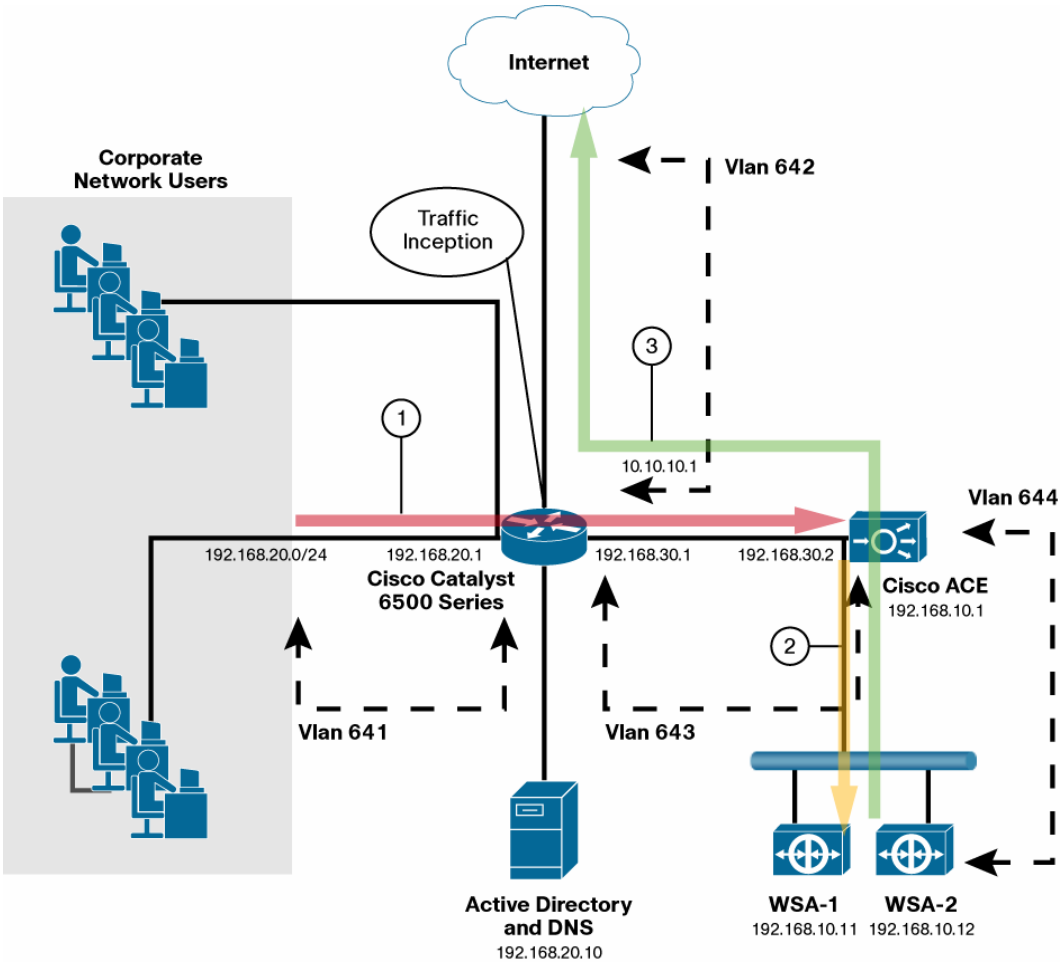
Cisco ACE can look at the URL requested by the client and determine the most appropriate proxy server to send it to based on the URL request, proxy server load, and availability. Cisco IronPort WSA supports request-based caching (passive caching) that is HTTP compliant. Requests are filled from the cache when a fresh (not stale) copy is available (cache hit). Cisco IronPort WSA does not support active caching or proactive refreshing of its cache; hence, dynamic pages (for example, URLs with cookies and Common Gateway Interface [CGI]) are fetched directly by the proxy on a per-request basis.

Health checks (probes) can easily be added to the Cisco ACE to help ensure the quality of the service. Cisco ACE will take a proxy server out of rotation when a failure is detected. If all proxy servers become unavailable, Cisco ACE allows all client requests to bypass them and sends the requests directly the originating servers (fail open).

Traffic Flow

Figure 2 shows the traffic flows for this solution.

Figure 2. Traffic Flow



© 2010 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

The traffic flow is as follows:

1. The Cisco Catalyst 6500 Series MSFC uses policy-based routing (PBR) on interface Vlan550 to route web traffic destined to TCP port 80 to the Cisco ACE.
2. Cisco ACE transparently load balances the traffic with the Cisco IronPort WSA farm by performing a Layer 2 MAC address rewrite, preserving the source and destination IP addresses of the connection. Cisco IronPort WSA validates the request with its configured security policies and delivers the requested content if a cached version is available (cache hit).
3. If Cisco IronPort WSA does not have the requested content or if the HTTP request includes the no-cache control option, Cisco IronPort WSA sends a request to the web server. Cisco IronPort WSA initiates a connection to the web server with the client IP address as the source address, with IP spoofing enabled. The Cisco Catalyst 6500 Series MSFC uses PBR on Vlan551 to forward return traffic (TCP traffic with source port 80) back to the requesting Cisco IronPort WSA.

Cisco ACE Design

Following are the best practices for configuring Cisco ACE for transparent caching:

- Virtual IP address: The virtual IP address typically is a catch-all address for a specific Layer 4 port.
- Predictor algorithm: To optimize caching, the typical predictor that can be used is **predictor hash url**. All other Cisco ACE predictors, such as **predictor hash header** and **predictor hash destination**, can also be used.
- Load-balancing policy: A Layer 4 class map is configured so that all requests will be load-balanced across Cisco IronPort WSA devices.
- MAC-sticky: Since the proxy servers have IP spoofing enabled, the TCP connections to the Internet that originate from the proxy servers will have the client IP address as the source. MAC-sticky is used on the interface connecting the Cisco IronPort WSA farm, and it enables Cisco ACE to route flow-based traffic by MAC address, bypassing a routing table decision. This approach is used to help ensure proper connection persistence for Cisco ACE.
- Probes: To verify the correct functioning of the Cisco IronPort WSA devices, you should enable HTTP probes. HTTP probes can be configured to request a page from one or more common internet websites. Note that if you send probes to multiple websites, you should add the “fail-on-all” option to the configuration section with the probe statements.
- Backup server farm: To help ensure uninterrupted service when all the Cisco IronPort WSA devices in the Cisco IronPort WSA server farm are down, you should configure a backup server farm that transparently forwards traffic to the Cisco Catalyst 6500 Series MSFC on Vlan540.

Cisco ACE, Cisco IronPort WSA, and Cisco Catalyst 6500 Series Switch Configuration

Cisco ACE supports up to 250 virtual contexts. When deploying Cisco ACE, the recommended practice is to use the Admin context to facilitate overall management of the Cisco ACE device and to create a designated context for each specific application for load balancing. In this solution, a context named “Cisco IronPort WSA” is created for the transparent proxy.

© 2010 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Admin Context Configuration

The Admin context configuration is shown here:

```
Generating configuration....

boot system image:c4710ace-mz.A3_2_5.bin

login timeout 0

hostname sandbox-pod3-aceapp2
clock timezone standard PST
clock summer-time standard PDT
ntp server 172.25.92.1


ip domain-name cisco.com
ip name-server 171.68.10.70
ip name-server 171.68.10.140

policy-map type management first-match mgmt
  class remote-access
    permit

interface vlan 110
  ip address 172.25.92.145 255.255.255.0
  service-policy input mgmt
  no shutdown

ip route 0.0.0.0 0.0.0.0 172.25.92.1

context ironport-Cisco IronPort WSA
  allocate-interface vlan 643-644
```

Cisco IronPort WSA Context Configuration

The Cisco IronPort WSA context configuration is shown here:

```
generating configuration....

access-list everyone line 10 extended permit ip any any

probe icmp PING
  ip address 192.168.30.1
probe http CISCO
  ip address 198.133.219.25
  interval 10
  faildetect 5
  passdetect interval 30
  request method head url /index.html
  expect status 200 200

probe http YAHOO
```

© 2010 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

```
  ip address 209.131.36.158
  interval 10
  faildetect 5
  passdetect interval 30
  request method head url /index.html
  expect status 200 200

rserver host MSFC
  ip address 192.168.30.1
  inservice
rserver host Cisco IronPort WSA-01
  ip address 192.168.10.11
  inservice
rserver host Cisco IronPort WSA-02
  ip address 192.168.10.12
  inservice
serverfarm host ROUTE
  transparent
  probe PING
  rserver MSFC
    inservice

serverfarm host Cisco IronPort WSAFARM
  transparent
  predictor hash url
  probe CISCO
probe YAHOO
fail-on-all
  rserver Cisco IronPort WSA-01 80
    inservice
  rserver Cisco IronPort WSA-02 80
    inservice

class-map match-all WEB-TRAFFIC
  2 match virtual-address 0.0.0.0 0.0.0.0 tcp eq www

policy-map type loadbalance first-match Cisco IronPort WSA-LB
  class class-default
    serverfarm Cisco IronPort WSAFARM backup ROUTE

policy-map multi-match LB
  class WEB-TRAFFIC
    loadbalance vip inservice
    loadbalance policy Cisco IronPort WSA-LB
    loadbalance vip icmp-reply active

interface vlan 643
  description To MSFC
  ip address 192.168.30.2 255.255.255.0
  access-group input everyone
```

© 2010 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

```
  service-policy input LB
  no shutdown
interface vlan 644
  description To Cisco IronPort WSA Proxy Interface (P1)
  ip address 192.168.10.1 255.255.255.0
  mac-sticky enable
  access-group input everyone
  no shutdown

ip route 0.0.0.0 0.0.0.0 192.168.30.1
```

Cisco Catalyst 6500 Series Configuration

The Cisco Catalyst 6500 Series configuration is shown here:

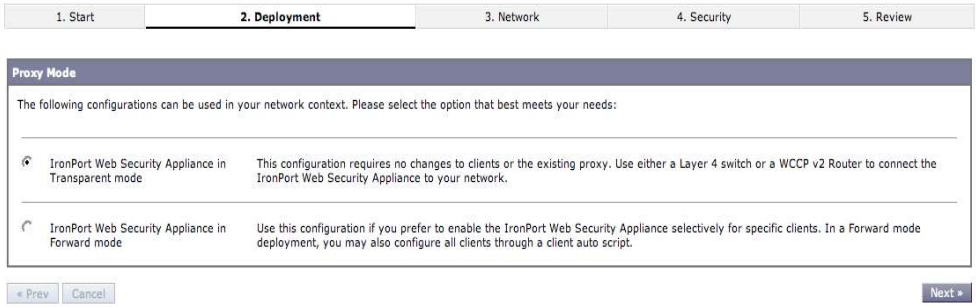
```
svclc multiple-vlan-interfaces
svclc module 3 vlan-group 1
svclc vlan-group 1  643,644

!
interface Vlan641
 description Cisco IronPort WSA-ClientUsers
 ip address 192.168.20.1 255.255.255.240
 ip policy route-map CLIENT-TCP80
!
interface Vlan642
 ip address 10.10.10.1 255.255.255.0
 ip policy route-map SERVER-TCP80
!
interface Vlan643
 description Cisco IronPort WSA-ACE_MSFC
 ip address 192.168.30.1 255.255.255.0
!
access-list 109 permit tcp any any eq www
access-list 110 permit tcp any eq www any
!
route-map SERVER-TCP80 permit 10
 match ip address 110
 set ip next-hop 192.168.30.2
!
route-map CLIENT-TCP80 permit 10
 match ip address 109
 set ip next-hop 192.168.30.2

! static routes to internet addresses hosted on a demo server
ip route 198.133.219.1 255.255.255.255 10.10.10.101
ip route 209.131.36.1 255.255.255.255 10.10.10.101
ip route 0.0.0.0 0.0.0.0 172.25.92.1
```

Cisco IronPort WSA Configuration

The Cisco IronPort WSA configuration is show here:

© 2010 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

1. In the initial System Setup wizard, select Transparent mode deployment. Transparent mode supports both explicit forward mode and WCCPv2 and Layer 4 switch environments.



Both management port M1 and web proxy data port P1 are set up

Cisco IronPort WSA-1:

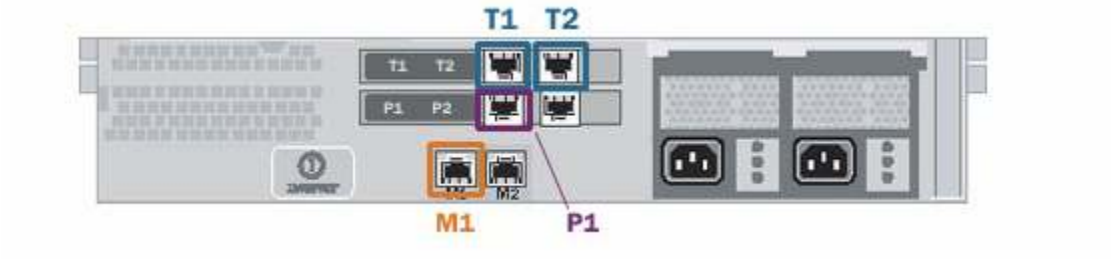
M1: 172.25.91.136

P1: 192.168.10.11

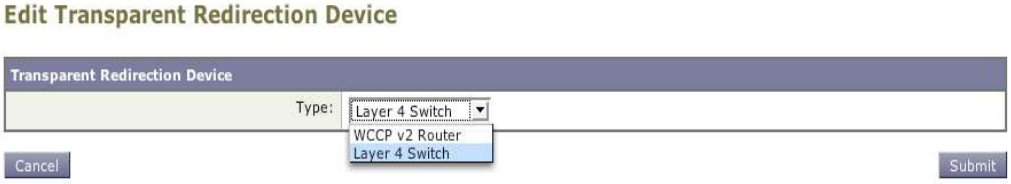
Cisco IronPort WSA-2:

M1: 172.25.91.137

P1: 192.168.10.12

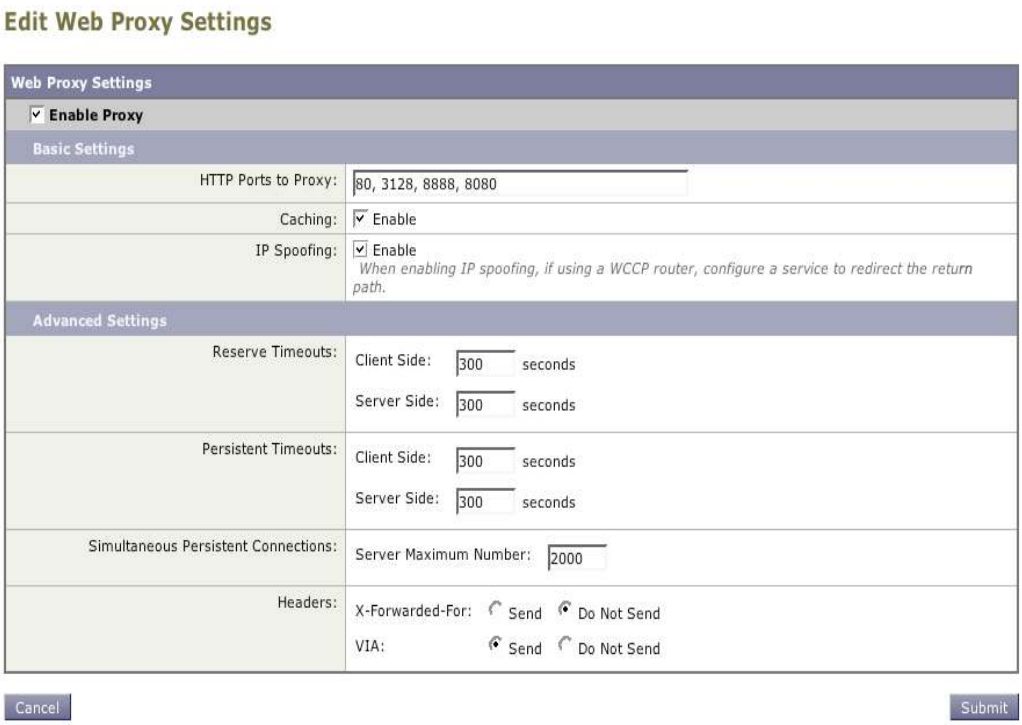


2. Make sure Layer 4 Switch is selected.



3. Enable IP Spoofing globally.

© 2010 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.



Conclusion

The robust Cisco ACE and Cisco IronPort WSA transparent proxy solution offers several configurable options that can be tuned according to the requirements. In addition, performance and throughput capabilities make this a highly scalable solution. Cisco ACE provides a high level of scalability, and with stateful redundancy and the capability to intelligently distribute traffic across Cisco IronPort WSA on a per-request basis, it provides an excellent solution.

For More Information

- For more information about Cisco ACE, visit http://www.cisco.com/go/ace.
- For more information about Cisco IronPort WSA, visit http://www.cisco.com/go/wsa.
- For more information about Cisco Application Networking Services (ANS), Cisco data center solutions for Cisco ANS, and Cisco ACE, visit http://www.cisco.com/go/applicationservices or contact your local Cisco account representative.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Printed in USA C07-623533-00 10/10

© 2010 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

© 2010 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.