Newer Cisco SBA Guides Available

This guide is part of an older series of Cisco Smart Business Architecture designs. To access the latest Cisco SBA Guides, go to http://www.cisco.com/go/sba

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.
Preface

Who Should Read This Guide
This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

Release Series
Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

month year Series

For example, the series of guides that we released in August 2011 are the “August 2011 Series”.

You can find the most recent series of SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba
Partner access: http://www.cisco.com/go/sbachannel

How to Read Commands
Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

configure terminal

Commands that specify a value for a variable appear as follows:

ntp server 10.10.48.17

Commands with variables that you must define appear as follows:

class-map [highest class name]

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

Router# enable

Long commands that line wrap are underlined. Enter them as one command:

wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

interface Vlan64
  ip address 10.5.204.5 255.255.255.0

Comments and Questions
If you would like to comment on a guide or ask questions, please use the forum at the bottom of one of the following sites:

Customer access: http://www.cisco.com/go/sba
Partner access: http://www.cisco.com/go/sbachannel

An RSS feed is available if you would like to be notified when new comments are posted.
# Table of Contents

**What's In This SBA Guide** ............................................................. 1
   - About SBA ................................................................. 1
   - About This Guide .......................................................... 1

**Introduction** ............................................................................. 2
   - The Purpose of This Document ............................................ 2
   - Graphical Interface Management ....................................... 2
   - Smart Business Architecture Borderless Networks for Enterprise Organizations .................................................. 3

**Enterprise Organizations Deployment Product List** ................. 4

**Internet Edge Configuration Files** .......................................... 6
   - ASA 5540
     - Internet Edge Firewall and Remote Access VPN ................. 6
   - ASA AIP SSM-40
     - Internet Edge Intrusion Prevention ................................. 11
   - Catalyst 2960-S Series Switch
     - Outside Switch .......................................................... 12
   - Catalyst 3750-X Series Switch
     - DMZ Switch .................................................................. 16
   - Catalyst 3750-X Series Switch
     - LAN Distribution Switch .............................................. 23
   - ACE 4710
     - DMZ Server Load Balancing ......................................... 27

---

All designs, specifications, statements, information, and recommendations (collectively, “Designs”) in this manual are presented “as is,” with all faults. Cisco and its suppliers disclaim all warranties, including, without limitation, the warranty of merchantability, fitness for a particular purpose, and noninfringement or arising from a course of dealing, usage, or trade practice. In no event shall Cisco or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use the Designs, even if Cisco or its suppliers have been advised of the possibility of such damages. The Designs are subject to change without notice. Users are solely responsible for their application of the Designs. The Designs do not constitute the technical or other professional advice of Cisco, its suppliers or partners. Users should consult their own technical advisors before implementing the Designs. Results may vary depending on factors not tested by Cisco.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.
About SBA
Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.
Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.
For more information, see the How to Get Started with Cisco SBA document:

About This Guide
This configuration files guide provides, as a comprehensive reference, the complete network device configurations that are implemented in a Cisco SBA deployment guide.
This guide provides the configuration files for the prerequisite deployment guide, as shown on the Route to Success below.

Route to Success
To ensure your success when implementing the designs in this guide, you should read any guides that this guide depends upon—shown to the left of this guide on the route above. Any guides that depend upon this guide are shown to the right of this guide.
For customer access to all SBA guides: http://www.cisco.com/go/sba
For partner access: http://www.cisco.com/go/sbachannel

February 2012 Series
Introduction

For Cisco partners and customers with 2000–10,000 connected users, we have created an “out-of-the-box” deployment that is simple, fast, affordable, scalable, and flexible. We have designed it to be easy—easy to configure, deploy, and manage.

The simplicity of this deployment, though, belies the depth and breadth of the architecture. Based on feedback from many customers and partners, Cisco has developed a solid network foundation with a flexible platform that does not require re-engineering to support additional Network or User services.

The Smart Business Architecture (SBA) Borderless Networks (BN) for Enterprise Organizations architecture is comprised of a single Design Guide, and Deployment guides and Configuration guides for each of the three sections: LAN, WAN, and Internet Edge.

The SBA BN for Enterprise Organizations Internet Edge Deployment Guide is a prescriptive reference design that provides step-by-step instructions for the deployment of the products in the design. It is based on Enterprise best practice principles. Based on feedback from customers and partners, Cisco has developed a solid network foundation as a flexible platform that does not require reengineering to include additional Network or User services.

This deployment guide has been architected to make your life a little bit—maybe even a lot—smoother. This architecture:

- Provides a solid foundation
- Makes deployment fast and easy
- Accelerates ability to easily deploy additional services
- Avoids the need for re-engineering of the core network

The Purpose of This Document

This document provides the available configuration files for the products used in the Smart Business Architecture Borderless Networks for Enterprise Organizations Internet Edge Deployment Guide. It is a companion document to the deployment guide as a reference for engineers who are evaluating or deploying the Smart Business Architecture.

Graphical Interface Management

There are products in this design where we have omitted the configuration file. Those products have browser-based graphical configuration tools. Please refer to the companion Smart Business Architecture Borderless Networks for Enterprise Organizations WAN Deployment Guide at http://www.cisco.com/go/sba for step-by-step instructions on configuring those products.
Smart Business Architecture Borderless Networks for Enterprise Organizations

February 2012 Series

Introduction
## Enterprise Organizations Deployment Product List

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Product</th>
<th>Part Numbers</th>
<th>Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internet Edge 5K</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall</td>
<td>ASA 5510 or</td>
<td>ASA5510-AIP10-SP-K9</td>
<td>8.4.2</td>
</tr>
<tr>
<td></td>
<td>ASA 5520 or</td>
<td>ASA5520-AIP20-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ASA 5540</td>
<td>ASA5540-AIP40-K9</td>
<td></td>
</tr>
<tr>
<td>IPS</td>
<td>SSM-AIP-10 or</td>
<td>*part of the firewall bundle</td>
<td>7.0.5aE4</td>
</tr>
<tr>
<td></td>
<td>SSM-AIP-20 or</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SSM-AIP-40</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software license for main ASA</td>
<td>250 or 500 SSL Session</td>
<td>ASA5500-SSL-250</td>
<td>*as Firewall</td>
</tr>
<tr>
<td>FW</td>
<td>license</td>
<td>ASA5500-SSL-500</td>
<td></td>
</tr>
<tr>
<td>Email Security</td>
<td>C370</td>
<td>C370-BUN-R-NA</td>
<td>Async OS 7.1.5-017</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*Please consult Trusted Partner or IronPort Sales Team for pricing and licensing</td>
<td></td>
</tr>
<tr>
<td>Web Security</td>
<td>S370</td>
<td>S370-BUN-R-NA</td>
<td>Async OS 7.1.2-080</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*Please consult Trusted Partner or IronPort Sales Team for pricing and licensing</td>
<td></td>
</tr>
<tr>
<td>Server Load Balancing</td>
<td>ACE 4710</td>
<td>ACE-4710-0.5F-K9</td>
<td>A5.1</td>
</tr>
<tr>
<td>Outside Switch</td>
<td>Catalyst 2960S</td>
<td>WS-C2960S-24TS-L</td>
<td>15.0(1)SE1</td>
</tr>
<tr>
<td>DMZ Switch</td>
<td>Catalyst 3750X</td>
<td>WS-C3750X-24T-S</td>
<td>15.0(1)SE1</td>
</tr>
<tr>
<td>Functional Area</td>
<td>Product</td>
<td>Part Numbers</td>
<td>Software Version</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------------------</td>
<td>-----------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Internet Edge 10K</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall</td>
<td>ASA 5520 or ASA 5540</td>
<td>ASA5520-AIP20-K9</td>
<td>8.4.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ASA5540-AIP40-K9</td>
<td></td>
</tr>
<tr>
<td>IPS</td>
<td>SSM-AIP-20 or SSM-AIP-40</td>
<td>*part of bundle above</td>
<td>7.0.5aE4</td>
</tr>
<tr>
<td>VPN</td>
<td>ASA 5520 and 500 SSL seats or ASA 5540 and 1000 SSL seats</td>
<td>ASA5520-SSL500-K9</td>
<td>8.4.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ASA5540-SSL1000-K9</td>
<td></td>
</tr>
<tr>
<td>Email Security</td>
<td>C370</td>
<td>C370-BUN-R-NA</td>
<td>Async OS 7.1.5-017</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*Please consult Trusted Partner or IronPort Sales Team for pricing and licensing</td>
<td></td>
</tr>
<tr>
<td>Web Security</td>
<td>S370</td>
<td>S370-BUN-R-NA</td>
<td>Async OS 7.1.2-080</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*Please consult Trusted Partner or IronPort Sales Team for pricing and licensing</td>
<td></td>
</tr>
<tr>
<td>Server Load Balancing</td>
<td>ACE 4710</td>
<td>ACE-4710-1F-K9</td>
<td>A5.1</td>
</tr>
<tr>
<td>Outside Switch</td>
<td>Catalyst 2960S</td>
<td>WS-C2960S-24TS-L</td>
<td>15.0(1)SE1</td>
</tr>
<tr>
<td>DMZ Switch</td>
<td>Catalyst 3750X</td>
<td>WS-C3750X-24T-S</td>
<td>15.0(1)SE1</td>
</tr>
</tbody>
</table>
Internet Edge Configuration Files

ASA 5540
Internet Edge Firewall and Remote Access VPN

The Cisco ASA firewall family sits between the organization’s internal network and the Internet, and is a fundamental infrastructural component that minimizes the impact of network intrusions while maintaining worker productivity and data security.

ASA Version 8.4(2)
!
hostname IE-ASA5540
domain-name cisco.local
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0/0
   nameif inside
   security-level 100
   ip address 10.4.24.30 255.255.255.224 standby 10.4.24.29
   summary-address eigrp 100 10.4.28.0 255.255.252.0 5
!
interface GigabitEthernet0/1
   description Trunk to DMZ-3750X GigabitEthernet X/0/24
   nameif dmz-mail
   security-level 50
   ip address 192.168.17.1 255.255.255.0 standby 192.168.17.2
!
interface GigabitEthernet0/1.1116
   description Web server DMZ connection on VLAN 1116
   nameif dmz-web
   security-level 50
   ip address 192.168.16.1 255.255.255.0 standby 192.168.16.2
!
interface GigabitEthernet0/1.1117
   description Email Security Appliance DMZ Connection on VLAN 1117
   vlan 1117
   nameif dmz-mail
   security-level 50
   ip address 192.168.17.1 255.255.255.0 standby 192.168.17.2
!
interface GigabitEthernet0/1.1123
   description Management DMZ connection on VLAN 1123
   vlan 1123
   nameif dmz-management
   security-level 50
   ip address 192.168.23.1 255.255.255.0 standby 192.168.23.2
!
interface GigabitEthernet0/2
   description LAN/STATE Failover Interface
!
interface GigabitEthernet0/3
   description Trunk to OUT-2960S GigabitEthernet X/0/24
   no nameif
   no security-level
   no ip address
!
interface GigabitEthernet0/3.16
   description Primary Internet connection on VLAN 16
   vlan 16
   nameif outside-16
   security-level 0
   ip address 172.16.130.124 255.255.255.0 standby 172.16.130.123
!
interface GigabitEthernet0/3.17
   description Resilient Internet connection on VLAN 17
   vlan 17
nameif outside-17
  security-level 0
  ip address 172.17.130.124 255.255.255.0 standby 172.17.130.123
interface Management0/0
  shutdown
  nameif management
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  management-only
!
ftp mode passive
clock timezone PST -8
clock summer-time PDT recurring
dns server-group DefaultDNS
domain-name cisco.local
same-security-traffic permit intra-interface
object network internal-network
  subnet 10.4.0.0 255.254.0.0
  description The organization’s internal network range
object network dmz-networks
  subnet 192.168.16.0 255.255.248.0
  description The organization’s DMZ network range
object network internal-network-ISPa
  subnet 10.4.0.0 255.254.0.0
  description PAT traffic from inside out the primary internet connection
object network internal-network-ISPb
  subnet 10.4.0.0 255.254.0.0
  description PAT traffic from inside out the resilient internet connection
object network outside-webserver-ISPa
  host 172.16.130.100
  description Webserver on ISP A
object network dmz-webserver-ISPa
  host 192.168.16.100
  description NAT the webserver in the DMZ to the outside address on ISP A
object network dmz-webserver-ISPb
  host 192.168.16.100
  description NAT the webserver in the DMZ to the outside address on ISP B
object network outside-webserver-ISPb
  host 172.17.130.100
  description Webserver on ISP B
object network NETWORK_OBJ_10.4.28.0_22
  subnet 10.4.28.0 255.255.252.0
object network outside-esa-ISPa
  host 172.16.130.25
  description ESA on ISP A
object network dmz-esa-ISPa
  host 192.168.17.25
  description NAT the ESA in the DMZ to the outside address on ISP A
object network dmz-esa-ISPb
  host 192.168.17.25
  description NAT the ESA in the DMZ to the outside address on ISP B
object network internal-dns
  host 10.4.48.10
  description DNS in the internal data center
object network internal-exchange
  host 10.4.48.25
  description Exchange server in the internal data center
object network internal-ntp
  host 10.4.48.17
  description NTP server in the internal data center
object-group service DM_INLINE_SERVICE_1
  service-object tcp destination eq ftp
  service-object tcp destination eq ftp-data
  service-object tcp destination eq tacacs
  service-object udp destination eq ntp
  service-object udp destination eq syslog
object-group service DM_INLINE_TCP_1 tcp
  port-object eq www
  port-object eq https
object-group service DM_INLINE_SERVICE_2
  service-object tcp destination eq domain
service-object udp destination eq domain
object-group network DM_INLINE_NETWORK_1
network-object 10.0.0.0 255.0.0.0
network-object 172.16.0.0 255.255.0.0
network-object 192.68.0.0 255.255.255.192
access-list global_access remark Permit management protocols from
the DMZ to the internal network
access-list global_access extended permit object-group DM_INLINE_ SERVICE_1 192.168.23.0 255.255.255.0 object internal-network
access-list global_access remark Allow anyone to access the
webserver in the DMZ
access-list global_access extended permit tcp any 192.168.16.0
255.255.255.0 object-group DM_INLINE_TCP_1
access-list global_access remark Permit the mail DMZ to sync with
the internal NTP server
access-list global_access extended permit udp 192.168.17.0
255.255.255.0 object internal-ntp eq ntp
access-list global_access remark The mail DMZ to do
lookups on the internal DNS
access-list global_access extended permit object-group DM_INLINE_ SERVICE_2 192.168.17.0 255.255.255.0 object internal-dns
access-list global_access remark Permit the mail DMZ to send SMTP
to the internal exchange server
access-list global_access extended permit tcp 192.168.17.0
255.255.255.0 object internal-exchange eq smtp
access-list global_access remark Permit SMTP traffic into the
email DMZ
access-list global_access extended permit tcp any 192.168.17.0
255.255.255.0 eq smtp
access-list global_access remark Deny traffic from any DMZ
network
access-list global_access extended deny ip object dmz-networks
any
access-list global_access remark Deny the use of telnet from the
internal network to external networks
access-list global_access extended deny tcp object internal-
network any eq telnet
access-list global_access remark Permit IP traffic from the
internal network to external networks
access-list global_access extended permit ip object internal-
etwork any log disable
access-list global_mpc extended permit ip any any
access-list RA_PartnerACL remark Partners can access this
internal host only
access-list RA_PartnerACL standard permit host 10.4.48.35
access-list RA_SplitTunnelACL remark Internal networks
access-list RA_SplitTunnelACL standard permit 10.4.0.0
255.254.0.0
access-list RA_SplitTunnelACL remark DMZ networks
access-list RA_SplitTunnelACL standard permit 192.168.16.0
255.254.248.0
access-list WCCP_Redirect remark Do not WCCP redirect connections
to these addresses
access-list WCCP_Redirect extended deny ip any object-group DM_ INLINE_NETWORK_1
access-list WCCP_Redirect remark WCCP redirect all other IP
addresses
access-list WCCP_Redirect extended permit ip any any
pager lines 24
logging enable
logging buffered informational
logging asdm informational
mtu inside 1500
mtu dmz-web 1500
mtu dmz-management 1500
mtu outside-16 1500
mtu outside-17 1500
mtu management 1500
mtu dmz-mail 1500
ip local pool RA-pool 10.4.28.1-10.4.31.255 mask 255.255.252.0
failover
failover lan unit primary
failover lan interface failover GigabitEthernet0/2
failover polltime unit msec 200 holdtime msec 800
failover polltime interface msec 500 holdtime 5
failover key *****
failover replication http
failover link failover GigabitEthernet0/2
failover interface ip failover 10.4.24.33 255.255.255.224 standby 10.4.24.34
monitor-interface dmz-web
monitor-interface dmz-management
monitor-interface outside-16
monitor-interface outside-17
monitor-interface dmz-mail
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
nat (inside, outside-16) source static any any destination static NETWORK_OBJ_10.4.28.0_22 NETWORK_OBJ_10.4.28.0_22 no-proxy-arp
route-lookup

object network internal-network-ISPa
  nat (any, outside-16) dynamic interface
object network internal-network-ISPb
  nat (any, outside-17) dynamic interface
object network dmz-webserver-ISPa
  nat (any, outside-16) static outside-webserver-ISPa
object network dmz-webserver-ISPb
  nat (any, outside-17) static outside-webserver-ISPb
object network dmz-esa-ISPa
  nat (any, outside-16) static outside-esa-ISPa
access-group global_access global

! router eigrp 100
  no auto-summary
  network 10.4.24.0 255.255.252.0
  network 192.168.16.0 255.255.248.0
  passive-interface default
  no passive-interface inside
  redistribute static

! route outside-16 0.0.0.0 0.0.0.0 172.16.130.126 128 track 1
route outside-17 0.0.0.0 0.0.0.0 172.17.130.126 254
route outside-16 172.18.1.1 255.255.255.255 172.16.130.126 1
route inside 0.0.0.0 0.0.0.0 10.4.24.1 tunneled
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
mgcp-pat 0:05:00
timeout sip 0:30:00 sip media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
aaa-server AAA-SERVER protocol tacacs+
  aaa-server AAA-SERVER (inside) host 10.4.48.15 key *****
  aaa-server AAA-SERVER (inside) host 10.4.48.15 timeout 5 key *****
user-identity default-domain LOCAL
aaa authentication enable console AAA-SERVER LOCAL
aaa authentication ssh console AAA-SERVER LOCAL
aaa authentication http console AAA-SERVER LOCAL
aaa authentication serial console AAA-SERVER LOCAL
aaa authentication serial console AAA-SERVER LOCAL
aaa authorization exec authentication-server
http server enable
http 192.168.1.0 255.255.255.0 management
http 10.4.0.0 255.254.0.0 inside
snmp-server host inside 10.4.48.35 community ***** version 2c
no snmp-server location
no snmp-server contact
snmp-server community *****
snmp-server enable traps snmp authentication linkup linkdown
coldstart warmstart
sla monitor 16
type echo protocol ipIcmpEcho 172.18.1.1 interface outside-16
sla monitor schedule 16 life forever start-time now
crypto ca trustpoint ASDM_TrustPoint0
  enrollment self
  subject-name CN=IE-ASA5540.cisco.local
  proxy-1dc-issuer
crl configure
!
track 1 rtr 16 reachability
telnet timeout 5
ssh 10.4.0.0 255.254.0.0 inside
ssh timeout 5
ssh version 2
console timeout 0
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
wccp 90 redirect-list WCCP_Redirect
wccp interface inside 90 redirect in
ntp server 10.4.48.17
ssl trust-point ASDM_TrustPoint0 outside-17
ssl trust-point ASDM_TrustPoint0 outside-16
webvpn
enable outside-16
enable outside-17
anyconnect image disk0:/anyconnect-linux-64-3.0.3054-k9.pkg 1
anyconnect image disk0:/anyconnect-macosx-1386-3.0.3054-k9.pkg 2
anyconnect image disk0:/anyconnect-win-3.0.3054-k9.pkg 3
anyconnect profiles ra_profile disk0:/ra_profile.xml
anyconnect enable
tunnel-group-list enable
group-policy GroupPolicy_AnyConnect internal
group-policy GroupPolicy_AnyConnect attributes
wins-server none
dns-server value 10.4.48.10
vpn-tunnel-protocol ssl-client
default-domain value cisco.local
webvpn
  anyconnect profiles value ra_profile type user
group-policy GroupPolicy_Administrators internal
group-policy GroupPolicy_Administrators attributes
  banner value Your access is via an unrestricted split tunnel.
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value RA_SplitTunnelACL
webvpn
  anyconnect profiles value ra_profile type user
group-policy GroupPolicy_Partner internal
group-policy GroupPolicy_Partner attributes
  banner value Your access is restricted to the partner server
  vpn-filter value RA_PartnerACL
webvpn
  anyconnect profiles value ra_profile type user
username admin password w2y.6Op4j7clVdk2 encrypted privilege 15
tunnel-group AnyConnect type remote-access
tunnel-group AnyConnect general-attributes
  address-pool RA-pool
authentication-server-group AAA-RADIUS
default-group-policy GroupPolicy_AnyConnect
tunnel-group AnyConnect webvpn-attributes
group-alias AnyConnect enable
group-url https://172.16.130.124/AnyConnect enable
group-url https://172.17.130.124/AnyConnect enable
!
class-map global-class
  match access-list global_mpc
class-map inspection_default
  match default-inspection-traffic
!
!policy-map type inspect dns preset_dns_map
ASA AIP SSM-40
Internet Edge Intrusion Prevention

This design employs the Cisco Adaptive Inspection Prevention Security Service Module (AIP-SSM) for IPS services in the Internet Edge Cisco ASA 5500 series firewalls.

service interface
exit

! ------------------------------

service authentication
exit

! ------------------------------

service event-action-rules rules0
exit

! ------------------------------

service host
network-settings
host-ip 10.4.24.27/27, 10.4.24.1
host-name IE-SSM40a
telnet-option disabled
access-list 10.4.0.0/15
dns-primary-server enabled
address 10.4.48.10
exit
dns-secondary-server disabled
dns-tertiary-server disabled
exit
time-zone-settings
offset -480
standard-time-zone-name GMT-08:00
exit
ntp-option enabled-ntp-unauthenticated
ntp-server 10.4.48.17
exit
summertime-option recurring
summertime-zone-name PDT
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service global-correlation
network-participation partial
exit
! ------------------------------
service aaa
aaa local

exit
! ------------------------------
service analysis-engine
virtual-sensor vs0
physical-interface GigabitEthernet0/1
exit
exit

Catalyst 2960-S Series Switch
Outside Switch

The Cisco Catalyst 2960-S Series are fixed-configuration, stackable, 10/10/1000 Ethernet switches, with PoE+ and non-powered versions designed for entry-level enterprise, midmarket, and remote-site networks.

version 15.0
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption

hostname OUT-2960S

enable secret 5 $1$mpDc$yDf4S8EBxGx3BhpwJRGin0
username admin password 7 0007421507545A545C
aaa new-model

aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization exec default group tacacs+ local
aaa session-id common

clock timezone PST -8 0
clock summer-time PDT recurring

switch 1 provision ws-c2960s-24pd-l
switch 2 provision ws-c2960s-24pd-l

stack-mac persistent timer 0

ip domain-name cisco.local
vtp mode transparent
udld enable

mls qos map cos-dscp 0 8 16 24 32 46 48 56

mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40 41 42 43 44 45
mls qos srr-queue output dscp-map queue 1 threshold 3 46 47
mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28 29 30 31 34 35
mls qos srr-queue output dscp-map queue 2 threshold 1 36 37 38 39
mls qos srr-queue output dscp-map queue 2 threshold 2 24
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3 4 5 6 7
mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11 13

mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
mls qos queue-set output 1 threshold 1 100 100 50 200
mls qos queue-set output 1 threshold 2 125 125 100 400
mls qos queue-set output 1 threshold 3 100 100 100 400
mls qos queue-set output 1 threshold 4 60 150 50 200
mls qos queue-set output 1 buffers 15 25 40 20
mls qos

crypto pki trustpoint TP-self-signed-2484937856
       enrollment selfsigned
       subject-name cn=IOS-Self-Signed-Certificate-2484937856
       revocation-check none
       rsakeypair TP-self-signed-2484937856

crypto pki certificate chain TP-self-signed-2484937856
certificate self-signed 02
        3082024D 308201B6 A0030201 02020102 300D0609 2A864886 F70D0101 04050030
        31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
43657274 69666963 6174652D 32343834 39333738 3536301E 170D3933 30333031 30303035 33355A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
70D3933 30333031 30303030 305A3031 312F302D 06035504 03132649
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 34383439
33373835 3630819F 300D0609 2A864886 F70D0101 01050003 81BD0030 81BD0092
81BD0281 8100A3B4 2A6BF845 BE1DC160 16BC6F54 748DD1D9 2268A32B E60C05F6 4EBF7F29
80D14119 FBDAAEF7 B58A239C 98454878 4F0E5B72 EF73A8B6 199B89A3 625EE067 6B3D9654 2D13F9A9 AE0EC8FF BB52B857 3C7ABD21 A854063D 7D00E5F1 8996F23D BA3F2CF8 658ECBD0 B612EE90 BA3D6AB 0FEBBB43 F525DAE7 B9F4D064
ip ssh version 2
!
!
macro name EgressQoS
mls qos trust dscp
queue-set 2
srr-queue bandwidth share 1 30 35 5
priority-queue out
@
!
interface FastEthernet0
description DMZ-3750X Gig1/0/3
ip address 192.168.23.6 255.255.255.0
!
interface GigabitEthernet1/0/1
!
interface GigabitEthernet1/0/20
description VPN-ASA5520 Gig0/3
switchport trunk allowed vlan 16,17
switchport mode trunk
logging event link-status
logging event trunk-status
shutdown
@
interface GigabitEthernet1/0/21
@
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
  description ISP-A
  switchport access vlan 16
  switchport mode access
  speed 100
duplex full
spanning-tree portfast!
interface GigabitEthernet1/0/24
  description IE-ASA5540b Gig0/3
  switchport trunk allowed vlan 16,17
  switchport mode trunk
logging event link-status
logging event trunk-status!
interface GigabitEthernet1/0/25
!
interface GigabitEthernet1/0/26
!
interface TenGigabitEthernet1/0/1
!
interface TenGigabitEthernet1/0/2
!
interface GigabitEthernet2/0/1
!
interface GigabitEthernet2/0/20
  description VPN-ASA5520 Gig0/3
  switchport trunk allowed vlan 16,17
  switchport mode trunk
logging event link-status
logging event trunk-status!
interface GigabitEthernet2/0/21
!
interface GigabitEthernet2/0/22
!
interface GigabitEthernet2/0/23
  description ISP-B
  switchport access vlan 17
  switchport mode access
  speed 100
duplex full
spanning-tree portfast!
interface GigabitEthernet2/0/24
  switchport trunk allowed vlan 16,17
  switchport mode trunk
logging event link-status
logging event trunk-status!
interface GigabitEthernet2/0/25
!
interface GigabitEthernet2/0/26
!
interface TenGigabitEthernet2/0/1
!
interface TenGigabitEthernet2/0/2
!
interface Vlan1
  no ip address
shutdown!
interface GigabitEthernet2/0/20
  description VPN-ASA5520 Gig0/3
  switchport trunk allowed vlan 16,17
  switchport mode trunk
logging event link-status
ip default-gateway 192.168.23.1
no ip http server
ip http authentication aaa
ip http secure-server
logging event trunk-status
shutdown!
Internet Edge Configuration Files

logging 10.4.48.35
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server system-shutdown
tacacs-server host 10.4.48.15 key 7 0812494D1B1C113C1712

line con 0
line vty 0 4
  transport input ssh
line vty 5 15
  transport input ssh
ntp server 10.4.48.17
end

Catalyst 3750-X Series Switch
DMZ Switch

The Cisco Catalyst 3750-X Series are fixed-port, stackable, 10/100/1000 Ethernet switches, with PoE+ and non-powered versions, that provide enhanced resiliency through the StackWise Plus and StackPower technologies.

version 15.0
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption

hostname DMZ-3750X

boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$ESPv$1llgFChdUfJ/JGgEszj.3.

username admin password 7 070C705F4D06485744
aaa new-model

aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization exec default group tacacs+ local

aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
switch 1 provision ws-c3750x-24
switch 2 provision ws-c3750x-24
stack-mac persistent timer 0
system mtu routing 1500
!
!
!
ip domain-name cisco.local
vtp mode transparent
udld enable
!
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue input bandwidth 70 30
mls qos srr-queue input threshold 1 80 90
mls qos srr-queue input priority-queue 2 bandwidth 30
mls qos srr-queue input cos-map queue 1 threshold 2 3
mls qos srr-queue input cos-map queue 1 threshold 3 6 7
mls qos srr-queue input cos-map queue 2 threshold 1 4
mls qos srr-queue input dscp-map queue 1 threshold 2 24
mls qos srr-queue input dscp-map queue 1 threshold 3 48 49 50 51
crypto pki trustpoint TP-self-signed-4251942912
    enrollment selfsigned
    subject-name cn=IOS-Self-Signed-Certificate-4251942912
    revocation-check none
    rsakeypair TP-self-signed-4251942912

crypto pki certificate chain TP-self-signed-4251942912
    certificate self-signed 01
      3082024D 308201B6 A0030201 02020101 300D0609 2A864886 F70D0101
      04050030
      31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D
      43657274
      6966696D 6174652D 34323531 39343239 3132301E 170D3933 30333031
      30303330
      3D35A17 0D323030 31303130 30303030 305A3031 312F302D 06035504
      03132649
      4F532D53 656C662D 5369676E 65642D43 65727469 66696666 7465642D
      32353139
      34323931 3230819F 300D0609 2A864886 F70D0101 01050003 81BD0030
      81890281
      8100CDF2 51F7000A E5C16406 B5DF1793 F0564644 30D4AA66 ED2E3B45
      3D7C02E9
      A052FC2A 111F4EA8 74EF4519 5F4E4F96 57F4497B 2F3CE90B 0A41A8AF
      A44BC629
      45AF9E56 10FA5AC6 166E15CA 44F61B88 7995EC7D FB8E8AFA 4BB2A87A
      FEAE1ED6
      F49779B1 0698BFAC 367CCF61 F5342DCE 98CC54A7 FF4C51E1 E7CF7536
      4AA9BC9E
      E3110203 010001A3 75307330 0F060355 1D130101 FF040530 030101FF
      30200603
      551D1104 19301782 154445DA 2D333735 30582E63 6973636F 2E6C6F63
      616C301F
      0603515D 23041830 168014EC 2B66755D EB85B077 14DCDB99 57285F88
      157EE930
      1D060355 1D0E0416 0414EC2B 66755DE8 B5B07714 DCDB9957 285F8815
      7E9300D

52 53 54 55
mls qos srr-queue input dscp-map queue 1 threshold 3 56 57 58 59
60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 32 33 40 41
42 43 44 45
mls qos srr-queue input dscp-map queue 2 threshold 3 46 47
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40 41
42 43 44 45
mls qos srr-queue output dscp-map queue 1 threshold 3 46 47
mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18 19
20 21 22 23
mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28 29
30 31 34 35
mls qos srr-queue output dscp-map queue 2 threshold 1 36 37 38 39
mls qos srr-queue output dscp-map queue 2 threshold 2 24
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51
52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59
60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3 4 5
6 7
mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11 13
15
mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
mls qos queue-set output 1 threshold 1 100 100 50 200
mls qos queue-set output 1 threshold 2 125 125 100 400
mls qos queue-set output 1 threshold 3 100 100 100 400
mls qos queue-set output 1 threshold 4 60 150 50 200
mls qos queue-set output 1 buffers 15 25 40 20
mls qos !
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1116-1119,1122-1124,1128 priority 24576
!
!
!port-channel load-balance src-dst-ip
!
vlan internal allocation policy ascending
!
vlan 1116-1119,1122-1124,1128
!
ip ssh version 2
!
!
macro name EgressQoS
mls qos trust dscp
queue-set 2
srr-queue bandwidth share 1 30 35 5
priority-queue out
@
!
interface Port-channel10
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1116,1119,1122-1124,1128
switchport mode trunk
logging event link-status
!
interface Port-channel11
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1116,1123,1124
switchport mode trunk
logging event link-status
!
interface Port-channel12
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1119,1128
switchport mode trunk
logging event link-status
!
interface FastEthernet0
no ip address
!
interface GigabitEthernet1/0/1
description DMZ-WLC_Guest-1 Gig0/0/1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1119,1128
switchport mode trunk
logging event link-status
logging event trunk-status
logging event bundle-status
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-group 12 mode on
!
interface GigabitEthernet1/0/2
description Webserver
switchport access vlan 1116
switchport mode access
logging event link-status
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
spanning-tree portfast
!
interface GigabitEthernet1/0/3
description DMZ-ACS4710a gigabitEthernet 1/1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1116,1123,1124
switchport mode trunk
logging event link-status
logging event trunk-status
logging event bundle-status
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-group 10 mode on
!
interface GigabitEthernet1/0/4
description DMZ-ACS4710b gigabitEthernet 1/1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1116,1123,1124
switchport mode trunk
logging event link-status
logging event trunk-status
logging event bundle-status
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-group 11 mode on
!
interface GigabitEthernet1/0/5
!
interface GigabitEthernet1/0/6
!
interface GigabitEthernet1/0/7
description VPN-ASR1002-1
switchport access vlan 1118
switchport mode access
logging event link-status
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
spanning-tree portfast
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
description OUT-2960Sa Fas0
switchport access vlan 1123
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22

description DMZ-ESAc370
switchport access vlan 1117
switchport mode access
logging event link-status
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
spanning-tree portfast
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24

description IE-ASA5540b Gig0/1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1116-1119,1122,1123,1128
switchport mode trunk
logging event link-status
logging event trunk-status
logging event bundle-status
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-group 12 mode on
!
interface GigabitEthernet2/0/1

description DMZ-WLC_Guest-1 Gig0/0/2
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1119,1128
switchport mode trunk
logging event link-status
logging event trunk-status
logging event bundle-status
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-group 12 mode on
!
interface GigabitEthernet2/0/2
!
interface GigabitEthernet2/0/3

description DMZ-ACS4710a gigabitEthernet 1/2
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1116,1123,1124
switchport mode trunk
logging event link-status
logging event trunk-status
logging event bundle-status
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-group 10 mode on
interface GigabitEthernet2/0/4
description DMZ-ACS4710b gigabitEthernet 1/2
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1116,1123,1124
switchport mode trunk
logging event link-status
logging event trunk-status
logging event bundle-status
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
channel-group 1 mode on
! interface GigabitEthernet2/0/5
! interface GigabitEthernet2/0/6
! interface GigabitEthernet2/0/7
description VPN-ASR1001-2 Gig0/3
switchport access vlan 1118
switchport mode access
logging event link-status
srr-queue bandwidth share 1 30 35 5
queue-set 2
priority-queue out
mls qos trust dscp
macro description EgressQoS
spanning-tree portfast
! interface GigabitEthernet2/0/8
! interface GigabitEthernet2/0/9
! interface GigabitEthernet2/0/10
! interface GigabitEthernet2/0/11
! interface GigabitEthernet2/0/12
! interface GigabitEthernet2/0/13
! interface GigabitEthernet2/0/14
! interface GigabitEthernet2/0/15
! interface GigabitEthernet2/0/16
! interface GigabitEthernet2/0/17
description OUT-2960Sa Fas0
switchport access vlan 1123
switchport mode access
spanning-tree portfast
! interface GigabitEthernet2/0/18
! interface GigabitEthernet2/0/19
! interface GigabitEthernet2/0/20
! interface GigabitEthernet2/0/21
!
interface GigabitEthernet2/0/22
!
interface GigabitEthernet2/0/23
!
interface GigabitEthernet2/0/24
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1116-1119,1122,1123,1128
  switchport mode trunk
  logging event link-status
  logging event trunk-status
  srr-queue bandwidth share 1 30 35 5
  queue-set 2
  priority-queue out
  mls qos trust dscp
  macro description EgressQoS
!
interface GigabitEthernet2/1/1
!
interface GigabitEthernet2/1/2
!
interface GigabitEthernet2/1/3
!
interface GigabitEthernet2/1/4
!
interface TenGigabitEthernet2/1/1
!
interface TenGigabitEthernet2/1/2
!
interface Vlan1
  no ip address
!
interface Vlan1123
  description In-band Management
  ip address 192.168.23.5 255.255.255.0
!
ip default-gateway 192.168.23.1

ip http server
ip http authentication aaa
ip http secure-server
!
logging esm config
logging 10.4.48.35
!
snmp-server community cisco RO
snmp-server community cisco123 RW
snmp-server system-shutdown
tacacs-server host 10.4.48.15 key 7 0812494D1B1C113C1712
!
!
!
!
line con 0
line vty 0 4
  transport input ssh
line vty 5 15
  transport input ssh
!
ntp server 10.4.48.17
end
Catalyst 3750-X Series Switch
LAN Distribution Switch

Configured as a single unit, but has independent load-sharing power supplies and processor for each switch in the StackWise Plus stack. The SBA for Enterprise Organizations—Borderless Network Architecture uses a pair of stacked 3750X switches that provide Layer 2 and Layer 3 switching.

version 15.0
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption

hostname IE-D3750X

boot-start-marker
boot-end-marker

enable secret 5 $1$wAhq$ITSE1YWfHimX3j/F6dWIT1

username admin password 7 104D580A061843595F

aaa new-model

aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization exec default group tacacs+ local

aaa session-id common
clock timezone PST -8 0
clock summer-time PDT recurring
switch 1 provision ws-c3750x-24
switch 2 provision ws-c3750x-24p

stack-mac persistent timer 0
system mtu routing 1500
ip routing

! ip domain-name cisco.local
ip multicast-routing distributed
vtp mode transparent
udld enable

! mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue input bandwidth 70 30
mls qos srr-queue input threshold 1 80 90
mls qos srr-queue input priority-queue 2 bandwidth 30
mls qos srr-queue input cos-map queue 1 threshold 2 3
mls qos srr-queue input cos-map queue 1 threshold 3 6 7
mls qos srr-queue input cos-map queue 2 threshold 1 4
mls qos srr-queue input dscp-map queue 1 threshold 2 24
mls qos srr-queue input dscp-map queue 1 threshold 3 48 49 50 51 52 53 54 55
mls qos srr-queue input dscp-map queue 1 threshold 3 56 57 58 59 60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 32 33 40 41 42 43 44 45
mls qos srr-queue input dscp-map queue 2 threshold 3 46 47
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 3 threshold 3 6 7
mls qos srr-queue output cos-map queue 4 threshold 3 1
mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40 41 42 43 44 45
mls qos srr-queue output dscp-map queue 2 threshold 3 46 47
mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18 19
mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28 29
mls qos srr-queue output dscp-map queue 2 threshold 1 36 37 38 39
mls qos srr-queue output dscp-map queue 2 threshold 2 24
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51
mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3 4 5
mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11 13
mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
mls qos queue-set output 1 threshold 1 100 100 50 200
mls qos queue-set output 1 threshold 2 125 125 100 400
mls qos queue-set output 1 threshold 3 100 100 100 400
mls qos queue-set output 1 threshold 4 60 150 50 200
mls qos queue-set output 1 buffers 15 25 40 20

crypto pki trustpoint TP-self-signed-3109522944
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-3109522944
  revocation-check none
  rsakeypair TP-self-signed-3109522944


crypto pki certificate chain TP-self-signed-3109522944
  certificate self-signed 01
    3082024D 308201B6 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
    31312F30 2D060355 04031326 49F532D3 53656C66 2D536967 6E65626D
    43657274
    69666963 6174652D 33313039 35323239 3434301E 170D3933 30333031
    30303038
    31365A17 0D323030 31303130 30303030 305A3031 312F302D 06035504

  certificate self-signed 02
    4F532D53 656C662D 5365626D 2D536967 6E65626D 30303030 305A3031 312F302D
    03030030
    32323934 3430819F 300D0609 2A864886 F70D0101 01050003 81BD0030
    81890281
    8100CBA6 8723FB92 308B472E 65011583 07218F7D 83D454E5 76830F54
    0FC5363B
    B30C6415 C9920269 137347AA E3FBBE50 70E701E2 0CA2A4E5 F97182CB
    21EA6914
    8EA7F5C7 14B39413 C5291C03 43A060DF 2D71B634 9B4608C4 26632FBB
    73E93C85
    55ADD3DF 825CD7A8 6F9C5182 6A6FD68C EBC90ABC 95B188A 36400029
    8CCD668F
    E1210203 010010A3 75307330 0F060355 1D130101 FF040503 030101FF
    30200603
    551D1104 19301782 1549452D 44333735 30582E63 6973636F 2E6C6663
    61C301F
    0603551D 23041830 16801466 731184E9 202FEE6C 1342C9DF 2E0DF45B
    A2C093F0
    1D060355 1D0E0416 04146673 118EA420 2F92EC61 324CD2F2 0DF45BA2
    2C9F300D
    06092896 4886F70D 01010405 00038181 00828331 0A95A46A E92B93A1
    C1FF774D
    5217EFDF 0EE83857 CE909CBA EF55D4C2 F380AE12 1AD92685 85EC11C2
    DC15B2C1
    D51364A3 4A8E9032 6E8516BC 69257136 57E76D63 490376CB 7A33F9E6
    3E67133B
    B8B013CC C7DE773D 75ABDFB9 AB193FCA 2FC792FC 9CF09431 F8C87255
    B9898DAB
    BD8170A7 37F56249 BA0DAADC ADDE3994 AB
    quit
  license boot level ipservices
  license boot level ipservices switch 2
  spanning-tree mode rapid-pvst
  spanning-tree extend system-id
  spanning-tree vlan 300 priority 24576
port-channel load-balance src-dst-ip

vlan internal allocation policy ascending

vlan 300
  name InternetEdge

ip ssh source-interface Loopback0
ip ssh version 2

macro name EgressQoS
  mls qos trust dscp
  queue-set 2
  srr-queue bandwidth share 1 30 35 5
  priority-queue out
@

interface Loopback0
  ip address 10.4.40.251 255.255.255.255
  ip pim sparse-mode

interface FastEthernet0
  no ip address
  no ip route-cache cef
  no ip route-cache
  shutdown

interface GigabitEthernet1/0/1

interface GigabitEthernet1/0/19
  description IE-SSM40a
  switchport access vlan 300
  switchport mode access
  spanning-tree portfast

interface GigabitEthernet1/0/20

interface GigabitEthernet1/0/21

interface GigabitEthernet1/0/22
  description WSAs370 M1
  switchport access vlan 300
  switchport mode access
  spanning-tree portfast

interface GigabitEthernet1/0/23

interface GigabitEthernet1/0/24
  description IE-ASA5540a Gig0/0
  switchport access vlan 300
  switchport mode access
  spanning-tree portfast

interface GigabitEthernet1/1/1

interface GigabitEthernet1/1/2

interface GigabitEthernet1/1/3

interface GigabitEthernet1/1/4
interface TenGigabitEthernet1/1/1
  description C6509-2 Ten4/3
  no switchport
  ip address 10.4.40.66 255.255.255.252
  ip pim sparse-mode
  ip summary-address eigrp 100 10.4.24.0 255.255.248.0
  logging event link-status
  carrier-delay msec 0
  srr-queue bandwidth share 1 30 35 5
  queue-set 2
  priority-queue out
  mls qos trust dscp
  macro description EgressQoS
  rsu active
!
interface TenGigabitEthernet1/1/2
!
interface GigabitEthernet2/0/1
!
interface GigabitEthernet2/1/1
!
interface GigabitEthernet2/1/2
!
interface GigabitEthernet2/1/3
!
interface GigabitEthernet2/1/4
!
interface TenGigabitEthernet2/1/1
  description C6509-1 Ten4/3
  no switchport
  ip address 10.4.40.70 255.255.255.252
  ip pim sparse-mode
  ip summary-address eigrp 100 10.4.24.0 255.255.248.0
  logging event link-status
  carrier-delay msec 0
  srr-queue bandwidth share 1 30 35 5
  queue-set 2
  priority-queue out
  mls qos trust dscp
  macro description EgressQoS
  rsu standby
!
interface TenGigabitEthernet2/1/2
!
interface GigabitEthernet2/0/19
  description IE-SSM40b
  switchport access vlan 300
  switchport mode access
  spanning-tree portfast
!
interface GigabitEthernet2/0/20
!
interface GigabitEthernet2/0/21
!
interface GigabitEthernet2/0/22
!
interface GigabitEthernet2/0/23
!
interface GigabitEthernet2/0/24
  description IE-ASA5540b Gig0/0
  switchport access vlan 300
  switchport mode access
  spanning-tree portfast
!
interface GigabitEthernet2/1/1
!
interface GigabitEthernet2/1/2
!
interface GigabitEthernet2/1/3
!
interface GigabitEthernet2/1/4
!
interface TenGigabitEthernet2/0/2
!
interface GigabitEthernet2/0/3
!
interface GigabitEthernet2/0/4
!
interface Vlan1
  no ip address
shutdown
!
interface Vlan300
description Internet Edge SVI
ip address 10.4.24.1 255.255.255.224
!
!
router eigrp 100
network 10.4.0.0 0.0.255.255
passive-interface default
no passive-interface TenGigabitEthernet1/1/1
no passive-interface TenGigabitEthernet2/1/1
no passive-interface Vlan300
eigrp router-id 10.4.40.251
nsf
!
!
ip http server
ip http authentication aaa
ip http secure-server
!
ip pim autorp listener
!
logging esm config
logging 10.4.48.35
!
smtp-server community cisco RO
smtp-server community cisco123 RW
smtp-server trap-source Loopback0
smtp-server system-shutdown
tacacs-server host 10.4.48.15 key 7 073C244F5C0C0D2E120B
!
!
line con 0
line vty 0 4
exec-timeout 0 0
transport input ssh
line vty 5 15
exec-timeout 0 0
transport input ssh
!
ntp server 10.4.48.17
end

ACE 4710
DMZ Server Load Balancing

The Cisco Application Control Engine (ACE) is the latest server-load balancing (SLB) offering from Cisco. From its mainstream role in providing Layer 4 through 7 switching, Cisco ACE also provides an array of acceleration and server loadoff load benefits, including TCP processing offload, Secure Socket Layer (SSL) offload, compression, and various other acceleration technologies.

peer hostname DMZ-ACE4710b
hostname DMZ-ACE4710a
interface gigabitEthernet 1/1
    channel-group 1
    no shutdown
interface gigabitEthernet 1/2
    channel-group 1
    no shutdown
interface gigabitEthernet 1/3
    shutdown
interface gigabitEthernet 1/4
    shutdown
interface port-channel 1
    ft-port vlan 1124
    switchport trunk allowed vlan 1116,1123
    port-channel load-balance src-dst-ip
    no shutdown

clock timezone standard PST
tacacs-server host 10.4.48.15 key 7 "VagwrtFjq"
aaa group server tacacs+ tacacs+
server 10.4.48.15
ntp server 10.4.48.17

aaa authentication login default group tacacs+ local

access-list ALL line 8 extended permit ip any any

ip domain-name cisco.local

class-map type management match-any remote_access
  2 match protocol xml-https any
  3 match protocol icmp any
  4 match protocol telnet any
  5 match protocol ssh any
  6 match protocol http any
  7 match protocol https any
  8 match protocol snmp any

policy-map type management first-match remote_mgmt_allow_policy
  class remote_access
    permit

interface vlan 1123
  ip address 192.168.23.10 255.255.255.0
  peer ip address 192.168.23.11 255.255.255.0
  access-group input ALL
  service-policy input remote_mgmt_allow_policy
  no shutdown

ft interface vlan 1124
  ip address 192.168.24.1 255.255.255.0
  peer ip address 192.168.24.2 255.255.255.0
  no shutdown

ft peer 1
  heartbeat interval 300
  heartbeat count 10
  ft-interface vlan 1124

ft group 1
  peer 1
  priority 120
  peer priority 110
  associate-context Admin
  inservice

ip route 0.0.0.0 0.0.0.0 192.168.23.1

class-map type management match-any remote_access
  2 match protocol xml-https any
  3 match protocol icmp any
  4 match protocol telnet any
  5 match protocol ssh any
  6 match protocol http any
  7 match protocol https any
  8 match protocol snmp any

policy-map type management first-match remote_mgmt_allow_policy
  class remote_access
    permit

interface vlan 1124
  ip address 192.168.24.1 255.255.255.0
  peer ip address 192.168.24.2 255.255.255.0
  no shutdown

context dmz-web
  allocate-interface vlan 1116

snmp-server community cisco group Network-Monitor

ft group 2
  peer 1
  priority 120
  peer priority 110
  associate-context dmz-web
  inservice

username admin password 5 $1$Htv9RSAG$/83t1X1O3uRGPlpSkGTq4.$1$dndTnbZX$zgSMmVL55bV6pWoTByTwt1 role Admin domain default-domain

username www password 5 $1$dndTnbZX$zgSMmVL55bV6pWoTByTwt1 role Admin domain default-domain

ssh key rsa 1024 force
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.