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 1 100 100 100 100 100 100 100 100 100

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

- About SBA .............................................................. 1
- About This Guide .................................................... 1

### Introduction .................................................................... 2

### Data Center Ethernet and Fibre Channel Infrastructure ................. 4

- Cisco Nexus 5548UPa .................................................. 4
- Cisco Nexus 5548UPb .................................................... 12
- Cisco MDS 9148a .......................................................... 21
- Cisco MDS 9148b .......................................................... 23
- Cisco Catalyst 2960s Management Switch ............................ 26

### Data Center Network Security ........................................... 29

- Cisco ASA 5585 - Primary ............................................ 29
- Cisco ASA 5585 IPS SSP - Primary .................................. 32
- Cisco ASA 5585 - Secondary .......................................... 34
- Cisco ASA 5585 IPS SSP - Secondary ............................... 37

### Data Center Application Resilience .................................... 39

- Cisco ACE - Primary .................................................... 39
- Cisco ACE - Secondary ................................................ 41

### Appendix A: Product List .................................................. 45

---

**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.
What's In This SBA Guide

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
For our partners and customers with up to 2500 connected users, Cisco has designed 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, masks 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.

For Cisco partners and customers whose data center will have up to 300 physical or virtual servers, Cisco has created a data center architecture that is flexible, scalable, reliable, and affordable. The step-by-step guidance in the data center deployment guides makes it easy to install, configure, and manage which reduces the time and cost needed to deploy your data center.

By building on to the foundation LAN and WAN architecture you’ve already deployed with the Cisco Smart Business Architecture (SBA) Borderless Network Foundation, the SBA Data Center lets you migrate from your current server farm without wasting time and expense reconfiguring your existing network foundation.

The following configuration files are provided:

- Data Center Ethernet and Fibre Channel Infrastructure
- Data Center Network Security
- Data Center Application Resilience

Refer to Appendix A for a complete list of products used in the lab testing of this design.

Figure 1 illustrates the complete Cisco SBA Midsize Data Center architecture.
Figure 1 - Cisco SBA midsize data center architecture
This section includes the Cisco Nexus 5500UP Series switches, used to build out the data center core Ethernet and Fibre Channel switching foundation, and the Cisco MDS 9100 Multilayer Fabric switches, used to extend your Fibre Channel networks for larger density requirements.

**Cisco Nexus 5548UPa**

The Cisco Nexus 5500UP switches operate as a pair to provide a resilient data center core for both Ethernet and Fibre Channel network transport. This switch is the Fibre Channel SAN-A switch.

```
version 5.1(3)N1(1)
feature fcoe
hostname dc5548ax
feature npiv
feature fport-channel-trunk
no feature telnet
no feature http-server
cfs eth distribute
feature pim
feature eigrp
feature udld
feature interface-vlan
feature hasp
feature lacp
feature vpc
feature lldp
feature fex
username admin password 5 $1$PmfWzpAr$Qb.H.MCdhiHoZJM0Vh/0i0 role network-admin
password strength-check
banner motd #Nexus 5000 Switch #
ssh key rsa 2048
ip domain-lookup
ip name-server 10.10.48.10
class-map type qos class-fcoe
class-map type queuing class-fcoe
  match qos-group 1
class-map type queuing class-all-flood
  match qos-group 2
class-map type queuing class-ip-multicast
  match qos-group 2
class-map type network-qos class-fcoe
  match qos-group 1
class-map type network-qos class-all-flood
  match qos-group 2
class-map type network-qos class-ip-multicast
  match qos-group 2
policy-map type network-qos jumbo
class type network-qos class-default
  mtu 9216
  multicast-optimize
system qos
  service-policy type queuing input fcoe-default-in-policy
  service-policy type queuing output fcoe-default-out-policy
  service-policy type qos input fcoe-default-in-policy
  service-policy type network-qos fcoe-default-nq-policy
fex 102
  pinning max-links 1
  description “FEX0102”
fex 103
  pinning max-links 1
  description “FEX0103”
slot 1
```
port 28-32 type fc
snmp-server source-interface trap loopback1
snmp-server user admin network-admin auth
md5 0x3b0ef3a64c1235ca3578bf32d1aaddf priv
0x3b0ef3a64c1235ca3578bf32d1aaddf localizedkey
snmp-server host 10.10.63.100 traps_version 2c public udp-port 1164
snmp-server community cisco123 group network-admin
snmp-server community cisco group network-operator
ntp server 10.10.48.17 use-vrf management
vrf context management
   ip route 0.0.0.0/0 10.10.63.1
vlan 1
vlan 148
   name Servers_1
vlan 149
   name Servers_2
vlan 150
   name Servers_3
vlan 153
   name FW_Outside
vlan 154
   name FW_Inside_1
vlan 155
   name FW_Inside_2
vlan 156
   name PEERING_VLAN
vlan 159
   name 1kv-Packet
vlan 160
   name 1kv-Control
vlan 161
   name VMotion
vlan 162
   name iSCSI
vlan 163
   name DC-Management
vlan 304
   fcoe vsan 4
vlan 912
   name ACE-Heartbeat
spanning-tree vlan 148-151,153-157,159-163 priority 24576
route-map static-to-eigrp permit 10
   match ip address 10.10.54.0/24
route-map static-to-eigrp permit 20
   match ip address 10.10.55.0/24
port-channel load-balance ethernet source-dest-port
vpc domain 10
   role priority 16000
   peer-keepalive destination 10.10.63.11 source 10.10.63.10
delay restore 360
peer-gateway
auto-recovery
vsan database
   vsan 4 name “General-Storage”
device-alias database
   device-alias name emc-a0-fc pwwn
50:06:01:61:3c:e0:30:59
   device-alias name emc-2-a0-fc pwwn
50:06:01:61:3c:e0:60:e2
   device-alias name Netapp-e2a-FCOE pwwn
50:0a:09:82:89:aa:df:b1
   device-alias name NetApp2-e2a-FCOE pwwn
50:0a:09:81:89:3b:63:be
   device-alias name p12-c210-27-vhba3 pwwn
20:00:58:8d:09:0e:e0:d2
   device-alias name p12-c210m1-1-vhba3 pwwn
20:00:e8:b7:48:44:5b:df
   device-alias name p12-c210m2-2-vhba3 pwwn
20:00:e8:b7:48:44:53:56
device-alias commit
fcdomain fcid database
  vsan 4 wwn 20:42:00:05:73:a2:b2:40 fcid 0xbc0000 dynamic
  vsan 4 wwn 20:41:00:05:73:a2:b2:40 fcid 0xbc0001 dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc0002 dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc0003 dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc0004 dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc0005 dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc0006 dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc0007 dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc0008 dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc0009 dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc000a dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc000b dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc000c dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc000d dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc000e dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc000f dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc0010 dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc0011 dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc0012 dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc0013 dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc0014 dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc0015 dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc0016 dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc0017 dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc0018 dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc0019 dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc001a dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc001b dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc001c dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc001d dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc001e dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc001f dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc0020 dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc0021 dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc0022 dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc0023 dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc0024 dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc0025 dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc0026 dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc0027 dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc0028 dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc0029 dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc002a dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc002b dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc002c dynamic
  vsan 4 wwn 20:00:58:8d:09:0e:e0:d2 fcid 0xbc002d dynamic

!       [p12-c210-27-vhba3]

interface Vlan1
  no shutdown
  description Servers_1
  no ip redirects
  ip address 10.10.48.2/24
  ip router eigrp 1
  ip passive-interface eigrp 1
  ip pim sparse-mode
  hsrp 148
  priority 110
  ip 10.10.48.1

interface Vlan148
  no shutdown
  description Servers_2
  no ip redirects
  ip address 10.10.49.2/24
  ip router eigrp 1
  ip passive-interface eigrp 1
  ip pim sparse-mode
  hsrp 149
  priority 110
  ip 10.10.49.1

interface Vlan149
  no shutdown
  description Servers_3
  no ip redirects
  ip address 10.10.50.2/24
  ip router eigrp 1
  ip passive-interface eigrp 1
  ip pim sparse-mode
  hsrp 150
  priority 110
  ip 10.10.50.1

interface Vlan150
  no shutdown
  description FW_Outside
  no ip redirects
  ip address 10.10.53.2/25
  ip router eigrp 1
  ip passive-interface eigrp 1
  ip pim sparse-mode
  hsrp 153
  priority 110
  ip 10.10.53.1
interface Vlan156
   no shutdown
   description 5k-to-5k-L3link
   no ip redirects
   ip address 10.10.56.1/30
   ip router eigrp 1
   ip pim sparse-mode

interface Vlan163
   no shutdown
   description DC-Management
   no ip redirects
   ip address 10.10.63.2/25
   ip router eigrp 1
   ip passive-interface eigrp 1
   hsrp 163
      priority 110
      ip 10.10.63.1

interface san-port-channel 29
   channel mode active
   switchport trunk allowed vsan 1
   switchport trunk allowed vsan add 4
   switchport trunk mode off

interface san-port-channel 31
   switchport trunk allowed vsan 1
   switchport trunk allowed vsan add 4

interface port-channel10
   switchport mode trunk
   spanning-tree port type network
   vpc peer-link

interface port-channel13
   switchport mode trunk
   switchport trunk allowed vlan 148,912
   spanning-tree port type edge trunk
   speed 1000

interface port-channel21
   description Link to Management Switch for VL163
   switchport mode trunk
   switchport trunk allowed vlan 163
   speed 1000
   vpc 21

interface port-channel27
   switchport mode trunk
   switchport trunk allowed vlan 162,304
   spanning-tree port type edge trunk
   vpc 27

interface port-channel50
   switchport mode trunk
   switchport trunk allowed vlan 148-151,154-155,159-163
   spanning-tree port type edge trunk
   speed 10000
   vpc 50

interface port-channel51
   switchport mode trunk
   switchport trunk allowed vlan 148-151,154-155,159-163
   spanning-tree port type edge trunk
   speed 10000
   vpc 51

interface port-channel53
   switchport mode trunk
   switchport trunk allowed vlan 153-155
   speed 10000
   vpc 53

interface port-channel54
switchport mode trunk
switchport trunk allowed vlan 153-155
speed 10000
vpc 54

interface port-channel102
  description dual-homed 2248
  switchport mode fex-fabric
  fex associate 102
  vpc 102

interface port-channel103
  description single-homed 2232PP
  switchport mode fex-fabric
  fex associate 103

interface vfcl
  bind interface Ethernet103/1/3
  no shutdown

interface vfcl27
  bind interface port-channel27
  switchport trunk allowed vsan 4
  no shutdown
vsan database
  vsan 4 interface vfcl
  vsan 4 interface vfcl27
  vsan 4 interface san-port-channel 29

interface fc1/28

interface fc1/29
  switchport trunk mode off
  channel-group 29 force
  no shutdown

interface vfcl30
  switchport trunk mode off
  channel-group 29 force
  no shutdown

interface fc1/31
  switchport description Link to dcm89142ax port fc1/13
  channel-group 31 force
  no shutdown

interface fc1/32
  switchport description Link to dcm89142ax port fc1/14
  channel-group 31 force
  no shutdown

interface Ethernet1/1
  description DC5585a Ten0/8
  switchport mode trunk
  switchport trunk allowed vlan 153-155
  channel-group 53 mode active

interface Ethernet1/2
  description DC5585b Ten0/8
  switchport mode trunk
  switchport trunk allowed vlan 153-155
  channel-group 54 mode active

interface Ethernet1/3
  description ACE 1 Gig 1/1
  switchport mode trunk
  switchport trunk allowed vlan 148,912
  speed 1000
  channel-group 13
  vpc orphan-port suspend

interface Ethernet1/4
  description ACE 1 Gig 1/2
  switchport mode trunk
switchport trunk allowed vlan 148,912
speed 1000
channel-group 13
vpc orphan-port suspend

interface Ethernet1/5

interface Ethernet1/6

interface Ethernet1/7

interface Ethernet1/8

interface Ethernet1/9
description Link to FI-A eth1/17
switchport mode trunk
switchport trunk allowed vlan 148-151,154-155,159-163
channel-group 50 mode active

interface Ethernet1/10
description Link to FI-A eth1/18
switchport mode trunk
switchport trunk allowed vlan 148-151,154-155,159-163
channel-group 50 mode active

interface Ethernet1/11
description Link to FI-B eth1/17
switchport mode trunk
switchport trunk allowed vlan 148-151,154-155,159-163
channel-group 51 mode active

interface Ethernet1/12
description Link to FI-B eth1/18
switchport mode trunk
switchport trunk allowed vlan 148-151,154-155,159-163
channel-group 51 mode active

interface Ethernet1/13
switchport mode fex-fabric
fex associate 102
channel-group 102

interface Ethernet1/14

interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17
description vpc peer link
switchport mode trunk
channel-group 10 mode active

interface Ethernet1/18
description vpc peer link
switchport mode trunk
channel-group 10 mode active

interface Ethernet1/19
description Core Ten1/4/6
no switchport
ip address 10.10.24.2/30
ip router eigrp 1
ip pim sparse-mode

interface Ethernet1/20
description Core Ten2/4/6
no switchport
ip address 10.10.24.6/30
ip router eigrp 1
ip pim sparse-mode

interface Ethernet1/21
switchport mode trunk
switchport trunk allowed vlan 163
speed 1000
cchannel-group 21 mode active

interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25
switchport mode fex-fabric
fex associate 103
cchannel-group 103

interface Ethernet1/26
switchport mode fex-fabric
fex associate 103
cchannel-group 103

interface Ethernet1/27
switchport mode trunk
switchport trunk allowed vlan 162,304
spanning-tree port type edge trunk
cchannel-group 27

interface mgmt0
ip address 10.10.63.10/25

interface loopback1
ip address 10.10.63.254/32
ip router eigrp 1
ip pim sparse-mode

interface Ethernet102/1/1
description Link to RVPN Lab B
switchport access vlan 148

spanning-tree port type edge

interface Ethernet102/1/2
switchport access vlan 157
spanning-tree port type edge

interface Ethernet102/1/3
description Link to Network Services ESX Servers
switchport access vlan 148
spanning-tree port type edge

interface Ethernet102/1/4
description Links to vWAAS CM { ESX }
switchport mode trunk
switchport trunk allowed vlan 150,163

interface Ethernet102/1/5
description Links to SJC23-Lab-NTP-B
switchport access vlan 148
spanning-tree port type edge

interface Ethernet102/1/6
description Link to Tanberg
switchport access vlan 148
spanning-tree port type edge

interface Ethernet102/1/7
description Link to MCU(Codian)
switchport access vlan 148
spanning-tree port type edge

interface Ethernet102/1/8

interface Ethernet102/1/9
description Link to ESX22 with BN Services & DC Management
VLANs
switchport mode trunk
switchport trunk allowed vlan 150,163
spanning-tree port type edge trunk

interface Ethernet102/1/10

interface Ethernet102/1/11
description TEMPORARY-CIMC-C210M2-2-ESX
switchport access vlan 163

interface Ethernet102/1/12
description TEMPORARY-MGMT-C210M2-2-ESX
switchport access vlan 163

interface Ethernet102/1/13
description Link to Network Services ESX Servers
switchport access vlan 148
spanning-tree port type edge

interface Ethernet102/1/14
switchport access vlan 163
spanning-tree port type edge

interface Ethernet102/1/15

!**************************************************************
! interfaces Ethernet102/1/16 to 102/1/47 are not
! configured and have been removed for brevity
!**************************************************************

interface Ethernet102/1/48

interface Ethernet102/1/49

interface Ethernet103/1/1
switchport access vlan 157
spanning-tree port type edge
speed 1000

interface Ethernet103/1/2

interface Ethernet103/1/3
switchport mode trunk
switchport trunk allowed vlan 148,304
spanning-tree port type edge trunk

interface Ethernet103/1/4
description C250M2-1 ESX
shutdown

interface Ethernet103/1/5
description C210M1-1 ESX
shutdown

interface Ethernet103/1/6
description C250M2-1 ESX (N1Kv)
switchport mode trunk
switchport trunk allowed vlan 148,153-155,159-161,163,304
spanning-tree port type edge trunk

interface Ethernet103/1/7
description C210M1-1 ESX (N1Kv)
switchport mode trunk
switchport trunk allowed vlan 148,153-155,159-161,163,304
spanning-tree port type edge trunk

interface Ethernet103/1/8
description C210M2-2 ESX (N1Kv)
switchport mode trunk
switchport trunk allowed vlan 148,153-155,159-161,163,304
spanning-tree port type edge trunk

interface Ethernet103/1/9
description ESX27 C200-M2
switchport mode trunk
switchport trunk allowed vlan 148,153-155,159-161,163
spanning-tree port type edge trunk
interface Ethernet103/1/10

!***********************************************************************
! interfaces Ethernet103/1/11 to 103/1/31 are not
! configured and have been removed for brevity
!***********************************************************************

interface Ethernet103/1/32
clock timezone PST -8 0
clock summer-time PDT 2 Sunday march 02:00 1 Sunday nov 02:00 60
line console
line vty
boot kickstart bootflash:/n5000-uk9-kickstart.5.1.3.N1.0.347.bin
boot system bootflash:/n5000-uk9.5.1.3.N1.0.347.bin
router eigrp 1
    router-id 10.10.63.254
    redistribute static route-map static-to-eigrp
ip route 10.10.54.0/24 Vlan153 10.10.53.126
ip route 10.10.55.0/24 Vlan153 10.10.53.126
ip pim rp-address 10.10.15.252 group-list 239.1.0.0/16
ip pim ssm range 232.0.0.0/8
no ip igmp snooping mrouter vpc-peer-link
vpc bind-vrf default vlan 900
interface fc1/29
interface fc1/30
interface fc1/31
interface fc1/32
interface fc1/28
interface fc1/29
interface fc1/30
interface fc1/31
interface fc1/32
zoneset distribute full vsan 4
!Full Zone Database Section for vsan 4
zone name p12-ucsb200m2-2-vhba3_netapp-2-e2a vsan 4
         member pwnn 50:0a:09:81:89:3b:63:be

Cisco Nexus 5548UPb

The Cisco Nexus 5500UP switches operate as a pair to provide a resilient
data center core for both Ethernet and Fibre Channel network transport.
This switch is the Fibre Channel SAN-B switch.
version 5.1(3)N1(1)
feature fcoe
hostname dc5548bx
feature npiv
feature fport-channel-trunk
no feature telnet
no feature http-server
cfs eth distribute
feature pim
feature eigrp
feature udld
feature interface-vlan
feature hsrp
feature lacp
feature vpc
feature lldp
feature fex
username admin password 5 $1$theIP.jx$DD7AhRcM1HhFZA2Ud/TMw1_
role network-admin
password strength-check

banner motd #Nexus 5000 Switch
#
ssh key rsa 2048
ip domain-lookup
ip name-server 10.10.48.10
class-map type qos class-fcoe
class-map type queuing class-fcoe
    match qos-group 1
class-map type queuing class-all-flood
    match qos-group 2
class-map type queuing class-ip-multicast
    match qos-group 2
class-map type network-qos class-fcoe
    match qos-group 1
class-map type network-qos class-all-flood
    match qos-group 2
class-map type network-qos class-ip-multicast
    match qos-group 2
policy-map type network-qos jumbo
    class type network-qos class-default
        mtu 9216
        multicast-optimize
system qos
    service-policy type queuing input fcoe-default-in-policy
    service-policy type queuing output fcoe-default-out-policy
    service-policy type qos input fcoe-default-in-policy
    service-policy type network-qos fcoe-default-nq-policy
fex 102
    pinning max-links 1
    description "FEX0102"
fex 103
    pinning max-links 1
    description "FEX0103"
slot 1
    port 28-32 type fc
snmp-server source-interface trap loopback1
snmp-server user admin network-admin auth
    md5 0xcb923b24b5215a886eaf8dff5466e077 localizedkey
    snmp-server host 10.10.63.100 traps version 2c public _udp-port_ 1163
snmp-server community cisco123 group network-admin
snmp-server community cisco group network-operator
ntp server 10.10.48.17 use-vrf management
vrf context management
    ip route 0.0.0.0/0 10.10.63.1
vlan 1
    vlan 148
        name Servers_1
    vlan 149
        name Servers_2
    vlan 150
        name Servers_3
    vlan 153
        name FW_Outside
    vlan 154
        name FW_Inside_1
    vlan 155
        name FW_Inside_2
    vlan 156
        name PEERING_VLAN
    vlan 159
        name 1kv-Packet
    vlan 160
        name 1kv-Control
    vlan 161
        name VMotion
    vlan 162
        name iSCSI
    vlan 163
        name DC-Management
    vlan 305
        fcoe vsan 5
    vlan 912
        name ACE-Heartbeat
spanning-tree vlan 148-151,153-157,159-163 priority 28672
route-map static-to-eigrp permit 10
  match ip address 10.10.54.0/24
route-map static-to-eigrp permit 20
  match ip address 10.10.55.0/24
port-channel load-balance ethernet source-dest-port
vpc domain 10
  peer-keepalive destination 10.10.63.10 source 10.10.63.11
delay restore 360
peer-gateway
auto-recovery
vsan database
  vsan 5 name “General-Storage”
device-alias database
  device-alias name emc-b0-fc pwwn 50:06:01:69:3c:e0:30:59
  device-alias name emc-2-b0-fc pwwn 50:06:01:69:3c:e0:60:e2
  device-alias name NetApp-e2b-FCOE pwwn 50:0a:09:81:89:ea:df:b1
  device-alias name NetApp2-e2b-FCOE pwwn 50:0a:09:82:89:3b:63:be
  device-alias name p12-c210-27-vhba4 pwwn 20:00:58:8d:09:0e:e0:d3
  device-alias name p12-c210m1-1-vhba4 pwwn 20:00:e8:b7:48:4d:5b:e0
  device-alias name p12-c250m2-1-vhba4 pwwn 20:00:e8:b7:48:4d:53:57
device-alias commit

fcdomain fcid database
  vsan 5 wwn 20:41:00:05:73:a3:82:c0 fcid 0x280000 dynamic
  vsan 5 wwn 20:42:00:05:73:a3:82:c0 fcid 0x280001 dynamic
  vsan 5 wwn 20:00:58:8d:09:0e:e0:d3 fcid 0x280002 dynamic
  vsan 5 wwn 24:1d:00:05:73:a3:82:c0 fcid 0x280003 dynamic
  vsan 5 wwn 20:00:00:25:b5:77:77:8f fcid 0x280004 dynamic
  vsan 5 wwn 20:00:00:25:b5:77:77:8e fcid 0x280005 dynamic
  vsan 5 wwn 20:00:00:25:b5:77:77:7f fcid 0x280006 dynamic
  vsan 1 wwn 20:41:00:05:73:a3:82:c0 fcid 0x120000 dynamic
  vsan 1 wwn 20:42:00:05:73:a3:82:c0 fcid 0x120001 dynamic
  vsan 5 wwn 20:00:00:25:b5:77:77:6e fcid 0x280007 dynamic
  vsan 5 wwn 20:00:00:25:b5:77:77:ff fcid 0x280008 dynamic
  vsan 5 wwn 20:00:00:25:b5:99:99:9f fcid 0x280009 dynamic
  vsan 5 wwn 20:00:00:25:b5:99:99:6f fcid 0x28000a dynamic
  vsan 5 wwn 50:0a:09:82:89:3b:63:be fcid 0x28000b dynamic

   [NetApp2-e2b-FCOE]

interface Vlan1

interface Vlan148
  no shutdown
description Servers_1
  no ip redirects
  ip address 10.10.48.3/24
  ip router eigrp 1
  ip passive-interface eigrp 1
  ip pim sparse-mode
  hsrp 148
    ip 10.10.48.1

interface Vlan149
description Servers_2
  no ip redirects
  ip address 10.10.49.3/24
  ip router eigrp 1
  ip passive-interface eigrp 1
  ip pim sparse-mode
  hsrp 149
    ip 10.10.49.1
interface Vlan150
  no shutdown
description Servers_3
  no ip redirects
  ip address 10.10.50.3/24
  ip router eigrp 1
  ip passive-interface eigrp 1
  ip pim sparse-mode
  hsrp 150
    ip 10.10.50.1
interface Vlan153
  no shutdown
description FW_Outside
  no ip redirects
  ip address 10.10.53.3/25
  ip router eigrp 1
  ip passive-interface eigrp 1
  ip pim sparse-mode
  hsrp 153
    ip 10.10.53.1
interface Vlan156
  no shutdown
description 5k-to-5k-L3link
  no ip redirects
  ip address 10.10.56.2/30
  ip router eigrp 1
  ip pim sparse-mode
interface Vlan163
  no shutdown
description DC-Management
  no ip redirects
  ip address 10.10.63.3/25
  ip router eigrp 1
  ip pim sparse-mode
  hsrp 163
    ip 10.10.63.1
interface san-port-channel 29
  channel mode active
  switchport trunk allowed vsan 1
  switchport trunk allowed vsan add 5
  switchport trunk mode off
interface san-port-channel 31
  switchport trunk allowed vsan 1
  switchport trunk allowed vsan add 5
interface port-channel10
  switchport mode trunk
  spanning-tree port type network
  vpc peer-link
interface port-channel113
  switchport mode trunk
  switchport trunk allowed vlan 148,912
  spanning-tree port type edge trunk
  speed 1000
interface port-channel21
  description Link to Management Switch for VL163
  switchport mode trunk
  switchport trunk allowed vlan 163
  speed 1000
  vpc 21
interface port-channel27
  switchport mode trunk
  switchport trunk allowed vlan 162,305
  spanning-tree port type edge trunk
  vpc 27

interface port-channel50
  switchport mode trunk
  switchport trunk allowed vlan 148-151,154-155,159-163
  spanning-tree port type edge trunk
  speed 10000
  vpc 50

interface port-channel51
  switchport mode trunk
  switchport trunk allowed vlan 148-151,154-155,159-163
  spanning-tree port type edge trunk
  speed 10000
  vpc 51

interface port-channel53
  switchport mode trunk
  switchport trunk allowed vlan 153-155
  speed 10000
  vpc 53

interface port-channel54
  switchport mode trunk
  switchport trunk allowed vlan 153-155
  speed 10000
  vpc 54

interface port-channel102
  description dual-homed 2248
  switchport mode fex-fabric
  fex associate 102
  vpc 102

interface port-channel103
  description single-homed 2232PP
  switchport mode fex-fabric
  fex associate 103

interface vfc1
  bind interface Ethernet103/1/3
  no shutdown

interface vfc27
  bind interface port-channel127
  switchport trunk allowed vsan 5
  no shutdown

vsan database
  vsan 5 interface vfc1
  vsan 5 interface vfc27
  vsan 5 interface san-port-channel 29

interface fc1/28

interface fc1/29
  switchport trunk mode off
  channel-group 29 force
  no shutdown

interface fc1/30
  switchport trunk mode off
  channel-group 29 force
  no shutdown

interface fc1/31
  switchport description Link to dcmds9148bx port fc1/13
  channel-group 31 force
  no shutdown

interface fc1/32
  switchport description Link to dcmds9148bx port fc1/14
channel-group 31 force
no shutdown

interface Ethernet1/1
description DC5585a Ten0/9
switchport mode trunk
switchport trunk allowed vlan 153-155
channel-group 53 mode active

interface Ethernet1/2
description DC5585b Ten0/9
switchport mode trunk
switchport trunk allowed vlan 153-155
channel-group 54 mode active

interface Ethernet1/3
description ACE 2 Gig 1/1
switchport mode trunk
switchport trunk allowed vlan 148,912
speed 1000
channel-group 13
vpc orphan-port suspend

interface Ethernet1/4
description ACE 2 Gig 1/2
switchport mode trunk
switchport trunk allowed vlan 148,912
speed 1000
channel-group 13
vpc orphan-port suspend

interface Ethernet1/5

interface Ethernet1/6

interface Ethernet1/7

interface Ethernet1/8

interface Ethernet1/9
description Link to FI-A eth1/19
switchport mode trunk
switchport trunk allowed vlan 148-151,154-155,159-163
channel-group 50 mode active

interface Ethernet1/10
description Link to FI-A eth1/20
switchport mode trunk
switchport trunk allowed vlan 148-151,154-155,159-163
channel-group 50 mode active

interface Ethernet1/11
description Link to FI-B eth1/19
switchport mode trunk
switchport trunk allowed vlan 148-151,154-155,159-163
channel-group 51 mode active

interface Ethernet1/12
description Link to FI-B eth1/20
switchport mode trunk
switchport trunk allowed vlan 148-151,154-155,159-163
channel-group 51 mode active

interface Ethernet1/13
switchport mode fex-fabric
fex associate 102
channel-group 102

interface Ethernet1/14

interface Ethernet1/15

interface Ethernet1/16
interface Ethernet1/17
  description vpc peer link
  switchport mode trunk
c  channel-group 10 mode active

interface Ethernet1/18
  description vpc peer link
  switchport mode trunk
c  channel-group 10 mode active

interface Ethernet1/19
  description Core Ten1/4/8
  no switchport
  ip address 10.10.24.10/30
  ip router eigrp 1
  ip pim sparse-mode

interface Ethernet1/20
  description Core Ten2/4/8
  no switchport
  ip address 10.10.24.14/30
  ip router eigrp 1
  ip pim sparse-mode

interface Ethernet1/21
  switchport mode trunk
  switchport trunk allowed vlan 163
  speed 1000
  channel-group 21 mode active

interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25
  switchport mode fex-fabric
  fex associate 103
  channel-group 103

interface Ethernet1/26
  switchport mode fex-fabric
  fex associate 103
  channel-group 103

interface Ethernet1/27
  switchport mode trunk
  switchport trunk allowed vlan 162,305
  spanning-tree port type edge trunk
  channel-group 27

interface mgmt0
  ip address 10.10.63.11/25

interface loopback1
  ip address 10.10.63.253/32
  ip router eigrp 1
  ip pim sparse-mode

interface Ethernet102/1/1
  description Link to RVPN Lab B
  switchport access vlan 148
  spanning-tree port type edge

interface Ethernet102/1/2
  switchport access vlan 157
  spanning-tree port type edge

interface Ethernet102/1/3
  description Link to Network Services ESX Servers
  switchport access vlan 148
  spanning-tree port type edge
interface Ethernet102/1/4
  description Links to vWAAS CM { ESX }
  switchport access vlan 150
  spanning-tree port type edge

interface Ethernet102/1/5
  description Links to SJC23-Lab-NTP-B
  switchport access vlan 148
  spanning-tree port type edge

interface Ethernet102/1/6
  description Link to Tandberg
  switchport access vlan 148
  spanning-tree port type edge

interface Ethernet102/1/7
  description Link to MCU(Codian)
  switchport access vlan 148
  spanning-tree port type edge

interface Ethernet102/1/8

interface Ethernet102/1/9
  description Link to ESX22 with BN Services & DC Management VLANs
  switchport mode trunk
  switchport trunk allowed vlan 150,163
  spanning-tree port type edge trunk

interface Ethernet102/1/10

interface Ethernet102/1/11
  description TEMPORARY-CIMC-C210M2-2-ESX
  switchport access vlan 163

interface Ethernet102/1/12
  description TEMPORARY-MGMT-C210M2-2-ESX

  switchport access vlan 163

interface Ethernet102/1/13
  description Link to Network Services ESX Servers
  switchport access vlan 148
  spanning-tree port type edge

interface Ethernet102/1/14
  switchport access vlan 163
  spanning-tree port type edge

interface Ethernet102/1/15
  !******************************************************************************************************************
  ! interfaces Ethernet102/1/16 to 102/1/47 are not configured and have been removed for brevity
  !******************************************************************************************************************

interface Ethernet102/1/16

interface Ethernet103/1/1
  switchport access vlan 157
  spanning-tree port type edge
  speed 1000

interface Ethernet103/1/2

interface Ethernet103/1/3
  switchport mode trunk
  switchport trunk allowed vlan 148,305
  spanning-tree port type edge trunk

interface Ethernet103/1/4
  description C250M2-1 ESX
  shutdown

interface Ethernet103/1/5
description C210M1-1 ESX
shutdown

interface Ethernet103/1/6
  description C250M2-1 ESX {N1Kv}
  switchport mode trunk
  switchport trunk allowed vlan 148,153-155,159-161,163,305
  spanning-tree port type edge trunk

interface Ethernet103/1/7
  description C210M1-1 ESX {N1Kv}
  switchport mode trunk
  switchport trunk allowed vlan 148,153-155,159-161,163,305
  spanning-tree port type edge trunk

interface Ethernet103/1/8
  description C210M2-2 ESX {N1Kv}
  switchport mode trunk
  switchport trunk allowed vlan 148,153-155,159-161,163,305
  spanning-tree port type edge trunk

interface Ethernet103/1/9
  description ESX27 C200-M2
  switchport mode trunk
  switchport trunk allowed vlan 148,153-155,159-161,163
  spanning-tree port type edge trunk

interface Ethernet103/1/10

******************************************************************************
! interfaces Ethernet103/1/11 to 103/1/31 are not
! configured and have been removed for brevity
******************************************************************************

interface Ethernet103/1/32
  clock timezone PST -8 0
  clock summer-time PDT 2 Sunday march 02:00 1 Sunday nov 02:00 60
  line console
  line vty
  boot kickstart bootflash:/n5000-uk9-kickstart.5.1.3.N1.0.347.bin
  boot system bootflash:/n5000-uk9.5.1.3.N1.0.347.bin
  router eigrp 1
    router-id 10.10.63.253
    redistribute static route-map static-to-eigrp
  ip route 10.10.54.0/24 Vlan153 10.10.53.126
  ip route 10.10.55.0/24 Vlan153 10.10.53.126
  ip pim rp-address 10.10.15.252 group-list 239.1.0.0/16
  ip pim ssm range 232.0.0.0/8
  no ip igmp snooping mrouter vpc-peer-link
  vpc bind-vrf default vlan 900
  interface fc1/29
  interface fc1/30
  interface fc1/31
  interface fc1/32
  interface fc1/28
  interface fc1/29
  interface fc1/30
  interface fc1/31
  interface fc1/32
  zoneset distribute full vsan 5
  !Full Zone Database Section for vsan 5
  zone name p12-ucsb200m2-2-vhba4_netapp-2-e2b vsan 5
    member pwwn 50:0a:09:82:89:3b:63:be
      [NetApp2-e2b-FCOE]
    member pwwn 20:00:00:25:b5:99:99:6f
  zoneset name FCOE_5 vsan 5
    member p12-ucsb200m2-2-vhba4_netapp-2-e2b
  zoneset activate name FCOE_5 vsan 5
  end
The Cisco MDS 9100 Multilayer Fabric switches provide support for a higher density Fibre Channel SAN by extending Fibre Channel ports from the core Nexus 5500UP switches for larger environments. This Cisco MDS 9100 switch extends the Fibre Channel SAN-A network transport.

version 5.0(7)
role name default-role
  description This is a system defined role and applies to all users.
  rule 5 permit show feature environment
  rule 4 permit show feature hardware
  rule 3 permit show feature module
  rule 2 permit show feature snmp
  rule 1 permit show feature system
username admin password 5 $1$00TFEaz1$6xUTFgrrbkYsjuDHuoIbxO
role network-admin
password strength-check
ssh key rsa 2048
ip domain-lookup
ip domain-name cisco.local
ip host mds9148ax 10.10.63.12
aaa group server radius radius
snmp-server user admin network-admin auth
md5 0xb7e5c6943fc9940b0a15061f195e6efc priv
0xb7e5c6943fc9940b0a15061f195e6efc localizedkey
snmp-server host 10.10.63.100 traps version 2c public udp-port 1165
rmon event 1 log trap public description FATAL(1) owner PMON@
FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@
CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@
ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@
WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO
snmp-server community cisco group network-operator
snmp-server community cisco123 group network-admin
ntp server 10.10.48.17
vsan database
  vsan 4 name “General-Storage”
device-alias database
  device-alias name emc-a0-fc pwnn 50:06:01:61:3c:e0:30:59
  device-alias name emc-2-a0-fc pwnn 50:06:01:61:3c:e0:60:e2
  device-alias name Netapp-e2a-FCOE pwnn 50:0a:09:82:89:df:b1
  device-alias name NetApp2-e2a-FCOE pwnn 50:0a:09:81:83:6b:63:be
  device-alias name p12-c210-27-vhba3 pwnn 20:00:58:8d:09:0e:e0:d2
  device-alias name p12-c210m1-1-vhba3 pwnn 20:00:e8:b7:48:44:5b:df
  device-alias name p12-c210m2-2-vhba3 pwnn 20:00:e8:b7:48:44:53:56
device-alias commit
fcdomain fcid database
  vsan 1 wwn 10:00:00:00:c9:86:44:59 fcid 0x010000 dynamic
  vsan 1 wwn 10:00:00:00:c9:86:44:23 fcid 0x010100 dynamic
  vsan 1 wwn 10:00:00:00:c9:86:44:87 fcid 0x010200 dynamic
  vsan 1 wwn 10:00:00:00:c9:92:81:01 fcid 0x010300 dynamic
  vsan 1 wwn 10:00:00:00:c9:91:d5:6d fcid 0x010400 dynamic
  vsan 1 wwn 10:00:00:00:c9:91:cd:41 fcid 0x010500 dynamic
  vsan 1 wwn 50:06:01:69:3c:e0:30:59 fcid 0x010600 dynamic
  vsan 1 wwn 10:00:00:00:c9:87:be:2b fcid 0x010700 dynamic
  vsan 1 wwn 20:42:00:00:05:9b:76:73:fc0d:fa:43:c0 fcid 0x010800 dynamic
  vsan 1 wwn 10:00:00:00:c9:87:be:2b fcid 0x010900 dynamic
  vsan 1 wwn 20:42:00:00:05:9b:76:73:fc0d:fa:43:c0 fcid 0x010900 dynamic
  vsan 1 wwn 50:06:01:69:3c:e0:30:59 fcid 0x010a00 dynamic
  vsan 1 wwn 10:00:00:00:c9:87:be:2b fcid 0x010b00 dynamic
  vsan 1 wwn 20:42:00:00:05:9b:76:73:fc0d:fa:43:c0 fcid 0x010c00 dynamic
  vsan 1 wwn 20:42:00:00:05:9b:76:73:fc0d:fa:43:c0 fcid 0x010d00 dynamic
  vsan 1 wwn 50:06:01:69:3c:e0:30:59 fcid 0x010e00 dynamic
  vsan 1 wwn 10:00:00:00:c9:87:be:2b fcid 0x010f00 dynamic
  vsan 1 wwn 20:42:00:00:05:9b:76:73:fc0d:fa:43:c0 fcid 0x011000 dynamic
vsan 1 wwn 20:02:00:24:e8:64:c5:89 fcid 0x011100 dynamic
vsan 1 wwn 20:02:00:24:e8:64:c5:62 fcid 0x011200 dynamic
vsan 1 wwn 20:02:00:24:e8:64:c5:6f fcid 0x011300 dynamic
vsan 1 wwn 20:02:00:24:e8:64:c5:62 fcid 0x011500 dynamic
vsan 1 wwn 50:06:01:61:3c:e0:30:59 fcid 0x011600 dynamic
  [emc-a0-fc]
vsan 1 wwn 50:06:01:61:3c:e0:60:e2 fcid 0x011700 dynamic
  [emc-2-a0-fc]
vsan 4 wwn 50:06:01:61:3c:e0:60:e2 fcid 0x0b9000000 dynamic
  [emc-2-a0-fc]

interface port-channel 1
  switchport mode E
  switchport trunk allowed vsan 1
  switchport trunk allowed vsan add 4
  switchport rate-mode dedicated
vsan database
  vsan 4 interface port-channel 1
  vsan 4 interface fc1/1
clock timezone PST -8 0
clock summer-time PDT 2 Sunday march 02:00 1 Sunday nov 02:00 60
ip default-gateway 10.10.63.1
switchname mds9148ax
line console
boot kickstart bootflash:/m9100-s3ek9-kickstart-mz.5.0.7.bin
boot system bootflash:/m9100-s3ek9-mz.5.0.7.bin
interface fc1/13
  switchport rate-mode dedicated
interface fc1/14
  switchport rate-mode dedicated
interface fc1/1
interface fc1/2
interface fc1/3
interface fc1/4
interface fc1/5
interface fc1/6
interface fc1/7
interface fc1/8
interface fc1/9
interface fc1/10
interface fc1/11
interface fc1/12
interface fc1/15

!******************************************************************************
! Interfaces fc1/16 to 1/47 are not configured and have been removed for brevity
******************************************************************************
!
interface fc1/48
interface fc1/13
  switchport mode E
interface fc1/14
  switchport mode E

system default zone distribute full
zoneset distribute full vsan 4
!Full Zone Database Section for vsan 4
zone name p12-ucsb200m2-2-vhba3_netapp-2-e2a vsan 4
  member pwwn 50:0a:09:81:89:3b:63:be
  [NetApp2-e2a-FCOE]
    member pwwn 20:00:00:25:b5:77:77:1f
zoneset name FCOE_4 vsan 4
  member p12-ucsb200m2-2-vhba3_netapp-2-e2a
zoneset activate name FCOE_4 vsan 4

interface fc1/1
  port-license acquire

interface fc1/2
  port-license acquire
interface fc1/3
  port-license acquire

interface fc1/4
  port-license acquire

interface fc1/5
  port-license acquire

interface fc1/6
  port-license acquire

interface fc1/7
  port-license acquire

interface fc1/8
  port-license acquire

interface fc1/9
  port-license acquire

interface fc1/10
  port-license acquire

interface fc1/11
  port-license acquire

interface fc1/12
  port-license acquire

interface fc1/13
  port-license acquire
  channel-group 1 force
  no shutdown

interface fc1/14
  port-license acquire

interface fc1/15
  port-license acquire

interface fc1/16

!***********************************************************************
! Interfaces fc 1/16 to 1/47 are not
! configured and have been removed for brevity
!***********************************************************************

interface fc1/48
interface mgmt0
  ip address 10.10.63.12 255.255.255.128
no system default switchport shutdown
end

---

Cisco MDS 9148b

The Cisco MDS 9100 Multilayer Fabric switches provide support for a higher density Fibre Channel SAN by extending Fibre Channel ports from the core Nexus 5500UP switches for larger environments. This MDS Cisco 9100 switch extends the Fibre Channel SAN-B network transport.

version 5.0(7)
role name default-role
  description This is a system defined role and applies to all
users.
    rule 5 permit show feature environment
    rule 4 permit show feature hardware
    rule 3 permit show feature module
    rule 2 permit show feature snmp
    rule 1 permit show feature system
username admin password 5 $1$hDWb4l4u$q7NztWmt/siWv6APicLC61
role network-admin
password strength-check
ssh key rsa 2048
ip domain-lookup
```
ip domain-name cisco.local
ip host mds9148bx 10.10.63.13
aaa group server radius radius
snmp-server user admin network-admin auth
md5 0x37f1a52be0e3ef1c358f5d0bf6e8623 priv
0x37f1a52be0e3ef1c358f5d0bf6e8623 localizedkey
snmp-server host 10.10.63.100 traps version 2c public udp-port 1166
rmon event 1 log trap public description FATAL(1) owner PMON@
FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@
CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@
ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@
WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO
snmp-server community cisco123 group network-admin
snmp-server community cisco group network-operator
ntp server 10.10.48.17
vsan database
  vsan 5 name "General-Storage"
device-alias database
  device-alias name emc-b0-fc pwwn 50:06:01:69:3c:e0:30:59
device-alias name emc-2-b0-fc pwwn 50:06:01:69:3c:e0:60:e2
device-alias name NetApp-e2b-FCOE pwwn 50:0a:09:81:89:ea:df:b1
device-alias name NetApp2-e2b-FCOE pwwn 50:0a:09:82:89:3b:63:be
device-alias name p12-c210-27-vhba4 pwwn 20:00:58:8d:09:0e:e0:d3
device-alias name p12-c210m1-1-vhba4 pwwn 20:00:e8:b7:48:4d:5b:e0
device-alias name p12-c250m2-1-vhba4 pwwn 20:00:e8:b7:48:4d:53:57
device-alias commit

fcdomain fcid database
  vsan 1 wwn 20:41:00:05:9b:76:b2:80 fcid 0xb40a00 dynamic
  vsan 1 wwn 10:00:00:00:c9:87:be:2a fcid 0xb40000 dynamic
  vsan 1 wwn 10:00:00:00:c9:86:44:80 fcid 0xb40100 dynamic
  vsan 1 wwn 20:42:00:05:9b:76:b2:80 fcid 0xb40b00 dynamic
  vsan 1 wwn 10:00:00:00:c9:91:d5:6c fcid 0xb40c00 dynamic
  vsan 1 wwn 10:00:00:00:c9:92:80:1c fcid 0xb40d00 dynamic
  vsan 1 wwn 50:06:01:60:3c:e0:60:e2 fcid 0xb40e00 dynamic
  vsan 1 wwn 10:00:00:00:c9:8c:60:b4 fcid 0xb40f00 dynamic
  vsan 1 wwn 10:00:00:00:c9:91:d4:0e fcid 0xb40500 dynamic
  vsan 1 wwn 10:00:00:00:c9:92:80:26 fcid 0xb40300 dynamic
  vsan 1 wwn 20:41:00:00:ec:b4:7d:cc fcid 0xb40400 dynamic
  vsan 1 wwn 10:00:00:00:c9:87:be:1c fcid 0xb41000 dynamic
  vsan 1 wwn 20:41:00:05:9b:76:b7:00 fcid 0xb40500 dynamic
  vsan 1 wwn 20:42:00:05:9b:76:b7:00 fcid 0xb40600 dynamic
  vsan 1 wwn 50:06:01:69:3c:e0:30:59 fcid 0xb41500 dynamic
  [emc-b0-fc]
  vsan 1 wwn 20:41:00:00:5b:76:b2:80 fcid 0xb40a00 dynamic
  [emc-2-b0-fc]
  vsan 1 wwn 20:42:00:00:ec:b4:7d:cc fcid 0xb40700 dynamic
  vsan 1 wwn 24:08:00:00:ec:b4:7d:cc fcid 0xb40800 dynamic
  vsan 1 wwn 10:00:00:00:c9:91:d4:0f fcid 0xb40900 dynamic
  vsan 1 wwn 20:41:00:05:73:ab:27:00 fcid 0xb41100 dynamic
  vsan 1 wwn 20:42:00:05:73:ab:27:00 fcid 0xb41200 dynamic
  vsan 1 wwn 25:00:00:00:73:ab:27:00 fcid 0xb41300 dynamic
  vsan 1 wwn 25:00:00:00:ec:fa:52:80 fcid 0xb41400 dynamic

interface port-channel 1
  switchport mode E
  switchport trunk allowed vsan 1
  switchport trunk allowed vsan add 5
  switchport rate-mode dedicated
vsan database
  vsan 5 interface port-channel 1
  vsan 5 interface fc1/1```
clock timezone PST -8 0
clock summer-time PDT 2 Sunday march 02:00 1 Sunday nov 02:00 60
ip default-gateway 10.10.63.1
switchname mds9148bx
line console
boot kickstart bootflash:/m9100-s3ek9-kickstart-mz.5.0.7.bin
boot system bootflash:/m9100-s3ek9-mz.5.0.7.bin
interface fc1/13
  switchport rate-mode dedicated
interface fc1/14
  switchport rate-mode dedicated
interface fc1/1
interface fc1/2
interface fc1/3
interface fc1/4
interface fc1/5
interface fc1/6
interface fc1/7
interface fc1/8
interface fc1/9
interface fc1/10
interface fc1/11
interface fc1/12
interface fc1/15
!
!****************************************************************************************
! Interfaces fc1/16 to 1/47 are not configured and have been removed for brevity
!****************************************************************************************
!
interface fc1/48
interface fc1/13
  switchport mode E
interface fc1/14
  switchport mode E
system default zone distribute full
zoneset distribute full vsan 5

!****************************************************************************************
! Full Zone Database Section for vsan 5
zoneset activate name FCOE_5 vsan 5
  member p12-ucsb200m2-2-vhba4_netapp-2-e2b vsan 5
  member pwwn 50:0a:09:82:89:3b:63:be
  [NetApp2-e2b-FCOE]
  member pwwn 20:00:00:25:b5:77:77:8f
zoneset name FCOE_5 vsan 5
  member p12-ucsb200m2-2-vhba4_netapp-2-e2b
  member pwwn 20:00:00:25:b5:77:77:8f

interface fc1/1
  port-license acquire
interface fc1/2
  port-license acquire
interface fc1/3
  port-license acquire
interface fc1/4
  port-license acquire
interface fc1/5
  port-license acquire
interface fc1/6
  port-license acquire
interface fc1/7
  port-license acquire
interface fc1/8
  port-license acquire
interface fc1/9
  port-license acquire
interface fc1/10
  port-license acquire
interface fc1/11
  port-license acquire
interface fc1/12
  port-license acquire
interface fc1/13
  port-license acquire
interface fc1/14
  port-license acquire
interface fc1/15
  port-license acquire
interface fc1/16
  port-license acquire
interface fc1/10
    port-license acquire

interface fc1/11
    port-license acquire

interface fc1/12
    port-license acquire

interface fc1/13
    port-license acquire
    channel-group 1 force
    no shutdown

interface fc1/14
    port-license acquire
    channel-group 1 force
    no shutdown

interface fc1/15
    port-license acquire
    !
    !****************************************************************************
    ! Interfaces fc 1/16 to 1/47 are not configured and have been removed for brevity
    !*****************************************************************************
    !
interface fc1/48
interface mgmt0
    ip address 10.10.63.13 255.255.255.128
no system default switchport shutdown
end

Cisco Catalyst 2960s Management Switch

The Cisco Catalyst 2960s provides the Ethernet out-of-band network for the data center switches, servers, and appliances. The Cisco Catalyst 3750X and 3560X series switches can be used to provide a more resilient Ethernet out-of-band network transport.

version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname MGMT2960Sx
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$9njb$EENEj118AzAV5ScQWkN15.
!
username admin privilege 15 password 7 141443180F0B7B7977
no aaa new-model
clock timezone PST -8 0
clock summer-time PDT recurring
switch 1 provision ws-c2960s-24ts-l
!
ip domain-name cisco.local
ip name-server 10.10.48.10
vtp mode transparent
udld enable
!
crypto pki trustpoint TP-self-signed-1303691904
    enrollment selfsigned
    subject-name cn=IOS-Self-Signed-Certificate-1303691904
    revocation-check none
    rsakeypair TP-self-signed-1303691904
!
crypto pki certificate chain TP-self-signed-1303691904
certificate self-signed 01
30820240 308201B7 A0030201 02020101 300D0609 2A864886 F70D0101
04050030
31312F30 2D060355 04031326 49F532D 53656C66 2D536967 6E65642D
43657274
69666963 6174652D 31333033 36393139 3034301E 170D3933 30333031
30303133
32395A17 0D323030 31303130 3035A303 312F302D 06035504
31332649
4F532D53 65C662D 53696766 65642D43 65726E66 66696361 74652D31
33303336
39313930 3430819F 300D0609 2A864886 F70D0101 01050003 818D0030
818D0281
8100AA1F 298D4C56 BC5D18DC 793243AF 6A361866 8A4E9C97
2C5D313A
0A90966 07F0B57D 693234C7 F32754D1 4A87428C 03CFECA6 8E036C41
59F27DAC
0114ED26 31E4D253 9FA7023A B6CD12C6 0F611771 88B72913 F194CD32
18F3C117
FDC97684 57B653FF 0C69E9B9 81CD1620 8196C97 2D35336E 2805366E
44E3D619
ECB70203 010001A3 76307430 0F060355 1D310101 FP040530 03D0110F
30210603
551D1104 1A301822 164D474D 54323936 3057382E 63697366 6F2E6C6E
63616C30
1F060355 1D230418 30168014 FFE48865 4B9A8A46 5C63466D BD1O62EA
A980EA3F
31D0603 551D0E04 160414FF E488654B AD8A46C 63466DBD 1062EA9
80EAE3F0
0D06092A 864886F7 0D010104 05303831 8105C5E9 7A1405C0 9CD3BC6A
80EAE3F0
0D06092A 864886F7 0D010104 05303831 8105C5E9 7A1405C0 9CD3BC6A
80EAE3F0
0D06092A 864886F7 0D010104 05303831 8105C5E9 7A1405C0 9CD3BC6A
80EAE3F0
529B419B A5CF9E4D 2EC7FE18 1DB34199 B90AD136 E52B0A19
78CCBF57
399D8DA8 2BF88006 F5D13283 9DC1982C 1135C0E7 148AA7A7 D82791D0
7CD5B9A9
8DC4124 C2F35F02 ED123A7A 98E65B56 6AA0DB08 198E2980 5CD8508C
D2B9A150
7FE20B10 8CE54EEF 4FB7F858 6A7AA073 4989
quit
! spanning-tree mode rapid-pvst
spanning-tree extend system-id
! port-channel load-balance src-dst-ip
! vlan internal allocation policy ascending
! vlan 163
  name DC-Management
! ip ssh version 2
! interface Port-channel1
  switchport trunk allowed vlan 163
  switchport mode trunk
! interface FastEthernet0
  no ip address
! interface GigabitEthernet1/0/1
  description DC5548a MGMT0
  switchport access vlan 163
  switchport mode access
spanning-tree portfast
! interface GigabitEthernet1/0/2
  description DC5548b MGMT0
  switchport access vlan 163
  switchport mode access
spanning-tree portfast
!***************************************************************************
! Interfaces GigabitEthernet 1/0/3 to 1/0/21 are configured the same way and have been removed for brevity
***************************************************************************
interface GigabitEthernet1/0/22
  switchport access vlan 163
  switchport mode access
  spanning-tree portfast

interface GigabitEthernet1/0/23
  description DC5548a Eth1/21
  switchport trunk allowed vlan 163
  switchport mode trunk
  channel-protocol lacp
  channel-group 1 mode active

interface GigabitEthernet1/0/24
  description DC5548b Eth1/21
  switchport trunk allowed vlan 163
  switchport mode trunk
  channel-protocol lacp
  channel-group 1 mode active

interface GigabitEthernet1/0/25

interface GigabitEthernet1/0/26

interface GigabitEthernet1/0/27

interface GigabitEthernet1/0/28

interface Vlan1
  no ip address

ip http server
ip http secure-server

logging esm config
snmp-server community cisco RO
snmp-server community cisco123 RW

line con 0
line vty 0 4
  login local
  transport input ssh
line vty 5 15
  login local
  transport input ssh

ntp server 10.10.48.17
end
Cisco ASA 5585 - Primary

The Cisco ASA 5585 Firewalls for the SBA data center are provisioned in pairs for resiliency. This is the primary firewall configuration.

ASA Version 8.4(2)
!
hostname dc5585
enable password 2y4FIGBVVyBLauOQ encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0/0
  shutdown
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/1
  description LAN/STATE Failover Interface
!
interface GigabitEthernet0/2
  shutdown
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/3
  shutdown
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/4
  shutdown
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/5
  shutdown
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/6
  shutdown
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/7
  shutdown
  no nameif
  no security-level
  no ip address
!
interface Management0/0
  shutdown
  no nameif
  no security-level
  no ip address
!
interface Management0/1
  shutdown
  no nameif
  no security-level
  no ip address
! interface TenGigabitEthernet0/8
description Trunk to DC5548x TenGigx/x/x
cchannel-group 10 mode passive
no nameif
no security-level
no ip address
!
interface TenGigabitEthernet0/9
description Trunk to DC5548x TenGigx/x/x
cchannel-group 10 mode passive
no nameif
no security-level
no ip address
!
interface GigabitEthernet1/0
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet1/7
shutdown
no nameif
no security-level
no ip address
!
interface TenGigabitEthernet1/8
shutdown
no nameif
no security-level
no ip address
!
interface TenGigabitEthernet1/9
shutdown
no nameif
no security-level
no ip address
!
interface Port-channel10
description ECLB Trunk to 5548 Switches
nameif outside
security-level 0
ip address 10.10.53.126 255.255.255.128 standby 10.10.53.125
!
interface Port-channel10.153
description DC VLAN Outside the FW
nameif outside
security-level 0
ip address 10.10.53.126 255.255.255.128 standby 10.10.53.125
!
interface Port-channel10.154
description DC VLAN Inside the Firewall
nameif DC-InsideFW
security-level 75
ip address 10.10.54.1 255.255.255.0 standby 10.10.54.2
!
interface Port-channel10.155
description DC VLAN Inside the FW w/ IPS
nameif DC-InsideIPS
security-level 75
ip address 10.10.55.1 255.255.255.0 standby 10.10.55.2
!
ftp mode passive
object network BladeWeb1Secure
host 10.10.54.100
object network BladeWeb2Secure
   host 10.10.55.100
object network Secure-Subnets
   subnet 10.10.54.0 255.255.255.0
object network SecureIPS-Subnets
   subnet 10.10.55.0 255.255.255.0
object network Mgmt-host-range
   range 10.10.48.224 10.10.48.254
object-group network Application-Servers
   description HTTP, HTTPS, DNS, MSExchange
   network-object object BladeWeb1Secure
   network-object object BladeWeb2Secure
object-group service MS-App-Services
   service-object tcp destination eq domain
   service-object tcp destination eq www
   service-object tcp destination eq https
   service-object tcp destination eq netbios-ssn
   service-object udp destination eq domain
   service-object udp destination eq nameserver
   service-object udp destination eq netbios-dgm
   service-object udp destination eq netbios-ns
object-group network DC_Secure_Subnet_List
   network-object object Secure-Subnets
   network-object object SecureIPS-Subnets
object-group service Mgmt-Traffic
   service-object tcp destination eq ssh
   service-object udp destination eq snmp
object-group network Bypass-Rule
   description Open Policy for Server Access
   network-object object BladeWeb1Secure
   network-object object BladeWeb2Secure
access-list global_access extended permit object-group MS-App-Services any object-group Application-Servers
access-list global_access extended permit object-group Mgmt-Traffic object Mgmt-host-range object-group DC_Secure_Subnet_List
access-list global_access extended permit ip any object-group Bypass-Rule log disable inactive

access-list global_mpc extended permit ip any any
pager lines 24
mtu outside 1500
mtu DC-InsideFW 1500
mtu DC-InsideIPS 1500
failover
failover lan unit primary
failover lan interface failover GigabitEthernet0/1
failover polltime unit msec 200 holdtime msec 800
failover polltime interface msec 500 holdtime 5
failover key *****
failover replication http
failover link failover GigabitEthernet0/1
failover interface ip failover 10.10.53.130 255.255.255.252
standby 10.10.53.129
monitor-interface outside
monitor-interface DC-InsideFW
monitor-interface DC-InsideIPS
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
route outside 0.0.0.0 0.0.0.0 10.10.53.1 1
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
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
user-identity default-domain LOCAL
http server enable
http 10.0.0.0 255.0.0.0 outside
no snmp-server location
no snmp-server contact

February 2012 Series
Cisco ASA 5585 IPS SSP - Primary

The Cisco ASA 5585 Firewall for the SBA data center is provisioned with an internal Intrusion Prevention System (IPS) security services processor (SSP). The combined Cisco ASA Firewall and IPS operate in resilient pairs. This is the primary Cisco ASA 5585 IPS SSP.

! Version 7.1(2)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S581.0   2011-07-11
! ------------------------------
service interface
exit

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

service authentication
exit

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

service event-action-rules rules0
overrides deny-packet-inline
override-item-status Enabled
risk-rating-range 100-100
exit
exit

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

service host
network-settings
host-ip 10.10.63.21/24, 10.10.63.1
host-name IPS-SSP20-A
telnet-option disabled
access-list 10.10.0.0/16
dns-primary-server enabled
address 10.10.48.10
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 10.10.48.17
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
exit

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

service analysis-engine
exit
Cisco ASA 5585 - Secondary

The Cisco ASA 5585 Adaptive Security Appliances for the SBA data center are provisioned in pairs for resiliency. Although this is the secondary Cisco ASA 5585, with the exception of a few lines, the configuration is the same as the primary Cisco ASA 5585.

ASA Version 8.4(2)

hostname dc5585
enable password 2y4F1GIVyBBLau0Q encrypted
passwd 2KFQnbNIdI.2KY0U encrypted
names

interface GigabitEthernet0/0
shutdown
no nameif
no security-level
no ip address

interface GigabitEthernet0/1
description LAN/STATE Failover Interface

interface GigabitEthernet0/2
shutdown
no nameif
no security-level
no ip address

interface GigabitEthernet0/3
shutdown
no nameif
no security-level
no ip address

interface GigabitEthernet0/4
shutdown
no nameif
no security-level

interface GigabitEthernet0/5
shutdown
no nameif
no security-level
no ip address

interface GigabitEthernet0/6
shutdown
no nameif
no security-level
no ip address

interface GigabitEthernet0/7
shutdown
no nameif
no security-level
no ip address

interface Management0/0
shutdown
no nameif
no security-level
no ip address

interface Management0/1
shutdown
no nameif
no security-level
no ip address

interface TenGigabitEthernet0/8
description Trunk to DC5548x TenGigx/x/x
cchannel-group 10 mode passive
no nameif
no security-level
no ip address
!
interface TenGigabitEthernet0/9
  description Trunk to DC5548x TenGigE TenGigE
  channel-group 10 mode passive
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet1/0
  shutdown
  no nameif
  no security-level
  no ip address
!
Interfaces GigabitEthernet 1/1 to 1/6
are unconfigured and have been removed for brevity
!*****************************************************************************
!
interface GigabitEthernet1/7
  shutdown
  no nameif
  no security-level
  no ip address
!
interface TenGigabitEthernet1/8
  shutdown
  no nameif
  no security-level
  no ip address
!
interface TenGigabitEthernet1/9
  shutdown
  no nameif
  no security-level
  no ip address
!
interface Port-channel10
  description ECLB Trunk to 5548 Switches
  no nameif
  no security-level
  no ip address
!
interface Port-channel10.153
  description DC VLAN Outside the FW
  vlan 153
  nameif outside
  security-level 0
  ip address 10.10.53.126 255.255.255.128 standby 10.10.53.125
!
interface Port-channel10.154
  description DC VLAN Inside the Firewall
  vlan 154
  nameif DC-InsideFW
  security-level 75
  ip address 10.10.54.1 255.255.255.0 standby 10.10.54.2
!
interface Port-channel10.155
  description DC VLAN Inside the FW w/ IPS
  vlan 155
  nameif DC-InsideIPS
  security-level 75
  ip address 10.10.55.1 255.255.255.0 standby 10.10.55.2
!
ftp mode passive
object network BladeWeb1Secure
  host 10.10.54.100
object network BladeWeb2Secure
  host 10.10.55.100
object network Secure-Subnets
  subnet 10.10.54.0 255.255.255.0
object network SecureIPS-Subnets
  subnet 10.10.55.0 255.255.255.0
object network Mgmt-host-range
  range 10.10.48.224 10.10.48.254
object-group network Application-Servers
description HTTP, HTTPS, DNS, MExchange
network-object object BladeWeb1Secure
network-object object BladeWeb2Secure
object-group service MS-App-Services
  service-object tcp destination eq domain
  service-object tcp destination eq www
  service-object tcp destination eq netbios-ssn
  service-object udp destination eq domain
  service-object udp destination eq nameserver
  service-object udp destination eq netbios-dgm
object-group network DC_Secure_Subnet_List
  network-object object Secure-Subnets
  network-object object SecureIPS-Subnets
object-group service Mgmt-Traffic
  service-object tcp destination eq ssh
  service-object udp destination eq snmp
object-group network Bypass-Rule
description Open Policy for Server Access
network-object object BladeWeb1Secure
network-object object BladeWeb2Secure
access-list global_access extended permit object-group MS-App-Services any object-group Application-Servers
access-list global_access extended permit object-group Mgmt-Traffic object Mgmt-host-range object-group DC Secure_Subnet_List
access-list global_access extended permit ip any object-group Bypass-Rule
log disable inactive
access-list global_mpc extended permit ip any any
pager lines 24
mtu outside 1500
mtu DC-InsideFW 1500
mtu DC-InsideIPS 1500
failover lan unit secondary
failover lan interface failover GigabitEthernet0/1
failover polltime unit msec 200 holdtime msec 800
failover polltime interface msec 500 holdtime 5
failover key *****
failover replication http
failover link failover GigabitEthernet0/1
failover interface ip failover 10.10.53.130 255.255.255.252
standby 10.10.53.129
monitor-interface outside
monitor-interface DC-InsideFW
monitor-interface DC-InsideIPS
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
route outside 0.0.0.0 0.0.0.0 10.10.53.1 1
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
user-identity default-domain LOCAL
http server enable
http 10.0.0.0 255.0.0.0 outside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown
coldstart warmstart
telnet timeout 5
ssh timeout 5
console timeout 0
!
tls-proxy maximum-session 1000
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 10.10.48.17
webvpn
username admin password w2Y.6Op4j7c1VDk2 encrypted
!
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
parameters
message-length maximum client auto
message-length maximum 512
policy-map global_policy

class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect ip-options
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
class global-class
ips inline fail-close
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
profile CiscoTAC-1
no active
destination address http https://tools.cisco.com/its/service/ddcse/services/DDCEService
destination address email callhome@cisco.com
destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory periodic monthly 11
subscribe-to-alert-group configuration periodic monthly 11
subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:77006c6818fae44e9eb91c103680c343

Cisco ASA 5585 IPS SSP - Secondary
The Cisco ASA 5585 Adaptive Security Appliance for the SBA data center is provisioned with an internal IPS SSP. The combined Cisco ASA and IPS operate in resilient pairs. Although this is the secondary Cisco ASA IPS SSP in the secondary Cisco ASA, with the exception of a few lines, the configuration is the same as the primary Cisco ASA IPS SSP in the primary Cisco ASA.

! Version 7.1(2)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S581.0   2011-07-11
! ------------------------------
service interface
eexit
! ------------------------------
service authentication
eexit
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Enabled
risk-rating-range 100-100
exit
risk-categories
risk-levels edit _r1
threshold 100
exit
risk-levels move _r1 begin
risk-levels move _r2 after _r1
risk-levels move _r3 after _r2
exit
exit
! ------------------------------
service host
network-settings
host-ip 10.10.63.23/24,10.10.63.1
host-name IPS-SSP20-B
telnet-option disabled
access-list 10.10.0.0/16
dns-primary-server enabled
address 10.10.48.10
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 10.10.48.17
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
exit
! ------------------------------
service analysis-engine
exit
exit
Cisco ACE - Primary

This Cisco ACE 4710 appliance is one of a resilient pair providing Layer 4 through Layer 7 switching services for the SBA data center. This is the primary ACE of the pair.

no ft auto-sync startup-config
boot system image:c4710ace-t1k9-mz.A5_1_0.bin

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 912
  switchport trunk native vlan 1
  switchport trunk allowed vlan 148
  no shutdown

access-list ALL line 8 extended permit ip any any

probe http http-probe
  interval 15
  passdetect interval 60
  request method head

expect status 200 200
open 1
probe icmp icmp-probe
  interval 15
  passdetect interval 60
rserver redirect redirect1
  conn-limit max 4000000 min 4000000
  webhost-redirection https://%h%p 302
  inservice
rserver host webserver1
  ip address 10.10.48.111
  conn-limit max 4000000 min 4000000
  probe icmp-probe
  inservice
rserver host webserver2
  ip address 10.10.48.112
  conn-limit max 4000000 min 4000000
  probe icmp-probe
  inservice
rserver host webserver3
  ip address 10.10.48.113
  conn-limit max 4000000 min 4000000
  probe icmp-probe
  inservice
rserver host webserver4
  ip address 10.10.48.114
  conn-limit max 4000000 min 4000000
  probe icmp-probe
  inservice
serverfarm host appfarm
  probe http-probe
  rserver webserver3 80
    conn-limit max 4000000 min 4000000
      inservice
    rserver webserver4 80
serverfarm redirect http-redirect
  rserver redirect1
    conn-limit max 4000000 min 4000000
    inservice
  rserver redirect2
    conn-limit max 4000000 min 4000000
    inservice
serverfarm host webfarm
  probe http-probe
  rserver webserver1 80
    conn-limit max 4000000 min 4000000
    inservice
  rserver webserver2 80
    conn-limit max 4000000 min 4000000
    inservice

sticky http-cookie APPSESSIONID app-sticky
  cookie insert browser-expire
serverfarm appfarm

ssl-proxy service app-ssl-proxy
  key cisco-sample-key
  cert cisco-sample-cert

class-map type http loadbalance match-any default-compression-exclusion-mime-type
description DM generated classmap for default LB compression
exclusion mime types.
  2 match http url .*gif
  3 match http url .*css
  4 match http url .*js
  5 match http url .*class
  6 match http url .*jar
  7 match http url .*cab
  8 match http url .*txt
  9 match http url .*ps
 10 match http url .*vbs
 11 match http url .*xsl
 12 match http url .*xml
 13 match http url .*pdf
 14 match http url .*swf
 15 match http url .*jpg
 16 match http url .*jpeg
 17 match http url .*jpe
 18 match http url .*png
class-map match-all http-vip
  2 match virtual-address 10.10.48.100 tcp eq www
class-map match-all http-vip-redirect
  2 match virtual-address 10.10.48.101 tcp eq www
class-map match-all https-vip
  2 match virtual-address 10.10.48.101 tcp eq https
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

policy-map type loadbalance first-match http-vip-17slb
  class default-compression-exclusion-mime-type
    serverfarm webfarm
    class class-default
      serverfarm webfarm
        compress default-method deflate
policy-map type loadbalance first-match http-vip-redirect-17slb
  class class-default
    serverfarm http-redirect
policy-map type loadbalance first-match https-vip-17slb
  class default-compression-exclusion-mime-type
Cisco ACE - Secondary

This Cisco ACE 4710 appliance is one of a resilient pair providing Layer 4 through Layer 7 switching services for the SBA data center. Although this is the secondary Cisco ACE of the pair, with the exception of a few lines, the configuration is the same as the primary Cisco ACE.

interface vlan 148
  ip address 10.10.48.119 255.255.255.0
  peer ip address 10.10.48.120 255.255.255.0
  access-group input ALL
  nat-pool 1 10.10.48.99 10.10.48.99 netmask 255.255.255.0 pat
  service-policy input remote_mgmt_allow_policy
  service-policy input int148
  no shutdown

interface gigabitEthernet 1/1
  no shutdown
interface gigabitEthernet 1/2
  no shutdown
interface gigabitEthernet 1/3
  shutdown
interface gigabitEthernet 1/4
  shutdown

access-list ALL line 8 extended permit ip any any
probe http http-probe
   interval 15
   passdetect interval 60
   request method head
   expect status 200 200
   open 1
probe icmp icmp-probe
   interval 15
   passdetect interval 60

rserver redirect redirect1
   conn-limit max 4000000 min 4000000
   webhost-redirection https://%h%p 302
   inservice
rserver host webserver1
   ip address 10.10.48.111
   conn-limit max 4000000 min 4000000
   probe icmp-probe
   inservice
rserver host webserver2
   ip address 10.10.48.112
   conn-limit max 4000000 min 4000000
   probe icmp-probe
   inservice
rserver host webserver3
   ip address 10.10.48.113
   conn-limit max 4000000 min 4000000
   probe icmp-probe
   inservice
rserver host webserver4
   ip address 10.10.48.114
   conn-limit max 4000000 min 4000000
   probe icmp-probe
   inservice
serverfarm host appfarm
   probe http-probe
   rserver webserver3 80
   conn-limit max 4000000 min 4000000
   inservice
   rserver webserver4 80
   conn-limit max 4000000 min 4000000
   inservice
serverfarm redirect http-redirect
   rserver redirect1
       conn-limit max 4000000 min 4000000
       inservice
serverfarm host webfarm
   probe http-probe
   rserver webserver1 80
       conn-limit max 4000000 min 4000000
       inservice
   rserver webserver2 80
       conn-limit max 4000000 min 4000000
       inservice
   sticky http-cookie APPSESSIONID app-sticky
       cookie insert browser-expire
   serverfarm appfarm
   ssl-proxy service app-ssl-proxy
       key cisco-sample-key
       cert cisco-sample-cert
   class-map type http loadbalance match-any default-compression-exclusion-mime-type
       description DM generated classmap for default LB compression
       exclusion mime_types.
       2 match http url .*gif
       3 match http url .*css
       4 match http url .*js
       5 match http url .*class
       6 match http url .*jar
       7 match http url .*cab
8 match http url .*txt
9 match http url .*ps
10 match http url .*vbs
11 match http url .*xsl
12 match http url .*xml
13 match http url .*ps
14 match http url .*swf
15 match http url .*jpg
16 match http url .*jpeg
17 match http url .*jpe
18 match http url .*png

class-map match-all http-vip
  2 match virtual-address 10.10.48.100 tcp eq www

class-map match-all http-vip-redirect
  2 match virtual-address 10.10.48.101 tcp eq www

class-map match-all https-vip
  2 match virtual-address 10.10.48.101 tcp eq https

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

policy-map type loadbalance first-match http-vip-17slb
  class default-compression-exclusion-mime-type
    serverfarm webfarm
  class class-default
    serverfarm http-redirect
  policy-map type loadbalance first-match https-vip-17slb
    class default-compression-exclusion-mime-type
    sticky-serverfarm app-sticky
    class class-default
    compress default-method deflate
    sticky-serverfarm app-sticky

policy-map multi-match int148
  class http-vip
    loadbalance vip inservice
    loadbalance policy http-vip-17slb
    nat dynamic 1 vlan 148
  class https-vip
    loadbalance vip inservice
    loadbalance policy https-vip-17slb
    nat dynamic 1 vlan 148
    ssl-proxy server app-ssl-proxy
  class http-vip-redirect
    loadbalance vip inservice
    loadbalance policy http-vip-redirect-17slb
  interface vlan 148
    ip address 10.10.48.120 255.255.255.0
    peer ip address 10.10.48.119 255.255.255.0
    access-group input ALL
    nat-pool 1 10.10.48.99 10.10.48.99 netmask 255.255.255.0 pat
    service-policy input remote_mgmt_allow_policy
    service-policy input int148
    no shutdown

ft interface vlan 912
  ip address 10.255.255.2 255.255.255.0
  peer ip address 10.255.255.1 255.255.255.0
  no shutdown
ft peer 1
  heartbeat interval 300
  heartbeat count 10
  ft-interface vlan 912
ft group 1
  peer 1
  associate-context Admin
  inservice

ip route 0.0.0.0 0.0.0.0 10.10.48.1

username admin password 5 $1$Ea1NDXE$5Gtqr6f7iiBRSoYMHGsIo.
role Admin domain default-domain
username www password 5 $1$vkTih071$XO963GMFgoXfeBujUC6b50 role
Admin domain default-domain
Appendix A: Product List

The following products and software versions have been validated for Cisco SBA.

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Product</th>
<th>Part Numbers</th>
<th>Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet Infrastructure</td>
<td>Nexus 5548UP</td>
<td>N5K-C5548UP-FA</td>
<td>NX-OS 5.1(3)N1(1)</td>
</tr>
<tr>
<td></td>
<td>Nexus 5548 Layer 3 Daughter Card</td>
<td>N55-D160L3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Nexus 2248TP</td>
<td>N2K-C2248TP-1GE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Nexus 2232PP</td>
<td>N2K-C2232PP-10GE</td>
<td></td>
</tr>
<tr>
<td>Storage Infrastructure</td>
<td>MDS 9148</td>
<td>DS-C9148D-8G16P-K9</td>
<td>NX-OS 5.0(7)</td>
</tr>
<tr>
<td></td>
<td>MDS 9124</td>
<td>DS-C9124-K9</td>
<td></td>
</tr>
<tr>
<td>Network Security</td>
<td>ASA 5585-X</td>
<td>ASA5585-S40-K9</td>
<td>ASA: 8.4.2</td>
</tr>
<tr>
<td></td>
<td>ASA 5585-X IPS SSP</td>
<td>ASA5585-SSP-IPS20</td>
<td>IPS: 7.1-2-E4</td>
</tr>
<tr>
<td>Application Resiliency</td>
<td>Cisco ACE 4710 Appliance</td>
<td>ACE-4710-0.5-K9</td>
<td>A5(1.0)</td>
</tr>
<tr>
<td>Computing Resources</td>
<td>UCS 6120XP 20-port Fabric Interconnect</td>
<td>N10-S6100</td>
<td>Cisco UCS Release version 2.0t</td>
</tr>
<tr>
<td></td>
<td>6-port 8Gb FC/Expansion module/UCS 6100 Series</td>
<td>N10-E0060</td>
<td></td>
</tr>
<tr>
<td></td>
<td>UCS 5108 Blade Server Chassis</td>
<td>N20-C6508</td>
<td></td>
</tr>
<tr>
<td></td>
<td>UCS 2104XP Fabric Extender</td>
<td>N20-I6584</td>
<td></td>
</tr>
<tr>
<td></td>
<td>UCS B200 M2 Blade Server</td>
<td>N20-B6625-1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>UCS B250 M2 Blade Server</td>
<td>N20-B6625-2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>UCS M81KR Virtual Interface Card</td>
<td>N20-AC0002</td>
<td></td>
</tr>
<tr>
<td></td>
<td>UCS C200 M2 Server</td>
<td>R200-1120402W</td>
<td></td>
</tr>
<tr>
<td></td>
<td>UCS C210 M2 Server</td>
<td>R210-2121605W</td>
<td></td>
</tr>
<tr>
<td></td>
<td>UCS C250 M2 Server</td>
<td>R250-2480805W</td>
<td></td>
</tr>
</tbody>
</table>
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.