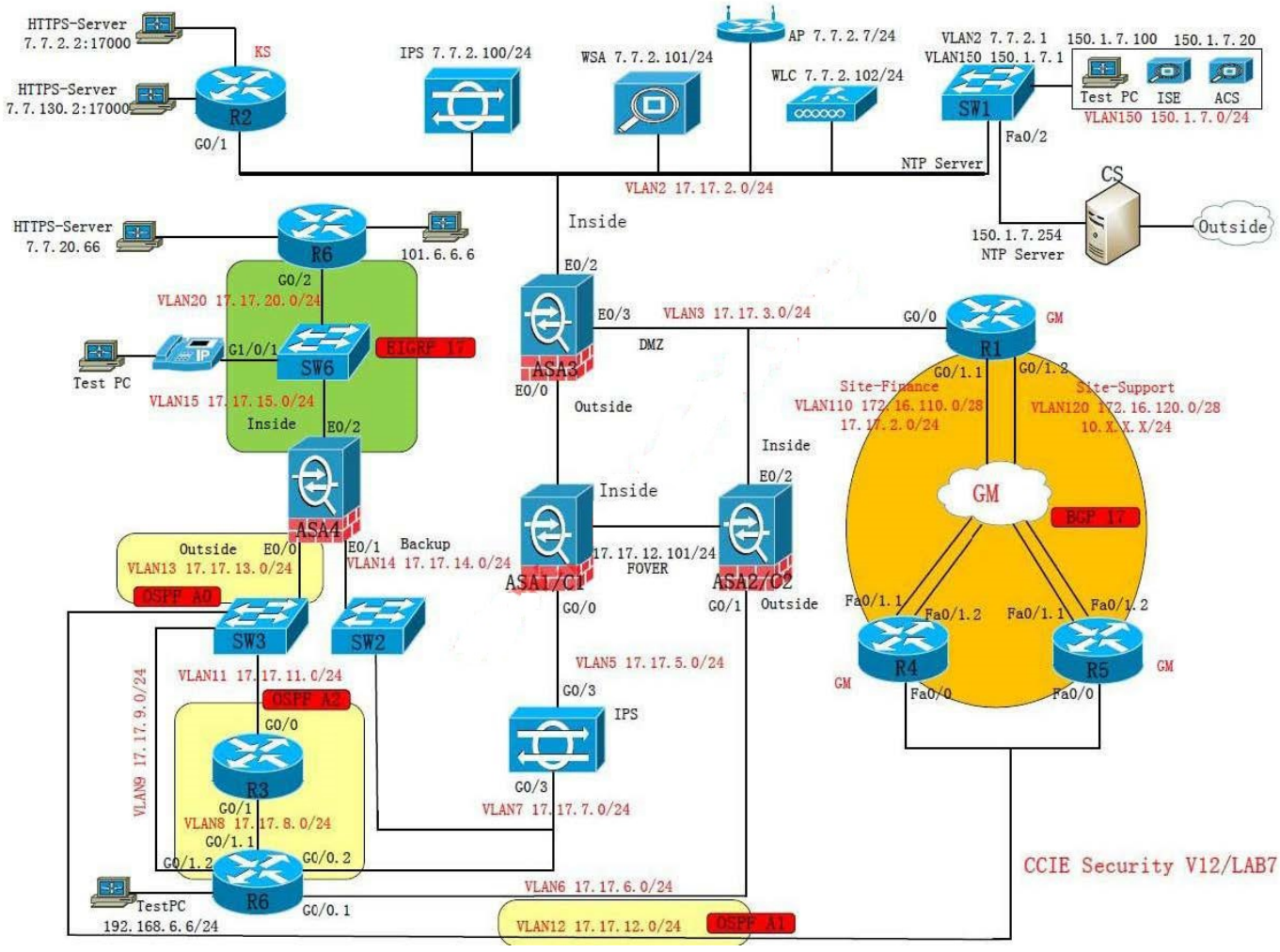
CCIE Security lab (v4.0)

Ver:S7

Update 2016-11-05


HTTPS-Server
7.7.2.2:17000
HTTPS-Server
7.7.130.2:17000
KS
R2
G0/1
IPS 7.7.2.100/24
WSA 7.7.2.101/24
AP 7.7.2.7/24
WLC 7.7.2.102/24
VLAN2 7.7.2.1
VLAN150 150.1.7.1
SW1
150.1.7.100
150.1.7.20
Test PC
ISE
ACS
VLAN150 150.1.7.0/24
Fa0/2
NTP Server
VLAN2 17.17.2.0/24
CS
150.1.7.254
NTP Server
Outside
HTTPS-Server
7.7.20.66
R6
101.6.6.6
G0/2
VLAN20 17.17.20.0/24
Test PC
G1/0/1
SW6
EIGRP 17
VLAN15 17.17.15.0/24
Inside
E0/2
ASA4
Inside
E0/2
E0/3
VLAN3 17.17.3.0/24
DMZ
ASA3
E0/0
Outside
G0/0
GM
R1
G0/1.1
G0/1.2
Site-Finance
VLAN110 172.16.110.0/28
17.17.2.0/24
Site-Support
VLAN120 172.16.120.0/28
10.X.X.X/24
GM
BGP 17
Outside
E0/0
VLAN13 17.17.13.0/24
OSPF A0
E0/1
Backup
VLAN14 17.17.14.0/24
Inside
E0/2
ASA1/C1
17.17.12.101/24
FOVER
ASA2/C2
G0/1
Outside
G0/0
SW3
SW2
VLAN11 17.17.11.0/24
OSPF A2
VLAN9 17.17.9.0/24
G0/0
R3
G0/1
VLAN8 17.17.8.0/24
G0/1.1
G0/1.2
G0/0.2
R6
G0/0.1
TestPC
192.168.6.6/24
VLAN5 17.17.5.0/24
G0/3
IPS
G0/3
VLAN7 17.17.7.0/24
VLAN6 17.17.6.0/24
VLAN12 17.17.12.0/24
OSPF A1
Fa0/1.1
Fa0/1.2
Fa0/1.1
Fa0/1.2
R4
R5
GM
GM
Fa0/0
Fa0/0
CCIE Security V12/LAB7

SECTION I. Perimeter Security

1.1 ASA3 Multiple security Zones Implementation

Task:

Configure ASA3 for multiple security zones using information in these tables

Interface	Nameif	Security	IP Address
E0/0	Outside	0	17.17.4.10/24
E0/2	Inside	100	7.7.2.10/24
E0/3	Dmz	50	17.17.3.10/24

To configure static routes:

Network	Zone	Next hop
7.7.16.6/32	Outside	17.17.4.12
7.7.5.0/24	Outside	17.17.4.12
17.17.13.0/24	Outside	17.17.4.12
17.17.12.0/24	Outside	17.17.4.12
17.17.14.0/24	Outside	17.17.4.12
17.17.8.0/24	Outside	17.17.4.12
150.1.7.1/32	Inside	7.7.2.1
150.1.7.20/32	Inside	7.7.2.1

SW4:

```
interface fa0/11 (outside)
sw host
sw acc vlan 4
exit

interface fa0/13 (inside)
sw host
sw acc vlan 2
exit

interface fa0/14 (dmz)
```

sw host
sw acc vlan 3
exit

ASA3:

interface Ethernet0/0

nameif outside

security-level 0

ip address 17.17.4.10 255.255.255.0

no shutdown

interface Ethernet0/2

nameif inside

security-level 100

ip address 7.7.2.10 255.255.255.0

no shutdown

interface Ethernet0/3

nameif dmz

security-level 50

ip address 17.17.3.10 255.255.255.0

no shutdown

==========route==========

route outside 17.17.5.0 255.255.255.0 17.17.4.12 1

route outside 7.7.16.6 255.255.255.255 17.17.4.12 1

route outside 17.17.8.0 255.255.255.0 17.17.4.12 1

route outside 17.17.12.0 255.255.255.0 17.17.4.12 1

route outside 17.17.13.0 255.255.255.0 17.17.4.12 1

route outside 17.17.14.0 255.255.255.0 17.17.4.12 1

route inside 150.1.7.1 255.255.255.255 7.7.2.1 1

route inside 150.1.7.20 255.255.255.255 7.7.2.1 1

1.2 ASA1-ASA2 Multiple context mode Active-Active Failover

Implementation

Task:

Configure ASA1-ASA2 in multiple context mode for active-active failover using information in these table:

Context name	Interface	Config-url
Admin	Management 0/0	Admin.cfg
C1	G0/0, G0/2	C1.cfg
C2	G0/1,g0/3	C2.cfg

C1 Interface	Nameif	Sec	Primary	Standby IP Address
G0/0	Outside	0	17.17.5.10/24	17.17.5.11/24
G0/2	Inside	100	17.17.4.12/24	17.17.4.11/24

To configure static routes:

Network	Zone	Next hop
4.4.4.4/32	Inside	17.17.4.10
5.5.5.5/32	Inside	17.17.4.10
7.7.16.6/32	Outside	17.17.5.2
17.17.12.0/24	Outside	17.17.5.6
17.17.13.0/24	Outside	17.17.5.6
17.17.14.0/24	Outside	17.17.5.2
17.17.8.0/24	Outside	17.17.5.6

C2 interface	Nameif	Security level	Primary IP Address	Standby IP Address
G0/1	Outside	0	17.17.6.10/24	17.17.6.11/24
G0/3	Inside	100	17.17.3.12/24	17.17.3.11/24

ASA1-ASA2	Name	Interface	Active IP address	Standby IP Address
Interface for Failover and stateful communication	Fover	G0/4	17.17.12.100/24	17.17.12.101/24

ASAs	Role	Active	Standby
ASA1	Primary	C1	C2
ASA2	Standby	C2	C1

SW2:

interface rang fa0/8 , fa0/13 (asa1-2 e0/0)

sw host

sw acc vlan 5

exit

interface rang fa0/9 , fa0/14 (asa1-2 e0/1)

sw host

sw acc vlan 6

exit

interface rang fa0/11 , fa0/15 (asa1-2 e0/2)

sw host

sw acc vlan 4

exit

interface rang fa0/12 , fa0/16 (asa1-2 e0/3)
sw host
sw acc vlan 3
exit

==========
System:

ASA1：

Interface e0/0

No shutdown

Exit

Interface e0/1

No shutdown

Exit

Interface e0/2

No shutdown

Exit

Interface e0/3

No shutdown

Exit

Interface m0/0

No shutdown

1.3 ASA3 NAT implementation

Task:

Configure ASA3 with network object NAT rules using information in these table

Inside address	Outside address
150.1.7.1	4.4.4.4
150.1.7.20	5.5.5.5

Inside address	DMZ Address
7.7.2.2	7.7.2.2

```
object network Inside1
 host 150.1.7.1
nat (inside,outside) static 4.4.4.4
object network Inside20
 host 150.1.7.20
nat (inside,outside) static 5.5.5.5
```

```
object network Inside2
 host 7.7.2.2
nat (inside,dmz) static 7.7.2.2
```

==========verify==========

ASA3(config)# packet-tracer input inside icmp 150.1.7.1 8 0 17.17.4.12

Phase: 1

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

MAC Access list

Phase: 2

Type: ROUTE-LOOKUP

Subtype: input

Result: ALLOW

Config:

Additional Information:

in 17.17.4.0 255.255.255.0 outside

Phase: 3

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 4

Type: INSPECT

Subtype: np-inspect

Result: ALLOW

Config:

Additional Information:

Phase: 5

Type: NAT

Subtype:

Result: ALLOW

Config:

object network INSIDE1

 nat (inside,outside) static 4.4.4.4

Additional Information:

Static translate 150.1.7.1/0 to 4.4.4.4/0

Phase: 6

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 11, packet dispatched to next module

Result:

input-interface: inside

input-status: up

input-line-status: up

output-interface: outside

output-status: up

output-line-status: up

Action: allow

ASA3(config)#

ASA3(config)# packet-tracer input inside icmp 150.1.7.20 8 0 17.17.4.12

Phase: 1

Type: ROUTE-LOOKUP

Subtype: input

Result: ALLOW

Config:

Additional Information:

in 17.17.4.0 255.255.255.0 outside

Phase: 2

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 3

Type: INSPECT

Subtype: np-inspect

Result: ALLOW

Config:

Additional Information:

Phase: 4

Type: NAT

Subtype:

Result: ALLOW

Config:

object network INSIDE2

nat (inside,outside) static 5.5.5.5

Additional Information:

Static translate 150.1.7.20/0 to 5.5.5.5/0

Phase: 5

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 12, packet dispatched to next module

Result:

input-interface: inside

input-status: up

input-line-status: up

output-interface: outside

output-status: up

output-line-status: up

Action: allow

ASA3(config)#

ASA3(config)# packet-tracer input inside icmp 7.7.2.2 8 0 17.17.3.1

Phase: 1

Type: ROUTE-LOOKUP

Subtype: input

Result: ALLOW

Config:

Additional Information:

in 17.17.3.0 255.255.255.0 DMZ

Phase: 2

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 3

Type: INSPECT

Subtype: np-inspect

Result: ALLOW

Config:

Additional Information:

Phase: 4

Type: NAT

Subtype:

Result: ALLOW

Config:

object network INSIDE3

nat (inside,DMZ) static 7.7.2.2

Additional Information:

Static translate 7.7.2.2/0 to 7.7.2.2/0

Phase: 5

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 13, packet dispatched to next module

Result:

input-interface: inside

input-status: up

input-line-status: up

output-interface: DMZ

output-status: up

output-line-status: up

Action: allow

ASA3(config)#

ASA3(config)# show nat

Auto NAT Policies (Section 2)

1 (inside) to (DMZ) source static INSIDE3 7.7.2.2

translate_hits = 1, untranslate_hits = 4

2 (inside) to (outside) source static INSIDE1 4.4.4.4

translate_hits = 1, untranslate_hits = 0

3 (inside) to (outside) source static INSIDE2 5.5.5.5

translate_hits = 1, untranslate_hits = 0

ASA3(config)#

1.4 ASA4 Route Mode implementation

Task:

Configure ASA4 using information in these tables:

Interface	Nameif	IP Address
E0/0	Outside	17.17.13.10/24
E0/1	Backup	17.17.14.10/24
E0/2	Inside	17.17.15.10/24

To configure static routes:

Network	Zone	Next hop
4.4.4.4/32	Outside	17.17.13.3
5.5.5.5/32	Outside	17.17.13.3
7.7.16.6/32	Inside	17.17.15.6

Solution

SW3:

interface fa0/13 (ASA3 e0/0)

sw host

sw acc vlan 13

exit