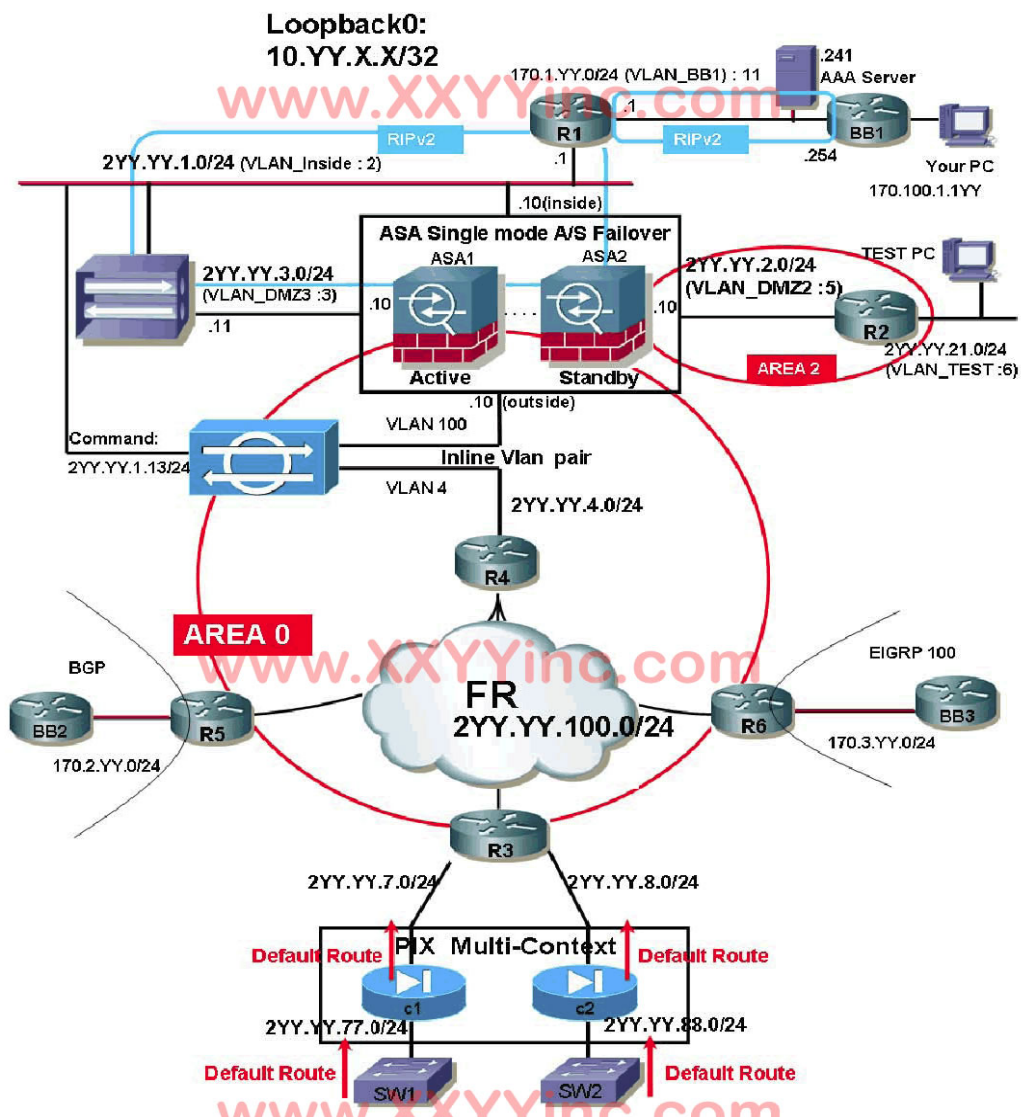


Cisco CCIE LAB Security Demo

V8

Update September, 2011



Pre-config (Routing see the topology)

R1 default route to 2YY.YY.1.10 . R2 default route to 2YY.YY.21.2

R4 default route to S0/0 R3 Static route 2yy. yy. 77. 0 point to 2yy. yy. 7. 1

R3 Static route 2yy. yy. 88. 0 point 2yy. yy. 8. 1

R3456 Frame-relay ospy network Point-to-multipoint. R3 redistribute static on ospf

Sw1 default route to 2YY.YY.77.1 Sw2 default route to 2YY.YY.88.1

1.1 ASA1 initialization

- Configure ASA 1 initialization , Use the exact names

Detail to Be Used

Interface name	interface	Security Level	IP Address
outside	Ethernet0/0	0	2YY.YY.4.10/24
inside	inside Ethernet0/1	100	2YY.YY.1.10/24
DMZ2	Ethernet0/2.2	20	2YY.YY.2.10/24
DMZ3	Ethernet0/2.3	30	2YY.YY.3.10/24

- Configure a default route pointing to the R4 IP address 2YY.YY.4.4
- Configure IP routing on ASA1

Interface	Protocol	Details	Redistribution
outside	OSPF	Area0	n/a
inside	RIPv2	--	RIP into OSPF only
DMZ2	OSPF	Area2	n/a
DMZ3	n/a	n/a	n/a

- You may allow any ICMP traffic in your ACL.
- Do NOT enable NAT control,

important Note:

- You must finish the configuration of Q3.1,Sensor Initialization, in the IPS section, configuring an inline **VLAN pair** between ASA1 outside(vlan 100) and R4 Ethernet0/0(vlan 4).
- When inline VLAN pair is configured correctly , traffic can pass between the ASA outside interface and R4
- Modify the switch parameters as appropriate to achieve this task

1.2 Cisco ASA Failover

- Configure LAN-based active/standby failover on ASA1 and ASA2
- ASA1 is the primary, and ASA2 is the secondary.
- Use Etheraet0/3 for the failover LAN interface as 'failover' with the IP address 2YY.YY.5.10 for active and 2YY.YY.5.20 for standby.
- Use the failover password cisco
- Use standby IP address as shown in the output below

1.3 PIX Initialization

Configure the admin, cl, and c2 contexts on the PIX as shown use the information given in the tables here. The context names are case-sensitive Admin Context Name ' admin'

Interface nameif	Allocate	Security Level	IP address
None	None	n/a	n/a

Context1 Name ' cl'

Interface nameif	Allocate	Security Level	IP address
outside	EthernetO	0	2YY. YY. 7. 1/24
inside	Ethernet1	100	2YY. YY. 77. 1/24

Context2 Name ' c2'

Interface nameif	Allocate	Security Level	IP address
outside	Ethernet2	0	2YY. YY. 8. 1/21
inside	Ethernet3	100	2YY. YY. 88. 1/24

- Configure a default route in the cl context pointing to R3 with the IP address 2YY. YY. 7.

3

- Configure a default route in the c2 context pointing to R3 with the IP address 2YY. YY. 8.

3

- You may allow any ICMP traffic in your ACL
- by default (no nat-control). Do NOT enable NAT control in any security contexts

1.4 Address Translations on ASA

- Configure static NAT on ASA1 for following conditions (do NOT enable NAT control):
- Telnet request to the ASA outside IP address 2YY.YY.4.10 on port 1123 should be redirected to the R1 Loopback0 IP address 10.YY.1.1
- Telnet request to the ASA outside IP address 2YY.YY.4.10 on port 2223 should be redirected to the R2 Loopback0 IP address 10.YY.2.2

Verify Telnet from R4:

```
RackYYR4#telnet 2YY.YY.4.10 1123 (will connect to R1)
```

```
RackYYR4#telnet 2YY.YY.4.10 2223 (will connect to R2)
```

- Configure policy Static NAT using the static command
- IP traffic destined for R4 Serial0/0, sourced from R1 Ethernet0/0(170.1.1.1), is translated As 2YY.YY.4.50 Verify the configuration with an extended ping from R1:
RackYYR1#ping 2YY.YY.100.4 source Etheraet0/0 (170.1.1.1)

1.5 Cisco IOS Firewall (CBAC)

- Configure CBAC on R6 and keep the following points under consideration:
- Configure the firewall outbound inspection on R6 Etheraet0/0 to protect your internal users from HTTP-based attacks coming from BB2
- Allow Java from a friendly site at 198.133.219.25 (www.cisco.com) while implicitly denying Java from all other sites.
- Configure an antispoofing ACL on the Etheraet0/0 ingress to prevent spoofing for the major net 2YY.YY.0.0/16 used in your network. Additionally, filter all RFC 1918 networks. You may permit any ICMP and Eigrp traffic in this ACL , Your ACL should Not have a permit ip any any statement.
- Fine-tune the firewall such that the router will start deleting half-open sessions when the number of half-open sessions reaches 1000 and stop deleting them when the number fails below 800.
- Ensure that all IP connectivity, IP routing , and configuration done in other sections of this exam continues to work after completion of this task

2.1 Troubleshooting DMVPN using mGRE

- RI and R6 are preconfigured for DMVPN using mGRE.
- RI is the hub and R6 is the spoke using IPsec profiles.
- There are three faults that have been injected into your preconfigurations, These issues can be related to either DMVPN IPsec configuration or other things within the network
- Configure an ASA firewall ACL to allow DMVPN (This is excluding the three faults)
- Ensure that the DMVPN tunnel gets established between RI and R6.

Verify the following outputs: Verify the following on RI and R6 show crypto isakmp sa

(Ensure that the state is QMIDLE) show crypto engine connections active

(Check the Encrypt/Decrypt counters)

Additionally, verify the following output on RI and R6: RackYYRI#show ip route eigrp 200

RackYYRI#ping 192.168.6.1 source loopback 10

2.2 VPN 3000 Concentrator Initialization

- The VPN 3000 Concentrator is NOT initialized. Initialize the VPN 3000 Concentrator using the details given in the table here.

Interface	IP address	VLAN	Routing Protocol
Public	2YY.YY.3.11/24	3	None (disabled)
Private	2YY.YY.1.11/24	2	RIPv2

- Configure interfaces for the VLANs on switch as shown in the table
- Configure default gateway to the ASA DMZ3 IP address: 2YY.YY.3.10
- Configure the hostname as 'RackYYVPN'.
- Modify the VPN 3000 Concentrator Telnet management port to 1123, verify on RI

RackYYRI#telnet 2YY.YY.1.11 1123

2.3 Remote-Access Cisco VPN Client

- Configure a remote-access VPN IPsec tunnel between the VPN3000 and the TEST PC.

Keep the following point under consideration:

- The VPN 3000 is the server site and the TEST PC is the client site.
- The following profile should be used: . Group name: VPN Client
- . Group password: cisco 123
- . Username and password: cisco and cisco 123

. Address pool range:170.1.YY.100 to 170.1.YY.200/24

- Static routes are permitted to complete this task.
- Ensure that you are able to ping 2YY.YY.4.4 on R4 from the R2 source FastEtheraet0/1.

```
RackYYR2#ping 2YY.YY.4.4 source FastEtheraet0/1
```

The Test PC is provided to verify this question. Place it in VLAN6,assign it with any IP address in the local subnet 2YY.YY.21.0/24,and add a static route for network 2YY.YY.0.0/16 pointing to 2YY.YY.21.2(R2).Ensure that you are able to ping R2 and R4 2YY.YY.4.4 form the TEST PC. Do NOT configure your default gateway to R2.

From the TEST PC, you should be able to successfully connect to the server using Cisco VPN Client that is provided.

2.4 ASA L2L

- Configure hub-and-spoke and spoke-to-spoke IPSec tunnels on the ASA , R3 and R5 using the following details:
 - The ASA firewall will be the hub.
 - R3 and R5 will be the spokes.
 - Use the pre-shared key 'cisco'
 - All spoke-to-spoke traffic should use IPSec tunnel via the hub.
 - Do not configure more than one crypto map on the spokes.
 - Ensure that the following ping commands are successful and that traffic is encrypted through IPSec .
 - Confirm the configuration using the show crypto engine connection active command.

```
RackYYRI#ping 10.YY.3.3 source loopback0 RackYYRI# ping 10.YY.5.5 source loopback0
```

```
RackYYR3# ping 10.YY.1.1 source loopback0 RackYYR3# ping 10.YY.5.5 source loopback0
```

```
RackYYR5# ping 10.YY.1.1 source loopback0 RackYYR5# ping 10.YY.3.3 source loopback0
```

Details to Be Used

	ASA1 HUB	R3 SPOKE	R5 SPOKE
Encrypt network via	loopback0 of 1 l	loopback0 of 3	oopback0 of 5
IPSec tunnel	10.yy.1.0/24	10.yy.3.0/24	10.yy.5.0/24
Crypto maps allowed	2 static crypto map	1 static crypto map	1 static crypto map

Use all other parameters as appropriate

3.1 IDS Initialization

Configure an inline VLAN pair using VLANs on FastEthernetl/O, where the first VLAN number is 4 and the second VLAN number is 100. Refer to the table here.

Parameter	Settings
Hostname	"RackYYIDS," where YY is your two-digit rack number (for example, for Rack 01,"Rack01IDS,"or for Rack ll,"Rackl 1IDS")
Management	Configure a command and control Interface in inside VLAN 2.
IP address	2yy.yy. 1.13/24
Default gateway	2yy.yy. 1.1
Inline VLAN pair	FastEthernetl/O,subinterface number 1 Vlan 1#4 (R4 Etheraet0/0) Vlan 2#100 (ASA1 outside)
ACL	2yy.yy.0.0/16,170.100.1.0/24,and 170.1 .yy.0/24
Enable signatures	ICMP echo and echo-reply to High alert severity

Refer to Diagram 2 for the switch port information.

Modify the switch parameters as appropriate to achieve this task

3.2 Application Inspection

- Configure deep packet inspection by enabling HTTP and FTP application inspection on the IOS appliance to prevent protocol abuse.
- Configure the custom AIC web port 8008 for HTTP traffic.

- Configure the maximum allowed HTTP requests per connection to 5

3.3 AIC Custom Signature

- Configure a new custom signature ID 62000 using the following parameters.
- Configure a MIME type signature based on the AIC engine.
- Do not use the SERVICE HTTP engine, use the AIC engine for HTTP.
- The signature must perform inspection for a large number of outstanding HTTP requests.
- Set the alarm severity to High alert.
- The following actions should occur upon signature matching:

Produce an alert

Do not transmit this packet and future packets on the TCP flow. Log packets outstanding the attacker victim address pair.

3.4 Signature Tuning

- Configure cisco IPS signature tuning for large ICMP data grams as follows:
- Modify the existing signature database for an IP datagram received with the protocol field of the IP header set to 1 (ICMP) and an IP length greater than 1024.
- Change the alarm severity to report this traffic as a High alert.
- Modify the signature to trigger for any IP datagram with a payload length ranging from
- To reduce the noise level, change the frequency to summarize the alerts.
- Make sure that you receive an alarm for this signature in the Event Viewer by using an extended ping with large ICMP packets with a datagram size in the range of 5000 to 10000 An example is given here on R4 of triggering this signature.

```
RackyyR4#ping 2yy.yy.4.10 size [5000-10000]
```

Type escape sequence to abort.

Sending 5, 10000-byte ICMP Echoes to 2yy.yy.4.10, timeout is 2 seconds:

```
!!!!
```

Success rate is 100 percent (5/5), round-trip min/avg/max = 28/30/32 ms

Note: No points will be awarded if alarms are not found in the Event Viewer.

4.1 Router Management and Access Control

- Configure user-based authentication, authorization and accounting on R5 using TACACS+ and keeping the following points under consideration:
- Configure ACS AAA client settings for R5 Loopback0 using TACACS+ with the key 'cisco',
- Configure a new user profile on the ACS (username "**user3**" with password "**cisco**") with privilege 3, and configure appropriate attributes for the authentication and authorization to complete this task.
- User3 should have the privileges needed to log in to router configuration mode and configure any routing protocols using the '**router**' command from global configuration mode,
- User3 should also be able to view the router configurations using the '**write term**' command; All other commands should be restricted.
- Configure R5 AAA for authentication and shell and command authorization, respectively.
- Configure R5 AAA to log all commands executed by user3 to the AAA server.
- Do not use '**default**' method it's use named method lists only, The console and aux ports should not be affected with AAA
- Adjust the ASA firewall ACL to allow R5 Loopback0 to communicate with the AAA server.
- As shown in diagram 1, the AAA server is located in BB1, with the IP address 170.1.yy.241.
-

Validate your configuration by telneting to R5 from any router or the TEST PC in your network. You can place the TEST PC in VLAN 6 and assign any IP address from the local subnet 2yy.yy.21.0/24 Add a static route for network 2yy.yy.0.0/16 pointing to 2yy.yy.21.2(R2)

4.2 Authentication for nonstandard application ports

Your organization is using a customized web application service running on TCP port 8080 in the BB1 network behind the ASA firewall. Configure the ACS and ASA firewall as follows: