CCNA Security 2.0 Practice Skills Assesement Part 2 – Packet Tracer

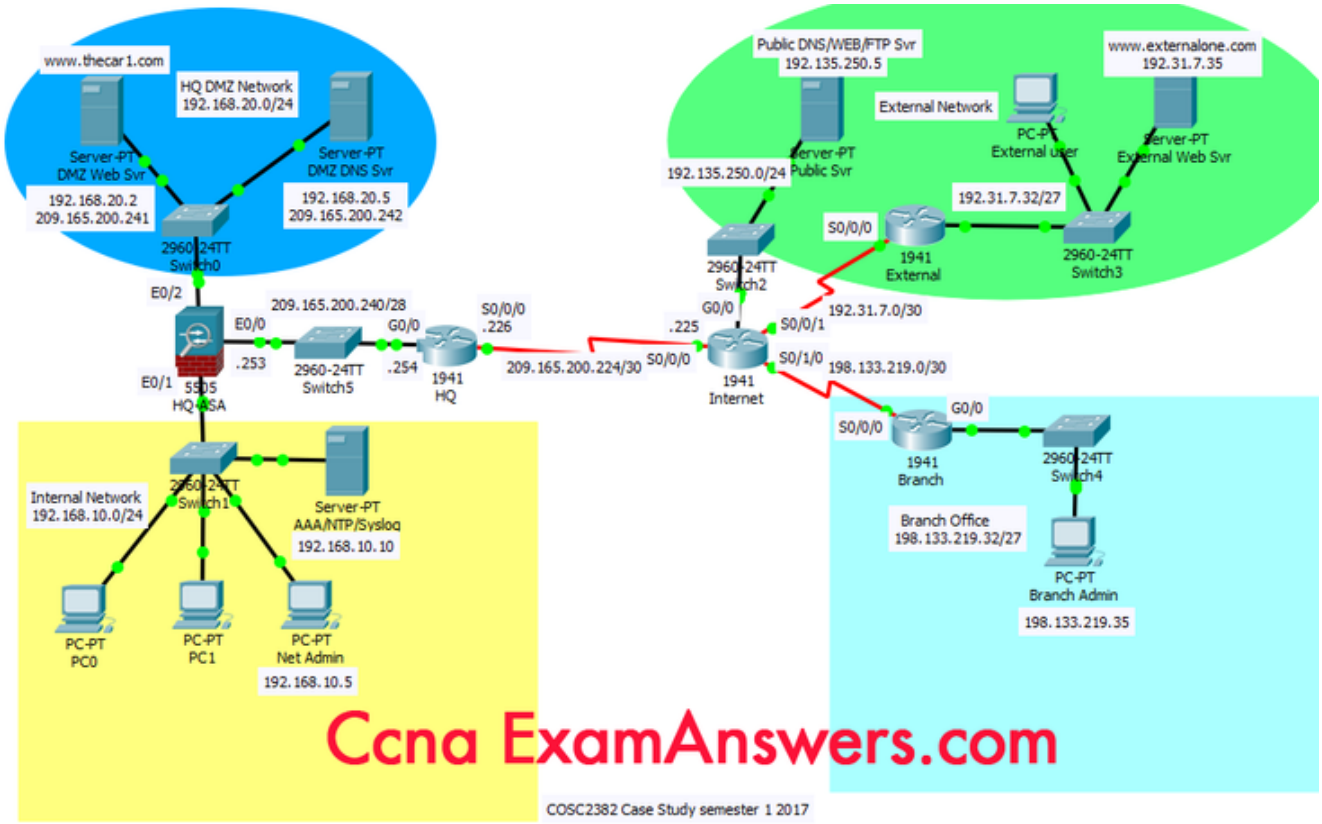
itexamanswers.net/ccna-security-2-0-practice-skills-assesement-part-2-packet-tracer.html

August 21, 2017

CCNA Security PT Practice SA – Part 2

A few things to keep in mind while completing this activity:

- Do not use the browser Back button or close or reload any Exam windows during the exam.
- Do not close Packet Tracer when you are done. It will close automatically.
- Click the Submit Assessment button to submit your work.



Introduction

In this practice Packet Tracer Skills Based Assessment, you will:

- Configure basic ASA device hardening and secure network management
- Configure DHCP and NAT on the ASA device
- Configure the ASA firewall to implement security policies
- Configure a site-to-site IPsec VPN

Addressing Table

Device	Interface	IP Address	Subnet Mask	Gateway	DNS server
Internet	S0/0/0	209.165.200.225	255.255.255.252	n/a	
	S0/0/1	192.31.7.1	255.255.255.252	n/a	
	G0/0	198.133.219.1	255.255.255.252	n/a	
	G0/0	192.135.250.1	255.255.255.0	n/a	
HQ	S0/0/0	209.165.200.226	255.255.255.252	n/a	
	G0/0	209.165.200.254	255.255.255.240	n/a	
HQ-ASA	E0/0	209.165.200.253	255.255.255.240	n/a	
	E0/1	192.168.10.1	255.255.255.0	n/a	
	E0/2	192.168.20.1	255.255.255.0	n/a	
Branch	S0/0/0	198.133.219.2	255.255.255.252	n/a	
	G0/0	198.133.219.62	255.255.255.224	n/a	
External Web Svr	NIC	192.31.7.35	255.255.255.224	192.31.7.62	
External PC	NIC	192.31.7.33	255.255.255.224	192.31.7.62	192.135.250.5
AAA/NTP/ Syslog Svr	NIC	192.168.10.10	255.255.255.0	192.168.10.1	
DMZ DNS Svr	NIC	192.168.20.5	255.255.255.0	192.168.20.1	
DMZ Web Svr	NIC	192.168.20.2	255.255.255.0	192.168.20.1	192.168.20.5
PC0 and PC1	NIC	DHCP client	255.255.255.0	192.168.10.1	192.168.10.10
Branch Admin	NIC	198.133.219.35	255.255.255.224	198.133.219.62	192.135.250.5
Net Admin PC	NIC	192.168.10.5	255.255.255.0	192.168.10.1	192.168.10.10

Note: Appropriate verification procedures should be taken after each configuration task to ensure that the task has been properly implemented.

Step 1: Configure Basic Device Hardening for the ASA device.

Note: HQ-ASA is already configured with a password **Thecar1Admin**.

a. Access HQ-ASA and enter the privileged mode with the enable password of **Thecar1Admin**.

b. Configure the domain name as **thecar1.com**.

c. Configure the inside, outside, and dmz interfaces with the following information:

- VLAN 1 – IP address 192.168.10.1/24, nameif **inside**, security-level **100**, assign to E0/1
- VLAN 2 – IP address 209.165.200.253/28, nameif **outside**, security-level **0**, assign to E0/0
- VLAN 3 – IP address 192.168.20.1/24, nameif **dmz**, security-level **70**, assign to E0/2
- Enable interfaces.

Step 2: Configure DHCP service on the ASA device for the internal network.

a. The DHCP pool is 192.168.10.25 – 192.168.10.35.
b. DHCP service should provide DNS server (AAA/NTP/syslog server) information.
c. Verify that the internal users (PC0 and PC1) obtain the dynamic addressing information correctly.

Step 3: Configure Secure Network Management for the ASA Device.

a. Enable the ASA device:
– as an NTP client to the AAA/NTP/Syslog server
– Enable the authentication to the NTP server.
– The authentication key is **key 1** with the password **corpkey**.

b. Configure the ASA device with AAA authentication and verify its functionality:

Note: the HQ-ASA is preconfigured with a username **Car1Admin** with password **adminpass01**
– Configure AAA to use the local database for SSH connections to the console port.
– Generate a RSA key pair to support with modulus size of **1024** bits.
– Configure HQ-ASA to accept SSH connections only from the Net Admin workstation.
– Configure SSH session timeout to be 20 minutes.

Step 4: Configure NAT Service for the ASA device for both inside and DMZ networks.

a. Create an object **inside-nat** with subnet 192.168.10.0/24 and enable the IP addresses of the hosts in the internal network to be dynamically translated to access the external network via the outside interface.
b. Create an object **dmz-dns-server** to statically translate the DNS server in the DMZ to the public IP address.
c. Create an object **dmz-web-server** to statically translate the web server in the DMZ to the public IP address.

Step 5: Configure ACL and firewall on the ASA device to implement the Security Policy.

a. Modify the default MPF application inspection global service policy to enable hosts in the Internal network to access the web servers on the Internet
– Create a class **inspection_default** that matches **default-inspection-traffic**.
– Create a policy-map **global_policy** and specify the **inspect** with **dns, ftp, http**, and **icmp**.
– Attach the policy map globally to all interfaces.

b. Configure an ACL to allow access to the DMZ servers from the Internet.
– Create, apply, and verify an extended named ACL (named **OUTSIDE-TO-DMZ**) to filter incoming traffic to the HQ-ASA. The ACL should be created in the order specified in the following guidelines ***(Please note, the order of ACL statements is significant only because of the scoring need in Packet Tracer.)***:
– HTTP traffic is allowed to DMZ Web Svr.
– DNS traffic (both TCP and UDP) is allowed to the DMZ DNS server (two separate ACEs).
– FTP traffic from the branch administrator workstation is allowed to the DMZ web server.
– The ACL should contain four ACEs.
– Verify HQ-ASA configurations. Both Net Admin and DMZ Web Svr can access the website www.externalone.com. Branch Admin can access the website www.thecar1.com. Branch Admin can also establish an FTP connection to the web server www.thecar1.com, using the username cisco and the password cisco.

Step 6: Configure a Site-to-Site IPsec VPN between the HQ Router and the Branch Router.

Note: The Branch and HQ routers have already been configured with a username of **CORPADMIN** and a password of **Ciscoccnas**. The enable secret password is ciscoclass.

The following tables list the parameters for the ISAKMP Phase 1 Policy and IPsec Phase 2 Policy:

ISAKMP Phase 1 Policy Parameters		ISAKMP Phase 2 Policy Parameters		
Key Distribution Method	**ISAKMP**	**Parameters**	**HQ Router**	**Branch Router**
Encryption Algorithm	AES	**Transform Set Name**	VPN-SET	VPN-SET
Number of Bits	256	**Transform Set**	esp-3des esp-sha-hmac	esp-3des esp-sha-hmac
Hash Algorithm	SHA-1	**Peer Host Name**	Branch	HQ
Authentication Method	Pre-share	**Peer IP Address**	198.133.219.2	209.165.200.226
Key Exchange	DH 2	**Encrypted Network**	209.165.200.240/28	198.133.219.32/27
IKE SA Lifetime	86400	**Crypto Map Name**	VPN-MAP	VPN-MAP
ISAKMP Key	Vpnpass101	**SA Establishment**	ipsec-isakmp	ipsec-isakmp

Configure an ACL (ACL 120) on the HQ router to identify the interesting traffic. The interesting traffic is all IP traffic between the two LANs (209.165.200.240/28 and 198.133.219.32/27).

a. Configure the ISAKMP Phase 1 properties on the HQ router. The crypto ISAKMP policy is **10**. Refer to the **ISAKMP Phase 1 Policy Parameters Table** for the specific details needed.

b. Configure the ISAKMP Phase 2 properties on the HQ router. Refer to the **ISAKMP Phase 2 Policy** Parameters Table for the specific details needed.

c. Bind the **VPN-MAP** crypto map to the outgoing interface.

d. Configure IPsec parameters on the Branch router using the same parameters as on the HQ router. Note that interesting traffic is defined as the IP traffic from the two LANs.

e. Save the running-config, then reload both the HQ and Branch routers.

f. Verify the VPN configuration by conducting an FTP session with the username **cisco** and the password **cisco** from the Branch Admin PC to the DMZ Web Svr. On the Branch router, check that the packets are encrypted. To exit the FTP session, type **quit**.

**** End of Question ****

Intruction – Answers (100% Scores)

HQ-ASA

```
enable
Thecar1Admin
conf term
domain-name thecar1.com

interface vlan 1
ip address 192.168.10.1 255.255.255.0
nameif inside
Security-level 100
no shutdown
exit
interface vlan 2
ip add 209.165.200.253 255.255.255.240
nameif outside
security-level 0
no shutdown
exit
interface vlan 3
No forward int vlan 1
ip add 192.168.20.1 255.255.255.0
nameif dmz
security-level 70
no shutdown
exit

interface e0/1
switchport acces vlan 1
no shutdown
exit
interface e0/0
switchport acces vlan 2
no shutdown
exit
int e0/2
switchport acces vlan 3
no shutdown
exit

dhcpd add 192.168.10.25-192.168.10.35 inside
dhcpd dns 192.168.10.10 interface inside
dhcpd option 3 ip 192.168.10.1
dhcpd enable inside

ntp authenticate
ntp authentication-key 1 md5 corpkey
ntp server 192.168.10.10
ntp trusted-key 1

aaa authentication ssh console LOCAL
ssh 192.168.10.5 255.255.255.255 inside
ssh timeout 20
object network inside-nat
subnet 192.168.10.0 255.255.255.0
```

```
nat (inside,outside) dynamic interface
exit
configure terminal
object network dmz-dns-server
host 192.168.20.5
nat (dmz,outside) static 209.165.200.242
exit
configure terminal
object network dmz-web-server
host 192.168.20.2
nat (dmz,outside) static 209.165.200.241
exit
configure terminal
class-map inspection_default
match default-inspection-traffic
policy-map global_policy
class inspection_default
inspect dns
inspect ftp
inspect http
inspect icmp
exit
service-policy global_policy global
access-list OUTSIDE-TO-DMZ extended permit tcp any host 209.165.200.241 eq 80
access-list OUTSIDE-TO-DMZ extended permit tcp any host 209.165.200.242 eq 53
access-list OUTSIDE-TO-DMZ extended permit udp any host 209.165.200.242 eq 53
access-list OUTSIDE-TO-DMZ extended permit tcp host 198.133.219.35 host 209.165.200.241
eq ftp
access-group OUTSIDE-TO-DMZ in interface outside
```

HQ Router

```
CORPADMIN
Ciscoccnas
enable
ciscoclass
conf ter

access-list 120 permit ip 209.165.200.240 0.0.0.15 198.133.219.32 0.0.0.31
crypto isakmp policy 10
encryption aes 256
authentication pre-share
group 2
lifetime 86400
hash sha
exit
crypto isakmp key Vpnpass101 address 209.165.200.226
crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
crypto map VPN-MAP 10 ipsec-isakmp
set peer 209.165.200.226
set transform-set VPN-SET
match address 120
exit
interface s0/0/0
crypto map VPN-MAP
end
copy running-config startup-config
```

Branch Router:

```
CORPADMIN
Ciscoccnas
enable
ciscoclass
conf ter

access-list 120 permit ip 209.165.200.240 0.0.0.15 198.133.219.32 0.0.0.31
crypto isakmp policy 10
encryption aes 256
authentication pre-share
group 2
lifetime 86400
hash sha
exit
crypto isakmp key Vpnpass101 address 198.133.219.2
crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
crypto map VPN-MAP 10 ipsec-isakmp
set peer 198.133.219.2
set transform-set VPN-SET
match address 120
exit
interface s0/0/0
crypto map VPN-MAP
end
copy running-config startup-config
```

Download Packet Tracer File:

[sociallocker id=”54558″]

CCNA Security 2.0 - Packet Tracer Practice Skills Assesement 2 876.94 KB
3070 downloads

...

Download

[/sociallocker]