ICT362 Network Security

Case Study

Version 15.2

1. If you require help with the case study you should make an appointment with me. You will need to have your case study router configurations up and running in the VM. Be prepared to answer questions about your router configurations and how you tested your configurations.

2. Please do **NOT** email your router configurations, debug output or show run output to me unless I specifically ask for it.

3. There are **NO** marks associated with the case study. The knowledge you learn from completing the case study will be examined in the practical exam and final exam. I do not release a model solution to the case study so doing nothing for the case study is not an option. I will give a mock practical exam in your last tutorial of the semester where I will provide students with a detailed solution. The mock practical exam will provide you with an understanding of what is required in the actual practical exam and provide feedback to you on how you will perform in the actual practical exam. The real practical exam is scheduled for 3 hours while the mock practical will only be for 90 minutes.

4. Make sure you fully understand what you are configuring and make sure you fully test your configurations. It is important to fully test everything as you go along. For example if you cannot get NAT working properly and you then move onto implementing CBAC on the routers it is a recipe for failure which will result in you not finishing the case study.

5. I will make references to documents that you should use to implement certain requirements. Make sure you follow them. I typically will talk about them in class and will perform whiteboard class participation exercises using them.

6. You are permitted to work in groups or as individuals to complete the case study. Students find having someone to work through the case study with is extremely beneficial to learning the concepts and debugging techniques. At the end of the day you need to know the material in the case study for the practical exam.

7. Use the VM that can be found the GNS3 computer image. The compressed iou-web-NS-CS-v151.zip can be found in LMS. You will need to uncompress the image using the **`CiscoIOUNSCS15`** password. Be sure to only use this VM exclusively for the Case Study. DO NOT USE THIS VM FOR ANYTHING ELSE SUCH AS LAB EXERCISES. You can use Vmware Player or Workstation to start the VM but only Workstation will allow you to take snapshots of your VM. Once started you will use a web browser with the IP address shown on the VM terminal window. This will give you GUI access to the IOU environment. To gain root access to the VM you will use the username `root` and password **`Seattle2015`**.

8. Be sure to use the `copy run start` command or equivalent along with the `wrx` command when you are finished working on the devices. The wrx command is an alias short cut command (see the running router configuration for the full command).

9. Use the username: ***admin*** and password ***admin*** to gain access to any router requiring verification. If you telnet or ssh into a router the router will timeout the session in 5 seconds once you have been validated.

10. Verifying SSH can be done by using the following command with the correct destination IP address. You will be required to use the **crypto key generate rsa mod 768** command on any device that requires SSH access. The following command is an example of how you would SSH into a device.

    ```
    ssh -l admin -c 3des 1.1.1.1
    ```

    you will then be asked for the password "admin".

1.0 NAT Requirements

Use ROUTE-MAPs to dynamically translate source addresses (Inside Private IP Addresses) to the Global IP Addresses. The lecture slides cover very specific information that you will use for configuring the routers. The following document describes the use of route-maps with NAT which some students have found to be useful in previous years.

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080093fca.shtml

Router R1

The ISP101 has allocated the Candy Land Corporation the Global IP address range of 11.11.11.128–11.11.11.254/25. Configure NAT on R1 to allow all the inside host networks 192.168.111.0/24, 192.168.112.0/24 and 192.168.113.0/24 access to the outside. The first 8 available global IP addresses have been reserved for future DMZ servers while the rest of the IP addresses range can be allocated for host translations. Use the extended ACL number 100 to permit the networks to use the NAT process along with the route-map name NAT_PROCESS to match the ACL. Configure a static NAT translation to the DMZ Server using the global IP address of 11.11.11.128. The Inside server does not require any NAT processing (dynamic or static) since it is not globally accessible.

Router R2

The ISP102 has allocated the Candy Land Corporation the Global IP address range of 22.22.22.192–22.22.22.254/25. Configure NAT on R2 to allow the inside network 192.168.2.0/24 access to the outside except for the InsideSrv22. Use the extended named ACL R2_NAT_ACL to permit the 192.168.2.0 network to use the NAT process along with the route-map name NAT_PROCESS to match the ACL. Configure a static NAT translation to the DMZ Server using the global IP address of 22.22.22.254. The Inside server does not require a static NAT mapping.

Router R3

The ISP103 has allocated the Candy Land Corporation the Global IP address range of 33.33.33.80-33.33.33.83/30. Configure PAT on R3 to allow the inside network 192.168.3.0/24 to use the address pool. Use the extended named ACL R3_NAT_ACL to permit the 192.168.3.0 network to use the NAT process along with the route-map name NAT_PROCESS to match the ACL.

Router R4

The ISP104 will dynamically allocate an IP address to the E0/1 interface of the router. Assume this will change on a regular basis so do not attempt to use the assigned IP address for any of your configurations. Configure all hosts on the 192.168.4.0/24 network to use the global IP address of the outside E0/1 interface (i.e. PAT or NAT overload). Use the extended ACL number 100 to permit the networks to use the NAT process along with the route-map name NAT_PROCESS to match the ACL.

The global IP addresses 1.1.1.1, 2.2.2.2, 3.3.3.3 and 4.4.4.4 can be used to test and verify router NAT translations. You can use the Internet Host 1 & 2 to verify access to the DMZ server along with any of the Inside Hosts at this time. **Be sure to verify that NAT is working 100% before starting the next section.**

2.0 Security Policy Requirements

You will NOT be able to test all the security policies until you have configured the rest of the case study requirements such as the Firewalls (CBAC & Zone-Based) and the DMVPNs. This will be the case for any traffic that goes from one site to another via the DMVPN which will use private addressing for the destination IP address.

Note: access to the Internet does NOT mean the hosts are permitted access to any of the internal networks on the other sites unless it has been allowed by a security policy.

HQ

1. All hosts on the General Staff networks 192.168.111.0/24 & 192.168.112.0/24 networks are allowed ICMP (ping) and SSH access to the INSIDERSrv114.
2. All hosts on the General Staff networks 192.168.111.0/24 & 192.168.112.0/24 are allowed full access to the others network.
3. Hosts below 64 on the 192.168.111.0/24 network are allowed full access to the Internet.
4. Hosts above 239 on the 192.168.112.0/24 network are allowed full access to the Internet
5. Hosts 20-35 on the IT Staff network 192.168.113.0/24 network are allowed full access to ANY network (i.e. they are permitted ANYWHERE).
6. All hosts on the 192.168.113.0/24 network are allowed full access to the Internet.
7. All external hosts are permitted ICMP (ping) and SSH access to the DMZSrv115 server.
8. NO traffic is allowed to originate from the DMZ network.

Regional Office

1. Hosts 1-20 on the 192.168.2.0/24 network are permitted full access to the Internet.
2. Hosts 1-15 on the 192.168.2.0/24 network are permitted ICMP and telnet access to the INSIDERSrv114.
3. All external hosts are permitted ICMP (ping) and SSH access to the DMZSrv23 server.
4. NO traffic is allowed to originate from the DMZ network.

Remote Office 1

1. Inside hosts 1 to 10 on the 192.168.3.0/24 network are permitted full access to the Internet.
2. Host 33 on the 192.168.3.0/24 network is permitted ICMP (ping) and telnet access to the INSIDESrv114 and INSIDESrv22.

Remote Office 2

1. Hosts 240-247 on the 192.168.4.0/24 network are permitted full access to the Internet.
2. Host 44 on the 192.168.4.0/24 network is permitted ICMP (ping) and telnet access to the INSIDESrv114 and INSIDESrv22.

3.0 IOS Firewall Requirements

Use meaningful variable names for route-maps, class-maps, policy-maps, etc. Always CAPITALIZE the variable names because this will make it easier for you and me to troubleshoot the router configurations. Be sure to inspect only the protocols that are defined in the previous section such as icmp and telnet.

Zone-Based Firewalls

You are required to implement a Cisco IOS Zone-Based Firewall on the HQ site (i.e. router R1) and the Remote Office 1 site (i.e. router R3). You will need to implement the security requirements from section 2.0 using a Zone-Based Firewall for both these sites. The following tables will define the different zones that you will need to implement.

The HQ site will use the following zones:

Zone Name	Description
INSIDE	Contains the 192.168.111.0/24 and 192.168.112.0/24 networks.
ITSTAFF	Contains the 192.168.113.0/24 network.
DMZ	Contains servers which will be accessible from Internal and External hosts (i.e. Internet).
INTERNAL-SERVERS	Contains only servers which are only accessible from internal host computers. This includes internal hosts from other sites via the VPN.
OUTSIDE	Any host that is not associated with any of the Candy Land sites (i.e. the Internet).
DMVPN	Used for traffic that will travel via the DMVPN to other Candy Land sites.

The Remote Office 1 will use the following zone:

Zone Name	Description
INSIDE	Contains all the internal networks that have host computers.
OUTSIDE	Any host that is not associated with any of the Candy Land sites (i.e. the Internet).
DMVPN	Used for traffic that will travel via the DMVPN to other Candy Land sites.

CBAC Firewalls

You are required to implement a Cisco IOS CBAC Firewall on the Regional Office site (i.e. router R2) and the Remote Office 2 site (i.e. router R4). Only the protocols defined in Section 2 are permitted through the firewall and each protocol is required to be inspected.

Router R2

Use the following naming conventions for the inspect statements:

Anything into the DMZ: INTO_DMZ

```
ip inspect name INTO_DMZ telnet timeout 60
```

Inside to Outside: INSIDE_TO_OUT

```
ip inspect name INSIDE_TO_OUT telnet timeout 60
```

VPN to Inside: VPN_TO_INSIDE - required for IT staff to access inside hosts.

```
ip inspect name  VPN_TO_INSIDE telnet timeout 60
```

Hint: For the Remote Office 2 site, you should use three inspects: two on the inside interface E0/0 (inward and outward direction) and one on the DMZ interface E0/1 (outward direction).

Router R4

Use the following naming conventions for the inspect statement:

Inside to Outside: INSIDE_TO_OUT

```
ip inspect name INSIDE_TO_OUT telnet timeout 60
```

VPN to Inside VPN_TO_INSIDE - required for IT staff to access inside hosts.

```
ip inspect name  VPN_TO_INSIDE telnet timeout 60
```

4.0 Dynamic Multipoint IPSec VPNs using GRE and NHRP

General Requirements

External access to the DMZ network servers will only be via the 11.11.11.128 or 22.22.22.254 IP addresses. The only exception is for internal hosts at the same site which will use the actual private IP address. All other site-to-site traffic (192.168.x.x. to 192.168.x.x) is to use the DMVPN if permitted by the security policy. All tunnel IP addresses are to use the 10.0.***T#***.***R#***/24 network where ***T#*** is the tunnel interface number and ***R#*** is the router number. For example R1 would use the 10.0.1.1 IP address for its tunnel interface IP address. Be sure to exclude all traffic that is going through the tunnel from the NAT process (i.e. 192.168.x.x to 192.168.x.x).

Hint: Get your GRE tunnels up and running with NHRP before implementing IPSec (i.e. do not apply "the tunnel protection ipsec profile" statement to the tunnel interface).

DMVPN Tunnel Parameters

Use the following information to modify the Hub and Spoke templates in Appendix A which will be used to configure the routers that are participating in the DMVPN network.

ISAKMP Parameters

Use the following router output to create the required router ISAKMP configuration. The authentication key is: `cisco12345`.

```
Global IKE policy
Protection suite of priority 10
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:    #1 (768 bit)
        lifetime:               1800 seconds, no volume limit
```

IPSec Parameters

Use the following router output to create the required router IPSec configuration. Use the naming convention defined below and set the IPSec security-association lifetime to 1800 seconds.

```
Transform set DMVPN_TRANSFORM: { esp-des  ah-md5-hmac }
   will negotiate = { Transport,  },
```

Required Naming Convention

Transform-set name:	DMVPN_TRANSFORM
Profile name:	DMVPN_PROFILE

Configure R1 as a DMVPN Hub with EIGRP routing

Use the modified Hub template to configure router R1 as the DMVPN Hub with the EIGRP routing protocol. Only advertise the tunnel network and any inside networks. Do NOT advertise the DMZ network or the public network.

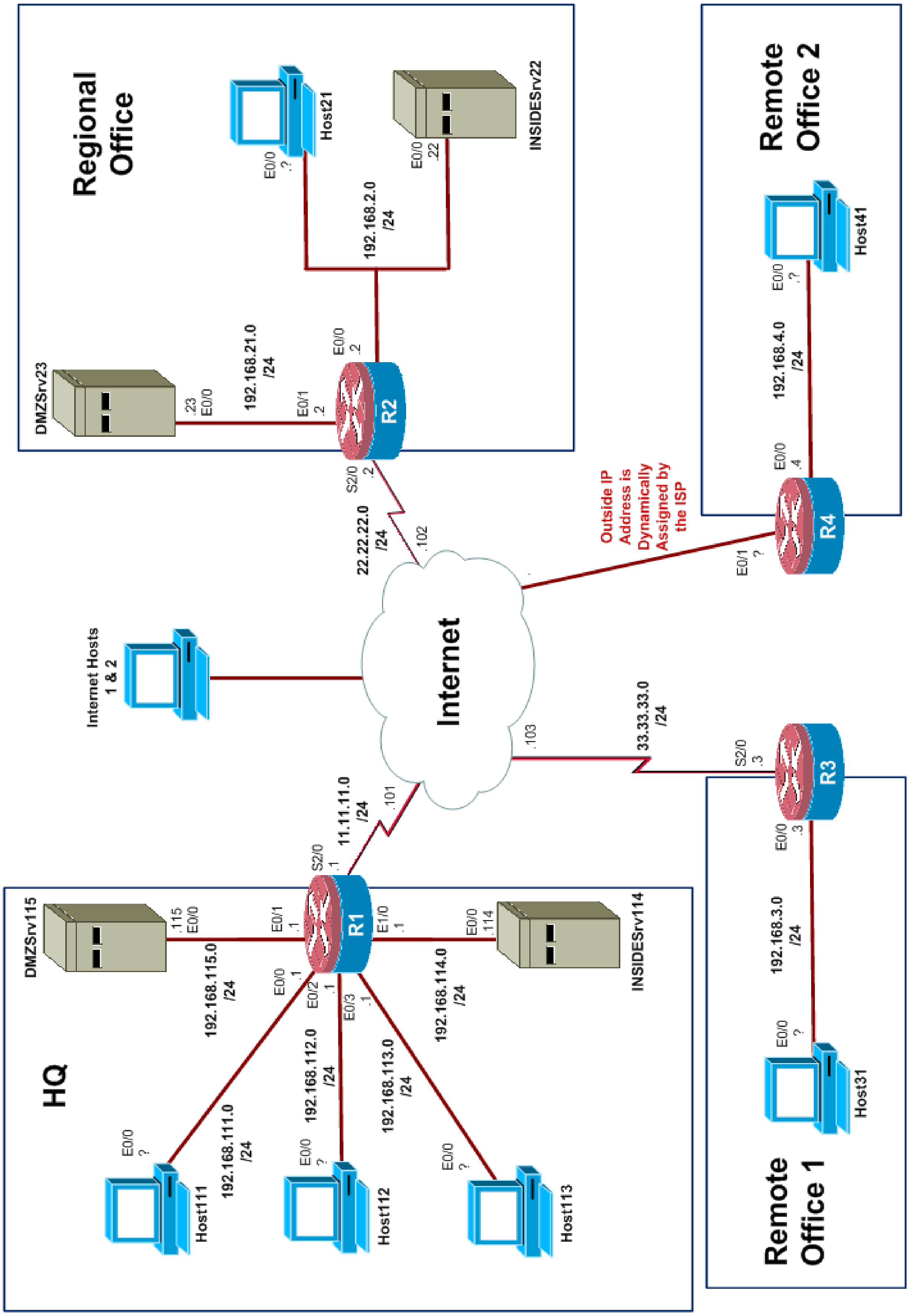
Configure R2, R3 & R4 as DMVPN Spokes with EIGRP routing

Use the modified Spoke template to configure routers R2, R3 & R4 as DMVPN spoke routers with the EIGRP routing protocol. Only advertise the tunnel network and any inside networks. Do NOT advertise the DMZ network or the public network. You will need to configure EIGRP routing on each router using the AS 1. Configure each of the routers to an EIGRP stub router.

Appendix A

```
******************************
HUB Template
******************************
 !
 crypto isakmp policy 10
 < insert isakmp parameters >
 crypto isakmp key <insert pre-shared key> address 0.0.0.0
 !
 crypto ipsec transform-set <insert transform set name and parameters>
  mode <insert mode>
 !
 crypto ipsec profile <insert profile name>
  set transform-set <insert transform set name>
 !
 !
 interface Tunnel1
 description *** Hub Template ***
 bandwidth 10000
 ip address <insert tunnel IP address and mask>
 no ip redirects
 ip mtu 1400
 no ip next-hop-self eigrp 1
 no ip split-horizon eigrp 1
 ip nhrp authentication cisco123
 ip nhrp map multicast dynamic
 ip nhrp network-id 100001
 ip nhrp holdtime 300
 ip nhrp registration no-unique
 ip nhrp registration timeout 120
 ip nhrp shortcut
 ip nhrp redirect
 ip tcp adjust-mss 1360
 load-interval 30
 tunnel source <insert Hubs outside interface>
 tunnel mode gre multipoint
 tunnel key 100001
 tunnel protection ipsec profile <insert ipsec profile name>
```

```
******************************
SPOKE Template
******************************
!
 crypto isakmp policy 5
< insert isakamp parameters >
 crypto isakmp key <insert pre-shared key> address 0.0.0.0
 !
 crypto ipsec transform-set <insert transform set name and parameters>
  mode <insert mode>
 !
 crypto ipsec profile <insert ipsec profile name>
  set transform-set <insert transform set name>
 !
 interface Tunnel1
 description *** Spoke Template ***
 bandwidth 192
 ip address <insert tunnel IP address and mask>
 no ip redirects
 ip mtu 1400
 ip nhrp authentication cisco123
 ip nhrp map multicast <insert Hub outside interface IP address>
 ip nhrp map <insert Hub tunnel IP and Hub outside interface IP address>
 ip nhrp network-id 100001
 ip nhrp holdtime 300
 ip nhrp nhs <insert Hub tunnel IP address>
 ip nhrp registration no-unique
 ip nhrp registration timeout 120
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 tunnel source <insert Spokes outside interface>
 tunnel mode gre multipoint
 tunnel key 100001
 tunnel protection ipsec profile <insert ipsec profile name>
```


Regional Office
DMZSrv23
.23
E0/0
192.168.21.0
/24
E0/1
.2
R2
E0/0
.2
192.168.2.0
/24
E0/0
.?
Host21
E0/0
.22
INSIDESrv22
S2/0
.2
22.22.22.0
/24
.102
Internet Hosts
1 & 2
Internet
Outside IP
Address is
Dynamically
Assigned by
the ISP
E0/1
?
R4
E0/0
.4
192.168.4.0
/24
E0/0
.?
Host41
Remote
Office 2
.101
11.11.11.0
/24
S2/0
.1
.103
33.33.33.0
/24
S2/0
.3
R3
E0/0
.3
192.168.3.0
/24
E0/0
?
Host31
Remote
Office 1
HQ
DMZSrv115
.115
E0/0
192.168.115.0
/24
E0/1
.1
R1
E1/0
.1
E0/0
.114
INSIDESrv114
192.168.114.0
/24
E0/0
.1
E0/2
.1
E0/3
.1
192.168.111.0
/24
192.168.112.0
/24
192.168.113.0
/24
E0/0
?
Host111
E0/0
?
Host112
E0/0
?
Host113