CCNA Security Case Study Section 2

Name: Raine Roberts	**ID:**
Module: Network Security COMP704	**Semester: 2**
Weight: 75 marks	**Pass Mark: 50% overall for both sections 1 & 2**
Due Date: Demonstrated in class over weeks 11 -13 and submitted in week 13	

Module Learning Outcomes:

- Configure, secure and troubleshoot network technologies and data communications, and justify the implementations.

Scenario

Rexnet industries is an expanding barrister company that provides legal representation for small to medium size businesses. They specialise in commercial law. The data that is circulated across the network is sensitive. Therefore, the technology used within the Rexnet domain needs to be secured and kept private.   The end users comprise barristers, IT Admin and other administration staff.

Rexnet Industries is designing its network and will include two offices named: Rexnet Head Quarters and Rexnet Branch. **Your goal is to secure and configure the central network PCs and intermediary devices.**

Marking Objectives

Part / Objective	Total Marks
Part 1: Setup and configure basic device settings on the switch, ASA and pcs	
Part 5: Configure ASA REXNET-HQ basic management and firewall settings and PAT using the CLI	**/15**
Part 6: Secure the network switch on the Rexnet Main Office Network	**/5**
Part 7: Configure a DMZ, static NAT, and ACLs on the HQ ASA using ASDM	**/15**
Part 8: Configure an IPsec site-to-site VPN between The Rexnet Branch router and the HQ ASA	**/10**
Part 9: Justification: critically reflect on the network and its configurations	**/30**
Total	**/75**

Parts 5 to 8: Assessment: See assessment marking sheet for how it will be marked on demonstration day.

For each part you must paste the appropriate running config and list the commands / output. You need to demonstrate this network to your tutor once you have completed all the configuration. Your marks will be determined based on your demonstration and your written submission.

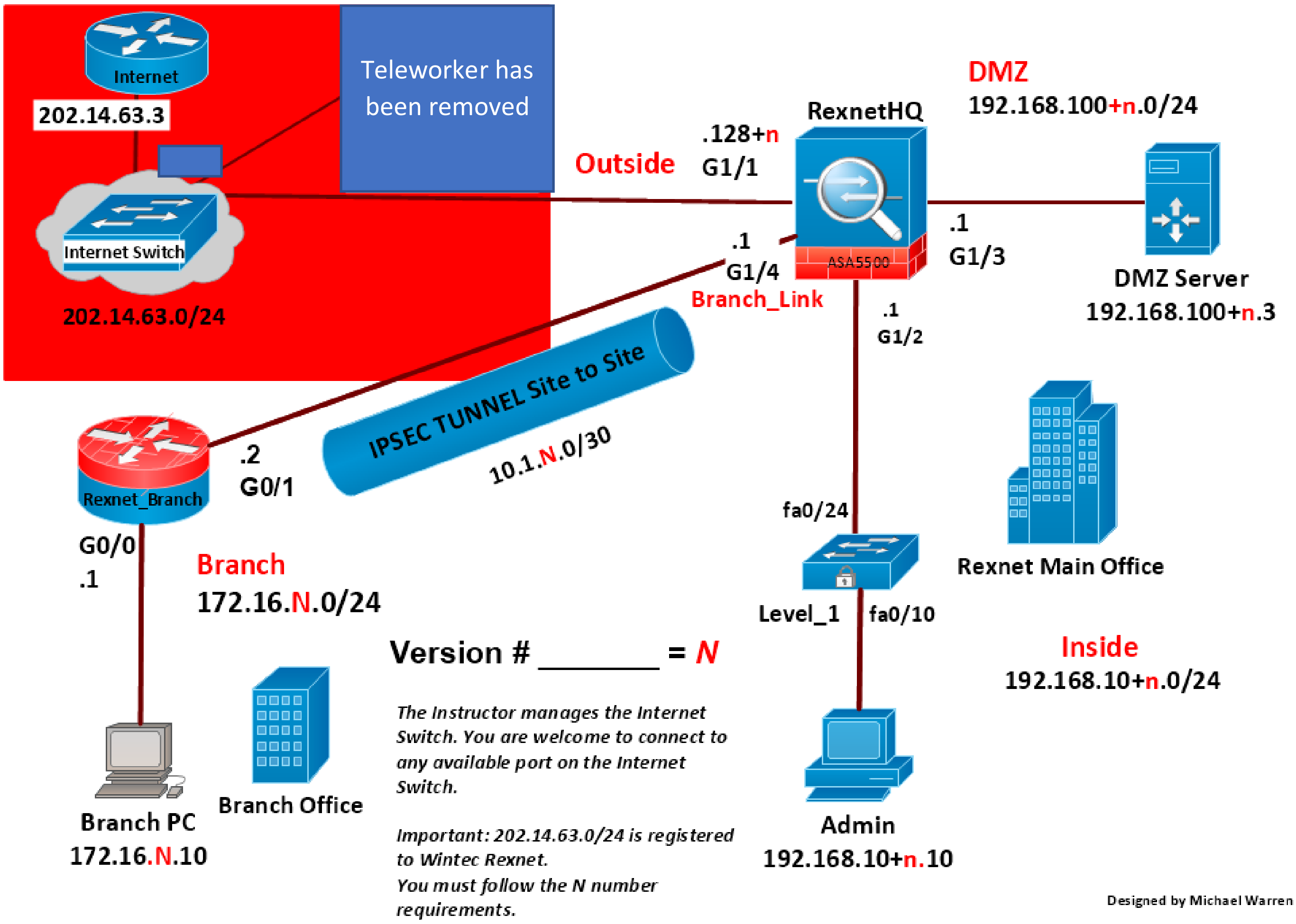
- ***If you do not get a section marked off on demonstration day in class, then you could potentially lose all the marks for that part. Small errors will incur a 1-3-mark deficit for each error. Failure to get the main function working for a part, or if a configuration is unsecure, will result in no marks allocated for that part. It is the tutor's decision on what marks are allocated for each part.***
- ***Your total mark for the case study is the addition of marks for both section 1 and 2. For example: Section 1 mark + Section 2 mark = Total mark overall.***

Required Equipment

- 1 ASA 5506-X with FirePOWER services, 8GE, AC, 3DES/AES
- 1 router (Cisco IOS Release 15.4(3)M2 image minimum with a Security Technology package license)
- 1 Switch (Cisco 2960 or comparable)
- 3 PCs (Windows, SSH Client)
- Cables as shown in the topology
- Public IPs available for this case study 202.14.63.130 – 202.14.63.170
- Putty Terminal emulation software or tera term
- The Tftpd32 freeware TFTP server is used in this task. Many other free TFTP servers are also available. If a TFTP server is currently unavailable on PC-A, you can download the latest version of Tftpd32 from https://tftpd64.software.informer.com/download/

Note: This lab uses the Tftpd32 TFTP server. This software also includes a syslog server, which runs simultaneously with the TFTP server.

Network Topology



The Instructor manages the Internet Switch. You are welcome to connect to any available port on the Internet Switch.

Important: 202.14.63.0/24 is registered to Wintec Rexnet. You must follow the N number requirements.

Instructions:

Refer to the network topology and set up your addressing. Be sure to replace the letter N or n with the number assigned to you by your instructor. The N number could be any number from 2 – 13.

Instructors make sure the Internet switch has internet connectivity before the students attempt this topology.

Addressing Table:

Device	Interface	IP Address	Subnet Mask	Default Gateway	DNS
Rexnet-HQ	G1/1 - Outside	202.14.63.128+N	255.255.255.0	NA	NA
	G1/2 – Inside	192.168.10+N.1	255.255.255.0	NA	NA
	G1/3 - DMZ	192.168.100+N.1	255.255.255.0	NA	NA
	G1/4 – Branch Link	10.1.N.1	255.255.255.252		
DMZ Server	NA	Inside local address 192.168.100+N.3 Inside global static address 202.14.63.140+N	255.255.255.0	192.168.100+N.1	1.1.1.1
Level_1 Switch	SVI VLAN 2	192.168.10+N.2	255.255.255.0	192.168.10+N.1	NA
Admin PC	F0/10	192.168.10+N.10	255.255.255.0	192.168.10+N.1	1.1.1.1
Rexnet-Branch	G0/0	172.16.N.1	255.255.255.0	NA	

	G0/1	10.1.N.2	255.255.255.252		
Branch PC	F0/2 or G0/0	172.16.N.10	255.255.255.0	172.16.N.1	1.1.1.1

Pre-Setup Instructions:

Before you start configuring your devices complete the following steps:

Step 1: Cable the network as shown in the topology

Step 2: Setup addressing on the PCs as you have outlined in the addressing table.

Note: Make sure you adjust the IP addresses accordingly to suit the N number provided to you by your instructor.

Part 1: Setup and configure basic device settings on the router, switches and pcs. Write the command(s) relevant next to each task.

Configure the Rexnet_Branch Router

Use the config from section 1 and adjust it to match the configuration required below. Do not use the NAT config from Moodle.

Tip: Configure logging synchronous on the console lines before you begin.

Task	Command(s)
Configure hostnames as shown in the topology	hostname Rexnet_Branch
Set the Clock. Time, date and year.	clock set 14:30:00 Nov 6 2024
Configure the interfaces as per the topology and addressing table	Complete
Disable DNS lookup	No ip-domain lookup
Configure a static default route on the Rexnet_Branch Router which sends all Internet Traffic out G0/1 interface to the ASA	**Rexnet_Branch(config)#ip route 0.0.0.0 0.0.0.0 10.2.13.1**
Configure another static route to the Rexnet_HQ private network	**Rexnet_Branch(config)#ip route 192.168.23.0 255.255.255.0 10.1.13.1**

Configure the Rexnet Main Office Switch

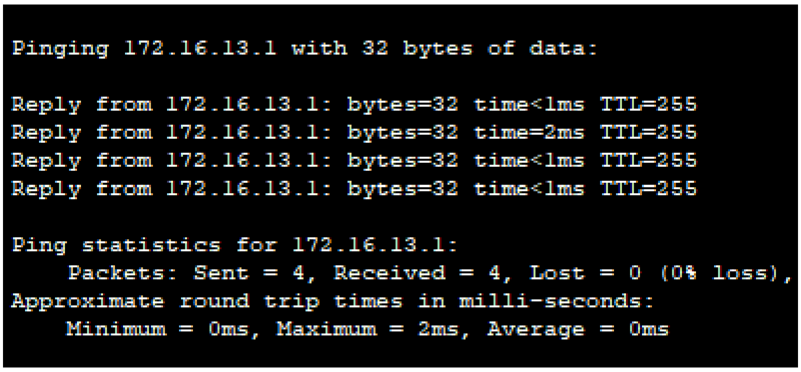
Tip: Configure logging synchronous on the console lines before you begin.

Task	Command(s)
Configure hostname as shown in the topology	hostname Level_1
Disable DNS lookup	Enable Conf t No ip domain-lookup
Configure the VLAN 2 SVI management address and the default gateway	Enable Conf t

	interface Vlan 2 ip address 192.168.23.2 255.255.255.0 no shutdown ip default-gateway 192.168.23.1

Verify connectivity:

- Verify connectivity between the following devices:
  - Branch PC and the Rexnet_Branch Router G0/0 interface

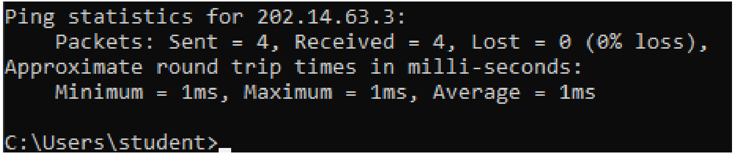
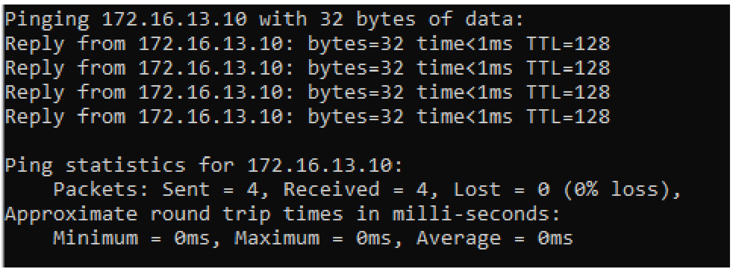


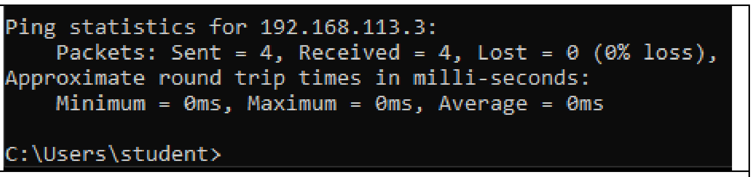
```
Pinging 172.16.13.1 with 32 bytes of data:

Reply from 172.16.13.1: bytes=32 time<1ms TTL=255
Reply from 172.16.13.1: bytes=32 time=2ms TTL=255
Reply from 172.16.13.1: bytes=32 time<1ms TTL=255
Reply from 172.16.13.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.16.13.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

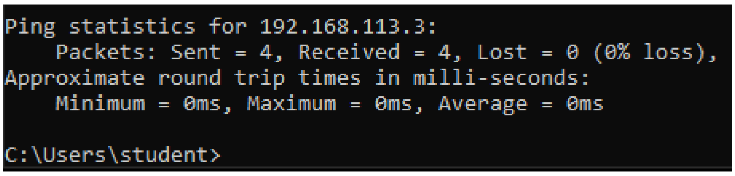
Part 5: Configure ASA REXNET-HQ basic management and firewall settings

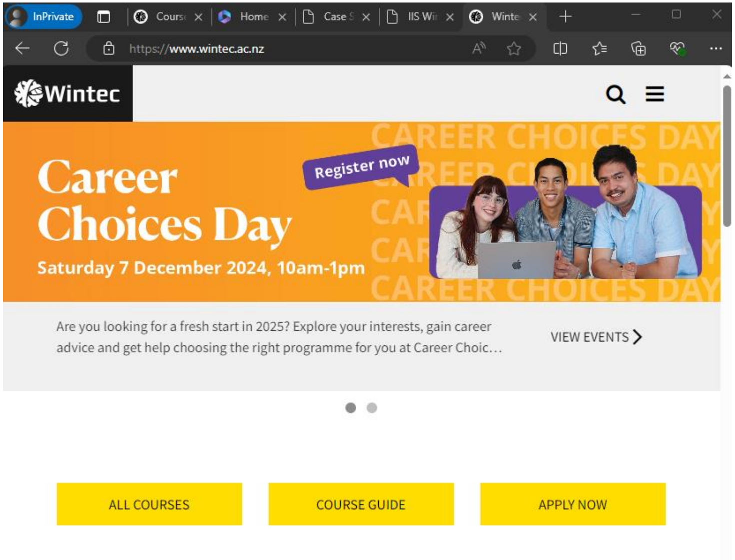
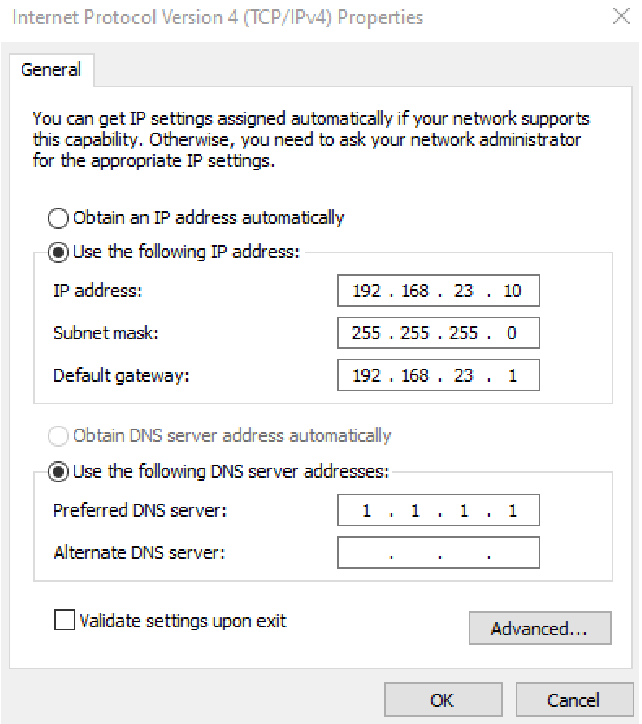
Task	Command(s)
Erase any default or previous configuration Bypass setup mode and use the CLI mode for this section. Pre-configure Firewall now through interactive prompts [yes]? No	**Enable** **Write erase**
Configure a Hostname and a domain name Hostname: Rexnet-HQ Domain: Rexnetsecurity.com	Enable Conf t Hostname Rexnet-HQ Domain-name Rexnetsecurity.com
Configure the privileged EXEC mode (enable) password	Enable Conf t Enable password cisco123
Add a username into the local database with admin privileges Username: admin Password: cisco123	Enable Conf t username Admin password cisco123
Configure console access using **aaa** and the local database	Enable Conf t aaa authentication ssh console LOCAL
Encrypt all passwords in the running config with aes	Enable Conf t key config-key password-encryption cisco123 password encryption aes
Set the date and time	Enable Conf t Ntp server 161.65.172.9

	Clock timezone NZST 12 clock set 14:30:00 Nov 6 2024
Configure the interfaces. Name and address them according to the topology and addressing table. Configure the security levels as follows: - Inside (main office) = 100 - Branch_Link = 100 - DMZ = 70 - Outside = 0	enable configure terminal interface GigabitEthernet1/1 nameif outside security-level 0 ip address 202.14.63.128 255.255.255.0 no shutdown interface GigabitEthernet1/2 nameif inside security-level 100 ip address 192.168.10.N 255.255.255.0 no shutdown interface GigabitEthernet1/3 nameif DMZ security-level 70 ip address 192.168.100.N 255.255.255.0 no shutdown interface GigabitEthernet1/4 nameif Branch_Link security-level 100 ip address 10.1.N.1 255.255.255.252 no shutdown wr
Configure SSH Configure AAA to use the local database for SSH user authentication. Create a RSA key 1024 bits Only the Admin PC on the Inside LAN is allowed SSH Access to the ASA. Version 2 Verify that this works.	Enable Config t aaa authentication ssh console LOCAL crypto key generate rsa modulus 1024 exit enable configure terminal aaa authentication ssh console LOCAL crypto key generate rsa modulus 1024 ssh version 2 access-list SSH_ACCESS extended permit tcp host 192.168.13.10 any eq 22 access-list SSH_ACCESS extended deny tcp any any eq 22 access-group SSH_ACCESS in interface inside write memory
Configure a static route to the Rexnet_Branch network through G1/4	Enable Conf t **Configure a static route** to the Rexnet_Branch network through G1/4
Configure a static default route pointing to the Internet Router 202.14.63.3	Rexnet-HQ(config)#route OUTSIDE 0.0.0.0 0.0.0.0 202.14.63.3

Configure PAT so that inside addresses on the Main Office and Branch networks, are translated to the public address on the Outside G1/1 interface Object-ID: INSIDE-NET Object-ID: BRANCH-NET	Enable Conf t object network INSIDE-NET subnet 192.168.23.0 255.255.255.0 nat (inside,outside) dynamic interface exit Conf t object network BRANCH-NET subnet object network BRANCH-NET subnet 172.16.13.0 255.255.255.0 nat (inside,outside) dynamic interface Exit Conf t
Modify the default MPF global policy to allow returning ICMP traffic back through the firewall. Verify that this works.	enable configure terminal ! Create an access list for ICMP access-list ICMP-ACL extended permit icmp any any ! Apply the access list to the inside interface access-group ICMP-ACL in interface inside ! Ensure the global policy inspects ICMP traffic policy-map global_policy class inspection_default inspect icmp ! Save the configuration write memory
Use the correct command to enable traffic between interfaces with the same security level. i.e. between the branch network and the Main Office	same-security-traffic permit inter-interface
Configure ASDM access to the ASA install ASDM Launcher	N/A
Verify PAT is working with the correct show commands. Paste the details of the show command in the box on the right.	Commands: Output:
From the ADMIN PC: See if you can ping the following and paste the following output in the right column box. • Internet Router 202.14.63.3 • Branch PC 172.16.N.10 • DMZ Server 192.168.100+N.3	Ping to Internet Router Output:  Ping statistics for 202.14.63.3: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 1ms, Average = 1ms C:\Users\student>_ Ping to Branch PC Output:  Pinging 172.16.13.10 with 32 bytes of data: Reply from 172.16.13.10: bytes=32 time<1ms TTL=128 Reply from 172.16.13.10: bytes=32 time<1ms TTL=128 Reply from 172.16.13.10: bytes=32 time<1ms TTL=128 Reply from 172.16.13.10: bytes=32 time<1ms TTL=128 Ping statistics for 172.16.13.10: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms Ping to DMZ Server 192.168.100+n.3 Output:

	
	`Ping statistics for 192.168.113.3:`
	`    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),`
	`Approximate round trip times in milli-seconds:`
	`    Minimum = 0ms, Maximum = 0ms, Average = 0ms`
	
	`C:\Users\student>`

From the Branch PC:
Verify that you can ping the following and paste the following output in the right column box.
- DMZ Server 192.168.100+N.3
	Ping to DMZ Server Output:
	
	`Ping statistics for 192.168.113.3:`
	`    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),`
	`Approximate round trip times in milli-seconds:`
	`    Minimum = 0ms, Maximum = 0ms, Average = 0ms`
	
	`C:\Users\student>`

Test access to an external website from the ADMIN PC. Enter the following into a browser from the ADMIN PC Open the Wintec website. www.wintec.ac.nz	Open a browser and enter www.wintec.ac.nz  InPrivate https://www.wintec.ac.nz Wintec Register now Career Choices Day Saturday 7 December 2024, 10am-1pm CAREER CHOICES DAY Are you looking for a fresh start in 2025? Explore your interests, gain career advice and get help choosing the right programme for you at Career Choic… VIEW EVENTS ALL COURSES COURSE GUIDE APPLY NOW  Internet Protocol Version 4 (TCP/IPv4) Properties General You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings. ○ Obtain an IP address automatically ● Use the following IP address: IP address: 192 . 168 . 23 . 10 Subnet mask: 255 . 255 . 255 . 0 Default gateway: 192 . 168 . 23 . 1 ○ Obtain DNS server address automatically ● Use the following DNS server addresses: Preferred DNS server: 1 . 1 . 1 . 1 Alternate DNS server: . . . □ Validate settings upon exit
	Total for Part 5 **/15 marks**

END of PART 5 Important

Copy and Paste your running config file for the ASA Rexnet-HQ in the box below.

Part 6: Secure the network switch on the Rexnet Main Office Network

Task	Command(s)
Assign and encrypt a privileged EXEC password **Password: class12345**	En Conf t Password cisco12345 Enable secret class12345 service password-encryption
Add a user in the local database for administrator access. Username: admin Privilege level: **15** Password: **cisco12345**	enable configure terminal username admin privilege 15 secret cisco12345
Configure SSH Access • IP domain-name: Rexnetsecurity.com • RSA keys 1024 • Only allow SSH version 2 • SSH timeouts: 120 seconds • SSH authentication retries 3	**enable** **configure terminal** **ip domain-name Rexnetsecurity.com** **crypto key generate rsa** **modulus 1024** **ip ssh version 2** **ip ssh time-out 120** **ip ssh authentication-retries 3** **end** **wr**
Configure the VTY lines. Configure the VTY lines for privilege level 15 access on login. Set the timeout value to log out a session after 15 minutes of inactivity. Allow for remote access using SSH only.	**enable** **configure terminal** **line vty 0 4** **privilege level 15** **Password cisco123** **Login** **exec-timeout 15** **transport input ssh** **End** **wr**
Write and configure a message of the day banner (MOTD). It must contain the word “Unauthorised”	**enable** **configure terminal** **banner motd # Welcome to Level_1. Unauthorised access is prohibited. #**
Disable HTTP and HTTP secure server.	**enable** **configure terminal** **no ip http server** **no ip http secure-server** **End**

	Wr
Encrypt all passwords stored in the running config file.	enable configure terminal service password-encryption End wr

Configure the AAA authentication and authorization settings.	**enable** **configure terminal** **aaa new-model** **aaa authentication login default local** **aaa authentication login vty-auth local** **aaa authorization exec default local** **aaa accounting exec default start-stop record** **aaa accounting commands 15 default start-stop record** **line vty 0 4** **login authentication vty-auth** **exit** **line con 0** **login authentication vty-auth** **End** **wr**
Configure 3 VLANs on the switch VLAN 2 for LAN Traffic VLAN 99 for Native VLAN traffic VLAN 199 for unused ports **Assign all useable LAN ports to VLAN 2**	vlan 2 name LAN_Traffic vlan 99 name Native_VLAN vlan 199 name Unused_Ports interface fa 0/10 switchport mode access switchport access vlan 2 No shutdown End wr
Enable PortFast and BPDU guard on fa0/10	**enable** **configure terminal** **interface fa0/10** **spanning-tree portfast bpduguard** **end** **write memory**

Prevent CAM Table attacks and configure basic port security on fa0/10 • Disable trunking • Only two mac addresses may be learnt per interface • This Mac address must be remembered dynamically to the running config file. • Violation mode shutdown	enable configure terminal interface fa0/10 switchport mode access switchport port-security switchport port-security maximum 2 switchport port-security mac-address sticky switchport port-security violation shutdown end write memory
Disable unused ports and assign them to VLAN 199	Conf t Interface range fastethernet 0/1-24 Switchport mode access Switchport access vlan 199 Shutdown Exit wr
Verify connectivity with the gateway from the ADMIN PC 192.168.10+n.1 Paste the output in the box on the right	Output of Ping command to Default Gateway Ip default-gateway 192.168.23.1
Verify SSH works to the Level_1 Switch from the Admin-PC	Paste the Putty Output
	Total for Part 6 **/5 marks**

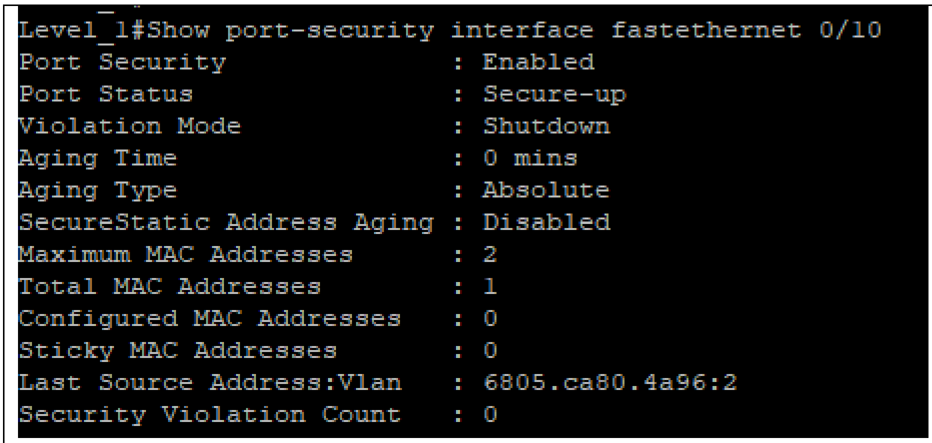
END of PART 6 Important for Marking

Verify the port security for interface fa0/10 below using the correct show command.

Copy and Paste your running config file for the Main Office Switch in the box below.

Command: Show port-security interface fastethernet 0/10

Contents of command:



```
Level_1#Show port-security interface fastethernet 0/10
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 6805.ca80.4a96:2
Security Violation Count   : 0
```

Level 1 Running Config

```
Level_1#show run
Building configuration...


Current configuration : 3628 bytes
!
! No configuration change since last restart
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Level_1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$rNq1$5KM.8jZSw7atgaFWcy8rm/
!
username admin secret 5 $1$srhP$CmwMAhJyn8xcJ9.fJ1u6u/
aaa new-model
!
!
```

```
aaa authentication login default local
aaa authorization exec default local
!
!
!
!
!
!
aaa session-id common
system mtu routing 1500
!
!
no ip domain-lookup
ip domain-name Rexnetsecurity.com
!
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip ssh version 2
!
!
!
!
!
interface FastEthernet0/1
```

```
switchport access vlan 199
switchport mode access
shutdown
!
interface FastEthernet0/2
switchport access vlan 199
switchport mode access
shutdown
!
interface FastEthernet0/3
switchport access vlan 199
switchport mode access
shutdown
!
interface FastEthernet0/4
switchport access vlan 199
switchport mode access
shutdown
!
interface FastEthernet0/5
switchport access vlan 199
switchport mode access
shutdown
!
interface FastEthernet0/6
switchport access vlan 199
switchport mode access
shutdown
!
interface FastEthernet0/7
switchport access vlan 199
switchport mode access
shutdown
!
```

```
interface FastEthernet0/8

switchport access vlan 199

switchport mode access

shutdown

!

interface FastEthernet0/9

switchport access vlan 199

switchport mode access

shutdown

!

interface FastEthernet0/10

description Connection to ADMIN-PC

switchport access vlan 2

switchport mode access

switchport port-security maximum 2

switchport port-security

spanning-tree portfast

spanning-tree bpduguard enable

!

interface FastEthernet0/11

switchport access vlan 199

switchport mode access

shutdown

!

interface FastEthernet0/12

switchport access vlan 199

switchport mode access

shutdown

!

interface FastEthernet0/13

switchport access vlan 199

switchport mode access

shutdown

!
```

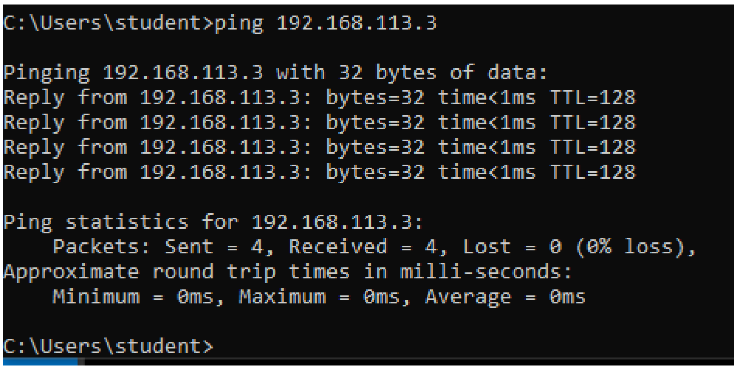
```
interface FastEthernet0/14

switchport access vlan 199

switchport mode access

shutdown

!

interface FastEthernet0/15

switchport access vlan 199

switchport mode access

shutdown

!

interface FastEthernet0/16

switchport access vlan 199

switchport mode access

shutdown

!

interface FastEthernet0/17

switchport access vlan 199

switchport mode access

shutdown

!

interface FastEthernet0/18

switchport access vlan 199

switchport mode access

shutdown

!

interface FastEthernet0/19

switchport access vlan 199

switchport mode access

shutdown

!

interface FastEthernet0/20

switchport access vlan 199

switchport mode access

shutdown
```

```
!
interface FastEthernet0/21
switchport access vlan 199
switchport mode access
shutdown
!
interface FastEthernet0/22
switchport access vlan 199
switchport mode access
shutdown
!
interface FastEthernet0/23
switchport access vlan 199
switchport mode access
shutdown
!
interface FastEthernet0/24
description Connection to RexnetHQ
switchport access vlan 2
switchport mode access
!
interface GigabitEthernet0/1
switchport access vlan 199
switchport mode access
shutdown
!
interface GigabitEthernet0/2
switchport access vlan 199
switchport mode access
shutdown
!
interface Vlan1
no ip address
shutdown
```

```
!
interface Vlan2
ip address 192.168.23.2 255.255.255.0
!
ip default-gateway 192.168.23.1
no ip http server
no ip http secure-server
!
!
!
vstack
banner motd ^C Welcome to Level_1, No Unauthorized Access ^C
!
line con 0
password 7 02050D480809
logging synchronous
line vty 0 4
exec-timeout 15 0
transport input ssh
line vty 5 15
!
ntp server 161.65.172.9
end
```

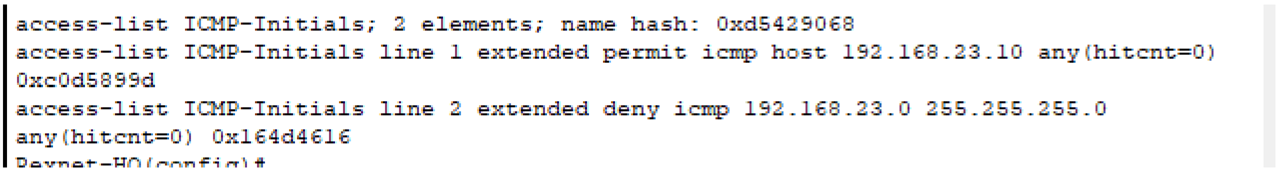
Part 7: Configure a DMZ, static NAT, and ACLs on the REXNET-HQ ASA using ASDM or the CLI

Task	Command(s)
Use ASDM or CLI to configure a static Nat to the DMZ Server. Use the following addresses to guide you: DMZ Server inside local address: 192.168.100+n.3 DMZ server static Public address: 202.14.63.140+n Server Name: DMZ-SERVER	enable configure terminal object network DMZ-SERVER host 192.168.113.3 nat (dmz,outside) static 202.14.63.140.N end Wr mem

Create an access list called OUTSIDE-DMZ that only allows the following protocols to the DMZ Server: - ICMP - HTTPS - HTTP Enable IIS on the DMZ server to test this through Control Panel\All Control Panel Items\Programs and Features > Windows features	enable configure terminal access-list OUTSIDE-DMZ extended permit icmp any host 192.168.113.3 access-list OUTSIDE-DMZ extended permit tcp any host 192.168.113.3 eq 443 access-list OUTSIDE-DMZ extended permit tcp any host 192.168.113.3 eq 80 access-group OUTSIDE-DMZ in interface outside End wr
View the DMZ access Rule generated by ASDM and paste a screen shot of this rule in the box below.	N/A
Verify that you can access the DMZ server from the Branch PC and from one of the Internal.rexnet PCs with the ACL in action. Ping 202.14.63.140+n Paste the output in the right-hand column	Ping to DMZ server from Branch PC Output:  C:\Users\student>ping 192.168.113.3 Pinging 192.168.113.3 with 32 bytes of data: Reply from 192.168.113.3: bytes=32 time<1ms TTL=128 Reply from 192.168.113.3: bytes=32 time<1ms TTL=128 Reply from 192.168.113.3: bytes=32 time<1ms TTL=128 Reply from 192.168.113.3: bytes=32 time<1ms TTL=128 Ping statistics for 192.168.113.3: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms C:\Users\student>
ACL 2: Write and apply an access-list called **ICMP-*Initials*** that only allows the admin to ping out of the network. All other IP addresses on the Rexnet Main Office network / subnet must not be allowed to ping outside but still can access the internet.	enable configure terminal access-list ICMP-Initials extended permit icmp host 192.168.23.10 any access-list ICMP-Initials extended deny icmp 192.168.23.0 255.255.255.0 any access-group ICMP-Initials in interface outside end write memory
	Total for Part 7 **/15 marks**

IMPORTANT for MARKING: Screen shot of the DMZ rule:

DMZ Access Rule:



```
access-list ICMP-Initials; 2 elements; name hash: 0xd5429068
access-list ICMP-Initials line 1 extended permit icmp host 192.168.23.10 any(hitcnt=0)
0xc0d5899d
access-list ICMP-Initials line 2 extended deny icmp 192.168.23.0 255.255.255.0
any(hitcnt=0) 0x164d4616
Rexnet-HQ(config)#
```

IMPORTANT for MARKING: YOU MUST Paste your running config for PART 7 Only below. Only paste what is appropriate for Part 7

```
RexnetHQ# show run
: Saved

:
: Serial Number: JAD21490H7N
: Hardware:   ASA5506, 4096 MB RAM, CPU Atom C2000 series 1250 MHz, 1 CPU (4 cores)
:
ASA Version 9.8(1)
!
hostname RexnetHQ
domain-name Rexnetsecurity.com
enable password $sha512$5000$GH7buFNstUeI5U5GGl+nmg==$6hDj7clhy8nIicwTrTk8wQ== pbkdf2
names

!
interface GigabitEthernet1/1
nameif outside
security-level 0
ip address 202.14.63.141 255.255.255.0
!
interface GigabitEthernet1/2
nameif inside
security-level 100
ip address 192.168.23.1 255.255.255.0
!
interface GigabitEthernet1/3
nameif DMZ
security-level 70
ip address 192.168.113.1 255.255.255.0
!
interface GigabitEthernet1/4
nameif BranchLink
security-level 100
ip address 10.1.13.1 255.255.255.252
!
interface GigabitEthernet1/5
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet1/6
shutdown
```

```
no nameif
no security-level
no ip address
!
interface GigabitEthernet1/7
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet1/8
shutdown
no nameif
no security-level
no ip address
!
interface Management1/1
management-only
shutdown
no nameif
no security-level
no ip address
!
banner motd Unauthorized Access is strictly Prohibited
ftp mode passive
clock timezone NZST 12
dns server-group DefaultDNS
domain-name Rexnetsecurity.com
same-security-traffic permit inter-interface
object network NAT
subnet 192.168.23.0 255.255.255.0
access-list VPN-ACL extended permit ip 192.168.23.0 255.255.255.0 172.16.12.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu DMZ 1500
mtu BranchLink 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
arp rate-limit 16384
!
object network NAT
nat (inside,outside) dynamic pat-pool interface
route outside 0.0.0.0 0.0.0.0 202.14.63.3 1
route BranchLink 172.16.13.0 255.255.255.0 10.1.13.2 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 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
timeout conn-holddown 0:00:15
timeout igp stale-route 0:01:10
user-identity default-domain LOCAL
```

```
aaa authentication enable console LOCAL
aaa authentication login-history
no snmp-server location
no snmp-server contact
service sw-reset-button
crypto ipsec ikev1 transform-set ESP-TUNNEL esp-aes esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map VPN-MAP 10 match address VPN-ACL
crypto map VPN-MAP 10 set peer 10.1.13.2
crypto map VPN-MAP interface BranchLink
crypto ca trustpool policy
crypto ikev1 enable BranchLink
crypto ikev1 policy 10
authentication pre-share
encryption aes
hash sha
group 2
lifetime 86400
telnet timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0

threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 161.65.172.9 source outside
dynamic-access-policy-record DfltAccessPolicy
username admin password $sha512$5000$MKk0osp4dubQhfQWx5nxOw==$sJv83K5B9678pod4vX1pDA==
pbkdf2
tunnel-group 10.1.13.1 type ipsec-l2l
tunnel-group 10.1.13.1 ipsec-attributes
ikev1 pre-shared-key 8 LeG4xtD7mUKROOtrsES8kAjSkdQg8BArYFQ=
!
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
  no tcp-inspection
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
  inspect icmp
!
service-policy global_policy global
prompt hostname context
call-home reporting anonymous prompt 2
call-home
profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/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
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
password encryption aes
Cryptochecksum:6445788c38b4818823a6b8d59619d392
: end
```

Part 8: Configure an IPsec site-to-site VPN between The Rexnet Branch router and the HQ ASA

- **Activate and verify the IPsec site-to-site VPN tunnel**

Instructions: Your company requires all communications between the Main Office and Branch to be encrypted in an IPsec Tunnel. Identify the steps below and configure an IPsec VPN between the Rexnet-HQ and the Rexnet-Branch. Note you must identify the steps and commands below.

1. **Configure the Rexnet-Branch Router**

Task	Command(s)
Step 1 and 2: Verify connectivity to admin-pc from Rexnet-Branch PC and that IKE is enabled.	
Step 3: Configure the ISAKMP policy and security associations for phase 1 on the REXNET ROUTER • Policy 10 • Authentication pre-share • Aes256 encryption • Hash sha	**En** **Conf t** **Crypto ikev1 policy 10** **Authentication pre-share** **Encryption aes** **Hash sha**

• DH	**Exit** **Crypto ikev1 enable BRANCH_LINK** **Exit** **Wr mem**
Step 4: Configure the pre-shared keys • Key: REXNET-KEY • Peer address 10.1.N.1	**En** **Conf t** **tunnel-group 10.1.13.1 type ipsec-l2l** **tunnel-group 10.1.13.1 ipsec-attributes** **ikev pre-shared-key REXNET-KEY** **Exit** **Wr mem**
Step 5: Configure the IPsec transform set Name: ESP-TUNNEL	**En** **Conf t** **crypto ipsec ikev1 transform-set ESP-TUNNEL esp-aes esp-sha-hmac** crypto map VPN-MAP 10 set peer 10.1.13.1 crypto map VPN-MAP 10 set ikev1 transform-set VPN-SET Exit Wr mem
Step 6: Define interesting traffic ACL name: VPN-ACL	**En** **Conf t** **access-list VPN-ACL extended permit ip object INSIDE-NET object BRANCH-NET** **End** **Wr mem**
Step 7: Create and apply a crypto map • Bind the ISAKMP policy 10 with peer, IPsec policy and ACL • Apply the crypto map to the g0/1 interface	**# ASA** En Conf t crypto map VPN-MAP 10 match address VPN-ACL crypto map VPN-MAP interface BRANCH_LINK #Brach Router En Conf t crypto isakmp policy 10 Authentication pre-share Encryption aes Group 2 Hash sha Lifetime 70000 Exit crypto ipsec transform-set ESP-TUNNEL esp-aes esp-sha-hmac crypto map VPN-MAP 10 ipsec-isakmp set peer 10.1.13.1 set transform-set ESP-TUNNEL Match address VPN-ACL end Wr Conf t ip access-list extended VPN-ACL permit ip 172.16.13.0 0.0.0.255 192.168.23.0 0.0.0.255 Exit interface gigabitEthernet 0/1 crypto map VPN-MAP Exit

c	

2. Configure the ASA REXNET-HQ as the Other VPN Endpoint

- Log into ASDM with the correct username and password from the ADMIN PC

Task	Command(s)
Using the ASDM Site to Site VPN wizard configure the IPsec VPN tunnel endpoint. Ensure the security ISAKMP and Security Associations match the configuration applied on the Rexnet-Branch Router. Note: NAT is not occurring on the Branch-Link interface so you will not need to exempt it from the configuration.	N/A
Create Interesting Traffic • From the branch pc 172.16.N.10 ping the Admin-PC 192.168.10+n.10 • Copy and paste the output from the Branch PC in the right column.	**Branch PC Output** **N/A**
Verify the IPsec Tunnel is working from the ASA Rexnet-HQ and provide a screen shot of the monitoring session. **Screen Shot:**	
Total **/10 marks**	

END of PART 8 Important for Marking

You Must copy and Paste your running config file for the ASA Rexnet-HQ and the Router REXNET-BRANCH in the box below. Only provide the section of the running config that is applicable for this part.

```
ASA Rexnet-HQ Config
RexnetHQ# show run
: Saved


:
: Serial Number: JAD21490H7N
: Hardware:   ASA5506, 4096 MB RAM, CPU Atom C2000 series 1250 MHz, 1 CPU (4 cores)
:
ASA Version 9.8(1)
!
hostname RexnetHQ
domain-name Rexnetsecurity.com
enable password $sha512$5000$GH7buFNstUeI5U5GGl+nmg==$6hDj7clhy8nIicwTrTk8wQ== pbkdf2
```

```
names

!
interface GigabitEthernet1/1
nameif outside
security-level 0
ip address 202.14.63.141 255.255.255.0
!
interface GigabitEthernet1/2
nameif inside
security-level 100
ip address 192.168.23.1 255.255.255.0
!
interface GigabitEthernet1/3
nameif DMZ
security-level 70
ip address 192.168.113.1 255.255.255.0
!
interface GigabitEthernet1/4
nameif BranchLink
security-level 100
ip address 10.1.13.1 255.255.255.252
!
interface GigabitEthernet1/5
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet1/6
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet1/7
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet1/8
shutdown
no nameif
no security-level
no ip address
!
interface Management1/1
management-only
shutdown
no nameif
no security-level
no ip address
!
banner motd Unauthorized Access is strictly Prohibited
ftp mode passive
clock timezone NZST 12
dns server-group DefaultDNS
```

```
domain-name Rexnetsecurity.com
same-security-traffic permit inter-interface
object network NAT
subnet 192.168.23.0 255.255.255.0
object network DMZ-SERVER-PUBLIC
host 202.14.63.153
object network DMZ-SERVER-LOCAL
host 192.168.113.3
access-list VPN-ACL extended permit ip 192.168.23.0 255.255.255.0 172.16.12.0 255.255.255.0
access-list OUTSIDE-DMZ extended permit icmp any host 192.168.113.3
access-list OUTSIDE-DMZ extended permit tcp any host 192.168.113.3 eq www
access-list OUTSIDE-DMZ extended permit tcp any host 192.168.113.3 eq https
access-list outside_access_in extended permit tcp any host 192.168.112.3 eq www
access-list outside_access_in extended permit tcp any host 192.168.113.3 eq www
access-list outside_access_in extended permit ip any host 192.168.113.3
pager lines 24
mtu outside 1500
mtu inside 1500
mtu DMZ 1500
mtu BranchLink 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
arp rate-limit 16384
!
object network NAT
nat (inside,outside) dynamic pat-pool interface
object network DMZ-SERVER-LOCAL
nat (DMZ,outside) static DMZ-SERVER-PUBLIC
access-group OUTSIDE-DMZ in interface outside
route outside 0.0.0.0 0.0.0.0 202.14.63.3 1
route BranchLink 172.16.13.0 255.255.255.0 10.1.13.2 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 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
timeout conn-holddown 0:00:15
timeout igp stale-route 0:01:10
user-identity default-domain LOCAL
aaa authentication enable console LOCAL
aaa authentication login-history
no snmp-server location
no snmp-server contact
service sw-reset-button
crypto ipsec ikev1 transform-set ESP-TUNNEL esp-aes esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map VPN-MAP 10 match address VPN-ACL
crypto map VPN-MAP 10 set peer 10.1.13.2
crypto map VPN-MAP interface BranchLink
crypto ca trustpool policy
crypto ikev1 enable BranchLink
crypto ikev1 policy 10
authentication pre-share
```

```
encryption aes
hash sha
group 2
lifetime 86400
telnet timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0

threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 161.65.172.9 source outside
dynamic-access-policy-record DfltAccessPolicy
username admin password $sha512$5000$MKk0osp4dubQhfQWx5nxOw==$sJv83K5B9678pod4vX1pDA==
pbkdf2
tunnel-group 10.1.13.1 type ipsec-l2l
tunnel-group 10.1.13.1 ipsec-attributes
ikev1 pre-shared-key 8 LeG4xtD7mUKROOtrsES8kAjSkdQg8BArYFQ=
!
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
  no tcp-inspection
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
  inspect icmp
!
service-policy global_policy global
prompt hostname context
call-home reporting anonymous prompt 2
call-home
profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/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
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
password encryption aes
Cryptochecksum:8f7bbe90ad7e732733bcbd918bf8ed2c
: end
RexnetHQ#

REXNET-BRANCH Config

Rexnet_Branch#show run
Building configuration...

Current configuration : 3409 bytes
!
! Last configuration change at 13:01:47 NZST Tue Nov 19 2024 by admin
! NVRAM config last updated at 10:59:49 NZST Tue Nov 19 2024
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Rexnet_Branch
!
boot-start-marker
boot-end-marker
!
!
security passwords min-length 10
logging buffered 10000
enable secret 9 $9$dbxBGRcE/f0YyU$/wpGzgCQA.ecrgFxC27Kn0W7DR9f5rR.2eOSGC2wXCc
!
aaa new-model
aaa local authentication attempts max-fail 6
!
!
aaa authentication login default local-case enable
aaa authentication login SSH-LOGIN local-case
!
!
!
!
!
aaa session-id common
memory-size iomem 15
clock timezone NZST 12 0
!
!
!
!
!
!
!
!
!
```

```
!
!
!
!
!
no ip domain lookup
ip domain name Rexnetsecurity.com
ip cef
login block-for 60 attempts 3 within 60
no ipv6 cef
!
multilink bundle-name authenticated
!
cts logging verbose
!
!
license udi pid CISCO1941/K9 sn FGL214392J0
license accept end user agreement
license boot module c1900 technology-package securityk9
!
!
username admin privilege 15 secret 9
$9$m1dwzXAMFSVsWk$QpNoOCP24ChIcoHzQABkIztovFkltIVdD9YjAZEETK2
username Service_Support privilege 0 view ServiceSupport secret 9
$9$ufpxFlJIiwO5vE$lfgXM1NSpzRkh/3hLRsYSGzGn5zH70HAEIZSeVNMjBg
secure boot-image
secure boot-config
!
redundancy
!
!
!
!
no cdp run
!
ip ssh version 2
!
!
crypto isakmp policy 10
encr aes
authentication pre-share
group 2
lifetime 70000
!
!
crypto ipsec transform-set ESP-TUNNEL esp-aes esp-sha-hmac
mode tunnel
!
!
!
crypto map VPN-MAP 10 ipsec-isakmp
set peer 10.1.13.1
set transform-set ESP-TUNNEL
match address VPN-ACL
!
!
!
!
```

```
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
description Local Network
ip address 172.16.13.1 255.255.255.0
ip access-group VPN-ACL in
duplex auto
speed auto
!
interface GigabitEthernet0/1
description WAN Uplink
ip address 10.1.13.2 255.255.255.252
ip access-group VPN-ACL out
duplex auto
speed auto
crypto map VPN-MAP
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
no ip address
shutdown
clock rate 2000000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 10.1.13.1
ip route 192.168.23.0 255.255.255.0 10.1.13.1
!
ip access-list extended VPN-ACL
permit ip 172.16.13.0 0.0.0.255 192.168.23.0 0.0.0.255
!
!
!
access-list 10 permit 172.16.13.10
access-list 10 deny   any
!
!
!
control-plane
!
!
privilege exec level 0 enable view
privilege exec level 0 enable
banner motd ^C No Unauthorized Access ^C
parser view ServiceSupport
secret 5 $1$T9QI$FCY4jXP5CraJmtQ1c2STK/
commands exec include ping
commands exec include reload
commands exec include all show
!
!
line con 0
privilege level 0
password 7 060506324F41584B564347
logging synchronous
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
access-class 10 in
exec-timeout 15 0
privilege level 0
login authentication SSH-LOGIN
transport input ssh
line vty 5 1370
access-class 10 in
exec-timeout 15 0
privilege level 0
login authentication SSH-LOGIN
transport input ssh
!
scheduler allocate 20000 1000
ntp authentication-key 1 md5 06340A39017A001400 7
ntp authenticate
ntp trusted-key 1
ntp master 1
ntp server 161.65.172.9
!
end

Rexnet_Branch#
```

PART 9: Justification

Justify 1 of the topics that you have implemented in this case study. Outline the reasoning behind the security configurations that you configured. Reasoning could include aspects such as:

- Any weaknesses and strengths of the configuration;
- The types of attacks this config is trying to defend against;
- How this configuration specifically defends against these attacks;

Note: This document should be more than 500 words and will provide credibility for the equipment configurations and implementation. You could use the following topics below to help guide you. Refer to the marking criteria below for details.

Topics

Only choose one of these topics.

1. **Switch Security**
2. **Task Performed:**
3. **Reasoning Behind the Config**

Switch Security Configuration Report

This report outlines the switch security configuration, detailing the tasks performed, the reasoning behind the settings, the strengths and weaknesses of the configuration, and how it defends against various types of attacks.

Tasks Performed

The main goal of this configuration was to secure the switch and enhance overall network security. Key tasks included setting up user authentication, enabling port security, using SSH for remote management, configuring VLANs, and securing the Spanning Tree Protocol (STP).

User authentication was configured using encrypted passwords (`enable secret` and `username admin secret`), ensuring that only authorized users could access the switch. AAA (Authentication, Authorization, and Accounting) was enabled to control user access and enforce security policies.

Port security was applied with the `switchport port-security maximum 2` setting on specific ports, such as FastEthernet0/10, to limit the number of devices that can connect to a port. This helps prevent unauthorized devices from accessing the network. The Spanning Tree Protocol was configured with PVST (Per VLAN Spanning Tree) and BPDU Guard to protect against attacks that could manipulate the switch's topology.

SSH was enabled (`ip ssh version 2`) to replace older and insecure protocols like Telnet, providing encrypted remote access. Unused ports were shut down using the `shutdown` command, reducing potential entry points for attackers. Unnecessary services like the HTTP server were also disabled to minimize vulnerabilities.

Reasoning Behind the Configuration

The purpose of this configuration is to strengthen the security of the switch and network. Encrypted passwords and AAA authentication ensure that only authorized users can access and configure the switch. Port security prevents unauthorized devices from connecting, and BPDU Guard protects against attacks that could disrupt the network's topology. SSH provides secure remote access, and shutting down unused ports reduces the attack surface. Disabling unnecessary services also limits potential security risks.

Strengths and Weaknesses of the Configuration

The configuration has several strengths. First, encrypted passwords and AAA authentication provide robust protection against unauthorized access. Port security limits the number of devices that can connect, reducing the risk of unauthorized devices being introduced. BPDU Guard prevents attacks that could disrupt the network's spanning tree topology, and SSH ensures that remote management is encrypted and secure.

However, there are some weaknesses. The port security setting, limiting each port to two MAC addresses, may be too restrictive in environments that need more devices on a port. Additionally, the configuration lacks Access Control Lists (ACLs), which could help further secure the network by controlling traffic. The shut-down `Vlan1` interface, which has no IP address, could cause confusion during troubleshooting. Finally, while a default gateway is configured, it could be a point of failure if compromised.

Attacks the Configuration Defends Against

This configuration helps protect against several types of attacks. It defends against MAC flooding by limiting the number of devices per port. It also protects against BPDU spoofing by using BPDU Guard, which disables any port receiving unauthorized BPDUs. The encrypted passwords and AAA authentication prevent unauthorized access to the switch, ensuring that only legitimate users can make changes.

Conclusion

This switch configuration provides strong security by limiting unauthorized access, preventing malicious devices from connecting, and protecting against attacks like MAC flooding and BPDU spoofing. While some adjustments, such as making port security settings more flexible and adding ACLs, could improve the configuration, it offers a solid foundation for securing the network.

Marking Criteria for Part 9 (30 marks)

Criteria
• Student outlines and explains the tasks they performed for one of the high-level topics (7 marks) • Student presents logical reasoning for the configuration   • Configuration is critiqued, identifying / explaining the following in your justification: ○ At least 4 weaknesses and strengths of the configuration (12 marks).   ○ 3 types of attacks this config is trying to defend against (6 marks).   ○ How this configuration specifically defends against these attacks (5 marks).   • Marks can be deducted for improper grammar
Total for part 9 **/30**

AFTER you have been marked and taken all your running configs.

CLEAN UP

Failure to clean up after yourself will result in loss of marks

1. **Erase all startup configs and reload all the devices**
2. **Pack your cables away neatly**

3. **Reset computer ip addresses and set Internet access back to normal**