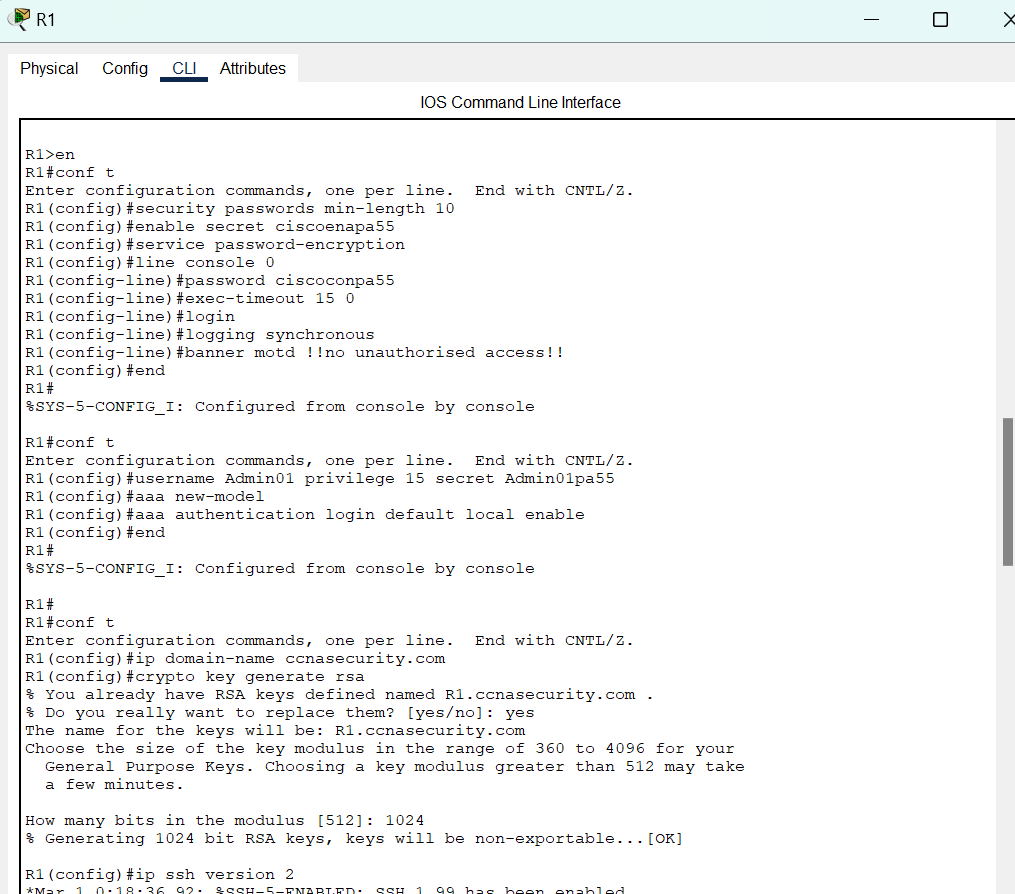
**STUDENT - PRODUCT ASSESSMENT TASK**

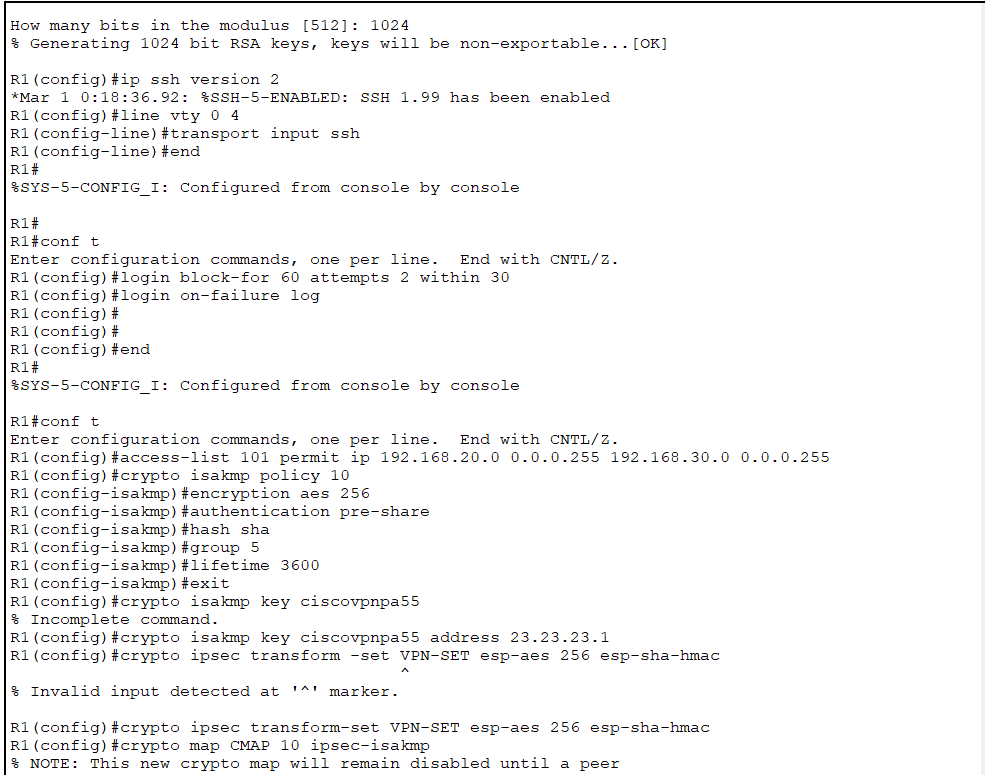
**PRODUCT ASSESSMENT TASK**

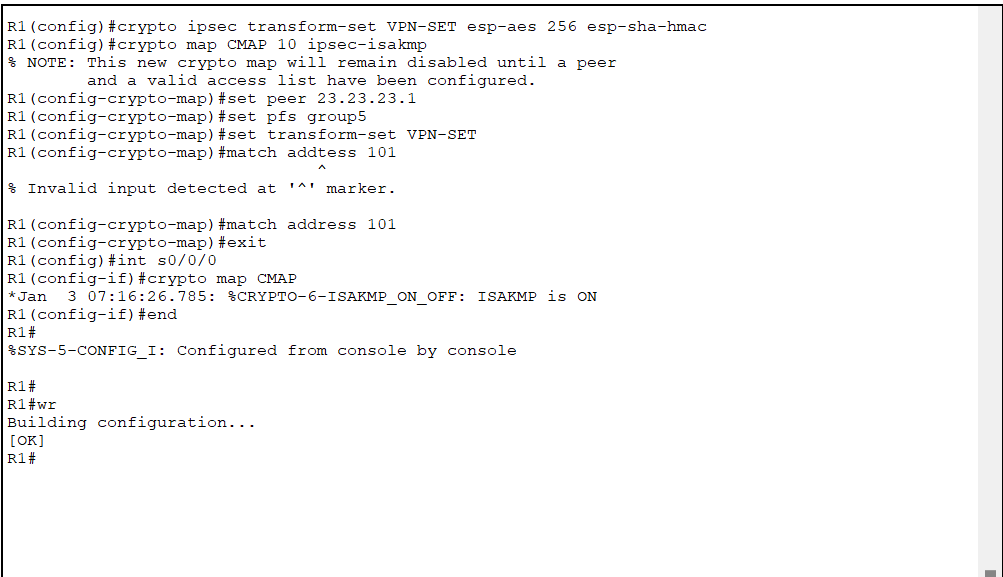
|  |  |  |  |
| --- | --- | --- | --- |
| Task Number | 3 of 3 | Task Name | Design and implement security perimeter architecture |
| National unit/s code | VU21991  ICTNWK509 | National unit/s title | Implement network security infrastructure for an organisation  Design and implement a security perimeter for ICT networks |
| National qualification code | 22334VIC | National qualification title | Certificate IV in Cyber Security |
| RMIT Program code | TBC | RMIT Course code | TBC |

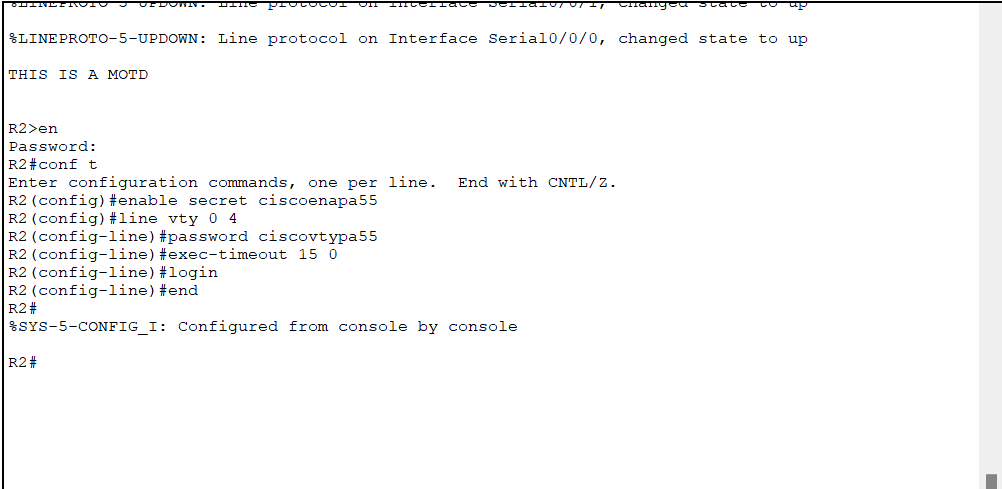
Section A **- Assessment Information**

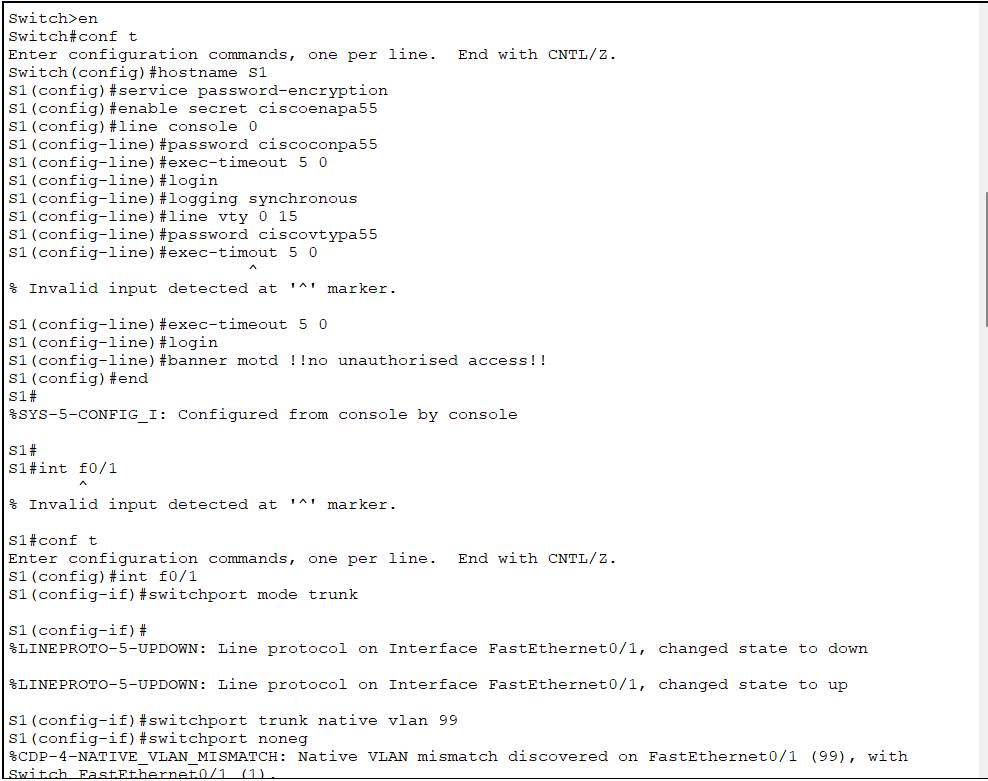
|  |  |  |
| --- | --- | --- |
| **Assessment duration and/or due date** | Teaching staff to confirm duration and date. | |
| **Task Instructions** | | |
| **Type of Product (tick which applies)**  ✓ Project  ☐ Report  ☐ Portfolio  ☐ Case study  **Summary and Purpose of Assessment**  This assessment is designed to allow the student to demonstrate their skills and knowledge in the design and implementation of a security perimeter for an organisation. This requires the student to demonstrate the following:   * Configure secure administrative access to network devices * Plan and design firewall solution * Implement firewall technologies * Investigate new firewall technologies * Configure perimeter to the secure network * Implement intrusion prevention systems (IPS) * Plan, design and configure network devices to provide secure fallover and redundancy * Demonstrate the fundamental operations of Cryptographic systems * Define and demonstrate the fundamentals of Virtual Private Networks (VPNs) * Plan, design and configure a VPN solution * Test and verify design performance   **Assessment Instructions**  Students are required to complete a range of tasks to review existing network topologies and security solutions, to identify the range of security risks to the organisation, and to design a secure network perimeter for the protection of the client data.  ***What***  *The following tasks must be completed in this assessment:*  You have recently been employed as a Cyber Security Consultant for IT Assurance Services. IT Assurance Services specialises in the provision of ICT services to a range of small and medium enterprises, including the conduct of cyber security vulnerability assessments and the subsequent design and implementation of risk mitigation solutions to secure client systems.  Your employer has asked you to review the existing network infrastructure for their client Jojo Pty Ltd and to design and implement an effective security perimeter. As part of this you are required to document all stages of the network and security perimeter design to explain the purpose and functionality of each aspect.  The following topology is currently implemented:     |  |  |  |  |  | | --- | --- | --- | --- | --- | | Addressing Table | | | | | | Device | Interface | IP Address | Subnet Mask | Default Gateway | | R1 | G0/0 | 209.165.200.233 | 255.255.255.248 | N/A | | S0/0/0 (DCE) | 12.12.12.1 | 255.255.255.252 | N/A | | Loopback 1 | 192.168.20.1 | 255.255.255.0 | N/A | | R2 | S0/0/0 | 12.12.12.2 | 255.255.255.252 | N/A | | S0/0/1 (DCE) | 23.23.23.2 | 255.255.255.252 | N/A | | R3 | G0/1 | 192.168.30.1 | 255.255.255.0 | N/A | | S0/0/1 | 23.23.23.1 | 255.255.255.252 | N/A | | S1 | VLAN 1 | 192.168.10.11 | 255.255.255.0 | 192.168.10.1 | | S2 | VLAN 1 | 192.168.10.12 | 255.255.255.0 | 192.168.10.1 | | S3 | VLAN 1 | 192.168.30.11 | 255.255.255.0 | 192.168.30.1 | | ASA | VLAN 1 (E0/1) | 192.168.10.1 | 255.255.255.0 | N/A | | VLAN 2 (E0/0) | 209.165.200.234 | 255.255.255.248 | N/A | | PC-A | NIC | 192.168.10.2 | 255.255.255.0 | 192.168.10.1 | | PC-B | NIC | 192.168.10.3 | 255.255.255.0 | 192.168.10.1 | | PC-C | NIC | 192.168.30.3 | 255.255.255.0 | 192.168.30.1 |   For your submission you will provide the following files:   * CISCO Packet Tracer Files * Documented System Design   **Your Task**  Using the information in the case study, complete the following steps to design and implement a security perimeter for Jojo Pty Ltd. For all tasks where you are required to configure network devices and services, you must include the configuration scripts and commands that you have used within the Documented System Design. Where possible screenshots should also be taken to confirm that devices and services have been configured and operate correctly.  **Initial Assessment and Planning**   1. Evaluate the security vulnerabilities found in the internetworking system provided above and provide a proposal for the for advanced security technologies to be implemented.   **Assessment of Security Vulnerabilities:**   * + - * Weak Authentication: Lack of strong passwords or multi-factor authentication.       * Unsecured Management Access: Remote management access (like Telnet) can be intercepted.       * No Network Segmentation: Vulnerable devices could be accessed from all parts of the network.       * Lack of Intrusion Prevention: No systems in place to detect and prevent unauthorized access.   **Proposed Advanced Security Technologies:**   * + - * Firewalls: Implement Zone-Based Policy Firewalls (ZPF) on routers and firewalls for packet inspection.       * Intrusion Prevention Systems (IPS): Deploy IPS to monitor traffic for malicious activities.       * VPNs: Use site-to-site VPNs for secure communications between branches.       * Network Segmentation: Implement VLANs to separate sensitive data from less secure traffic.       * Access Control Lists (ACLs): Configure ACLs to restrict access to network resources based on security policies.  1. Build the interworking system shown in the topology diagram for Jojo Pty Ltd using the CISCO Packet Tracer simulation software. In this design you will use Router 1941, switch 2960 and ASA 5505 2. Provide a description of the process for configuring secure administrative access to the network.   Enable ssh for secure management:  R1>en  R1#conf t  R1(config)#ip domain-name ccnasecurity.com  R1(config)#crypto key generate rsa  How many bits in the modulus [512]: 1024  R1(config)#ip ssh version 2  R1(config)#line vty 0 4  R1(config-line)#transport input ssh  R1(config-line)#login local  R1(config-line)#end  R1#        Create a local user account with privilege level:  R1(config)#username Admin privilege 15 secret Adminenapa55     1. Provide a description of the process for the allocation of user command privileges for network devices.   User command privileges can be configured using privilege levels system. By default, level 15 is full access.  Level 0: Limited access, usually just basic commands.  Level 1: User EXEC mode, allowing basic monitoring commands (read-only access).  Level 15: Full access to all commands, including configuration commands (full administrative access).  By using privilege levels, network administrators can control what commands users can execute, thereby enhancing security and reducing the risk of accidental or malicious changes to the device configuration.  **Router and Switch Configuration**   1. Configure the routers and switches within the network topology.    1. Configure the routers to the following settings:       1. Change the hostnames from default to R1, R2 and R3 respectively.          * Router1 (config)# hostname R1          * Router2 (config)# hostname R2          * Router3 (config)# hostname R3       2. Configure interface IP addresses as given in addressing table.   R1 (config)# int g0/0  R1 (config)# ip address 209.165.200.233 255.255.255.248  R1 (config)# no shutdown  R1(config)# interface S0/0/0  R1(config-if)# ip address 12.12.12.1 255.255.255.252  R1(config-if)# no shutdown  R1(config)# interface Loopback 1  R1(config-if)# ip address 192.168.20.1 255.255.255.0  R1(config-if)# no shutdown  We repeat for R2 and R3 with their given IPs from the addressing table.         * + 1. Configure Routing using OSPFv2 and Process ID 1 on R1, R2 and R3.   R1(config)# router ospf 1  R1(config-router)# network 12.12.12.0 0.0.0.3 area 0  R1(config-router)# network 209.165.200.232 0.0.0.7 area 0            # sh ip ospf database   * 1. Configure the switches to the following settings:      1. Change the hostnames from default to S1, S2 and S3 respectively.   S1(config)# hostname S1  S2(config)# hostname S2  S3(config)# hostname S3   * + 1. Configure trunking between S1 and S2.   S1 and S2  conf t  interface FastEthernet 0/1  switchport mode trunk  switchport trunk native vlan 99  switchport nonegotiate  end   * + 1. Configure Vlan1 IP addresses and default gateway as shown in addressing table.   S1(config)# interface VLAN 1  S1(config-if)# ip address 192.168.10.11 255.255.255.0  S1(config-if)# exit  S1(config)# ip default-gateway 192.168.10.1       * 1. Ping between the routers and ping between Loopback 1 and PC-C should be successful. Take a screenshot to confirm that this is successful.   R1# ping 12.12.12.2  R2# ping 12.12.12.1    **Loopback**  R1# ping 192.168.20.1  PC-C ping 192.168.20.1     1. Undertake troubleshooting of peripheral I/O devices including installation and configuration as required.   # sh ip int brief (to check interface state)  **Configure Firewall and IPS Settings**   1. Configure a Zone-Based Policy Firewall (ZPF) on R3 using the following requirements.    * 1. Create zones named IN-ZONE and OUT-ZONE.   # zone security IN-ZONE  # zone security OUT-ZONE   * + 1. Create an ACL number 110 that defines internal traffic, which permits all IP protocols from the 172.30.3.0/24 source network to any destination.   # access-list 110 permit ip 172.30.3.0 0.0.0.255 any  # access-list 110 deny ip any any   * + 1. Create a class map named INTERNAL-CLASS-MAP that uses the match-all option and ACL 110.   # class-map type inspect match-all INTERNAL-CLASS-MAP  # match access-group 110  # exit   * + 1. Create a policy map named IN-2-OUT-PMAP that uses the class map INTERNAL-CLASS-MAP to inspect all matched traffic.   # policy-map type inspect IN-2-OUT-PMAP  # class type inspect INTERNAL-CLASS-MAP  # inspect   * + 1. Create a zone pair named IN-2-OUT-ZPAIR that identifies IN-ZONE as the source zone and OUT-ZONE as the destination zone.   # zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE  # service-policy type inspect IN-2-OUT-PMAP  # exit   * + 1. Specify that the IN-2-OUT-PMAP policy map is to be used to inspect traffic between the two zones.   # service-policy type inspect IN-2-OUT-PMAP   * + 1. Assign G0/1 as an IN-ZONE member and S0/0/1 as an OUT-ZONE member.   # interface g0/1 zone-member security IN-ZONE  # exit  # interface s0/0/1 zone-member security OUT-ZONE  # end       1. Configure an Intrusion Prevention System (IPS) on R3 using the following requirements:    * 1. Create a directory in flash named ipsdir and set it as the location for IPS signature storage.   # mkdir ipsdir  # conf t  # ip ips config location flash:ipsdir   * + 1. Create an IPS rule named IPS-RULE.   # ip ips name IPS-RULE   * + 1. Retire the all signature category with the retired true command (all signatures within the signature release).   # ip ips signature-category  # category all  # retired true  # exit   * + 1. Unretire the IOS\_IPS Basic category with the retired false command.   # category ios\_ips basic  # retired false  # exit   * + 1. Apply the rule inbound on the S0/0/1 interface.   # exit  # <Enter>  # interface s0/0/1  # ip ips IPS-RULE in          **Note:** Within Packet Tracer, the routers already have the signature files imported and in place. They are the default XML files in flash. For this reason, it is not necessary to configure the public crypto key and complete a manual import of the signature files.  **Configuration of secure site-to-site VPN**   1. Answer the following in relation to Virtual Private Network (VPN) technologies:    1. Provide an explanation of the advantages and operation of VPNs.   **Cost-Effective Remote Connectivity**: VPNs allow businesses to connect remote users to their corporate network securely, utilizing affordable third-party internet access instead of expensive dedicated WAN links.  **Secure Remote Access**: VPN technology ensures that only authenticated users or devices can connect to the corporate network, maintaining a secure environment for remote work.  **Encrypted Communication**: VPNs create a secure "tunnel" for data transmission, encrypting information to protect it from interception while traveling across the internet.  **Flexibility and Ease of Use**: SSL VPNs can be accessed through modern web browsers without needing additional client software, making it easy for users to connect from any device.  **Enhanced Productivity**: By enabling secure remote access to network resources, VPNs help boost workforce productivity, allowing employees to work from anywhere.  **Support for Multiple Topologies**: VPNs can be configured in various topologies (like hub-and-spoke, point-to-point, and full mesh), providing flexibility in how networks are structured and connected.  **Scalability**: VPNs can easily accommodate new users and devices, making it simple for businesses to expand their network as needed.  **Reduced IT Support Costs**: By using cloud-based VPN solutions, companies can lower expenses related to maintaining in-house servers and IT staff, as the service provider handles much of the infrastructure.  **Protection Against Threats**: VPNs can implement security measures such as two-factor authentication and endpoint security checks to help prevent unauthorized access and mitigate risks from remote devices.  **Bypass Geo-Restrictions**: VPNs allow users to access content and services that may be restricted based on their geographic location, enhancing overall access to information and resources.  <https://www.cisco.com/c/en/us/solutions/small-business/resource-center/security/how-does-a-vpn-work.html#~types-of-vpn-topologies>   * 1. Provide a summary of the operation of Internet Protocol Security (IPSec) VPNs.   Internet Protocol Security (IPsec) is a suite of protocols designed to secure internet communications by encrypting and authenticating IP packets, ensuring that sensitive data sent over public networks remains confidential and protected. It works by facilitating key exchange between devices to establish encryption, adding headers to packets for authentication and encryption, and transmitting these secure packets using UDP for efficient routing. At the destination, packets are decrypted for use. IPsec includes protocols like the Authentication Header (AH), which provides authentication without encryption, and the Encapsulating Security Payload (ESP), which encrypts data and authenticates it. It operates in two modes: Tunnel Mode, which encrypts the entire packet and is ideal for site-to-site connections, and Transport Mode, which encrypts only the payload, commonly used for device-to-device communications. Overall, IPsec is essential for creating secure, encrypted connections over the internet and is widely utilized in VPNs to protect sensitive information from unauthorized access.  <https://www.cloudflare.com/learning/network-layer/what-is-ipsec/>   * 1. Provide a description of how tunnelling operates in relation to VPNs   Tunneling in VPNs refers to the process of creating a secure, encrypted connection between two or more devices over a public network, such as the internet. This is achieved by encapsulating data packets within a new packet that includes additional headers for routing and security. When a user connects to a VPN, their device establishes a "tunnel" to a VPN server. Within this tunnel, the original data is encrypted, making it unreadable to anyone who might intercept it during transmission. The tunnel essentially acts like a protective envelope, ensuring that the data remains private and secure from external threats. There are different tunneling protocols, such as IPsec, which can operate in two modes: Tunnel Mode and Transport Mode. In Tunnel Mode, the entire original packet, including the IP header, is encrypted, while a new IP header is added for routing. This mode is often used for site-to-site connections. In Transport Mode, only the payload of the packet is encrypted, allowing the original IP header to remain visible to intermediate routers. Tunneling is crucial for VPNs as it enables secure communication over potentially unsafe networks, allowing users to access sensitive information and resources while maintaining privacy and security.  <https://www.cloudflare.com/learning/network-layer/what-is-ipsec/>  Bottom of Form   1. Configure the security of R1 for secure connections.    1. Enable the Security Technology Package licence on R1. Save the running configuration before reloading and take a screenshot to confirm this.   # license boot level security   * 1. Configure the access list:      1. Create an access list to identify interesting traffic on R1   # access-list 101 permit ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255   * + 1. Configure ACL 101 to allow traffic from the R1 Lo1 network to the R3 G0/1 LAN.   1. Configure the **crypto isakmp policy 10** Phase 1 properties on R1 and the shared crypto key ciscovpnpa55 using the following parameters:      1. Key distribution method: **ISAKMP > # crypto isakmp policy 10**      2. Encryption: **aes 256 > # encryption aes 256**      3. Hash: **sha > # hash sha**      4. Authentication method: **pre-shared > # authentication pre-share**      5. Key exchange: **DH Group 5 > # group 5**      6. IKE SA lifetime: **3600 > # lifetime 3600**      7. ISAKMP key: **ciscovpnpa55 > # crypto isakmp key ciscovpnpa55 add 23.23.23.1**      1. Create the transform set VPN-SET to use esp-aes 256 and esp-sha-hmac. Then create the cryptomap CMAP that binds all of the Phase 2 parameters together. Use sequence number 10 and identify it as an ipsec-isakmp map. Use the following parameters:    * + - R3(config)#crypto isakmp key ciscovpnpa55 add 23.23.23.        - R3(config)#crypto ipsec transform-set VPN-SET esp-aes 256 esp-sha-hmac        - R3(config)#crypto map CMAP 10 ipsec-isakmp        - % NOTE: This new crypto map will remain disabled until a peer and a valid access list have been configured.        - R3(config-crypto-map)#set peer 23.23.23.1        - R3(config-crypto-map)#set transform-set VPN-SET        - R3(config-crypto-map)#match add 110        - R3(config-crypto-map)#exit        - R3(config)#int s0/0/1        - R3(config-if)#crypto map CMAP        - R3(config-if)#END          1. Verify that the Security Technology Package Licence is enabled on R3. Repeat the site-to-site VPN configurations on R3 so that they mirror all configurations from R1. Save the running configuration before reloading and take a screenshot to confirm this.   R3(config)#crypto isakmp key ciscovpnpa55 add 12.12.12.1  R3(config)#crypto ipsec transform-set VPN-SET esp-aes 256 esp-sha-hmac  R3(config)#crypto map CMAP 10 ipsec-isakmp  % NOTE: This new crypto map will remain disabled until a peer  and a valid access list have been configured.  R3(config-crypto-map)#set peer 12.12.12.1  R3(config-crypto-map)#set transform-set VPN-SET  R3(config-crypto-map)#match add 110  R3(config-crypto-map)#exit  R3(config)#int s0/0/1  R3(config-if)#crypto map CMAP  \*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP\_ON\_OFF: ISAKMP is ON  R3(config-if)#  R3(config-if)#END     1. Ping the Lo1 interface on R1 from PC-C. On R3, use the **show crypto ipsec sa** command to verify that the number of packets is more than 0, which indicates that the IPsec VPN tunnel is working. Take screen shot     From PCC > Ping 192.168.20.1   1. Undertake troubleshooting of peripheral I/O devices including installation and configuration as required.   R3 > sh crypto ipsec sa  # sh running-config  # sh ospf int brief  **Configuration of ASA Basic Security and Firewall Settings**   1. Answer the following in relation to firewall technologies:    1. Provide a description of the operation of access lists (ACLS’s) in relation to firewalls   Access Control Lists (ACLs) are rules that manage incoming and outgoing traffic on devices like routers and firewalls. They allow or block traffic based on criteria such as IP addresses, protocols, or port numbers. ACLs evaluate each data packet in order: if a packet matches a rule, it follows that action; if not, it’s usually denied. There are Standard ACLs, which filter by source IP addresses, and Extended ACLs, which provide more control by filtering based on both source and destination IPs, protocols, and port numbers. ACLs help enforce security policies and protect networks from unauthorized access.   * 1. Provide a description of the function and operations of a firewall in the mitigation of network attacks   Firewalls protect trusted networks from untrusted ones, like the Internet. They filter traffic by checking packets against security rules to block malicious traffic while allowing legitimate traffic. Many use stateful inspection to track active connections for smarter filtering. Some inspect application-layer traffic to prevent specific attacks. Firewalls may also include intrusion prevention systems to monitor and block threats, and they log traffic patterns to help identify unusual behavior.   * 1. Provide a description of the purpose of Authentication, Authorisation and Accounting (AAA) procedures to provide access to network devices   **Authentication:** This is the process of verifying who a user or device is. It typically involves usernames and passwords or other methods like digital certificates. Authentication ensures that only authorized users can access the network.  **Authorization:** After authentication, authorization decides what resources and actions the user or device can access. It sets permissions and roles to control access to specific data, applications, or devices.  **Accounting:** This function tracks user activity on the network by logging access attempts and monitoring resource usage. Accounting is important for auditing and compliance, providing a record of who accessed what and when.   * 1. Provide a description of the operations of firewall inspection rules   Firewall inspection rules decide who gets in and who doesn’t. these rules determine what traffic is allowed to pass through the firewall based on criteria like IP addresses, ports, and protocols. For example, if a rule allows traffic from a certain port, only data matching the criteria will be allowed through while the rest gets blocked. It’s a way to control and secure the flow of data in and out of a network.  <https://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/416/user/guide/CSMUserGuide/fwinsp.pdf>   1. Configure the VLAN interfaces on ASA:    1. For the VLAN 1 interface, configure the addressing to use **192.168.10.1/24**   # interface Vlan1  # nameif inside  # security-level 100  #no ip 192.168.1.1 255.255.255.0  # ip address 192.168.10.1 255.255.255.0       * 1. For the VLAN 2 interface, remove the default DHCP setting and configure the addressing to use **209.165.200.234/29**   # interface Vlan2  # nameif outside  # security-level 0  # no ip address dhcp  # ip address 209.165.200.234 255.255.255.248     1. Configure the hostname, domain name, enable password and console password using the following settings:    * 1. The ASA hostname is **CCNAS-ASA**. > # hostname CCNAS-ASA      2. The domain name is **ccnasecurity.com**. > # domain-name ccnasecurity.com      3. The enable mode password is **ciscoenapa55 >** # enable password ciscoenapa55 2. Create a user and configure AAA to use the local database for remote authentication using the following settings:    * 1. Configure a local user account named admin with the password **adminpa55**. Do not use the encrypted attribute.   # username admin password adminpa55   * + 1. Configure AAA to use the local ASA database for SSH user authentication.   # aaa authentication ssh console LOCAL   * + 1. Allow SSH access from the outside host PC-C with a timeout of **10** minutes.   # ssh 192.168.30.3 255.255.255.255 outside  # ssh timeout 10   1. Configure the ASA as a DHCP server using the following settings:    * 1. Assign IP addresses to inside DHCP clients from 192.168.10.5 to 192.168.10.30.   # dhcpd address 192.168.10.5-192.168.10.30 inside   * + 1. Enable DHCP to listen for DHCP client requests.   # dhcpd enable inside   1. Configure static routing and NAT using the following settings:    * 1. Create a static default route to the next hop router (R1) IP address.   # route outside 0.0.0.0 0.0.0.0 209.165.200.233   * + 1. Create a network object named inside-net and assign attributes to it using the subnet and nat commands.   # object network inside-net  #subnet 192.168.10.0 255.255.255.0   * + 1. Create a dynamic NAT translation to the outside interface   # subnet 192.168.10.0 255.255.255.0  # nat (inside, outside) dynamic interface       1. Conduct configuration of perimeter security and penetration testing:    1. Test a Brute Force Attack while trying to login through Telnet on the perimeter router      * 1. Complete a Denial of Service (DOS) attack (ping-t) to test IPS on the perimeter router      * 1. Test that traffic is encrypted that travels across the VPN between R1 and R3      1. Undertake troubleshooting of peripheral I/O devices including installation and configuration as required.   No troubleshooting required  ***Where***  *This assessment will be completed during classroom time and outside classroom time. The classroom will be a standard lecture or computer lab environment. Students must successfully complete all parts of this assignment to achieve a satisfactory result.*  ***How***  *Students will be assessed against the criteria listed in the marking guide in Section B of this task. To achieve a satisfactory result, students will need to address all criteria satisfactorily.*  **Instructions on submitting students’ Product Assessment**  Students need to submit this assignment through CANVAS with the naming convention of: <Student\_Number>\_<Student\_Full\_Name> \_Project.zip  **Additional Instructions:**   1. Attempt ALL the questions/tasks in this Assignment. 2. Performance requirement: 3. **Satisfactory (S) performance**- met the minimum requirement of all the tasks listed for the Assignment Task. 4. **Not Yet Satisfactory (NYS) performance** - did not meet the minimum requirement of all the tasks listed for the Assignment Task. 5. Students need to achieve satisfactory (S) results in all two (2) assessments to be deemed Competent (CA). | | |
| **Conditions for assessment** | | |
| * You will be observed undertaking this assessment task by a qualified assessor. * You can negotiate a suitable time and location for assessment at least one week prior to the assessment taking place. * You must complete the task within the maximum allowed duration as directed by the assessor. * This is an individual assessment task. You will be assessed individually against all assessment criteria. * You can make arrangements with the assessor at least one week prior to the assessment due date if they require special allowance or allowable adjustment to this task. * Students found in breach of assessment conditions can be charged with academic misconduct, have their results cancelled, be excluded from the program and receive other penalties. Penalties can also apply if a student’s test material is copied by others. * Plagiarism is the presentation of the work, idea or creation of another person as though it is one’s own. It is a form of cheating and is a very serious academic offence that may lead to expulsion from the University. Plagiarised material can be drawn from, and presented in, written, graphic and visual form, including electronic data, and oral presentations. Plagiarism occurs when the origin of the material used is not appropriately cited. * RMIT special consideration is to enable you to maintain your academic progress despite adverse circumstances. The process for special consideration can be found at <http://www.rmit.edu.au/students/specialconsideration> * Students with a disability or long-term medical or mental health condition can apply for adjustments to their study and assessment conditions (Reasonable Adjustments and Equitable Assessment Arrangements) by registering with the Equitable Learning Services (ELS) at <https://www.rmit.edu.au/students/support-and-facilities/student-support/equitable-learning-services>  If you already registered with ELS and your study plan is approved, please inform your teacher if this assessment task is not adjusted in line with approved study plan. * Please ensure your full and correct name is written on the student version of this assessment task (do not use nicknames or abbreviations). * You can appeal the assessment decision according to the [RMIT Assessment Appeal Processes](https://www.rmit.edu.au/content/dam/rmit/documents/about/policy/assessment/assessment-processes.pdf) * You will have the opportunity to resubmit any tools that are deemed unsatisfactory (one resubmission allowed per unit, so that means you have two opportunities to submit) | | |
| **Equipment/resources students must supply:** | | **Equipment/resources to be provided by RMIT or the workplace:** |
| * Pens * Notebook * Laptop (optional) | | * Onsite computers with internet connectivity * Canvas access |

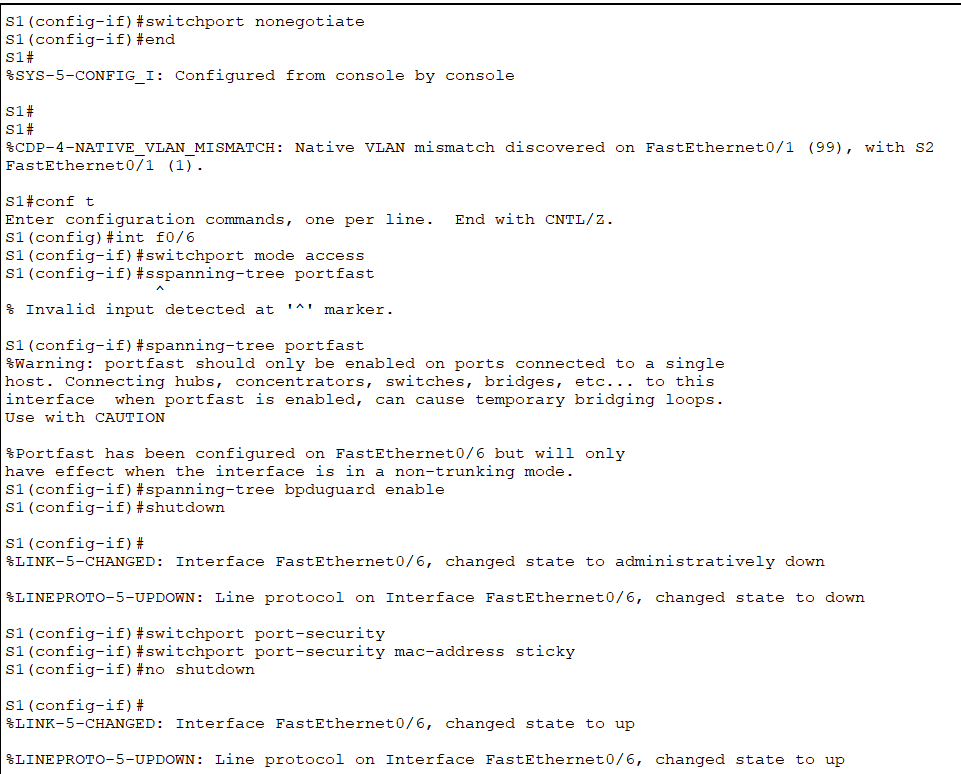


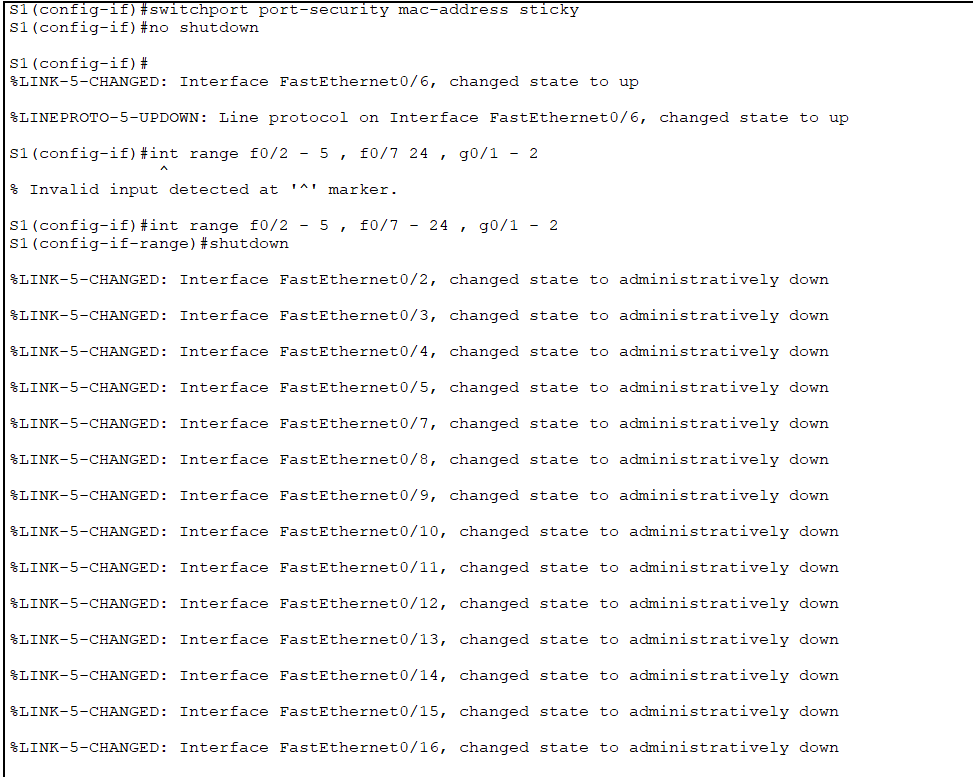


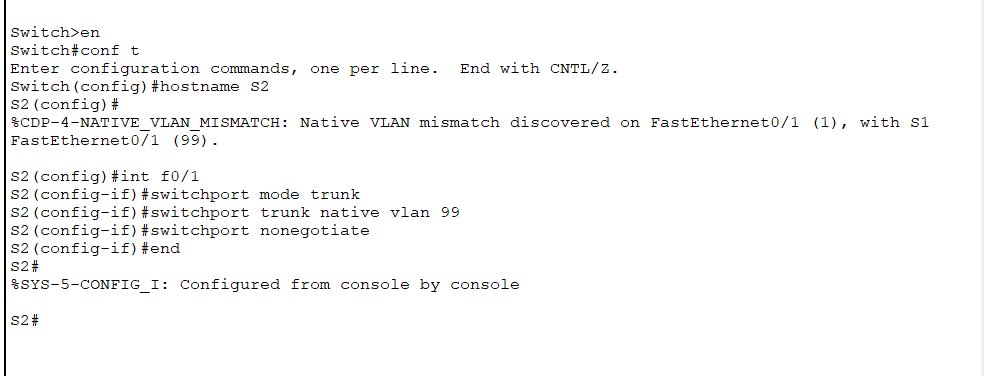


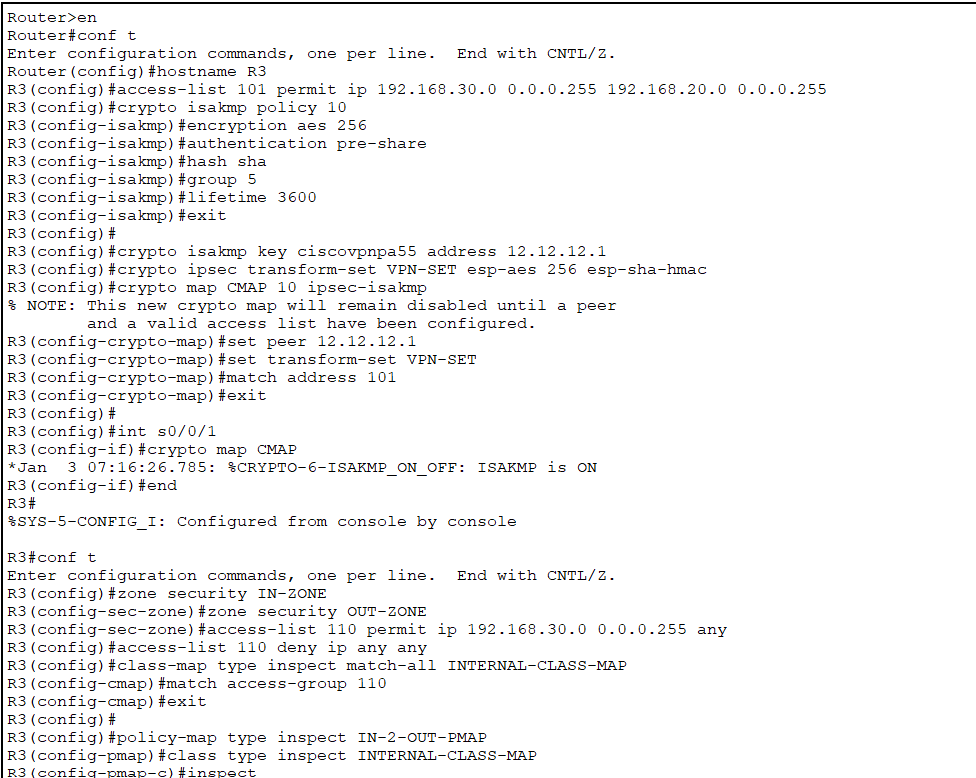


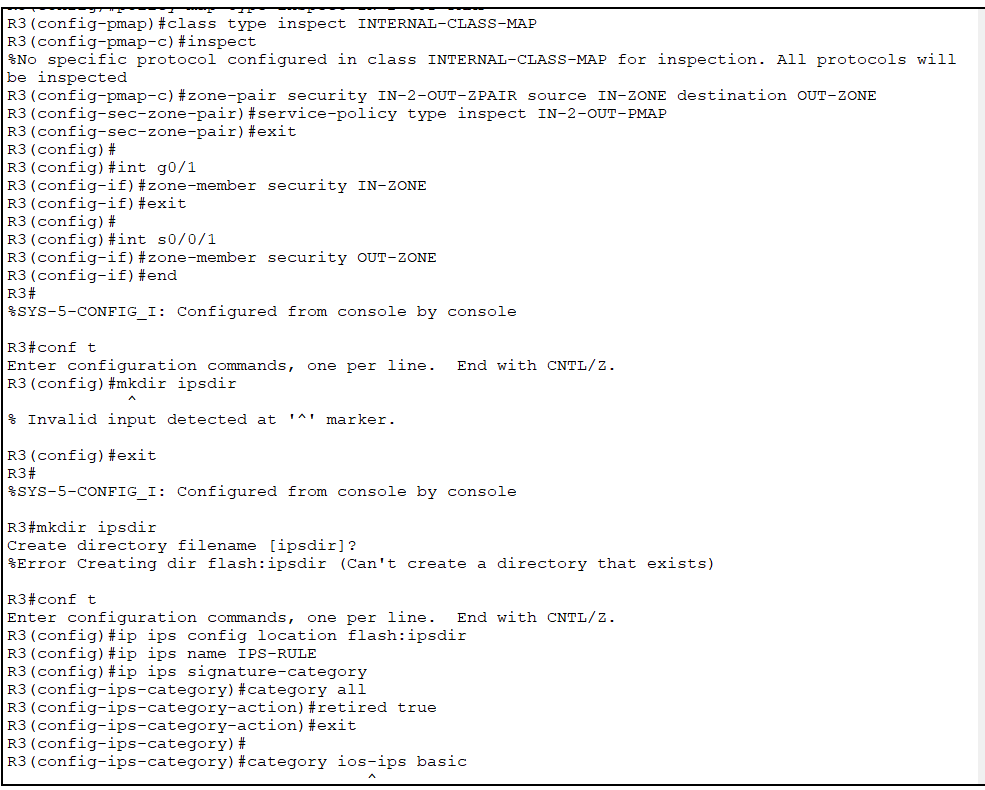


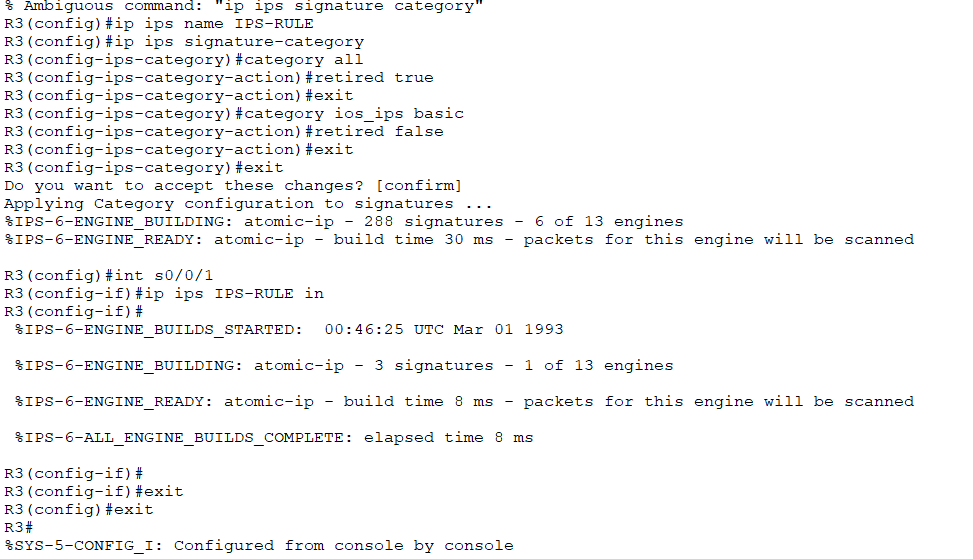


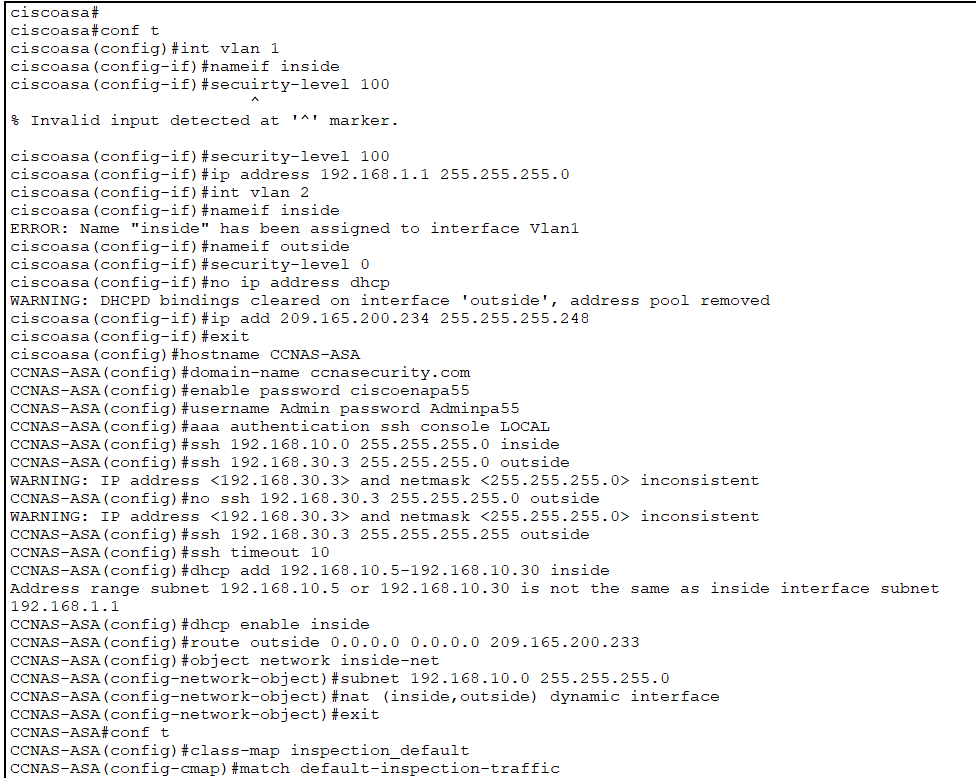


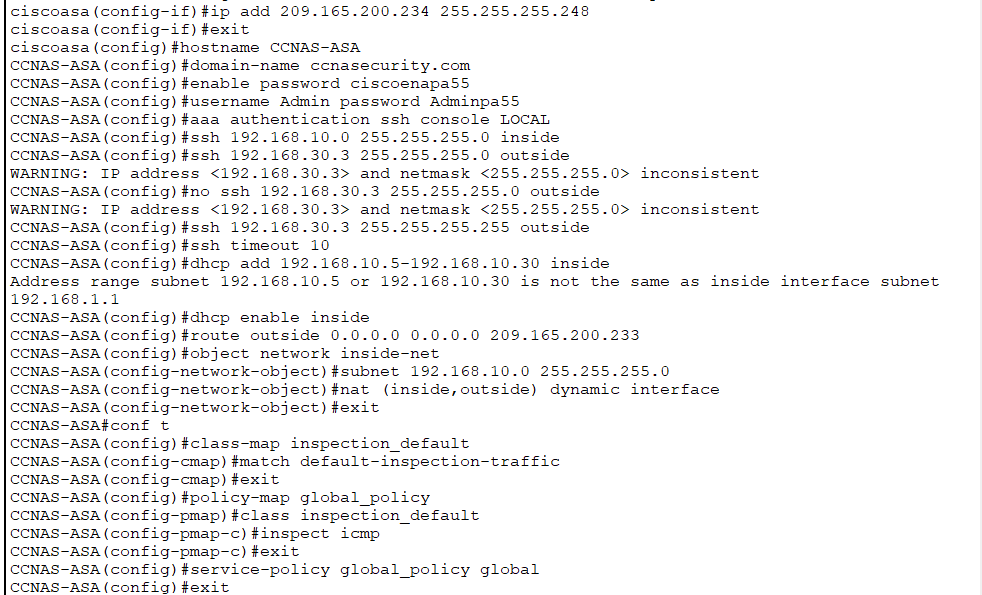












Section B **– Assessment Guide**

|  |  |
| --- | --- |
| **TASK:** | *Students need to complete all the tasks listed below. Students must be deemed satisfactory in all the tasks to successfully complete this assessment.* |

|  |  |  |  |
| --- | --- | --- | --- |
| Key Criteria that must be demonstrated | | | |
| **Criteria for assessment** | **Satisfactory** | | **Marking Guide** |
| **Y** | **N** |
| 1. Evaluation of the security vulnerabilities found in the internetworking system and provision of a proposal for the implementation of advanced security technologies. | ☐ | ☐ |  |
| 1. Building of the internetworking system shown in the topology using CISCO Packet Tracer simulation software with the correct router, switch and ASA as per the specifications | ☐ | ☐ |  |
| 1. Provided description of the process for configuring secure administrative access to the network. | ☐ | ☐ |  |
| 1. Provided a description of the process for allocation of user command privileges for network devices. | ☐ | ☐ |  |
| 1. Configured the routers and switches within the network topology | ☐ | ☐ |  |
| * 1. Configured routers to change the host names, configure the interface IP addresses, and confirue routing using OSPFv2 and Process ID 1 on the routers. | ☐ | ☐ |  |
| * 1. Configured switches to change the host names, configure trunking and configure Vlan IP addresses and default gateway | ☐ | ☐ |  |
| * 1. Tested successfully for ping between routers and Ping between Loopback 1 and PC-C with screenshot provided | ☐ | ☐ |  |
| 1. Undertaken troubleshooting of peripheral I/O devices including installation and configuration as required | ☐ | ☐ |  |
| 1. Configured a Zone-Based Policy Firewall (ZPF) on R3 in accordance with the requirements specified. | ☐ | ☐ |  |
| 1. Configured an Intrusion Prevention System (IPS) on R3 in accordance with the requirements specified. | ☐ | ☐ |  |
| 1. Answered the questions in relation to Virtual Private Network Technologies. |  |  |  |
| * 1. Provided an explanation of the advantages and operation of Virtual Private Networks | ☐ | ☐ |  |
| * 1. Provided a summary of the operations of Internet Protocol Security VPNs | ☐ | ☐ |  |
| * 1. Provided a description of how tunnelling operates in relation to VPNs. | ☐ | ☐ |  |
| 1. Configured the security of R1 for secure connections. | ☐ | ☐ |  |
| * 1. Enabled the Security Technology Package Licence on R1 and provided screenshot as evidence | ☐ | ☐ |  |
| * 1. Configured the access list on R1 to identify interesting traffic and to allow the specified traffic between the network and lan | ☐ | ☐ |  |
| * 1. Configured the cryptographic requirements as specified. | ☐ | ☐ |  |
| 1. Created the transform set VPN-SET using the requirements as specified. | ☐ | ☐ |  |
| 1. Verified that the Security Technology Package Licence is enabled on R3 and repeated site-to-site VPN configurations on R3 to mirror configurations from R1 with screenshot provided as evidence. | ☐ | ☐ |  |
| 1. Tested for successful ping of Lo1 interface on R1 from PC-C and used the **show crypto ipsec sa** command to verify the number of packets is greater than 0 to confirm that the IPsec VPN tunnel is working with a screen shot provided. | ☐ | ☐ |  |
| 1. Undertaken troubleshooting of peripheral I/O devices including installation and configuration as required | ☐ | ☐ |  |
| 1. Answered the questions in relation to firewall technologies | ☐ | ☐ |  |
| * 1. Provide a description of the operation of access lists (ACLS’s) in relation to firewalls | ☐ | ☐ |  |
| * 1. Provide a description of the function and operations of a firewall in the mitigation of network attacks | ☐ | ☐ |  |
| * 1. Provide a description of the purpose of Authentication, Authorisation and Accounting (AAA) procedures to provide access to network devices | ☐ | ☐ |  |
| 1. Configured the VLAN interfaces on ASA following the provided specifications. | ☐ | ☐ |  |
| * 1. Configured the VLAN 1 interface addressing to use **192.168.10.1/24** | ☐ | ☐ |  |
| * 1. Configured the VLAN 2 interface to remove the default DHCP setting and configure the addressing to use **209.165.200.234/29** | ☐ | ☐ |  |
| 1. Configured the hostname, domain name, enabled password and console password following the required specifications. | ☐ | ☐ |  |
| 1. Created a user and configured AAA to use the local database for remote authentication using the required settings. | ☐ | ☐ |  |
| 1. Configured the ASA as a DHCP server using the required settings | ☐ | ☐ |  |
| 1. Configured static routing and NAT using the required settings. | ☐ | ☐ |  |
| 1. Conducted configuration of perimeter security and penetration testing. | ☐ | ☐ |  |
| * 1. Tested a Brute Force Attack while trying to login through Telnet on the perimeter router. | ☐ | ☐ |  |
| * 1. Completed a Denial of Service (DOS) attack using ping-t to test the IPS on the perimeter router. | ☐ | ☐ |  |
| * 1. Tested that the traffic is encrypted that travels across the VPN between R1 and R3. | ☐ | ☐ |  |
| 1. Undertaken troubleshooting of peripheral I/O devices including installation and configuration as required | ☐ | ☐ |  |

Section C – **Feedback to Student**

|  |  |  |  |
| --- | --- | --- | --- |
| **Has the student successfully completed this assessment task?** | | **Yes** | **No** |
|  |  |
| **Feedback to the student** | | | |
|  | | | |
| **Student signature** |  | | |
| **Assessor name and signature** |  | | |
| **Date** |  | | |