**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.   nothing is configured securely for the routers so we will be adding security to all the routers and configuring site to site VPN, Firewall, IPS and AAA authentication   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.   Adding password protection to routers for privileged mode   1. Provide a description of the process for the allocation of user command privileges for network devices.   Enabling secrets will create a password to prevent unauthorized access  **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.       2. Configure interface IP addresses as given in addressing table.       3. Configure Routing using OSPFv2 and Process ID 1 on R1, R2 and R3.    2. Configure the switches to the following settings:       1. Change the hostnames from default to S1, S2 and S3 respectively.       2. Configure trunking between S1 and S2.       3. Configure Vlan1 IP addresses and default gateway as shown in addressing table.    3. Ping between the routers and ping between Loopback 1 and PC-C should be successful. Take a screenshot to confirm that this is successful. 2. Undertake troubleshooting of peripheral I/O devices including installation and configuration as required.       **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.      2. Create an ACL number 110 that defines internal traffic, which permits all IP protocols from the 192.168.30.0/24 source network to any destination.      3. Create a class map named INTERNAL-CLASS-MAP that uses the match-all option and ACL 110.      4. Create a policy map named IN-2-OUT-PMAP that uses the class map INTERNAL-CLASS-MAP to inspect all matched traffic.      5. Create a zone pair named IN-2-OUT-ZPAIR that identifies IN-ZONE as the source zone and OUT-ZONE as the destination zone.      6. Specify that the IN-2-OUT-PMAP policy map is to be used to inspect traffic between the two zones.      7. Assign G0/1 as an IN-ZONE member and S0/0/1 as an OUT-ZONE member. 2. 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.      2. Create an IPS rule named IPS-RULE.      3. Retire the all signature category with the retired true command (all signatures within the signature release).      4. Unretire the IOS\_IPS Basic category with the retired false command.      5. Apply the rule inbound on the S0/0/1 interface.   **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.   VPNS offer elavated security by encrypting traffic and making it difficult for third parties to intercept the data also protecting your privacy as it will hide your IP address and location   * 1. Provide a summary of the operation of Internet Protocol Security (IPSec) VPNs.   IPSec VPNs work by encapsulating your traffic in IP packets those packets are then encrypted using a variety of algorithms. Ipsec VPNs also use authentication protocols to make sure only authorized users can access the VPN   * 1. Provide a description of how tunnelling operates in relation to VPNs   Tunneling is the proccess in which VPN packets reach their intended destination typically a private network. It works by creating a private tunnel between your device and the VPN server, all traffic is routed through this tunnel and encrypted   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.    2. Configure the access list:       1. Create an access list to identify interesting traffic on R1       2. Configure ACL 101 to allow traffic from the R1 Lo1 network to the R3 G0/1 LAN.    3. 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**       2. Encryption: **aes 256**       3. Hash: **sha**       4. Authentication method: **pre-shared**       5. Key exchange: **DH Group 5**       6. IKE SA lifetime: **3600**       7. ISAKMP key: **ciscovpnpa55** 2. 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:    * 1. Transform set: **VPN-SET**      2. Transform encryption: **esp-aes 256**      3. Transform authentication: **esp-sha-hmac**      4. Perfect Forward Secrecy (PFS): **group5**      5. Crypto map name: **CMAP**      6. SA establishment: **ipsec-isakmp**      7. Bind the crypto map (**CMAP**) to the outgoing interface 3. 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. 4. 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      1. Undertake troubleshooting of peripheral I/O devices including installation and configuration as required.   **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   ACLs are a rule that is used to control traffic flow in and out a network they can be used to block traffic based on a variety of factors from the source IP to the destination and the source port or the destination port and protocol   * 1. Provide a description of the function and operations of a firewall in the mitigation of network attacks   Firewalls help mitigate network attacks by blocking malicious traffic, they can block traffic that comes from known attack sources and traffic that is using known attack vendors. They also help by kimit access to resources on the network and firewalls monitor traffic on the network   * 1. Provide a description of the purpose of Authentication, Authorisation and Accounting (AAA) procedures to provide access to network devices   AAA procedures are used to provided secure access to network devices they do this by verifying the identity of the user such as username and passwords then they determine what resources the user has access to finally they track user activity on the network for auditing purposes   * 1. Provide a description of the operations of firewall inspection rules   Firewall inspection rules are used to inspect traffic and determine wheather to allow or block it   1. Configure the VLAN interfaces on ASA:    1. For the VLAN 1 interface, configure the addressing to use **192.168.10.1/24**    2. For the VLAN 2 interface, remove the default DHCP setting and configure the addressing to use **209.165.200.234/29** 2. Configure the hostname, domain name, enable password and console password using the following settings:    * 1. The ASA hostname is **CCNAS-ASA**.      2. The domain name is **ccnasecurity.com**.      3. The enable mode password is **ciscoenapa55** 3. 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.      2. Configure AAA to use the local ASA database for SSH user authentication.      3. Allow SSH access from the outside host PC-C with a timeout of **10** minutes. 4. 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.      2. Enable DHCP to listen for DHCP client requests. 5. Configure static routing and NAT using the following settings:    * 1. Create a static default route to the next hop router (R1) IP address.      2. Create a network object named inside-net and assign attributes to it using the subnet and nat commands.      3. Create a dynamic NAT translation to the outside interface 6. 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.   ***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** |  | | |