|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Introduction  Securing a data centre within a campus network is paramount to safeguarding sensitive information, maintaining operational integrity, and preserving the confidentiality, integrity, and availability of critical data and resources. An effective security strategy for a data centre in a campus network involves a multifaceted approach that encompasses both physical and digital security measures.  Scope:  The project consists of following modules:   1. **VPN:**   A VPN, or Virtual Private Network, is a secure and private connection between your device and the internet. It encrypts your data and hides your IP address, providing anonymity and protecting your online activities from surveillance or data breaches. VPNs are commonly used to access geo-restricted content, enhance online security, and maintain privacy while browsing the internet.  **WORKING OF VPN:**  A VPN works by creating a secure tunnel between your device and a remote server. All your internet traffic is encrypted and routed through this tunnel, making it difficult for anyone to intercept or view your data. This allows you to browse the internet anonymously and access websites or services that may be restricted in your location.  Algorithms**:**  These algorithms are often used in combination to provide a secure and robust encryption scheme in VPNs.  **1.** **AES (Advanced Encryption Standard):** A symmetric encryption algorithm widely used for its strong security and efficiency.  **2.** **RSA (Rivest-Shamir-Adler-man):** An asymmetric encryption algorithm commonly used for key exchange and digital signatures.  **3.** **Diffie-Hellman (DH):** A key exchange algorithm that allows two parties to establish a shared secret key over an unsecured channel.  **4.** **3DES (Triple Data Encryption Standard):** A symmetric encryption algorithm that applies the DES algorithm three times for added security.   1. **Tunnel:**   **There are two main types of tunnels used in VPNs:**  **1. Remote Access VPN:** This type of tunnel is used by individual users to securely connect to a private network over the internet. It enables remote workers or travelers to access resources on a corporate network as if they were physically present in the office. Remote Access VPNs typically use protocols like Point-to-Point Tunnelling Protocol (PPTP), Layer Tunnelling Protocol (L2TP), or Secure Socket Tunnelling Protocol (SSTP).  **2. Site-to-Site VPN:** This type of tunnel is used to connect two or more local networks (LANs) located in different geographical locations. It allows secure communication between these networks over the public internet. Site-to-Site VPNs often use protocols such as Internet Protocol Security (IPsec) or Generic Routing Encapsulation (GRE) to establish and secure the tunnel between the networks.  These types of tunnels serve different purposes but both aim to create secure connections and protect data transmitted over the internet.   1. **KEYS:**   In encryption, there are two main types of keys used:   * **Symmetric Key:** Also known as a secret key, symmetric key encryption uses the same key for both encryption and decryption. The sender and receiver of the encrypted data share this secret key. Common symmetric key algorithms include AES (Advanced Encryption Standard) and 3DES (Triple Data Encryption Standard). * **Asymmetric Key:** Also known as public-key encryption, asymmetric key encryption uses a pair of mathematically related keys: a public key and a private key. The public key is freely distributed, while the private key is kept secret. The sender uses the recipient's public key to encrypt the data, and the recipient uses their private key to decrypt it. Asymmetric key algorithms include RSA (Rivest-Shamir-Adleman) and Elliptic Curve Cryptography (ECC). * Both types of keys play a crucial role in ensuring secure communication and protecting data integrity in encryption processes.  1. **IPSec:**   IPsec, short for Internet Protocol Security, is a widely used protocol suite for securing internet communication at the IP (Internet Protocol) network layer. It provides a framework for authentication, encryption, and integrity of IP packets. IPsec can be implemented in both transport mode (securing individual connections) and tunnel mode (securing entire networks). It offers protection against unauthorized access, eavesdropping, and tampering, making it suitable for VPNs, site-to-site connections,    and securing remote access. IPsec operates at the network layer, ensuring end-to-end security for IP-based communication.   1. **Crypto Map Command:**   The "crypto map" command is used in Cisco IOS (Internetwork Operating System) to define a crypto map entry, which is a set of parameters that define the IPsec policy for a VPN (Virtual Private Network) connection. The command is typically used in the context of configuring IPsec on Cisco routers or security appliances.  Here is a general outline of the "crypto map" command and its function:   * **Define the crypto map entry:** The command begins with the "crypto map" keyword followed by a unique map name or sequence number to identify the crypto map entry. * **Specify the match criteria:** The "match address" parameter is used to define the traffic that will be protected by the crypto map. It can be an access control list (ACL) or a specific traffic selector. * **Configure the IPsec transform set:** The "set transform-set" parameter is used to specify the encryption and authentication algorithms to be used for the IPsec tunnel. It references a preconfigured transform set that defines the security protocols, such as encryption algorithm, authentication method, and Diffie-Hellman group. * **Apply the crypto map to an interface:** Finally, the crypto map is applied to a specific interface using the "interface" command followed by the "crypto map" map-name command. This associates the defined crypto map with the selected interface to protect the traffic specified in the match criteria. * By configuring the crypto map with appropriate parameters, you can establish secure IPsec tunnels for VPN connections, site-to-site communication, or remote access on Cisco networking devices.  1. **ISAKMP Command:**   The "ISAKMP" command is used in Cisco IOS (Internetwork Operating System) to configure the ISAKMP (Internet Security Association and Key Management Protocol) parameters for IPsec VPN (Virtual Private Network) connections. ISAKMP is responsible for negotiating and establishing the security associations used in IPsec.  Here is a general outline of the "ISAKMP" command and its function:   * **Enable ISAKMP:** The command "crypto ISAKMP enable" globally enables the ISAKMP functionality on the Cisco device. * **Configure ISAKMP policies:** ISAKMP policies define the acceptable security parameters and negotiation settings for the IPsec VPN. The command "crypto ISAKMP policy" followed by a sequence number is used to create an ISAKMP policy. Within the policy, you can specify parameters such as encryption algorithms, authentication methods, Diffie-Hellman group, lifetime, and more. * **Define pre-shared keys or certificates:** To authenticate the IPsec peers, you need to configure either pre-shared keys or digital certificates. Pre-shared keys are shared secret keys that must match on both   ends of the IPsec tunnel. The command "crypto ISAKMP key" is used to configure a pre-shared key.  Alternatively, you can use certificates for authentication by configuring the necessary certificate-  related commands.   * **Specify the ISAKMP profile:** The "crypto ISAKMP profile" command is used to create an ISAKMP profile that associates the previously defined ISAKMP policies and authentication methods. The profile is then applied to specific interfaces using the "set ISAKMP-profile" command under the interface configuration. * By using the "ISAKMP" command and its related subcommands, you can configure the necessary parameters to enable and customize the ISAKMP functionality for IPsec VPNs on Cisco devices.         Requirement Specification  Hardware Requirement   |  |  |  |  | | --- | --- | --- | --- | | Sl. No. | Device | Component Name | Quantity | | 1 | Cisco Router | 1. 2911 series 2. 2811 series | 08 | | 2 | Switch | 2960 | 05 | | 3 | Server | Server | 04 | | 4 | Access Point | Access-Point | 08 | | 5 | Laptop | Laptop | 08 |   Security Requirement  This security requirement is the combination of design and security policies. A security requirement is a statement of needed security functionality that ensures one of many different security properties of software is being satisfied. Security requirements are derived from industry standards, applicable laws, and a history of past vulnerabilities.    Architectural Design  Building design  BUILDING – 1  FLOOR - 4 Project Team 1   |  |  |  |  | | --- | --- | --- | --- | | Host | IP Address | Server | Access Policy  (Server) | | Member 1 | 10.0.0.2 | Server 1 | Through VPN | | Member 2 | 10.0.0.3 | Server 1 | Through VPN |   FLOOR - 3 Project Team 2   |  |  |  |  | | --- | --- | --- | --- | | Host | IP Address | Server | Access Policy  (Server) | | Member 1 | 20.0.0.2 | Server 2 | Through VPN | | Member 2 | 20.0.0.3 | Server 2 | Through VPN |     FLOOR - 2 Project Team 3   |  |  |  |  | | --- | --- | --- | --- | | Host | IP Address | Server | Access Policy  (Server) | | Member 1 | 30.0.0.2 | Server 3 | Through VPN | | Member 2 | 30.0.0.3 | Server 3 | Through VPN |   FLOOR - 1 Project Team 4   |  |  |  |  | | --- | --- | --- | --- | | Host | IP Address | Server | Access Policy  (Server) | | Member 1 | 40.0.0.2 | Server 4 | Through VPN | | Member 2 | 40.0.0.3 | Server 4 | Through VPN |   Data Centre  Data Centre-1   |  |  |  | | --- | --- | --- | | Host | IP Address | VLAN | | Team1 Server | 100.0.0.2 | V2 | | Team2 Server | 110.0.0.2 | V3 | | Team3 Server | 120.0.0.2 | V4 | | Team4 Server | 121.0.0.2 | V5 |   ISP-Router    ISPR1   |  |  |  | | --- | --- | --- | | Host | IP Address | VLAN | | ISPR1 | 81.0.0.1 | S0/3/1 | |  | 90.0.0.1 | G0/0 |   ISPR2   |  |  |  | | --- | --- | --- | | Host | IP Address | VLAN | | ISPR2 | 122.0.0.1 | S0/3/0 | |  | 90.0.0.2 | G0/0 |   Complete Architectural    **Configuration:-** **Building- 01**  **Router-B1F4R1**  >en  #config t  #hostname ProjectTeam1  #int g0/0  #ip address 10.0.0.1 255.0.0.0  #no shut  #int g0/1  #ip address 50.0.0.1 255.0.0.0  #no shut  #exit  #router rip  #network 10.0.0.0  #network 50.0.0.0  #exit  **Router-B1F3R2**  >en  #config t  #hostname ProjectTeam2  #int g0/0  #ip address 20.0.0.1 255.0.0.0  #no shut  #int g0/1  #ip address 50.0.0.2 255.0.0.0  #no shut  #int g0/2  #ip address 60.0.0.1 255.0.0.0  #no shut  #exit  #router rip  #network 20.0.0.0  #network 50.0.0.0  #network 60.0.0.0  #exit  **Router-B1F2R3**  >en  #config t  #hostname ProjectTeam3  #int g0/0  #ip address 30.0.0.1 255.0.0.0  #no shut  #int g0/1  #ip address 60.0.0.2 255.0.0.0  #no shut  #int g0/2  #ip address 70.0.0.1 255.0.0.0  #no shut  #exit  #router rip  #network 30.0.0.0  #network 60.0.0.0  #network 70.0.0.0  #exit  **Router-B1F1R4**  >en  #config t  #hostname ProjectTeam4  #int g0/0  #ip address 40.0.0.1 255.0.0.0  #no shut  #int g0/1  #ip address 70.0.0.2 255.0.0.0  #no shut  #int s0/3/0  #ip address 80.0.0.1 255.0.0.0  #no shut  #exit  #router rip  #network 40.0.0.0  #network 70.0.0.0  #network 80.0.0.0  #exit  **Router- VPNR1**  >en  #config t  #hostname VPNR1  #int s0/3/0  #ip address 81.0.0.2 255.0.0.0  #no shut  #int s0/3/1  #ip address 80.0.0.2 255.0.0.0  #no shut  #exit  #router rip  #network 81.0.0.0  #network 80.0.0.0  #exit  #crypto isakmp policy 10  #encr aes 256  #hash md5  #group 5  #lifetime 86400  #authentication pre-share  #exit  #crypto isakmp key 123 address 122.0.0.2  #access-list 100 permit icmp 81.0.0.0 0.255.255.255 122.0.0.0 0.255.255.255  #crypto ipsec transform-set ts esp-aes 256 esp-md5-hmac  #crypto map mymap 10 ipsec-isakmp  #set peer 122.0.0.2  #set transform-set ts  #set pfs group5  #match address 100  #exit  #int s0/3/0  #crypto map map |
| **Configuration:-** **Data Centre**  **Router-DCR1**  >en  #config t  #hostname DCR1  #int f0/0  #no ip address  #no shut  #int f0/0.2  #encapsulation dot1q 2  #ip address 100.0.0.1 255.0.0.0  #no shut  #int f0/0.3  #encapsulation dot1q 3  #ip address 110.0.0.1 255.0.0.0  #no shut  #int f0/0.4  #encapsulation dot1q 4  #ip address 120.0.0.1 255.0.0.0  #no shut  #int f0/0.5  #encapsulation dot1q 5  #ip address 121.0.0.1 255.0.0.0  #int s0/3/1  #ip address 122.0.0.2 255.0.0.0  #no shut  #exit  #router rip  #network 100.0.0.0  #network 110.0.0.0  #network 120.0.0.0  #network 121.0.0.0  #network 122.0.0.0  #exit  #crypto isakmp policy 10  #encr aes 256  #hash md5  #group 5  #lifetime 86400  #authentication pre-share  #exit  #crypto isakmp key 123 address 81.0.0.2  #access-list 100 permit icmp 122.0.0.0 0.255.255.255 122.0.0.0 0.255.255.255  #crypto ipsec transform-set ts esp-aes 256 esp-md5-hmac  #crypto map mymap 10 ipsec-isakmp  #set peer 81.0.0.2  #set transform-set ts  #set pfs group5  #match address 100  #exit  #int s0/3/1  #crypto map mymap  **Switch-DCS1**  >en  #config t  #hostname DCS1  #vtp domain abc  #vlan 2  #name Team1 Server  #vlan 3  #name Team2 Server  #vlan 4  #name Team3 Server  #vlan 5  #name Team4 Server  #exit  #int f0/2  #switchport mode access  #switchport access vlan 2  #int f0/3  #switchport mode access  #switchport access vlan 3  #int f0/4  #switchport mode access  #switchport access vlan 4  #int f0/5  #switchport mode access  #switchport access vlan 5  #int f0/1  #switchport mode trunk |
| **Configuration:-** **ISP**  **Router-ISPR1**  >en  #config t  #hostname ISPR1  #int g0/0  #ip address 90.0.0.1 255.0.0.0  #no shut  #int S0/3/1  #ip address 81.0.0.1 255.0.0.0  #no shut  #exit  #router rip  #network 81.0.0.0  #network 90.0.0.0  #exit  **Router-ISPR2**  >en  #config t  #hostname ISPR2  #int g0/0  #ip address 90.0.0.2 255.0.0.0  #no shut  #int S0/3/0  #ip address 122.0.0.1 255.0.0.0  #no shut  #exit  #router rip  #network 90.0.0.0  #network 122.0.0.0  #exit  Access Point Configuration  Building 1  Floor 4- Project Team 1  Floor 3- Project Team 2  Floor 2- Project Team 3  +  Floor 1- Project Team 4  Testing and Validation  Building 1- Project Team 4 to Team1 Server    VPNR1 to DC    VPNR1 to DC-IPSec Ping  Conclusion  • The implementation of network design and ACLs has significantly improved network connectivity and security by mitigating vulnerabilities and enforcing access controls within the organization's network infrastructure. The project's findings and recommendations provide a excellent connectivity between networks and distribution of networks for different departments for ongoing security enhancements, ensuring the floor design, network design and security policies.  • Implementation of Security Measures: The project implemented a range of security measure access control mechanisms. These measures provided layers of defence to safeguard the network against unauthorized access, data breaches, and malicious activities.  • Continuous Monitoring and Improvement: The project established a framework for continuous monitoring and improvement, including regular security assessments, vulnerability scanning, and patch management. This proactive approach ensures that the network security remains up to date and effective against emerging threats. |