|  |
| --- |
| Introduction:  In this project, the data movement between two campus (location 1 and location 2) which are protected by firewalls, are secured using Industry standard data encryption policy with IPSec VPN Tunnel. The tunnels are originated from and terminated at the outside interfaces (internet facing interfaces) of the Firewalls. The ASA firewalls are configured with static and default routing along with necessary NAT process. ISP connections are provided to both the locations at layer 3.  Cisco Adaptive Security Appliance (ASA) is a versatile network security device that combines several functions such as firewall, VPN concentrator, and intrusion prevention. Here's a detailed explanation of its working principle:  Scope Of the Project :  Overview:  **1. Firewall Functions**  The Cisco ASA primarily functions as a stateful firewall, which means it monitors the state of active connections and makes decisions based on the context of the traffic.  Packet Filtering:   * Stateless Filtering: This is based on static rules that inspect each packet in isolation. * Stateful Filtering: ASA maintains a state table to track the state of active sessions. It inspects packets based on connection state and allows or denies packets based on the context. * Access Control Lists (ACLs): Used to permit or deny traffic based on source/destination IP addresses, ports, and protocols. * Security Levels: Interfaces are assigned security levels (0 to 100). Higher security levels are considered more trusted, and traffic flow is controlled between interfaces based on these levels.   **2. Network Address Translation (NAT)**  ASA provides NAT capabilities to modify IP addresses in packet headers for various purposes:   * Static NAT: Maps a specific internal IP address to a specific external IP address. * Dynamic NAT: Maps an internal IP address to an external IP address from a pool of available addresses. * Port Address Translation (PAT): Multiple internal IP addresses are mapped to a single external IP address, using different ports to differentiate sessions.   **3. Virtual Private Network (VPN)**  ASA supports various types of VPNs to provide secure communication over untrusted networks:   * Site-to-Site VPN: Connects two or more fixed sites securely over the internet * IPsec VPN: Provides confidentiality, integrity, and authentication for data between sites. * RemoteAccessVPN: Allows individual users to securely connect to the network. * SSL VPN: Uses Secure Socket Layer (SSL) protocol for secure remote access. * IPsec VPN: Also supports remote access for individual users.   **4**. **Intrusion Prevention System (IPS)**  ASA includes an IPS to detect and prevent malicious activities:   * Signature-Based Detection: Compares traffic against a database of known attack patterns. * Anomaly-Based Detection: Identifies unusual patterns that may indicate an attack. * Policy-Based Detection: Uses predefined security policies to detect and block attacks.   **5. Content Security and Filtering**  ASA can perform content inspection to protect against various threats:   * URL Filtering: Blocks access to undesirable or malicious websites. * Anti-Malware: Scans traffic for viruses, worms, and other malware. * Email Filtering: Inspects email traffic to prevent spam and phishing attacks.   6. **High Availability and Scalability**  ASA supports features to ensure high availability and scalability:   * Failover: Provides redundancy by having a standby unit that takes over in case the primary unit fails. * Active/Standby Failover: One unit is active, and the other is in standby mode. * Active/Active Failover: Both units are active and share the load. * Clustering: Multiple ASA devices can be clustered to provide load balancing and increased throughput.   **7. Management and Monitoring**  Cisco ASA offers various tools for management and monitoring:   * Command Line Interface (CLI): Provides detailed control over ASA configurations. * Adaptive Security Device Manager (ASDM): A graphical interface for easier management and configuration. * Logging and Reporting: Supports syslog and SNMP for logging events and monitoring performance.   **8. Access Management**  ASA controls access to network resources through:   * Identity-Based Access Control: Integrates with directory services like LDAP and Active Directory to enforce user-based policies. * Multifactor Authentication: Enhances security by requiring multiple forms of verification.   **9. Advanced Threat Protection**  Cisco ASA integrates with other Cisco security solutions for advanced threat protection:  Cisco ASA functions as a comprehensive security solution that combines multiple security technologies into a single device. It provides robust firewall capabilities, secure VPN connections, intrusion prevention, and advanced threat protection, all managed through versatile interfaces and integrated with broader network security infrastructures. Its stateful inspection, NAT capabilities, and high availability features make it a critical component in securing modern networks.  Working of IPSec:  IPSec (Internet Protocol Security) is a suite of protocols designed to secure Internet Protocol (IP) communications by authenticating and encrypting each IP packet in a data stream. Here's a detailed explanation of its working principle:  **1. Components of IPSec**  IPSec consists of several key components that work together to provide security:   * **Protocols**:   + **Authentication Header (AH)**: Provides data integrity, authentication, and anti-replay protection.   + **Encapsulating Security Payload (ESP)**: Provides confidentiality, along with data integrity, authentication, and anti-replay protection. * **Security Associations (SA)**:   + **SA**: A relationship between two or more entities that describes how the entities will use security services to communicate securely.   + **Security Parameter Index (SPI)**: Identifies the SA. * **Key Management**:   + **Internet Key Exchange (IKE)**: A protocol used to negotiate, create, and manage SAs. IKE has two versions: IKEv1 and IKEv2.   **2. Modes of Operation**  IPSec operates in two primary modes:   * **Transport Mode**:   + **Purpose**: Protects the payload of the IP packet.   + **Usage**: Typically used for end-to-end communication between two hosts.   + **How it Works**: The original IP header is retained, and IPSec headers are inserted between the IP header and the transport-layer header (e.g., TCP/UDP). * **Tunnel Mode**:   + **Purpose**: Protects the entire IP packet.   + **Usage**: Commonly used for network-to-network communications (e.g., VPNs).   + **How it Works**: The entire original IP packet is encapsulated within a new IP packet, with IPSec headers applied to the outer IP packet.   **3. IPSec Protocols**  IPSec operates in two Protocols:  **Authentication Header (AH):**   * **Functionality**: Provides data integrity, origin authentication, and anti-replay protection. * **How it Works**:   + AH adds a header to the packet that includes a cryptographic checksum, which ensures the packet has not been altered.   + It authenticates the entire packet, including the IP header, except for mutable fields that can change in transit.   **Encapsulating Security Payload (ESP):**   * **Functionality**: Provides confidentiality (encryption), data integrity, origin authentication, and anti-replay protection. * **How it Works**:   + ESP encrypts the payload of the IP packet.   + It can also provide authentication and integrity for the encrypted data.   + ESP headers and trailers are added to the packet, encapsulating the payload and providing encryption.   **4. Key Exchange and Management**  **Internet Key Exchange (IKE):**   * **Purpose**: Negotiates and establishes SAs between IPSec peers. * **Phases**:   + **Phase 1**: Establishes a secure, authenticated channel called the IKE SA.     - **Main Mode**: Uses six messages to establish the SA with enhanced security.     - **Aggressive Mode**: Uses three messages to establish the SA more quickly but with less security.   + **Phase 2**: Uses the secure channel from Phase 1 to negotiate IPSec SAs for data transmission.     - **Quick Mode**: Exchanges three messages to negotiate the IPSec SAs. * **IKEv2**: An improvement over IKEv1, with enhanced security features and efficiency in establishing SAs.   **5. Security Associations (SAs)**   * **Definition**: A set of policies and keys used to protect communication. * **Function**: Each SA is unidirectional, meaning separate SAs are required for inbound and outbound traffic. * **Components**:   + **SPI**: Identifies the SA.   + **IPsec Protocol**: Specifies whether AH or ESP is used.   + **Encryption and Authentication Algorithms**: Define how data is encrypted and authenticated.   + **Lifetime**: Specifies how long the SA is valid.   **6. Packet Processing in IPSec**  **Inbound Packet Processing:**   * **Decapsulation**: Strips the outer IP header if in Tunnel Mode. * **Decryption**: Decrypts the payload if ESP is used. * **Authentication**: Verifies data integrity and authenticity using AH or ESP. * **Replay Protection**: Ensures the packet is not a duplicate to prevent replay attacks.   **Outbound Packet Processing:**   * **Encapsulation**: Adds a new IP header if in Tunnel Mode. * **Encryption**: Encrypts the payload if ESP is used. * **Authentication**: Adds a cryptographic checksum using AH or ESP. * **Replay Protection**: Adds sequence numbers to packets to enable replay protection.     **7. Applications of IPSec**   * **Virtual Private Networks (VPNs)**: Securing data transmission over untrusted networks. * **End-to-End Security**: Protecting communications between individual devices. * **Network-to-Network Security**: Securing data flow between two networks, such as in   IPSec is a comprehensive suite of protocols designed to secure IP communications by providing confidentiality, integrity, authentication, and anti-replay protection. By leveraging AH, ESP, and IKE for key management, IPSec ensures secure communication across various network configurations and applications, making it a fundamental technology for network security. |
| Requirement Specification  Hardware Requirement   |  |  |  |  | | --- | --- | --- | --- | | Sl. No. | Device | Component Name | Quantity | | 1 | Cisco Router | 2911 series | 03 | | 2 | Switch | 2960 | 02 | | 3 | ASA Device (Firewall) | 5506 series | 02 | | 5 | PC | PC | 04 |   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  Complete Architectural    Location 1   |  |  |  | | --- | --- | --- | | Host | IP Address | Access Policy  (Server) | | Member 1 | 10.0.0.2 | Through VPN | | Member 2 | 10.0.0.3 | Through VPN |   Location 2   |  |  |  | | --- | --- | --- | | Host | IP Address | Access Policy  (Server) | | Member 1 | 60.0.0.2 | Through VPN | | Member 2 | 60.0.0.3 | Through VPN |   **Configuration:-** **Router**  **Router-Location1**  >en  #config t  #hostname Location1  #int g0/0  #ip address 10.0.0.1 255.0.0.0  #no shut  #int g0/1  #ip address 20.0.0.1 255.0.0.0  #no shut  #exit  #router rip  #network 10.0.0.0 0.0.0.255 area 0  #network 20.0.0.0 0.0.0.255 area 0  #exit  **Router-Location2**  >en  #config t  #hostname Location2  #int g0/0  #ip address 60.0.0.1 255.0.0.0  #no shut  #int g0/1  #ip address 50.0.0.2 255.0.0.0  #no shut  #exit  #router rip  #network 60.0.0.0 0.0.0.255 area 0  #network 50.0.0.0 0.0.0.255 area 0  #exit |
| **Configuration:-** **ISP**  **Router-ISPR1**  >en  #config t  #hostname ISPR1  #int g0/0  #ip address 30.0.0.2 255.0.0.0  #no shut  #int g0/1  #ip address 40.0.0.1 255.0.0.0  #no shut  #exit  #router ospf 1  #network 30.0.0.0 0.0.0.255 area 0  #network 40.0.0.0 0.0.0.255 area 0  #exit  **Configuration:-** **ASA**  **ASA-ASA1**  >en  #config t  #hostname ASA1  #int g1/1  #nameif inside  #security-level 100  #ip address 20.0.0.2 255.0.0.0  #int g1/2  #nameif outside  #security-level 0  #ip address 30.0.0.1 255.0.0.0  2.#object network mynetwork  #Subnet 10.0.0.0 255.0.0.0  #Nat (inside, outside) dynamic interface  3.#route outside 0.0.0.0 0.0.0.0 30.0.0.2  4.#access-list hq extended permit icmp any any  #access-list hq extended permit tcp any any eq www  #access-list hq extended permit tcp any any eq 443  #access-list ho-bo extended permit ip 10.0.0.0 255.0.0.0 60.0.0.0 255.0.0.0  #access-group hq in interface outside  5.# crypto ipsec ikev1 transform-set a1>a2 esp-3des esp-sha-hmac  #crypto map mymap 10 match address ho-bo  #crypto map mymap 10 set peer 40.0.0.2  #crypto map mymap 10 set ikev1 transform-set a1>a2  #crypto ikev1 enable outside  #crypto ikev1 policy 10  #encr 3des  #authentication pre-share  #group 2  # tunnel-group 40.0.0.2 type ipsec-l2l  #tunnel-group 40.0.0.2 ipsec-attributes  #ikev1 pre-shared-key cisco  6.#router ospf 1  #router-id 1.1.1.1  #network 20.0.0.0 255.0.0.0 area 0  #network 30.0.0.0 255.0.0.0 area 0  **ASA-ASA2**  >en  #config t  #hostname ASA2  #int g1/1  #nameif inside  #security-level 100  #ip address 50.0.0.1 255.0.0.0  #int g1/2  #nameif outside  #security-level 0  #ip address 40.0.0.2 255.0.0.0  2.#object network mynetwork1  #Subnet 60.0.0.0 255.0.0.0  #Nat (inside, outside) dynamic interface  3.#route outside 0.0.0.0 0.0.0.0 40.0.0.1  4.#access-list hq1 extended permit icmp any any  #access-list hq1 extended permit tcp any any eq www  #access-list hq1 extended permit tcp any any eq 443  #access-list ho-bo extended permit ip 60.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0  #access-group hq1 in interface outside  5.# crypto ipsec ikev1 transform-set a1>a2 esp-3des esp-sha-hmac  #crypto map mymap 10 match address ho-bo  #crypto map mymap 10 set peer 30.0.0.1  #crypto map mymap 10 set ikev1 transform-set a1>a2  #crypto ikev1 enable outside  #crypto ikev1 policy 10  #encr 3des  #authentication pre-share  #group 2  # tunnel-group 30.0.0.1 type ipsec-l2l  #tunnel-group 30.0.0.1 ipsec-attributes  #ikev1 pre-shared-key cisco  6.#router ospf 1  #router-id 2.2.2.2  #network 40.0.0.0 255.0.0.0 area 0  #network 50.0.0.0 255.0.0.0 area 0  Testing and Validation  Location 1 Users to Location 2 Users    Location 2 Users to Location 1 Users    ASA1 - IPSEC Configuration    ASA2 - IPSEC Configuration    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. |