IPsec Advanced

Definition

- Provides security services at the IP layer
- A framework of services
- Adds security to the upperlayers in the OSI model By Implementing a new set of headers
- Utilizes Security Associations (SA)
  - A router to router IPsec VPN will use two SA's (One in each direction)

Two Frame Formats

Authentication Header

- Both change the datagram
  - Authentication Header AH
  - Encapsulating Security Payload ESP
- Works with NAT

Encapsulating Security Payload

- ESP
- IP Protocol 50
- Provides
  - Confidentiality Encryption
  - Integrity
  - Origin Authentication
- Supports
  - Tunnel Mode
    - Original datagram is placed in the encrypted ESP payload
    - Uses encrypted ESP headers
      - Cannot detect tampering whilst delivered
      - Although payload is fully secure
  - Transport Mode
    - Keeps the existing IP header and encrypts the original payload
    - Only authenticates the ESP header and payload
      - Cannot detect tampering whilst delivered
      - Although payload is fully secure

Two Protection Modes

Transport Mode

- Protects the payload of the original IP datagram
- Used for end to end sessions
- Cannot be used When NAT is required

Tunnel Mode

- Protects entire datagram
- Places whole datagram in a new datagram
- Used for network to network connections
- Works with NAT

Key Exchange

- In IPsec, Key Exchange is provided by the Internet Key Exchange IKE
- IKE provides scalability for exchanging keys between IPsec
- IKE is synonymous with ISAKMP (Internet Security Association and Key Management Protocol)

IKE has two phases

IKE Phase One

- No security is currently in place
- Master secret is exchanged to authenticate the peers
- IKE Phase One sets the secure channel for the data encryption key exchange which is done in IKE Phase two
  - IKE Phase One negotiates IKE SAs
- IKE SA parameters are agreed at Phase One
  - Hash
  - Authentication
- Two Modes
  - Aggressive Mode
    - Eliminates several Phase One steps
    - Faster but less secure Three way packet exchange
    - Typically used in Remote Access VPNs
  - Main Mode
    - Slower but more secure Six way packet exchange Cisco devices use main mode
    - Can respond to peers that use aggressive mode uses
- Diffie-Hellman (DH) to create the secure channel

IKE Phase Two

- IKE negotiates the IPsec SAs and generates the required key material for IPsec
- Transform set and all other IPsec parameters are agreed at Phase Two
- One Mode
  - Quick Mode
    - Reinitiates to refresh the SA
- Perfect Forward Secrecy (PFS)
  - If enabled, occurs at IKE Phase Two
  - Carries out a new DH exchange witheach Quick Mode

Configuration

Step 1 enable

- IKE Phase One
- Enable ISAKMP Router
  - (config)#crypto isakmp enable
- ISAKMP is enabled by default

Step 2 policy

- Define the ISAKMP policy
- Parameters that are used during ISAKMP negotiation
  - Authentication
    - Pre-Share
      - Have to set a pre-shared key
      - Router(config)#crypto isakmp key cisco123 address 1.1.1.1
      - Would set the key cisco123 for the peer 1.1.1.1
    - RSA-Encr
    - RSA-Sig
  - Encryption
    - 3DES
    - DES
    - AES
      - 128-bit
      - 1932-bit
      - 256-bit
  - Hash
    - MD5
    - SHA
  - DH Group (key exchange)
    - 1
    - 2
    - 5
  - SA Lifetime
    - 60-86400 Seconds
- Defaults
  - Encryption
    - DES 56-bit
  - Hash
    - SHA
  - Authentication
    - RSA-Sig
  - DH Group
    - 1
    - 768-bit
  - SA Lifetime
    - 86400 Seconds (One Day)

Step 3 identity

- Configure the ISAKMP Identity method
  - Router(config)#crypto isakmp identity {address | hostname}
- Options
  - IP Address
  - Hostname
- Default
  - IP Address

Step 4 transform sets

- IKE Phase Two
- Define IPsec Transform Sets
  - Router(config)#crypto ipsec transform-set myset esp-des esp-md5-hmac
  - This would create a transform set called myset
  - using ESP and DES for Encryption
  - using ESP and MD5 for Authentication
- You are then in crypto transformconfiguration mode
- Further configuration
  - Router(cfg-crypto-trans)#mode {transport | tunnel}
  - Sets the mode to either Transport or Tunnel
  - Default is Tunnel

Step 5 ACL

- Define Crypto ACL
- Crypto ACL is the ACL that specifies the traffic to be sent over the VPN
- Example
  - Router(config)#access-list 199 permit ip host 1.1.1.1 host 2.2.2.2
  - Would encrypt traffic with IPsec from host 1.1.1.1 to host 2.2.2.2

Step 6 map

- Define Crypto Maps
  - Router(config)#crypto map mymap 10 ipsec-isakmp
  - Configures a Crypto Map with a sequence number of 10
    - The Crypto Map will use ISAKMP
  - Crypto Map configuration commands
    - description: Description of the Crypto Map
    - dialer: Dialer related commands
    - match: Match crypto ACL
    - reverse-route: Commands for reverse route injection
    - set:
      - peer Identifies the IPsec peer
      - transform-set Identifies which transform set to use
    - pfs: Use PFS or not
    - security-association: Set SA parameters Lifetime
- Crypto maps pull together variousparts used to set up the IPsec SAs
- Types
  - Static
    - All entries are pre-configured
  - Dynamic
    - Entries are configured dynamically as the result of IPsec negotiation
- Apply the Crypto Map
  - Crypto Maps are applied to the interface where thetraffic leaves and enters a router
  - You must apply the crypto map boththe the physical and logical interfacewhen using GRE tunnels