VPNs, Tunneling & GRE

Module Overview

- Virtual Private Network (VPN)
- Tunneling
- Generic Routing Encapsulation (GRE)

VPN Overview

- Virtual Private Network (VPN) serves as a logical connection
  - Its primary function is to provide end-to-end connectivity
    - Usually built over an unsecured network, such as the Internet
- VPNs rely on Tunneling
  - A process of encapsulating the original packet into a new header
  - Relies on three protocols :
    - Carrier, Encapsulating & Passenger
- Not all VPN implementations are secure

VPN Types

- Remote Access
  - Connects a single endpoint to a remote network
    - e.g. Teleworker, mobile device
- Site-to-Site (LAN-LAN or L2L)
  - Connects two or more networks together
  - Often used to build private WANs

Secure VPN Implementations

- IP security (IPsec)
  - Remote Access & Site-to-Site
- Secure Socket Layer (SSL) / Transport Layer Security (TLS)
  - Remote Access
  - Allows to access a network using a browser

Insecure VPN Implementations

- Generic Routing Encapsulation (GRE)
  - Multi-protocol tunneling mechanism defined in RFC 2784
  - Supports multicast traffic

Normal Packet

Tunnel Packet

- DMVPN

GRE Configuration

- GRE tunnel is represented through a tunnel interface
  - **interface tunnel *nr***
    - **tunnel mode gre [ip|ipv6]**
    - **[ip|ipv6] address *ip_addr mask***
    - **tunnel source**
    - **tunnel destination**

- Verification
  - **show interfaces**

IPsec Overview

Module Overview

- Protocol overview
- Phase I
- Phase II
- Rekeying

IP Security (IPsec) Overview

- The most common implementation of VPNs
  - RFC 4301 „Security Architecture for the Internet Protocol”
  - Layer 3

- IPsec Security Services
  - Authentication
  - Data Confidentiality
  - Data Integrity
  - Anti-replay

IPsec Overview

- IPsec consists of multiple protocols & standards
  - Internet Security Association & Key Management Protocol (ISAKMP)
    - A framework describing core IPsec functions for secure communication (RFC 2408)
      - Specifies that keying & authentication should occur
      - Describes the procedures to establish, negotiate, modify & delete tunnel information
  - Internet Key Exchange (IKE) is an implementation of ISAKMP
    - Performs main Control Plane functions, like key exchange, authentication, etc.
    - IKEv1 (RFC 2409) & IKEv2 (RFC 7296)

IPsec Overview

- IPsec heavily relies on Cryptography
  - Control Plane
    - Key Management : DH, ECDH
    - Authentication : PSK, RSA, ECDSA
  - Data Plane
    - Security Protocols : ESP, AH
    - Confidentiality : DES, 3DES, AES, SEAL
    - Data Integrity and Origin Authentication : MD5, SHA-1, SHA-2

- IPsec is a framework of open standards
  - Obsolete technologies can be replaced without changing the framework

IPsec Overview

- IPsec VPNs are negotiated in phases
  - ISAKMP/IKE Phase I
    - Performed in one of two Modes : Main (MM) or Aggressive (AM)
  - ISAKMP/IKE Phase II
    - Quick Mode (QM)
- Both negotiations run over UDP port 500 by default
  - Successful Phase I negotiation results in an IKE Security Association (SA)
  - Successful Phase II negotiation results in two separate IPsec SAs
- SAs are re-negotiated („rekeying”) before their lifetime expires

Phase I

- Phase I negotiation exchanges
  - IKE Policy
  - Diffie-Hellman (DH)
  - Authentication
- Main Mode uses 6 messages/packets for all three exchanges
  - Secures the entire Authentication exchange including IKE Identities
- Aggressive Mode requires only 3 packets to perform Phase I
  - Authentication exchange & IKE Identities go unprotected
  - Useful for Remote Access with key-based authentication (key selection)

Phase I

- IKEv1 Phase I Policy must match between the VPN peers
  - Encryption : DES, 3DES, AES (128, 192, 256)
  - Hash : MD5, SHA-1, SHA-2 (256, 384, 512)
  - Diffie-Hellman Group : 1, 2, 5, 14, 15, 16 or ECDH* 19, 20 and 24
  - Authentication Method : Pre-Shared Key, Digital Certificates (RSA or ECDSA*)
  - Lifetime : does not have to be the same
- DH securely negotiates symmetric keys over an unprotected network
- Authentication with certificates requires PKI
  - If Pre-Shared Key is used, it must be symmetric

Phase II

- Quick Mode negotiation
  - Encryption & Hashing functions (3DES, MD5, etc.)
  - Proxy Identities (traffic to be protected)
    - ACL must be mirror-image
  - Security Protocol (AH or ESP)
  - Encapsulation Mode (Transport or Tunnel)
  - (Optional) Perfect Forward Secrecy (PFS)
    - Enables an additional DH exchange to derive a fresh set of symmetric keys
- All Quick Mode settings must match between the peers

IPsec Rekeying

- IKE & IPsec SAs are periodically re-negotiated
  - The rekeying process takes place right before SA expiration
    - Default IKE SA lifetime is 24 hours (**lifetime**)
    - Default IPsec SA lifetime is 1 hour or 4,608,000 KB (**crypto ipsec security-association lifetime**)
  - There must be an existing Phase I SA to rekey Phase II (data) tunnels
  - Idle SAs don't have to be rekeyed or just maintaned
    - Enable idle timeout with **crypto ipsec security-association idle-time**

IPsec Tunneling

Module Overview

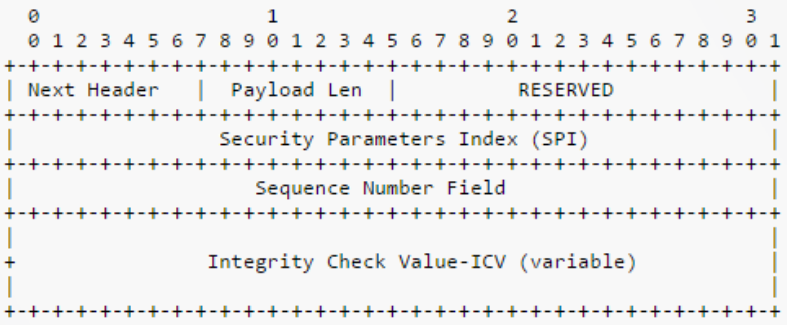
- Encapsulation Modes
- Security Protocols

IPsec Encapsulation Modes

- Tunnel Mode
  - Creates a virtual tunnel (new IP header)
  - Allows to protect traffic between different sites and/or non-IPsec capable devices
- Transport Mode
  - Tunnel-less protection
  - Communicating devices are IPsec endpoints in the same time
    - They must run IPsec software
  - Proxy ACL must include addresses of VPN endpoints themselves
    - A non-IPsec tunnel may be built between the VPN peers to protect other communication

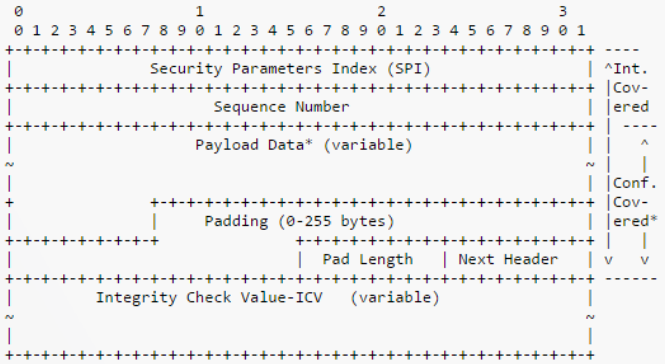
IPsec Security Protocols

- Authentication Header (AH)
  - RFC 4302
  - IP Protocol 51
  - Offers Data Integrity, Authentication and Replay Protection
    - No encryption
  - Protects the entire packet, including the header
- Header structure



IPsec Security Protocols

- Encapsulating Security Payload (ESP)
  - RFC 4303
  - IP Protocol 50
  - Offers Data Integrity, Authentication, Confidentiality and Replay Protection
    - Integrity checks are performed on the ESP header and entire payload
    - Encryption is performed on the entire payload (but not on Transport /ESP headers)
- Header structure



IPsec on the ASA

Module Overview

- Tunnel Group
- Group Policy

Tunnel Group

- ASA mandatory VPN components :
  - Tunnel Group & Group Policy

- Tunnel Group can be thought of as a Connection Profile
  - A virtual interface for terminating & controlling VPN connections
    - Each L2L session corresponds to a single Tunnel Group
    - A single Tunnel Group can handle multiple Remote Access sessions
  - Controls the VPN connection by choosing a Group Policy
    - Few settings can be set directly, such as AAA database or DHCP/DNS
  - Attributes not configured in a custom Tunnel Group will be inherited from the default TG (**show run all tunnel-group**)

Tunnel Group Selection

- Digital Certificates
  - Certificate OU field (other field/fields can be selected with a Certificate Map)
  - IKE Identifier of the VPN peer (IKE_ID)
  - VPN peer's IP address (source IP address from the incoming IKE packets)
  - Pre-configured „DefaultRAGroup" acts as a catch-all
    - Change with **tunnel-group-map default-group**

- Pre-Shared Keys
  - Aggressive Mode : IKE_ID, then VPN peer's IP address
  - Main Mode : VPN peer's IP address
  - If nothing was matched & VPN is L2L the „DefaultL2LGroup" TG will be used

Group Policy

- A container for VPN connection settings & attributes
  - Makes application of the VPN policy easier & more scalable
  - Group Policy settings & attributes
    - Allowed VPN protocol
    - Split Tunneling List & Policy
    - IP address pool, session timeout, ACL filters & more

- VPN attributes can be also defined by other methods (in order) :
  - Dynamic Access Profile (DAP), User Profile, Group Policy, Default Group Policy
  - Any undefined attributes will be inherited from the Default Group Policy
    - **show run all group-policy**

Implementing L2L IPsec VPN IOS - ASA

Module Overview

- Configuration syntax IOS
- Configuration syntax ASA
- Hands-on example

IPsec Configuration - IOS

- Phase I Policy
  - **crypto isakmp policy**
    - **authentication**
    - **encryption**
    - **hash**
    - **group**
    - **lifetime**

- Authentication Credentials
  - **crypto isakmp key**
  - **crypto pki trustpoint** (digital certificates)

IPsec Configuration - IOS

- Phase II Algorithms & Encapsulation Mode
  - **crypto ipsec transform-set**
    - **mode [transport | tunnel]**

- Proxy ACL
  - **access-list**

IPsec Configuration - IOS

- Crypto Map
  - **crypto map ipsec-isakmp**
    - **set peer**
    - **set transform-set**
    - **match address**

- Enable IPsec
  - **interface**
    - **crypto map**

IPsec Configuration - IOS

- Verification
  - **show crypto isakmp sa**
  - **show crypto ipsec sa**
  - **show crypto session [detail]**

IPsec Configuration - ASA

- Phase I & II Settings
  - **crypto ikev1 policy**
  - **access-list**
  - **crypto ipsec ikev1 transform-set**

- Crypto Map
  - **crypto map set peer**
  - **crypto map set ikev1 transform-set**
  - **crypto map match address**
  - **crypto map set trustpoint** (digital certificates)
  - **crypto map interface**
  - **crypto ikev1 enable**

IPsec Configuration - ASA

- Group Policy configuration
  - **group-policy [internal | external]**
  - **group-policy attributes**

- Tunnel Group configuration
  - **tunnel-group type ipsec-l2l**
  - **tunnel-group general-attributes**
    - **default-group-policy**
  - **tunnel-group ipsec-attributes**
    - **ikev1 pre-shared-key**
    - **trust-point** (digital certificates)

IPsec Configuration - ASA

- Verification
  - **show crypto isakmp sa**
  - **show crypto ipsec sa**
  - **show vpn-sessiondb**

IOS Advanced IPsec Solutions

Module Overview

- Design considerations
- GRE & IPsec
- Virtual Tunnel Interfaces

IPsec Design Considerations

- IPsec VPNs for large-scale inter-site connectivity
  - VPN peer detection
    - Static vs Dynamic
  - Dynamic IP address support
  - Routing
  - Administrative overhead
  - Transport overhead
    - Fragmentation issues
      - Pre-fragmentation & MTU tuning

Crypto Maps

- Limitations
  - Manual peer configuration
    - Static IPs
      - Except a dynamic crypto map
  - Multicast traffic is not supported
    - No dynamic routing
  - Large administrative overhead

- Pros
  - Low transport overhead

GRE with Crypto Maps

- Limitations
  - Peers defined manually
    - Static IPs only
  - Large administrative overhead
  - Additional tunneling overhead

- Pros
  - Dynamic Routing
  - One ACL entry per VPN peer
  - GRE tunnel interfaces simplify policy configuration
    - QoS, Filtering, etc.

Configuration Example

int tunnel

[ip | ipv6] address, tunnel source, tunnel destination

router [ospf | eigrp | rip | bgp]

access-list permit gre *tunnel-source tunnel-destination*

crypto map ipsec-isakmp

set peer, set transform-set, match address

interface

crypto map

GRE with IPsec Profile

- IPSec Profile
  - Replaces Crypto Map
  - Routing controls the encryption domain
    - No Proxy ACLs
  - Configured with **crypto ipsec profile**
    - Applied on tunnel interfaces with **tunnel protection ipsec profile**

- Limitations
  - Manual peer configuration
    - No dynamic IPs
  - Additional tunneling overhead

Configuration Example

```
crypto ipsec profile
  set transform-set

int tunnel
  [ip | ipv6] address
  tunnel source
  tunnel destination
  tunnel protection ipsec profile

router [ospf | eigrp | rip | bgp]
```

Virtual Tunnel Interface (VTI)

- Flexible tunneling solution for IP traffic only
  - Static (SVTI) or Dynamic (DVTI)
  - Works with IPsec Profiles
    - No crypto maps or Proxy ACLs
  - Supports multicasts & dynamic routing
  - Enabled with **tunnel mode ipsec [ipv4 | ipv6]**

- Limitations
  - Manual peer configuration
    - No dynamic IPs

SVTI Configuration Example

```
crypto ipsec profile
  set transform-set

int tunnel
  [ip | ipv6] address
  tunnel source
  tunnel destination
  tunnel protection ipsec profile
  tunnel mode ipsec [ipv4 | ipv6]

router [ospf | eigrp | rip | bgp]
```

Dynamic Multipoint VPN

- Scalable & flexible solution for large-scale VPNs
  - Dynamic Spoke-Spoke tunnels
  - Dynamic IPs
  - Dynamic routing
  - Easy to maintain

IPsec & IPv6

Module Overview

- IPv6 IPsec - ASA
- IPv6 IPsec - IOS

IPsec & IPv6 - ASA

- Configuration syntax remains unchanged
  - Use IPv6 addresses instead of IPv4
    - **tunnel-group**
    - **access-list**
    - **crypto map set peer**
- IPv6 Control Plane
  - **ipv6 route**

IPsec & IPv6 - IOS

- Common Elements
  - Phase I Policy & Phase II Transform Set syntax does not change
  - Pre-Shared Key is defined with **crypto iskamp key address ipv6**
  - Configuration refers to IPv6 addresses

- IPv6 Control Plane
  - Static (**ipv6 route**)
  - Dynamic routing
    - RIPng/EIGRPv6/OSPFv3/MBGP

IOS IPv6 Implementation Details

- Crypto Map
  - Proxy ACL must be IPv6 (**ipv6 access-list**)
  - Crypto map needs „**ipv6**” (**crypto map ipv6**)
    - Apply with **ipv6 crypto map**

- GRE
  - Tunnel encapsulation mode defines IPsec transport
    - For IPv6 use **tunnel mode gre ipv6**
  - Tunnel’s IP address determines what can be encapsulated
    - For IPv6 use **ipv6 address**

IOS IPv6 Implementation Details

- VTI
  - IPv6 VTI can only carry IPv6 traffic
    - **tunnel mode ipsec ipv6** & **ipv6 address**

- Verification
  - **show crypto isakmp sa**
  - **show crypto ipsec sa**
  - **show crypto session [detail]**
  - **show interface tunnel *nr***