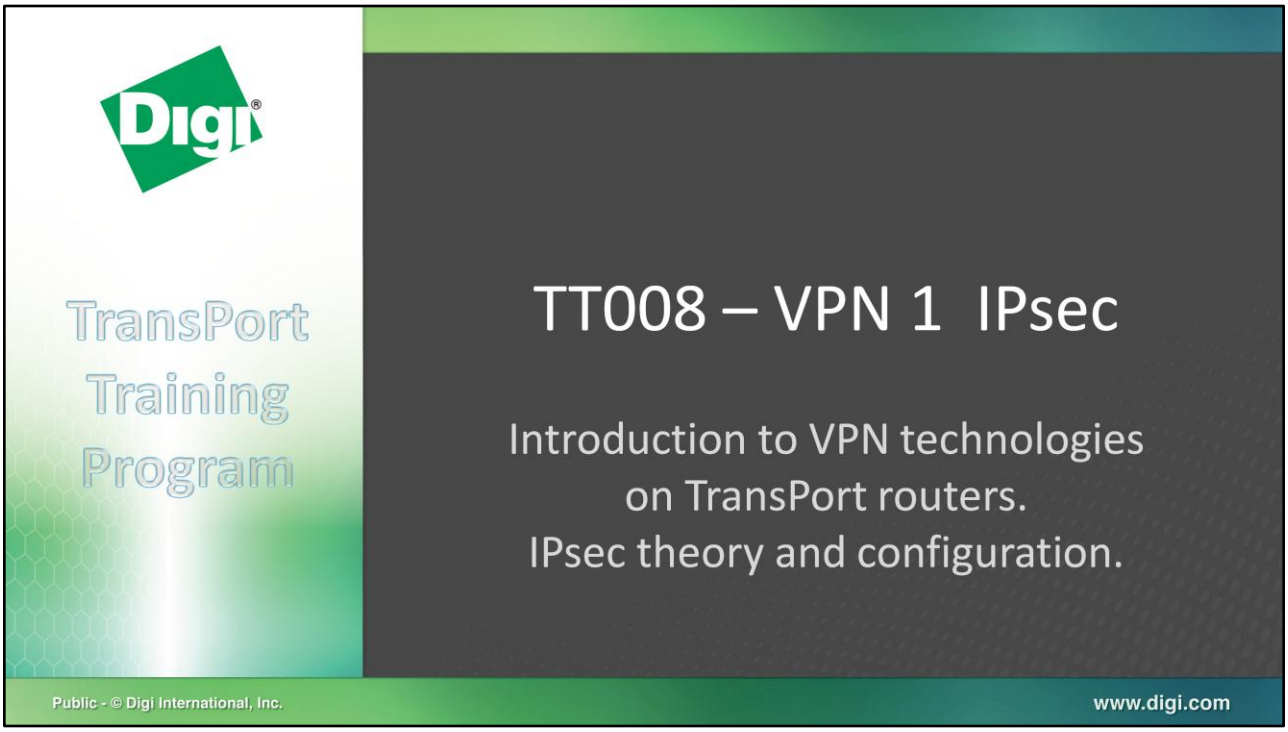

TransPort
Training
Program
TT008 – VPN 1 IPsec
Introduction to VPN technologies
on TransPort routers.
IPsec theory and configuration.
Public - © Digi International, Inc.
www.digi.com

TransPort VPN Technologies

- IPsec
  - Remote Access
  - LAN to LAN
  - Easy VPN
  - DMVPN (Covered in separate module)
- Open VPN
- PPTP
- L2TP (often used with PPP and IPsec)
- GRE (not encrypted – often used with IPsec)

Open VPN has its own module
L2TP is covered later in the this module
GRE is covered in it's own module

Open VPN

- SSL based VPN
- Open Standard
- Not highly scalable in Digi implementation
- Versions 2.1 & 2.2 supported
- Compression not supported in Digi implementation (license required)
- X.509 certificates supported
- Routes injected during negotiation
- Client mode and server mode support in Digi implementation
- Covered in module “TT022 VPN 2 – Open VPN”

PPTP

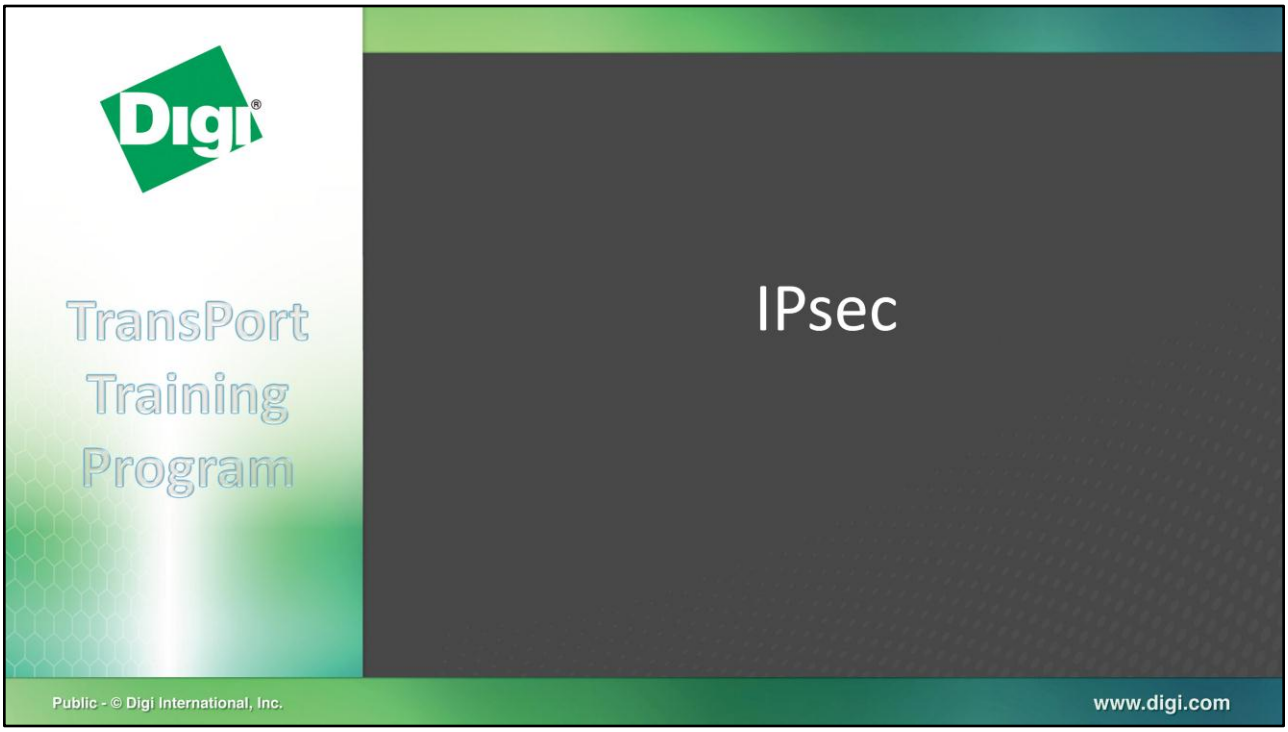
- Point to Point Tunneling Protocol
- Implemented via control session (TCP) + GRE tunnels
  - GRE can be troublesome through firewalls/NAT
- Must be linked to a PPP interface
- Can be encrypted via MPPE (Microsoft Point to Point Encryption) configured on the PPP interface

L2TP

- Layer 2 Tunnelling Protocol
- TCP based (port 1723) so can traverse NAT and Firewalls
- Must be linked to a PPP interface so can only be used for IP in TransPort routers currently.
- Ethernet bridging over L2TP NOT currently supported
- Optionally supports authentication
- Usually used in conjunction with IPsec
- Can be used with MS Windows and the majority of operating systems for Remote Access VPN without the need to install client software.
- Covered later in this module.

GRE

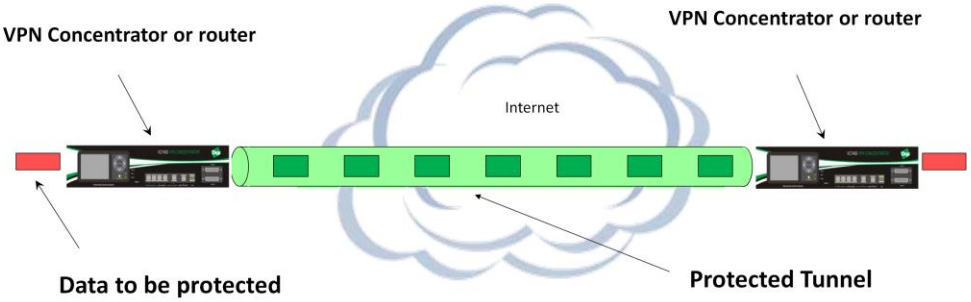
- Generic Routing Encapsulation
- No encryption
- Tunnel key (authentication) optional
- IP Protocol number (47) assigned – not UDP or TCP based
- Because there is no TCP/UDP port number, it can be troublesome through NAT/Firewall if not encapsulated in IPsec.
- Often needed for use with routing protocols for the virtual interfaces it creates (with keep-alives)
- Used with DMVPN – module “TT025 VPN3 – DMVPN”


TransPort
Training
Program
IPsec
Public - © Digi International, Inc.
www.digi.com

Why use IPsec?

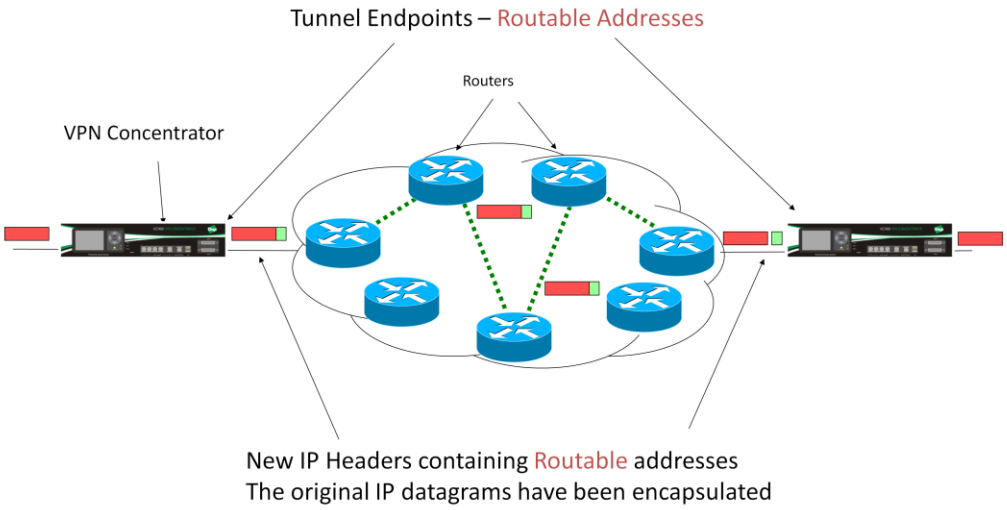
- APNs that provide an IP address that cannot be routed to from the WAN typically require the use of VPN or GRE for most projects. (e.g. 10.x.x.x address)
- Outside of the USA it is very common for mobile operators to assign IP addresses that are not accessible inbound from the Internet.
- The TransPort can build an IPsec tunnel to a host on the Internet with a fixed IP address. The cellular TransPort is usually configured to keep the tunnel active 24/7.
- You can then contact the TransPort (or any devices on its LAN) by routing through this tunnel at any time.
- NAT Traversal (NAT-T) is required for plans with private IP addresses which are NAT'd by the provider, this necessitates that the remote TransPort sends keep-alive data on a regular basis.

Virtual Private Networks



- A VPN is implemented as a tunnel between two end points
- Insecure traffic (red) is encapsulated in IP datagrams (green) and transported over the Internet
- The tunnel authenticates and/or encrypts the traffic to prevent tampering and viewing

The Data Tunnel in practice



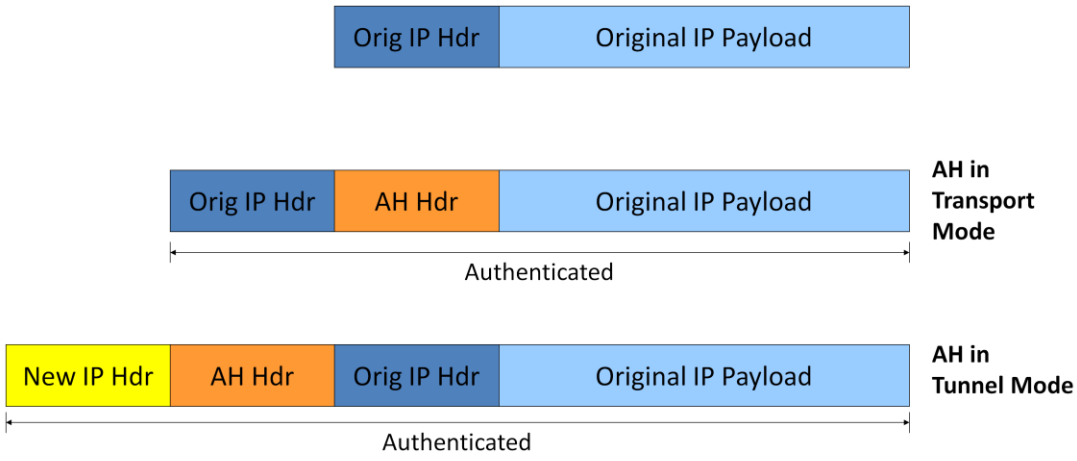
IPsec Features

- IPsec is designed to provide a basic number of features
  - It provides a set of options for
  - Secrecy (encryption)
  - Authentication
  - Integrity
  - Key Exchange
  - Non-Repudiation
  - Anti-Replay

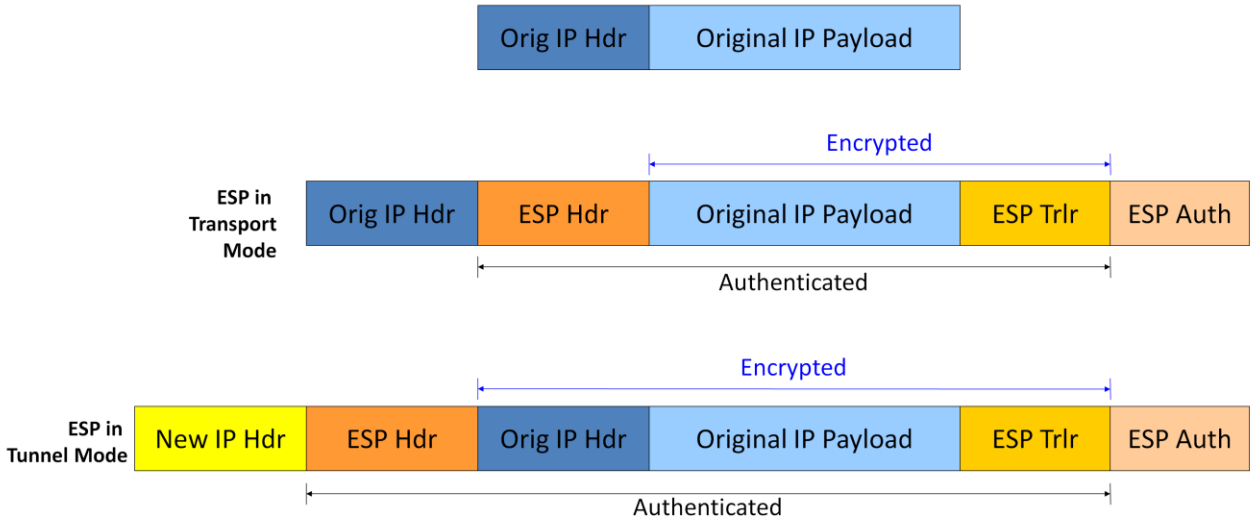
IPsec Basics

- IPsec has two main modes of operation
  - Transport and Tunnel
- IPsec provides authentication and/or encryption
  - AH: Authentication Header
  - ESP: Encrypted Security Payload
- IPsec ESP Tunnel Mode is most widely used
- Authentication can be achieved using
  - Pre-shared Secret (a.k.a. Pre-shared keys or PSK)
  - X.509 Certificates

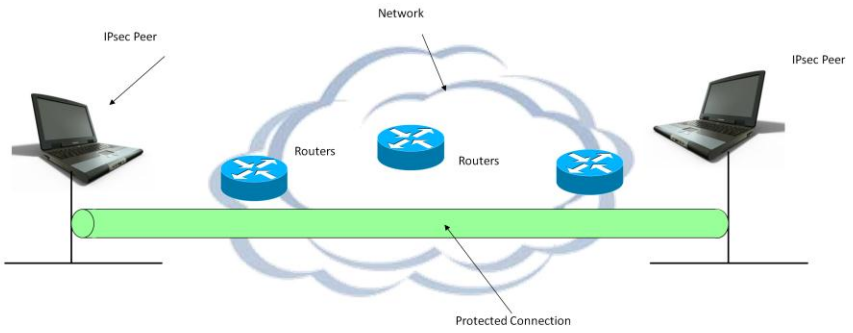
AH: Authenticates Everything



ESP: Authentication and Encryption

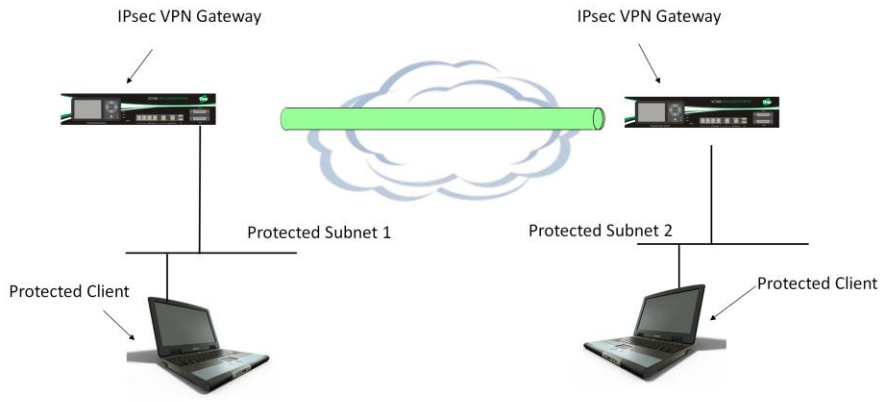


Transport Mode



- End-to-End protection over the network from host to host
- IP Packets are encrypted but IP addresses do not normally change
- Transport mode is rarely used

Tunnel Mode (LAN to LAN topology)



- This is the more usual model for IPsec and provides secure communication between two networks over an insecure network e.g. the Internet
- All traffic is secured

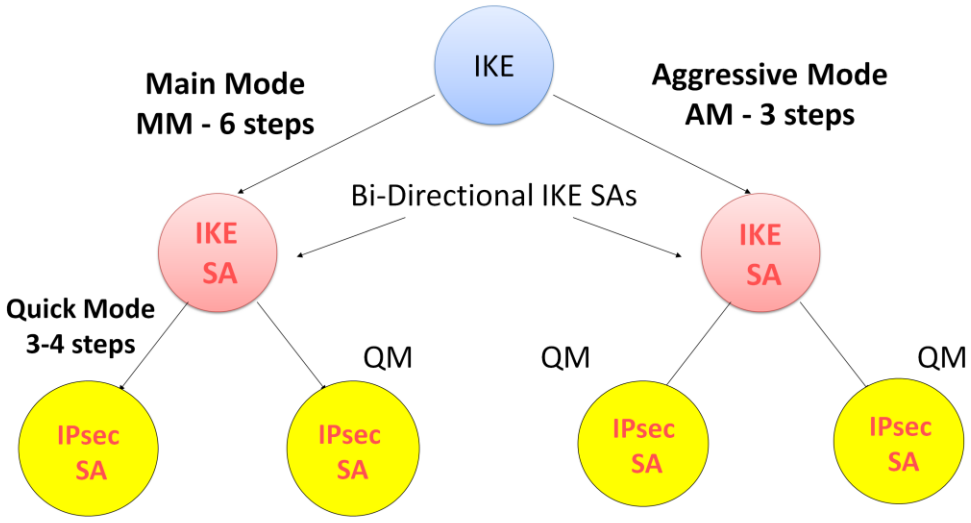
Internet Key Exchange (a)

- The Internet Security Association and Key Management Protocol (ISAKMP) is defined in RFC 2408
- ISAKMP was developed by the NSA and defines the methods by which two peers can communicate and construct messages for Security Associations (SAs) e.g. IPsec
- OAKLEY provides the principle of exchange modes which IKE simplifies
- SKEME provides the principles of authenticated key exchanges using public key encryption and sharing secrets

Internet Key Exchange (b)

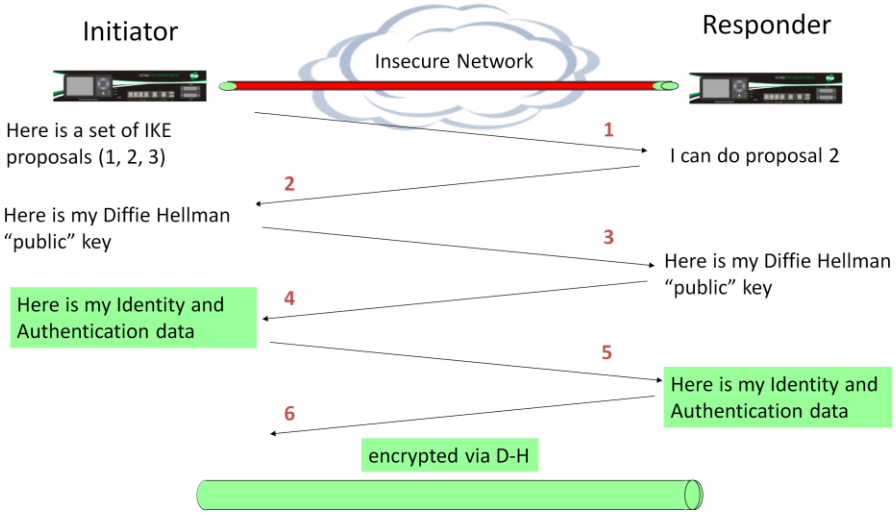
- IKE as defined in RFC 2409 is a subset of ISAKMP and implements parts of 2 key management protocols OAKLEY and SKEME
- The purpose of IKE is to allow two parties to dynamically and securely exchange keying material over an insecure channel
- Keying material is then used for encryption and mutual authentication for IPsec SAs The initial exchange can be authenticated using :
  - Pre-Shared Secrets PSS
  - Raw Public Keys
  - Public Certificates (DSA or RSA)

IKE/IPsec Operations



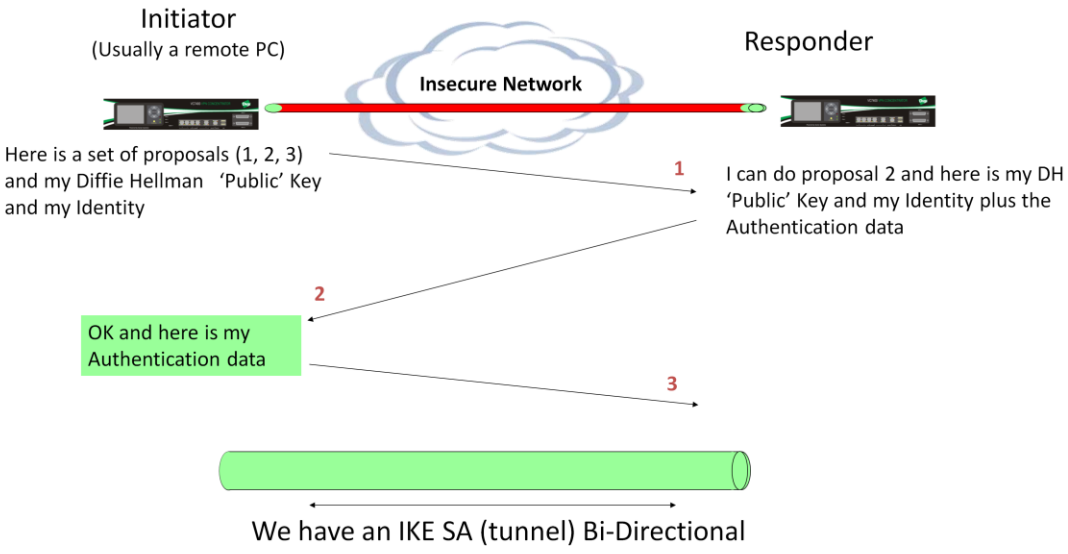
Uni-Directional IPsec SA's aka IKE phase 2 SA's

IKE Main Mode Setup

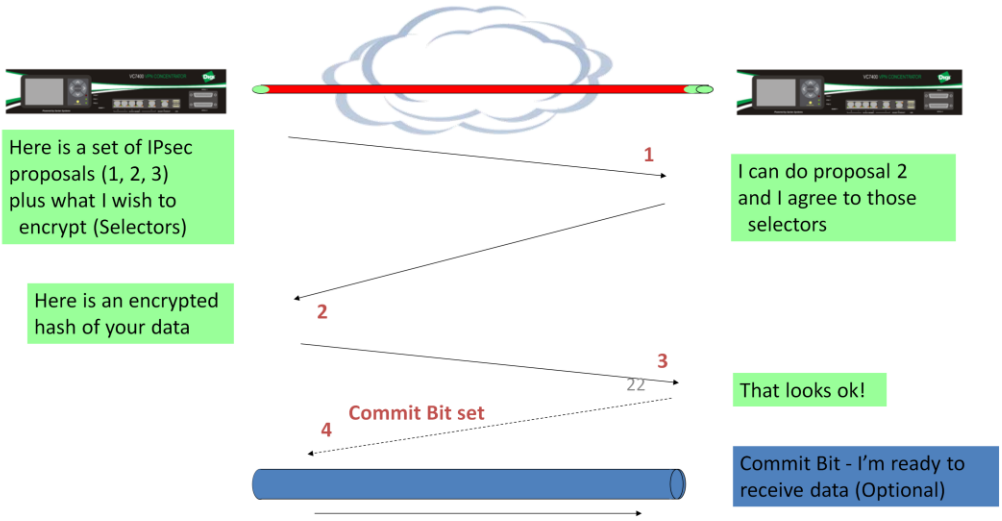


We have an IKE SA (tunnel) Bi-Directional

IKE Aggressive Mode Setup

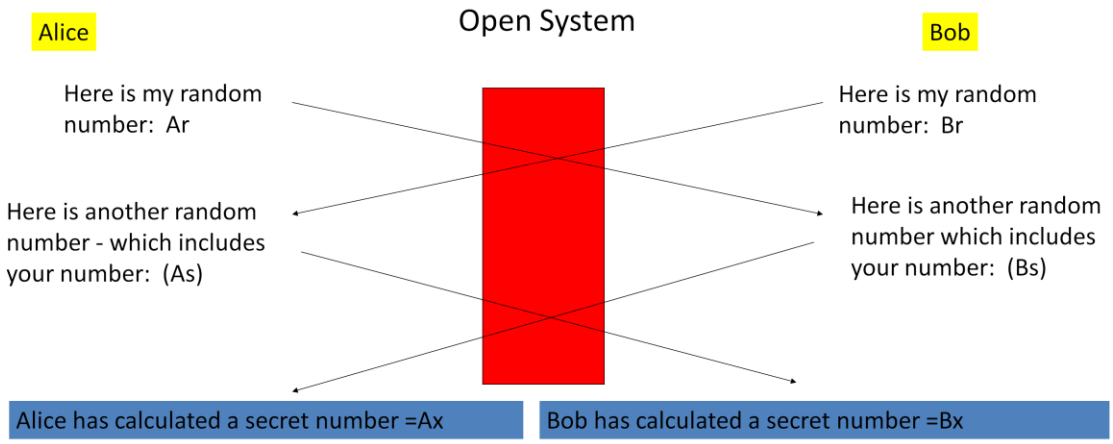


IPsec Security Association Creation (IKE Phase 2)



We have an IPsec SA (tunnel) Uni-Directional

Diffie-Hellman Protocol



Both sides have arrived at the same number because Ax = Bx

A Base number and Prime are agreed during the initial exchanges e.g 2 and DHG-5

Choosing Your IPsec Technologies

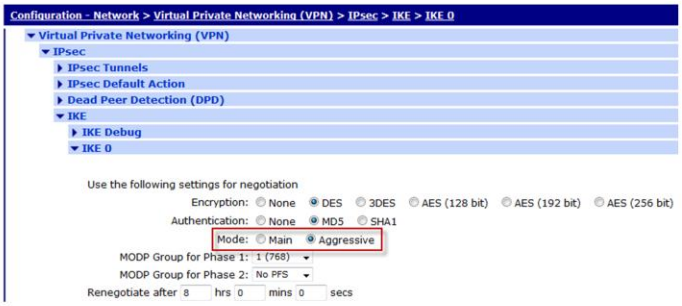
- The protocols defined within IPsec include:
  - ISAKMP -Internet Security Association and Key Management Protocol
  - AH Authentication Header
  - ESP Encapsulating Security Payload
  - HMAC Hash Message Authentication Code
  - MD5 Message Digest 5
  - SHA-1 Security Hash Algorithm
  - DES Data Encryption Standard
  - 3DES Triple DES
  - AES Advanced Encryption Standard

Choosing Your IPsec Technologies

- The specific variant of security used will depend on the level of security required.
- For financial transaction information, the highest level of security should be applied, especially if it is crossing a public network i.e. the Internet
  - 3DES or AES 192 minimum encryption (AES is recommended as it is more efficient)
  - SHA1 authentication hash algorithm (MD5 has been deemed not secure)
- Remember: The settings chosen must match on each end of the VPN tunnel!

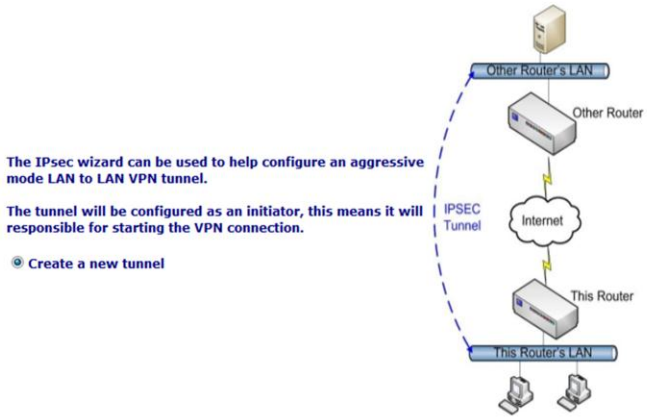
IKE – Aggressive Mode

- If the wireless plan can only provide dynamic IP addresses, it is not possible to know the IP address of the interface when creating the configuration
- In this case IKE must use “Aggressive Mode”



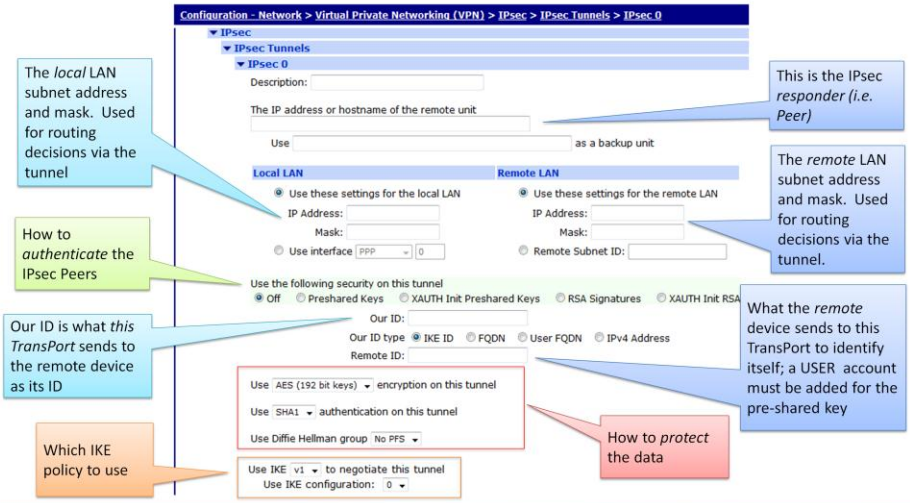
IPsec Tunnel Wizard

- A simple Aggressive Mode IPsec Tunnel can be configured using the “Create an aggressive mode LAN to LAN IPsec tunnel” wizard



IPsec – Manually Configure Tunnel (a)

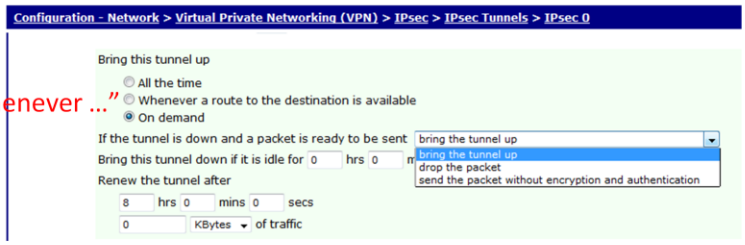
- Once the IPsec parameters are determined, configure the IPsec tunnel
- Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec n (CLI: `eroute n`)



IPsec – Manually Configure Tunnel (b)

- Continue down the page to determine when to bring up the tunnel, the tunnel (phase 2) lifetime, and to finish basic tunnel configuration:

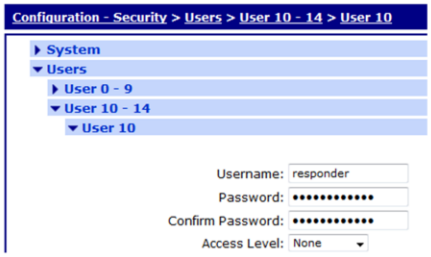
Normal recommended setting = "whenever …"



- Configure Advanced settings as required (but generally are not needed)
- Remember to APPLY and SAVE your changes!

IPSec – Pre-Shared Key

- A **User Account** must be created for the Pre-Shared Key via Configuration – Security > Users > User 10 - 14
- The Username is the IPSec **Remote ID** (either the peer IP address or ID)
- The Password is the **Pre-Shared Key**
- E.g., if the Remote ID is “responder” and the PSK is “th1s1stheKEY”:
  - Username: responder
  - Password: th1s1stheKEY
  - Access Level: low or none



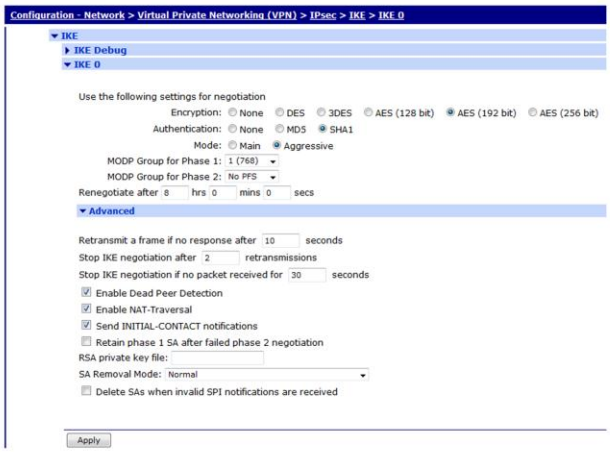
Why do we use 10 onwards ?

It’s away from the standard users normally.
It defaults to a low security access.
It’s just convention and easy if we all do it the same way.

Any user number will work.

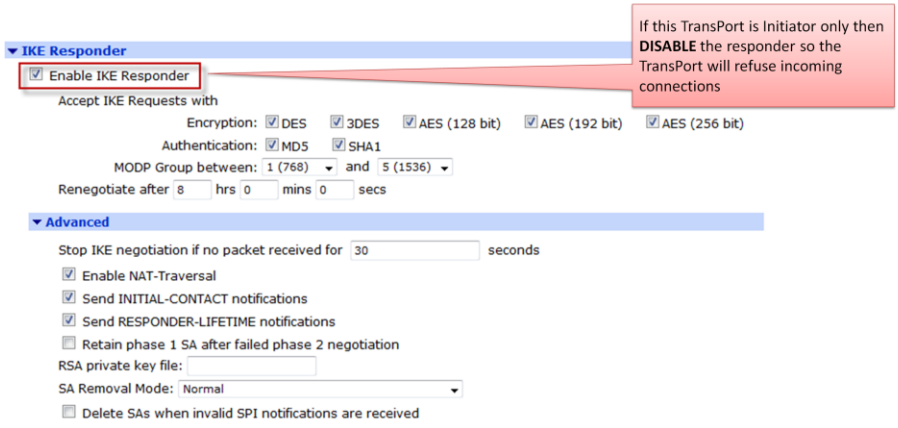
IKE Initiator

- Configure the appropriate IKE Configuration (0 or 1) as selected in the IPsec tunnel via Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE n
- Normally it will be necessary to enable Aggressive mode
- MODP group for phase 2 will apply a minimum accepted level for phase 2. In the configuration of phase 2 (IPsec tunnel) the setting can be un-configured, the same, or higher.

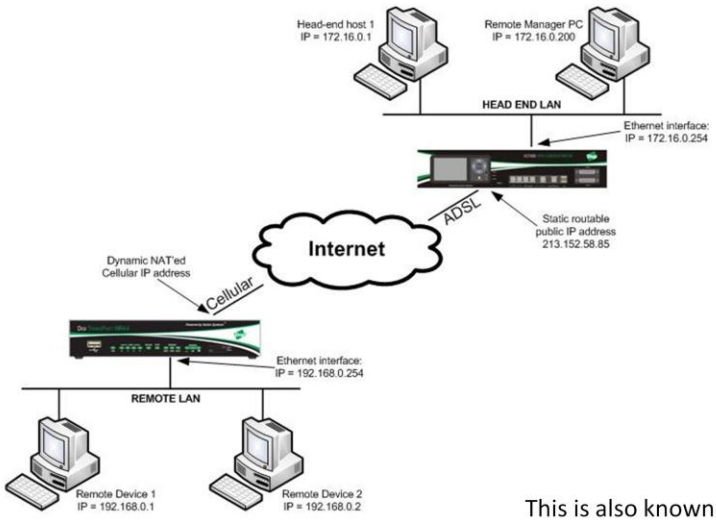


IPsec – IKE Responder

- In some cases the TransPort is used for VPN termination
- Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE Responder



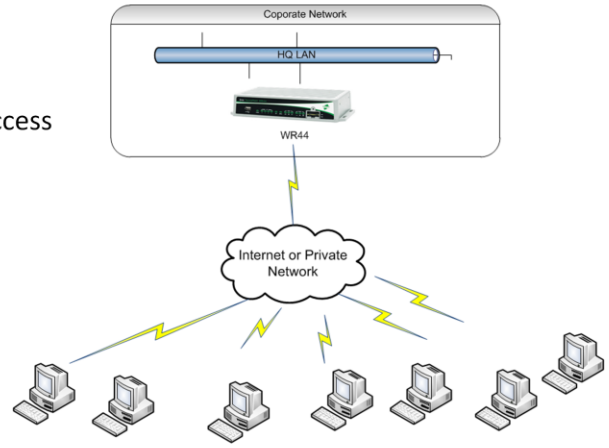
Using IPsec over Cellular



This is also known as LAN to LAN IPsec

Remote Access Technologies

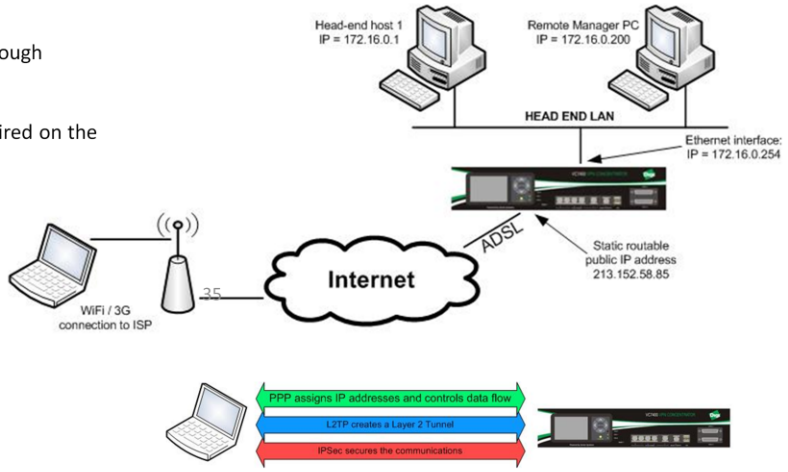
- When mobile users need secure network access from a laptop a different method is used
- Windows does not support plain IPsec VPNs
- Many remote users only need a few remote access VPNs configured on the head-end router.
- The available options are:
  - PPP over L2TP over IPsec (recommended)
  - PPTP
  - The GreenBow IPsec VPN client installed on laptop
  - OpenVPN client installed on laptop



PPP over L2TP over IPsec VPN

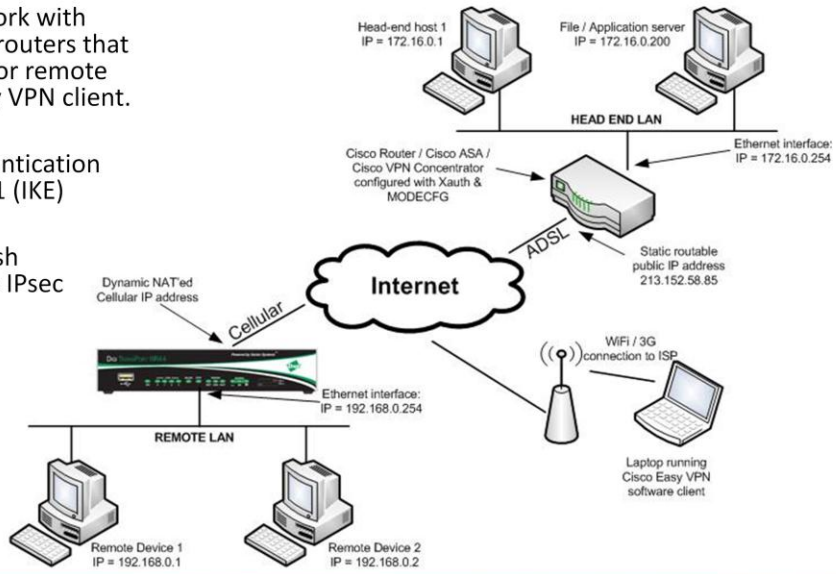
Common solution for remote users running the Windows OS that need secure access to the corporate LAN. The benefit of running this type of VPN is that the remote laptop can be assigned an IP address in the range of the local LAN, allowing software using NetBIOS and any other software applications that don't support routed connections to work correctly.

- L2TP IPsec VPNs work well through NAT'ed connections
- No extra VPN software is required on the Windows laptop



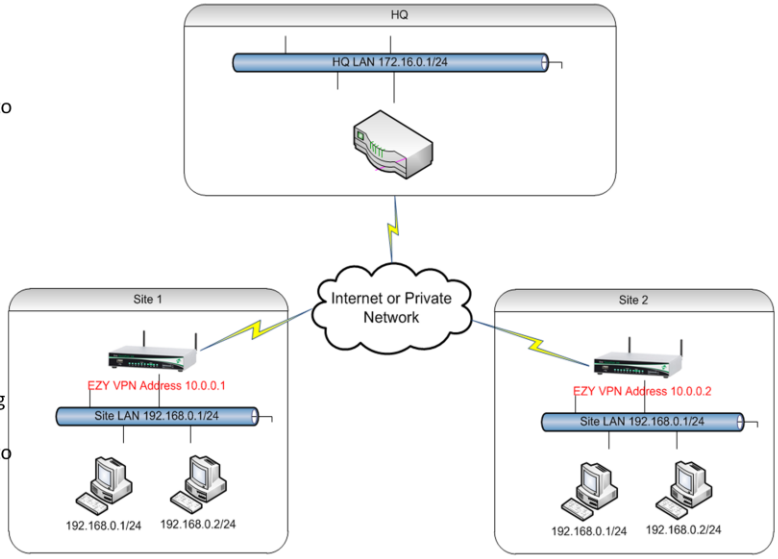
TransPort with Cisco Easy VPN

- TransPort routers will work with existing Cisco head end routers that are already configured for remote access via the Cisco Easy VPN client.
- Xauth is Extended authentication that occurs after phase 1 (IKE)
- MODECFG is used to push attributes to the remote IPsec client



Easy VPN

- MODECFG used to push virtual IP address (VIP) to sites
- Xauth used for 2 factor authentication
- Site LAN's can have overlapping IP addresses
- Site LAN can access HQ LAN
- HQ LAN cannot access site LAN directly
- HQ LAN can access site hosts via Port Forwarding
- NEM (Network Extension Mode) - same as LAN to LAN IPSEC



Summary

- VPNs & IPsec
- The Data Tunnel in action
- IPsec Basics
- Tunnel Modes
- IKE/IPsec Operations
- IKE Mode setup
- Diffie-Hellman Protocol
- Choosing your IPsec technologies
- NAT Traversal
- Using IPsec over GPRS

HOPS – IPsec Tunnels

- Work with a partner to configure an IPsec VPN tunnel between 2 TransPort routers
- For reference, see Application Note 10
  IPsec Over W-WAN using Digi TransPort Routers with Pre-shared keys
- Use the Analyser to diagnose problems (see AN10)