Protecting the Network – VPN & IPsec

INFO-6078 – Managing Enterprise Networks

FANSHAWE

Protecting the Network

- At times, we connect to insecure networks such as those provided in public places such as at events or airports
- When connected to these networks, we may be exposing our devices to unwanted monitoring or attack
- Our own organization may also want to provide access to internal resources to users who are travelling without exposing the data to the greater internet
- To help protect data in transit, many organizations use VPN technologies to securely exchange data when connected to insecure networks

Virtual Private Networks (VPN)

- A VPN is a private network created in software and secured with encryption that allows data to be securely transmitted over the internet

Some reasons we may implement a VPN:

- Confidentiality
  - When we need to ensure that data that may be intercepted is unreadable to third arties
  - VPNs encrypt data to ensure confidentiality
  - The difficulty of decrypting the data is directly tied to the length of the key used to encrypt

Virtual Private Networks (VPN)

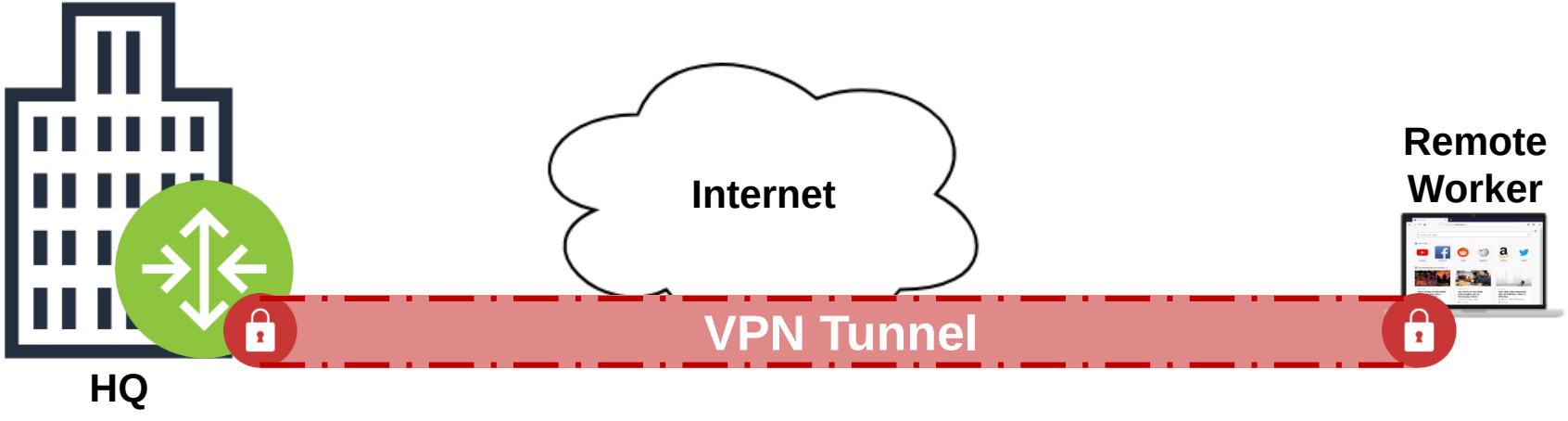
- Integrity
  - Data integrity ensure that the data has not been intercepted and modified during transit
  - The hash-based message authentication code (HMAC) algorithm identifies if data has been modified and will drop the message if tampering is detected
- Authentication
  - Validates the remote party before exchanging data
  - Hashing is also used to verify the sender of each message, as hashing each packet with a code only the communicating devices know verifies the sender

VPN Types

- Commonly implemented VPNs:
  - IPsec
    - Framework for securing network communications
  - Secure Shell (SSH)
    - Commonly used to administer remote systems
    - Requires user authentication
  - Secure Socket Layer (SSL)/Transport Layer Security (TLS)
    - Popular with websites and ecommerce
  - OpenVPN
    - Open-Source VPN solution
  - Multiprotocol Label Switching (MPLS) VPN
    - Supported by a provider network

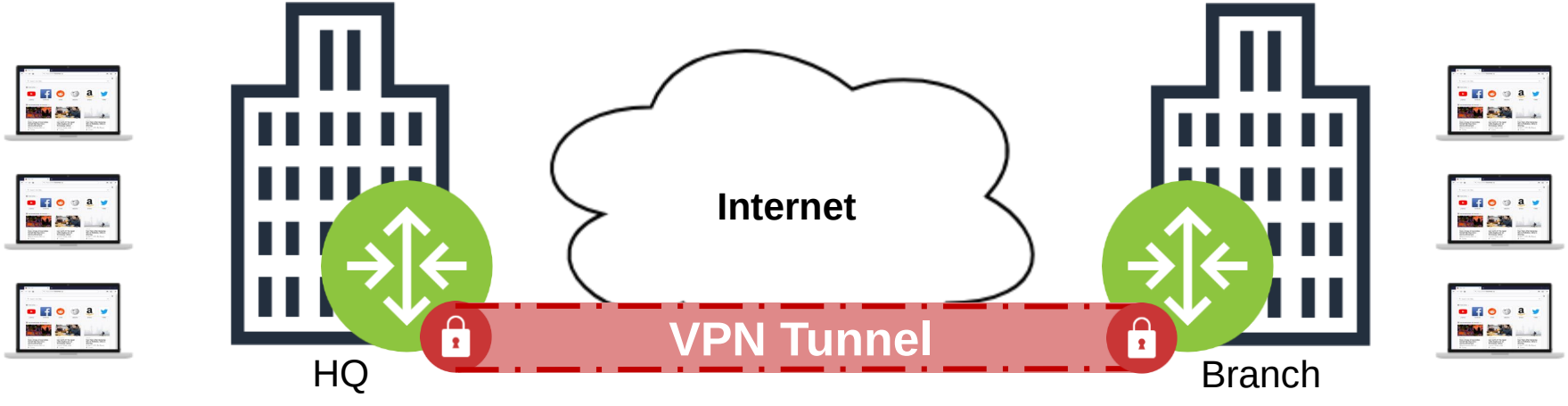
VPN Topology - Remote Access

- Remote access VPNs allow remote workers outside of the corporate network to access resources
- Often having only a laptop or smartphone to connect, remote access VPNs provide access to network resources as if the user was on-site
- Usually offered via client VPN software

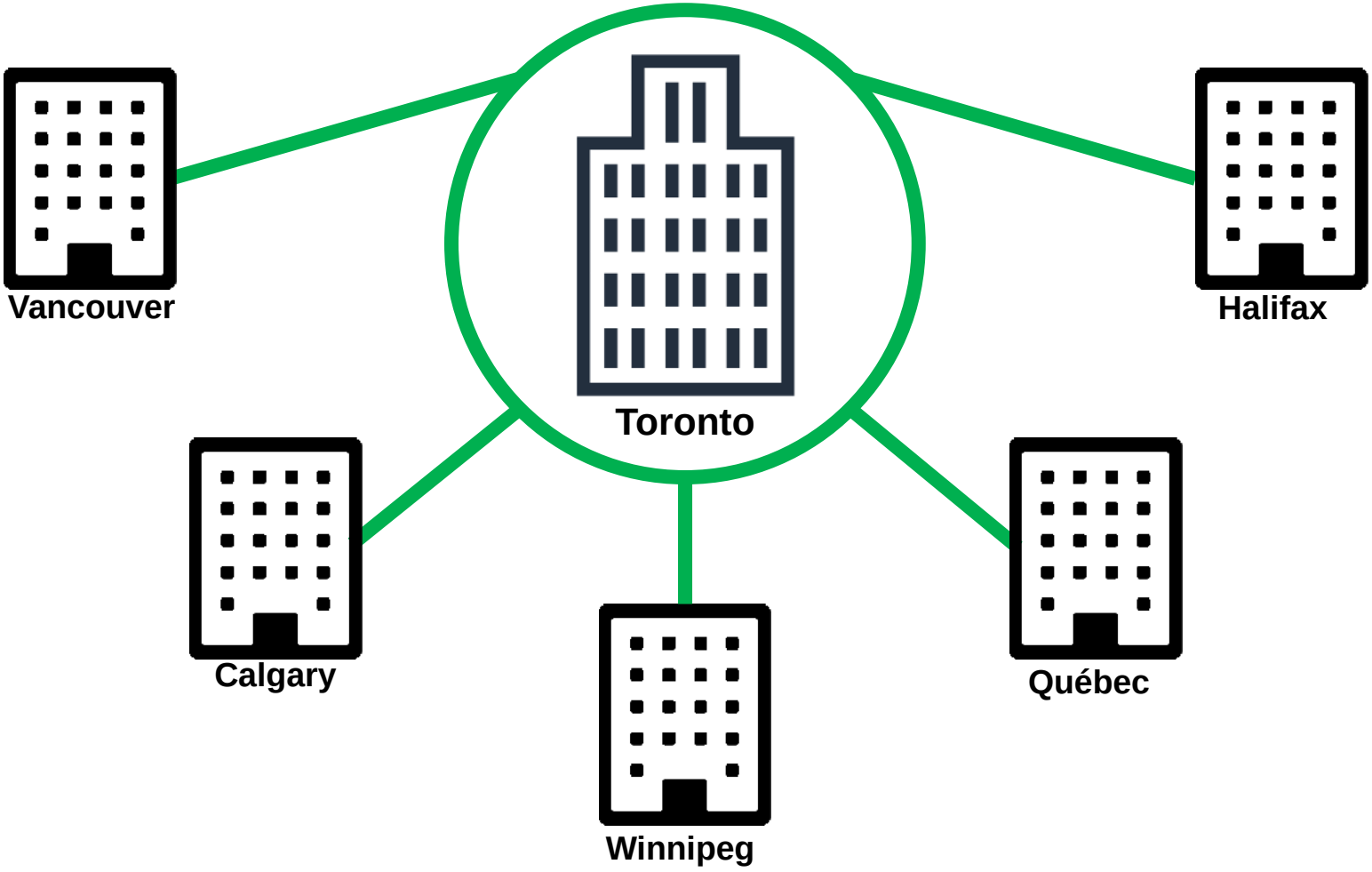


VPN Topology - Site-to-Site

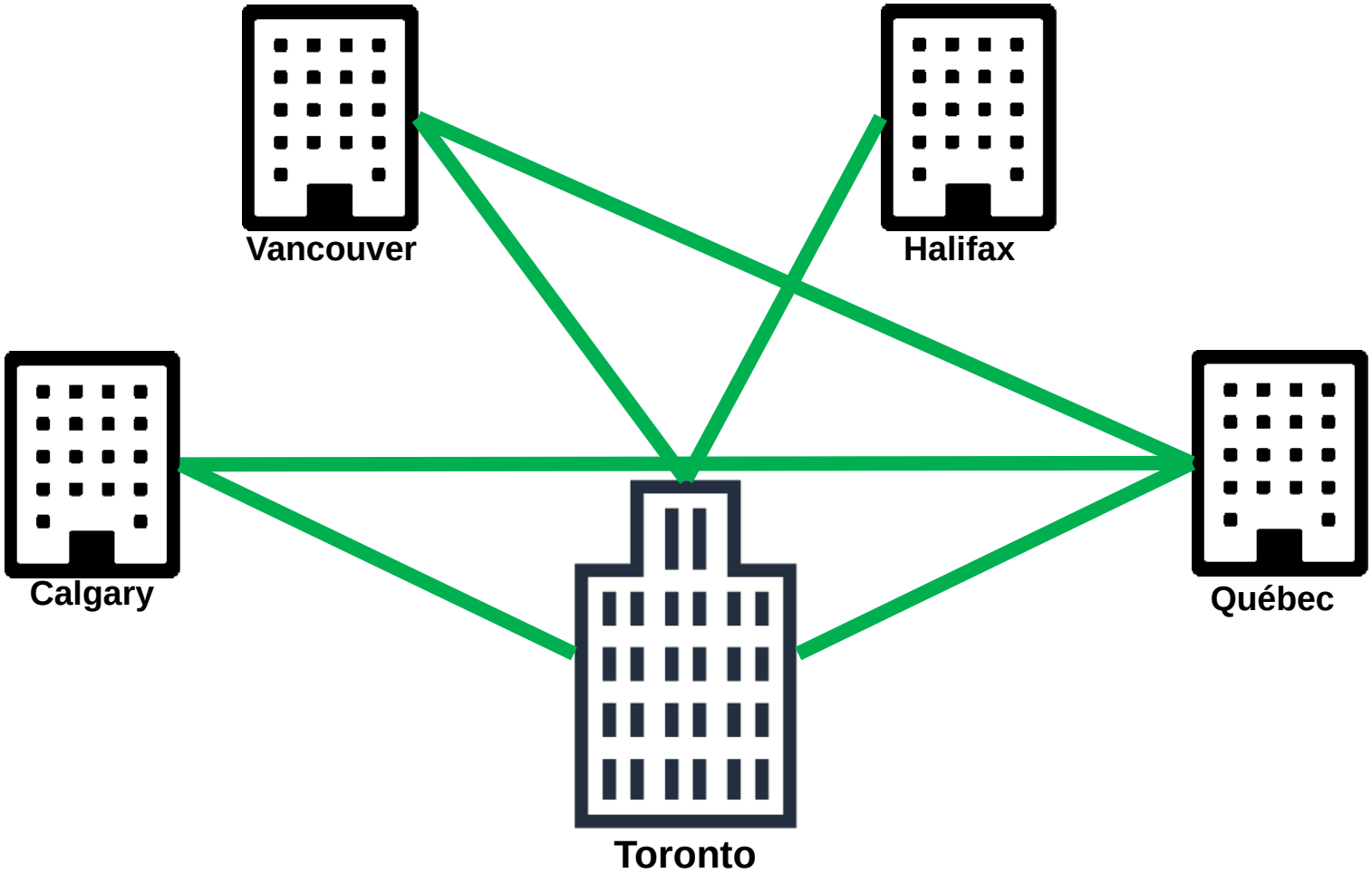
- Connects remote sections of the corporate network
- VPN endpoints are usually static, and do not change location or address
- Configured on a VPN gateway, the connection is transparent to client devices



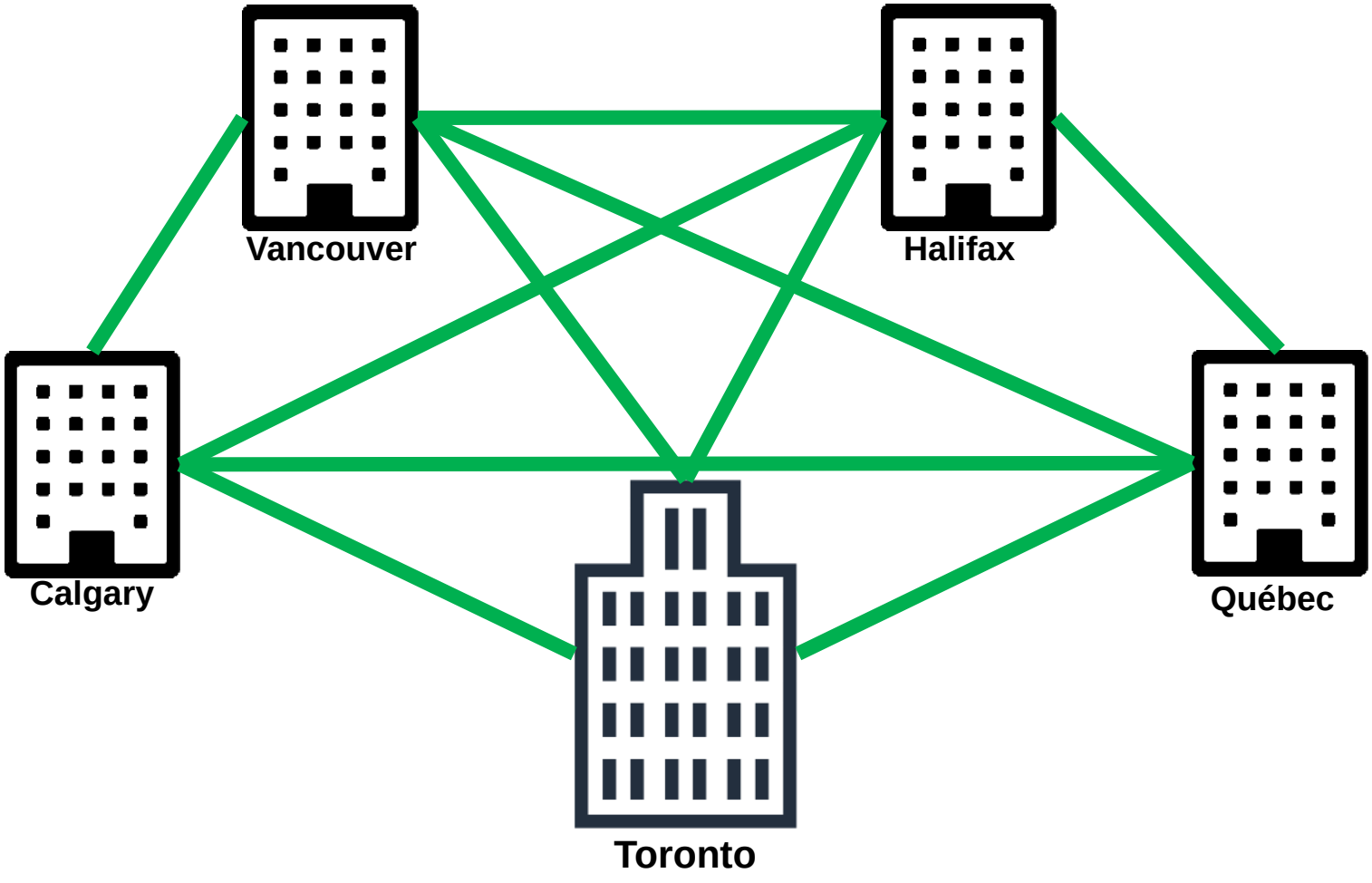
Physical VPN Topologies – Hub & Spoke



Physical VPN Topologies – Partial Mesh



Physical VPN Topologies – Full Mesh

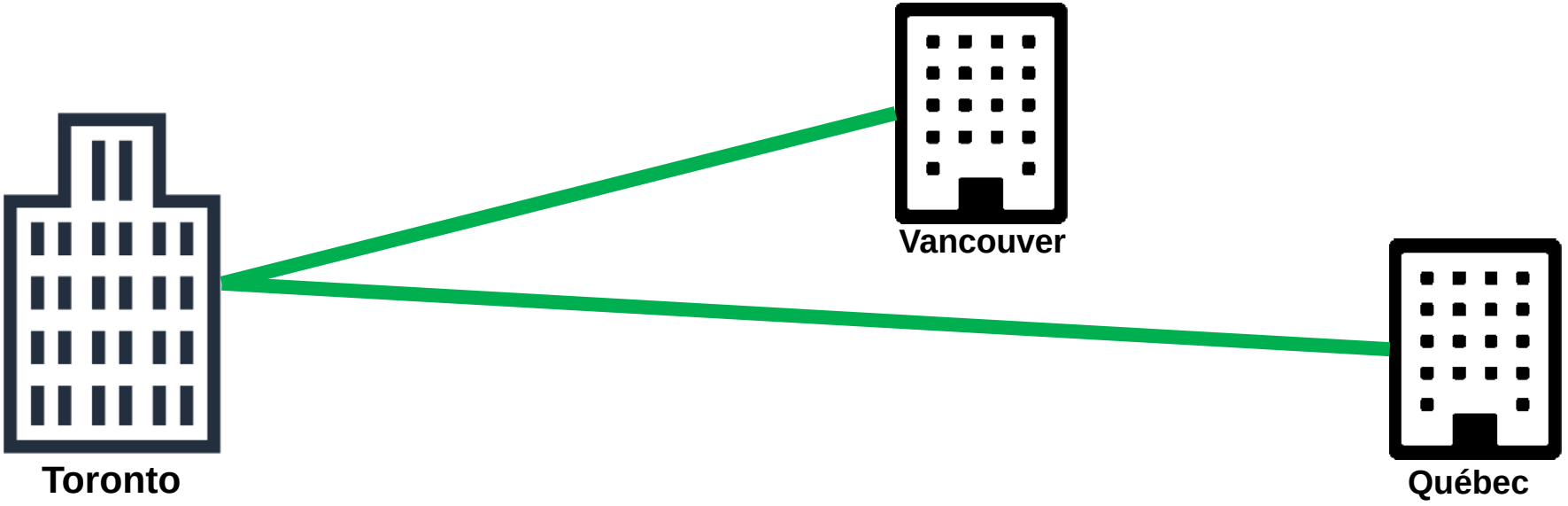


Always-On VPN

- An always-on VPN is used to provide seamless connection to corporate resources when users travel off of the corporate campus
- Always-on VPN use location awareness to detect when the device is connected to an external network and automatically activates the VPN connection
- Lockdown mode can be used to protect the user when the VPN is not available
- Microsoft DirectAccess is an example of an always-on VPN

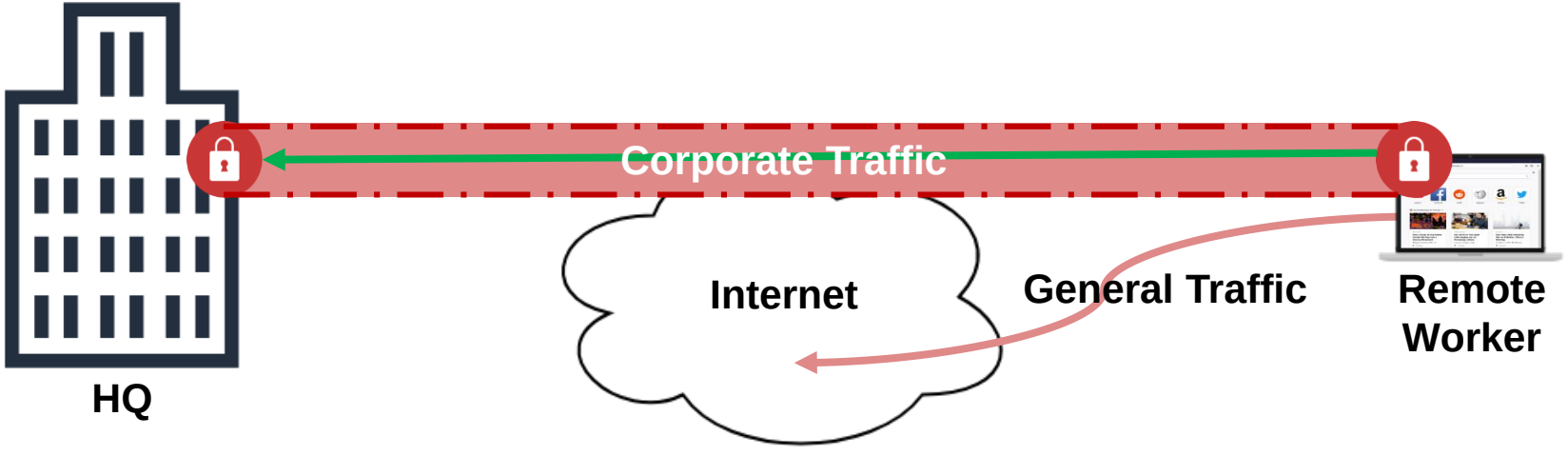
Hairpining

- When using VPNs, it is possible that traffic my enter an interface and need to be rerouted out that same interface
- This is a common occurrence when remote access VPNs route internet traffic through the VPN, or in hub and spoke topologies



Split-Tunnel VPN

- A split-tunnel describes a VPN connection where corporate resources are available through the VPN, but general internet traffic is routed directly to the internet from the local interface and does not cross the VPN
- Split-tunneling is used to reduce traffic volume at VPN gateways and improve latency on user devices

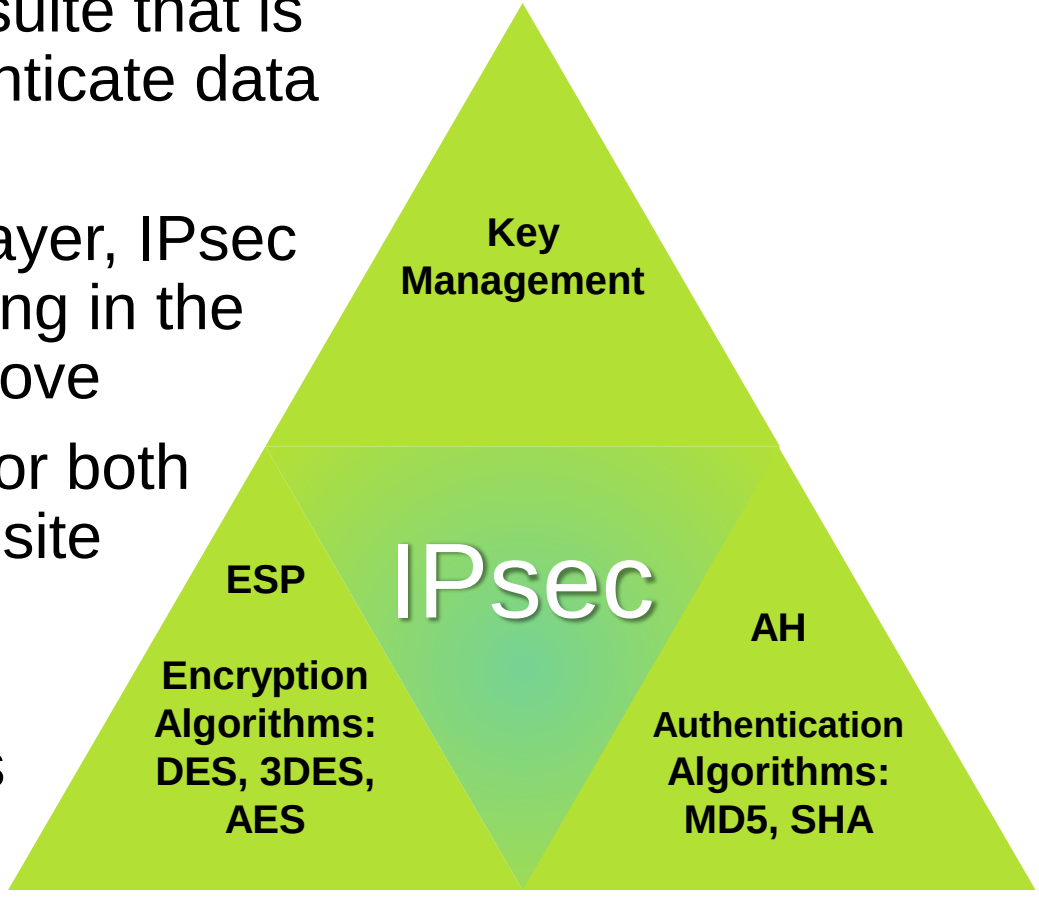


Secure Socket Layer (SSL) VPN

- Many websites make use of Secure Socket Layer (SSL) or Transport Layer Security (TLS) VPNs to not only secure site traffic, but also to protect users payment information
- Encapsulates layers 5-7 of the OSI model
- Operates over TCP port 443
- PCIDSS requires the use of encryption technology to when handling credit card transactions

IP Security (IPsec)

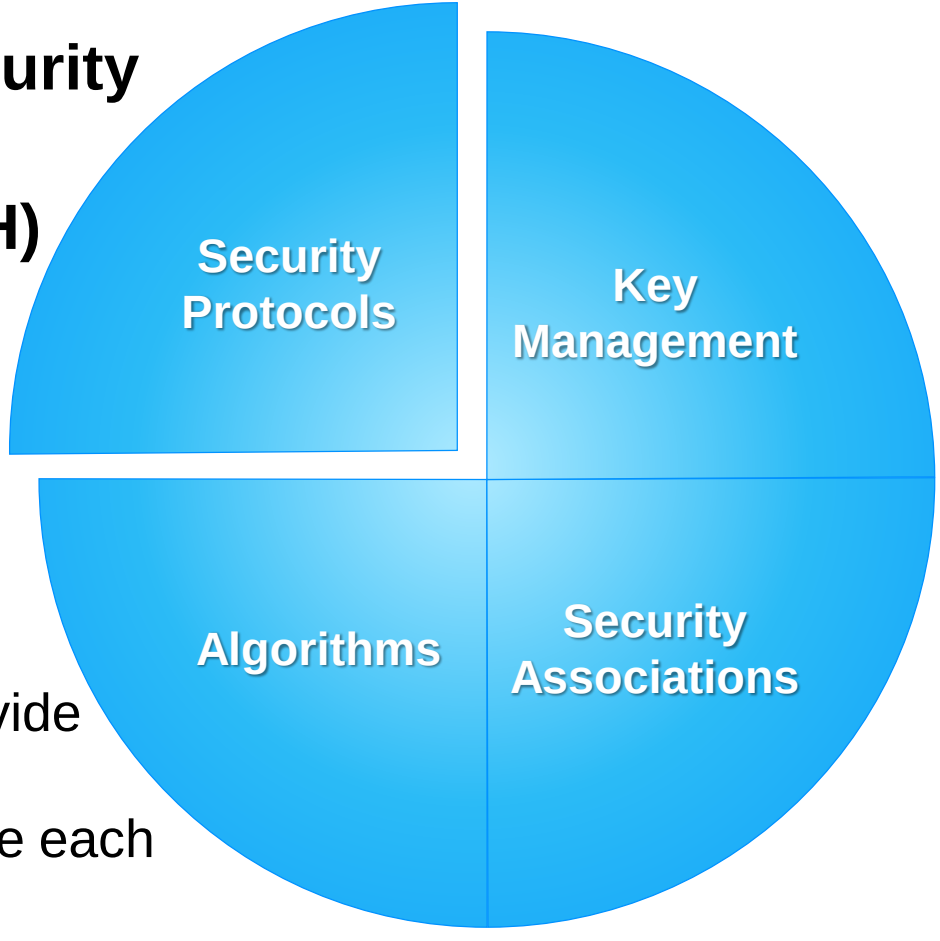
- IPsec is an IETF protocol suite that is used to encrypt and authenticate data sent across a VPN
- Operating at the network layer, IPsec can secure protocols running in the OSI transport layer and above
- IPsec is a suitable option for both remote access and site-to-site VPNs
- IPsec is flexible, and not bound to specific protocols or features



IPsec – Security Protocols

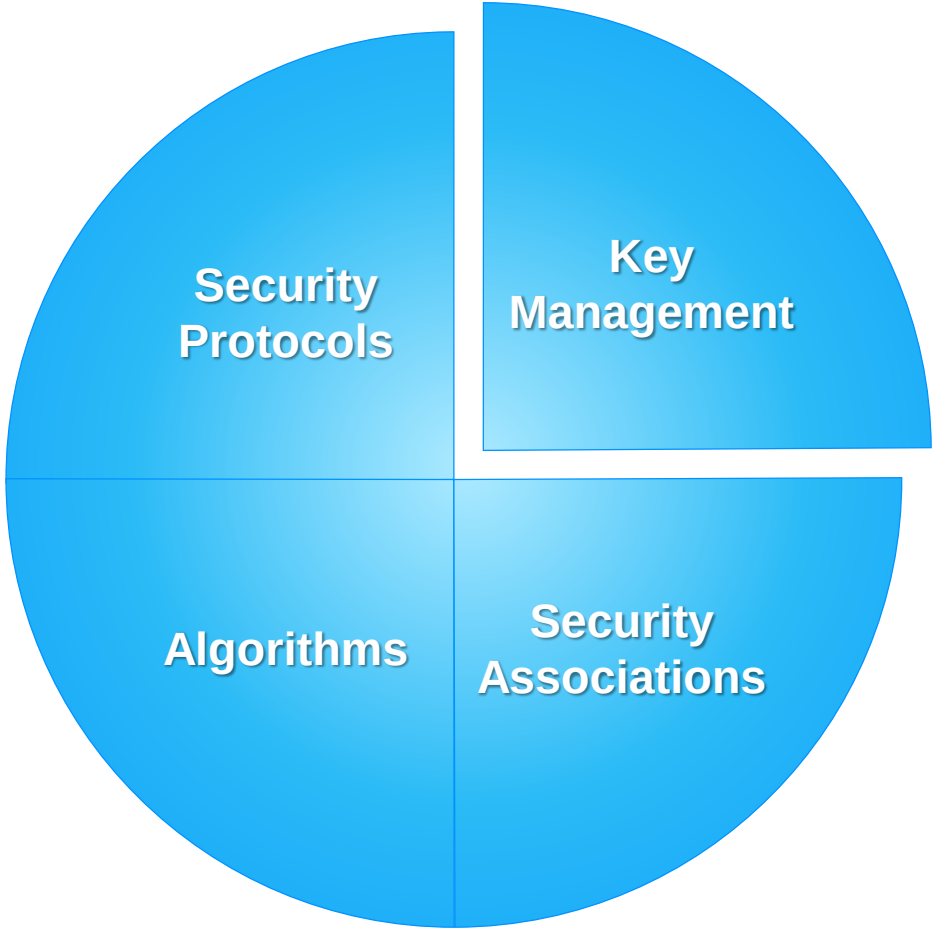
IPsec has the following security protocols:

- **Authentication Header (AH)**
  - Hashes headers and data to verify authenticity
- **Encapsulating Security Payload (ESP)**
  - Allows the payload to be encrypted
  - Combined with hashing to provide authentication and integrity
  - Anti-replay mechanisms ensure each packet is unique



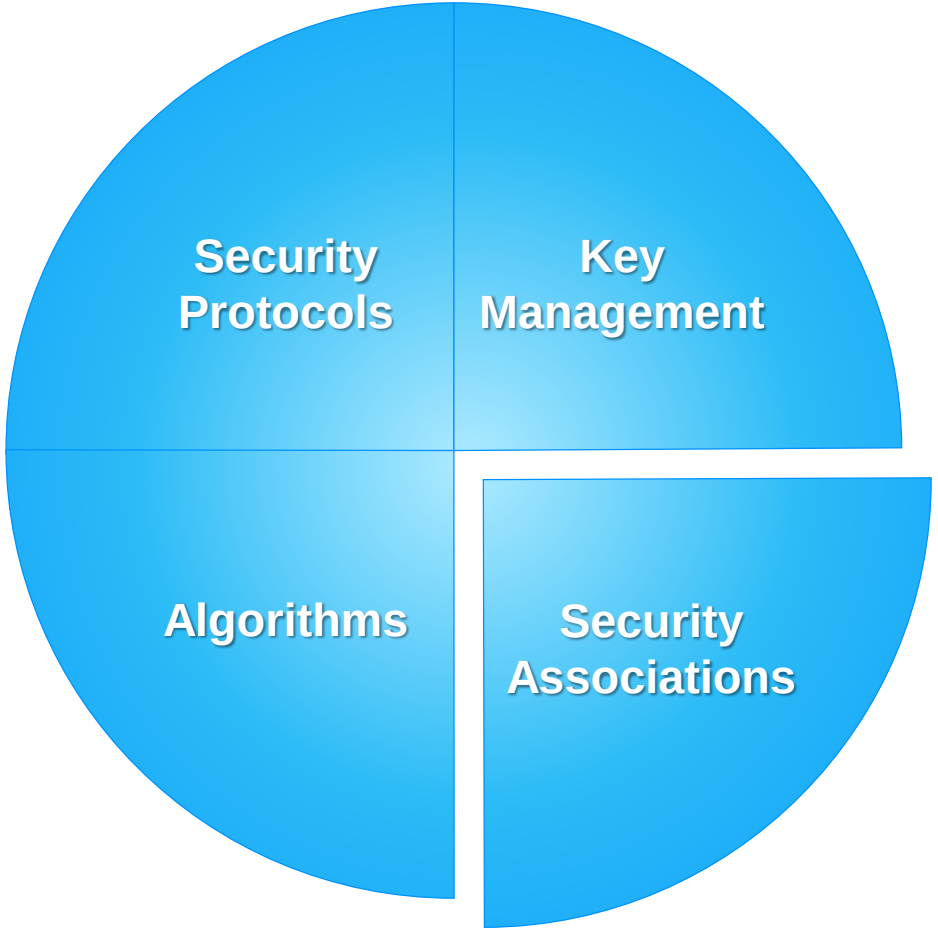
IPsec – Key Management

- IPsec can use the following key management techniques:
  - Manual
    - Suitable for smaller deployments
  - Internet Key Exchange (IKE)
    - Recommended for enterprise environments



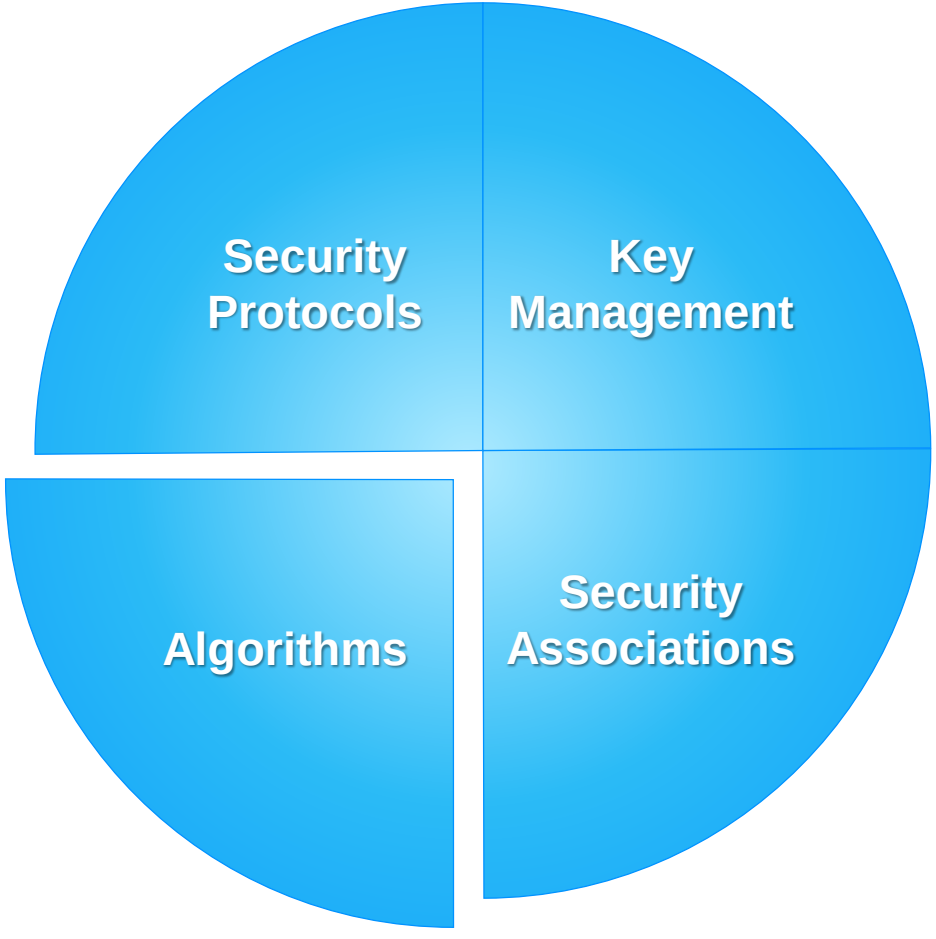
IPsec – Security Associations

- A security association defines the relationship two VPN endpoints share
- The association identifies the protocols, algorithms and keys used for AH and ESP
- Both endpoints must share the same associations for a successful connection



IPsec – Algorithms

- IPsec algorithms describe key exchange, integrity, encryption and authentication



IPsec Components

Protocol	**AH**	**ESP**	**ESP + AH**	
Confidentiality	**DES**	**3DES**	**AES**	
Integrity	**MD5**	**SHA-1**	**SHA-2**	
Authentication	**PSK**	**RSA**		
Diffie-Hellman	**DH1**	**DH2**	**…**	**DH20**

IPsec Operation Modes

- When IPsec is used AH and ESP offers two operation modes:
  - **Transport**
    - Authenticates the IP payload via hashing
    - Encrypts layers 4-7 of the OSI model
    - The original IP header is used to route data across the network
  - **Tunnel**
    - Authenticates and encrypts the entire IP packet
    - A second IP header is created and the encrypted message is placed within
    - The new IP header is used to route the packet

Internet Key Exchange (IKE)

- IKE is used to create security associations in IPsec
- IKE is a combination of the Oakley protocol, the Internet Security Association Key Management Protocol (ISAKMP) and Diffie Hellman key exchange to calculate shared secrets
- Cryptographic keys are then derived from the shared secrets
- The power of Diffie-Hellman is that a third party that intercepts all of the exchanged messages will be unable to decrypt the keys
- Diffie-Hellman is referred to by DH group, with later groups supporting longer and newer keys

Internet Key Exchange (IKE) – Phase 1

- IKE operates on UDP port 500 and completes the key exchange two phases:

Phase 1:

- Endpoints negotiate a secure communication channel by using Diffie-Hellman to generate a shared secret
- The peers also perform the initial negotiation of the security associations
- Operation modes for phase 1 include main and aggressive
  - Aggressive mode establishes a connection faster as it utilizes a three-way handshake, opposed to main modes six-way handshake

***IKEv1 aggressive mode is vulnerable to cracking attacks**

Internet Key Exchange (IKE) – Phase 2

Phase 2:

- Peers utilize the secure channel created in phase 1 to negotiate the parameters of the security association
- Negotiation will result in a unique set of keys for two unidirectional security associations
- Phase 2 operates in quick mode
- Quick mode is also responsible for the regeneration of security associations when the SA lifetime expires

Internet Key Exchange version 2 (IKEv2)

- Officially ratified in 2010, IKEv2 improves the protocol with the addition of:
  - NAT traversal
    - IKE and ESP messages are encapsulated and sent over UDP port 4500
    - This allows the messages to be sent over networks that employ NAT
  - Denial of Service (DoS) resilience
    - IKEv2 verifies the sender is active before performing cryptographic computations
    - This prevents DOS attacks from spoofed IP addresses

IPsec Operation

- IPsec operation can be broken into five major phases:
  1. The source identifies “interesting” traffic destined for the destination
     - Interesting traffic is generally defined by an ACL
  2. IKE phase one begins negotiating security associations with the destination and a secured channel is created by calculating a shared secret
  3. IKE phase two negotiates parameters of the security association policy over the phase one channel
  4. The tunnel is created and data is exchanged
  5. The tunnel is terminated either by an administrator, or times out from inactivity

IPsec – Multicast Traffic

- IPsec supports transmitting unicast traffic over the tunnel; however, dynamic routing protocols like Open Shortest Path First (OSPF) or Enhanced Interior Gateway Routing Protocol (EIGRP), as well as many other protocols communicate via multicast transmissions
- To allow protocols that require multicast communications, a second unencrypted tunnel needs to be setup within the IPsec VPN
- The tunnel can use the Generic Routing Encapsulation (GRE) to transmit the traffic