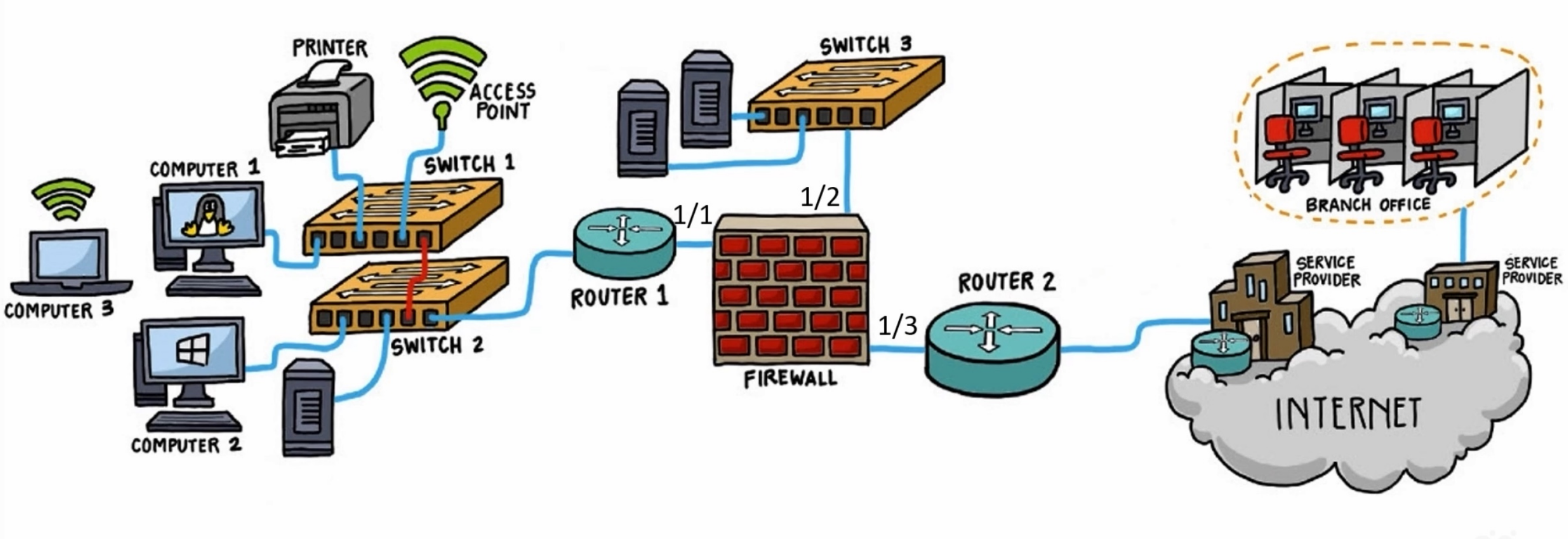
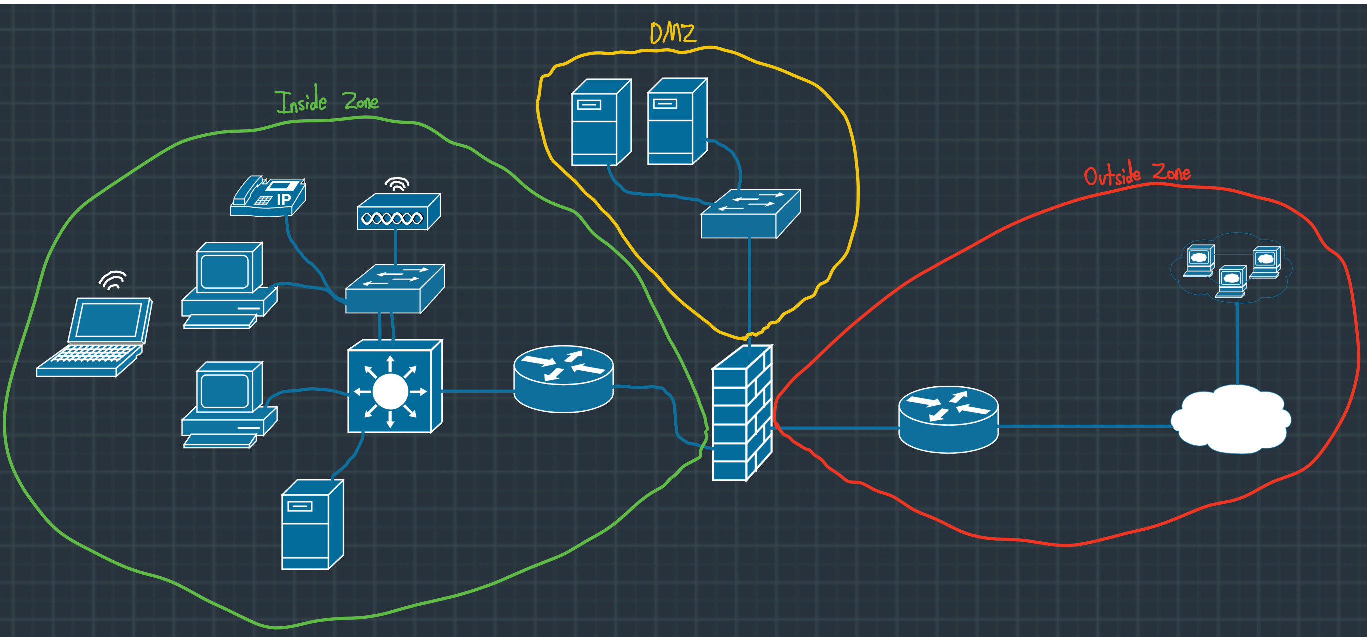
Img Cite: CBT Nuggets





Network Security Notes

Network Security Fundamentals:

- Types of Firewalls:
  - One of the earliest methods of firewalls is packet filtering (ACLs)
    - Not efficient for the amount and types of network traffic today (too granular, not scalable)
  - Internal/Inside Zone: Internal/Inside "trusted" networked devices, devices the company owns/manages
  - External/Outside Zone: External/Outside "public" networked devices, devices the company does not own/manage (internet)
  - Traffic can be managed based on these zones and rules by firewalls (ex. traffic by default if originated from external zone coming to the internal zone, will be denied)
  - Stateful Firewall: A type of firewall that will remember the state of the session; Filters on L3 and L4 information
    - When a packet from the inside zone through the firewall to the internet, the firewall will record and remember aspects of the sent packet request
    - If a reply packet comes in and it doesn't perfectly match the requested information, the packet will be dropped
    - If a reply packet comes in and matches, it will be dynamically let back in by the firewall's stateful table
    - Need to be able to control the initial flows of traffic (traffic sourced from the inside zone)
    - Lots of false positives and dropped packets compared to stateless
  - Next-Generation/Application Aware Firewall: Can do everything a stateful firewall can, but can also filter based on higher layers like the application layer
    - Packet filtering based on policy, could allow Google but not Google Drive
    - Can allow application X but not Y even if they share the same IP or port

- Intrusion Detection Systems and Intrusion Prevention Systems:
  - Both IDS and IPS must be "trained" using average network flows or must go through a period of "learning"
    - The network traffic must be pulled from during normal operational hours to form a network baseline
  - Through this, the system can recognize irregular network and take action against it
  - IDS: A way to detect and alert when an attack is occurring on the network
    - Has 2 popular implimentations:
      - Via Firewall (if supported): Train the firewall to pay attention to network traffic and set off alerts when appropriate
      - Via Port Mirror: Copy all networked traffic off a switch (or off full network) to an IDS (Static IP)
        - Can analyze all traffic being routed through the connected device and sets off alerts when appropriate
  - IPS: A way to detect when an attack is occurring on the network and prevent it
    - Commonly implemented on firewalls before traffic reaches the inside zone
    - Must be in-line with the traffic it is analyzing
  - Types of Traffic Indentification:
    - True Positive
    - True Negative
    - False Positive
    - False Negative
- Virtual Private Networks (VPNs): VPNs talked about above with CCNA, refrence page 18
  - Remote Access VPN terminates at a firewall
    - Split tunneling
  - Site-to-site VPN uses VPN tunnels using IPsec
- Data Loss Prevention: Methodology for how to prevent company/corporate information from leaving the company unintentionally
  - Identify what data to secure through end user training; end users should know and understand the type of data they need to secure
  - Firewalls should be able to decrypt TLS/SSL sessions momentarily to look at the L3, L4, and L7 data to see what is going out and whether it should be stopped
    - Policies and exclusions should be put in place regarding what types of traffic to do or not do decryption on (do not decrypt PII/passwords)
    - Enabling this decryption enables application layer inspection where it can see the unencrypted data and read the payloads of the packet to see if it should be dropped
- Unified Threat Management: A central security appliance that can perform multiple security funtions as a single device
  - Seperate devices work too, it depends on the bandwidth of the network, a UTM shouldn't throttle it
    - More to manage, but seperation of duties is present, higher cost with multiple devices
  - Features of UTMs:
    - Anti-malware/Virus protection
    - Anti-spam
    - Content filtering (URL filtering)
    - DLP
    - Stateful filtering
    - IDS/IPS
    - VPN support

- Endpoint Security: Things/Elements to improve the security of end node devices in a network
  - Endpoints include user workstations, PCs, and servers
  - Endpoints should have limited access-control rights, anti-malware software, and host-based IDS/IPS
  - Software Firewall/Personal firewalls deny or permit certain types of activities to the filesystem
  - If malicious software is identified on a computer the system must be quarantined
    - The computer is logically removed from the network so it can't harm the other systems
  - Malicious software is identified by signatures, anomolies in network traffic to or from the endpoint, or container-based protection and analysis
    - Container-based software is software that runs independently to every other software application on an endpoint
  - Mobile device endpoints have security features too including remote wipes, full disk encryption, and mobile device management
- Identity, Access, & Configuration Management:
  - Authentication, Authorization, Accounting, reference page 16
    - Authentication Portal (User-ID on Palo Alto)
  - Zero-Trust: Do not trust users connecting to manage services, authenticate each time (no central admin account)
  - Identity management with AD
  - Groups help to manage access (Role-based access control)
  - Least privledge (do not have privledge creep)
  - Configuration Management: Includes configuration baselines to help manage scope creep of configured network devices (old configs not being removed)
    - Can have various baselines for different types of devices stored in a central database
    - Changes to these baselines must go through the change control process

Cyberattack Lifecycle:

- Steps of the cyberattack lifecycle include:

① - Reconnaissance: Two types, active and passive

② - Weaponization: The way in which an attacker will prepare to attack a target (social engineering)

③ - Exploitation: Triggering the attack

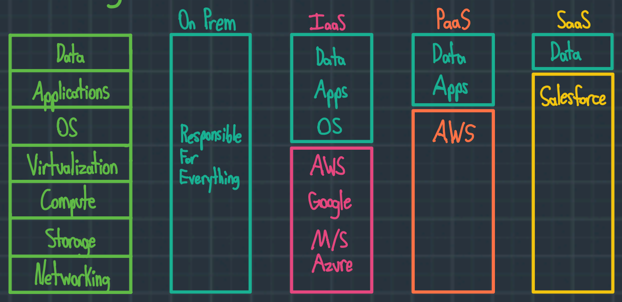
④ - Installation: Malicious code is installed on the target system

⑤ - Command & Control: The stage when the attacker has full access to the target system
  - Stateful filtering allows this to take place because the origin of the connection is from the local network going out
  - Encryption, proxies, port hopping and tunneling can all be used by the attacker to evade detection
  - A next generation firewall can help prevent these more than a stateful firewall via application layer inspection and decryption

⑥ - Actions on the Objective: The attacker gains access to the system and can carry out their plans

- Advance Persistent Threats: Cyber attacks that remain on systems for extended durations without being discovered
  - Advanced: Refers to skills, tools and resources required to pull something like this off
  - Persistent: Time, attacks to infiltrate a system will likely be slow to evade any intrusion detection and to remain in the system as long as possible
  - Threat: Deliberate and focused, the goal of the attacker on the target system

Cloud Technologies:



Virtual Machines:

- Types of VMs include:
  - Type 1 hypervisor: Also known as a bare-metal hypervisor, this VM runs on direct access to the hardware resources
  - Type 2 hypervisor: VM applications installed on the host operating system (VMware Player/VirtualBox)
- Containers: Application-focused VM with just enough resources to run the required application (ex. Docker)
  - More efficient if you need to run apps only like in PaaS or SaaS (Known as Container as a Service, CaaS)

VPNs

Site-to-site VPN:

IPsec: Data integrity and Privacy

-IKEv1 and IKEv2

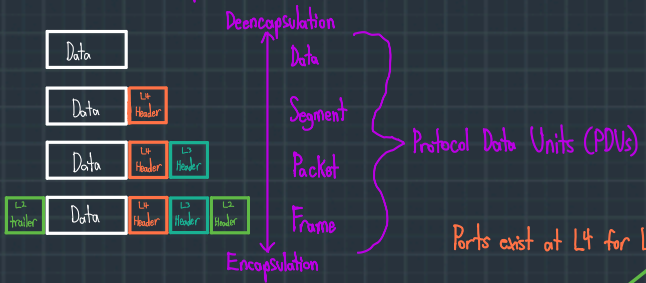
-Authentication methods for IPsec include preshared Keys and/or digital certificates

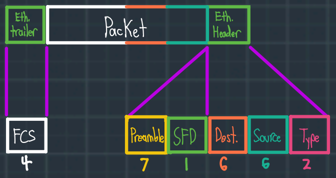
-A tunnel is made between 2 sites to logically route traffic between the two sites

Ethernet Frames:

-OSI Model data encapsulation:

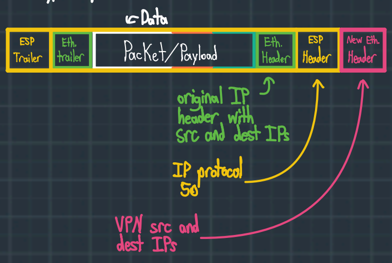
Review from CCNA

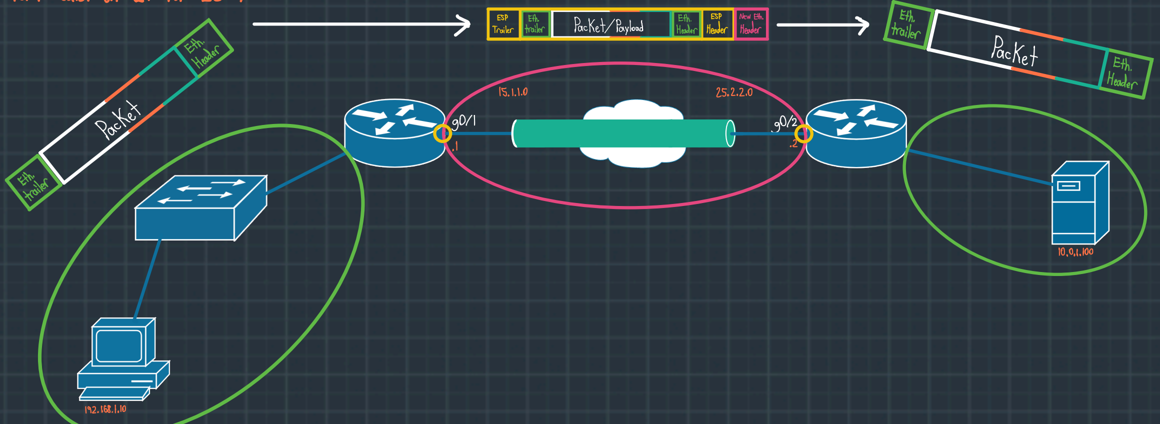




Ports exist at L4 for L5-7

New encrypted packet with IPsec:





IPsec:

IPsec combines the following security protocols:

-Internet Key Exchange (IKE) provides a framework for policy negotiation and Key management to IPsec

-Authentication Header (AH) provides encapsulation for authentication of user traffic. (Mostly obsolete)

-Encapsulating Security Payload (ESP) provides encapsulation for encryption and authentication of user traffic. ← always used over or with AH

-IPsec provides security services at the IP layer by enabling a system that:

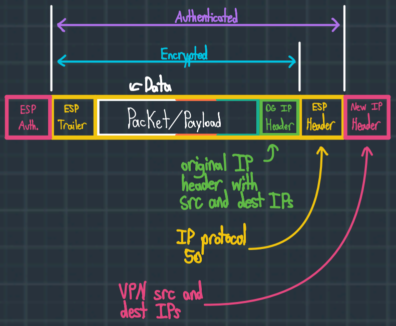
-Chooses required security protocols

-Determines the algorithm(s) to use for the service(s)

-Puts in place any cryptographic Keys that are required to provide the requested services

-IPsec can protect one or more paths between pairs of hosts or security gateways

-IPsec operates in 1 of 2 modes tunnel mode or transport mode



Tunnel Mode:

-Encapsulates the payload and IP header and adds a new IP header

-Then sends the packet to the other side of the VPN tunnel

-Routing across the intermediary (internet) is done based on the new IP header

-Using tunnel mode leads to additional packet expansion of approx. 20 bytes due to the new IP header

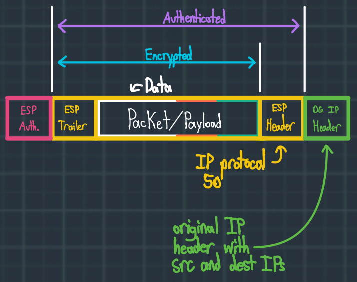
* -Due to this additional packet overhead, it is recommended that the maximum MTU of a frame going over a VPN tunnel in tunnel mode is 1,400 bytes to avoid packet fragmentation

Transport Mode:

-Only encapsulates the payload of the IP packet and leaves the IP header untouched

-Transport mode is applicable to either gateway or host implementations and provides protection for upper-layer protocols

-Requires original IP packet to be routable over the transport network or another tunneling mechanism must already be in place such as GRE



Security Associations:

-A Security Association (SA) is a simple description of current traffic protection parameters that can be applied to specific user traffic flows

-Note: The major function of IKE is to establish and maintain security associations

-AH/ESP provide security services to an SA

-If AH or ESP protection is applied to a traffic stream, 2 SAs are created to provide protection to the traffic stream

-To secure typical bidirectional communication between 2 hosts or security gateways, 2 IPsec SAs (one in each direction) are required

Internet Key Exchange:

-Defined by RFC 2408, IKE automatically establishes a shared security policy and authenticated Keys for services that require them (IPsec)

-IKE creates an authenticated, secure connection between 2 entities and negotiates their security associations on behalf of the IPsec stack

-The 2 entities must authenticate themselves to each other and establish shared session Keys that IPsec encapsulations and algorithms will use to transform cleartext user traffic into ciphertext

-IKE SA is bidirectional, where IPsec SA is unidirectional

-In a typical IPsec configuration, IKE is used to provide:

- -Scalability
- -Manageable manual configuration
- -SA characteristics negotiation
- -Automatic Key generation
- -Automatic Key refresh

-There are 2 standardized versions of the IKE protocol, IKEv1 and IKEv2

IKEv1:

-Has 2 distinct phases, Phase 1 and Phase 2

-These phases represent the 2 SAs that are going to be built during IKE

-2 tunnels, 1 per phase

IKE Phase 1:

-The goal of Phase 1 is to establish an asymmetric bidirectional communication channel/tunnel to share further symmetric Keying material for IKE Phase 2

-This shared channel is used to establish shared Keying material using a Diffie-Hillman Key exchange

-Phase 1 can either operate in main or aggresive modes

- -Main Mode:
  - -More flexible negotiation of the IKE protection policy
  - -Always protects peer identity
  - -Does not support dynamically addressed peers when performing PSK authentication
  - -Takes 6 messages by default to exchange Keying information
- -Aggressive Mode:
  - -Less flexible negotiation of the IKE protection policy
  - -Does not protect peer identities
  - -Supports dynamically addressed peers when performing PSK authentication using names (not IPs) to associate particular peers
  - -Takes 3 messages by default to exchange Keying information

-To establish an IKE Phase 1 tunnel, there are 5 basic things that must be agreed upon: (HAGLE)

- -H: Hashing (HMAC); Options include MD5, SHA1, SHA2, etc.
- -A: Authentication; Options include RSA/Digital Certificates or PSKs
- -G: Group (Diffie-Hillman); The higher the #, the more secure it is
- -L: Lifetime; Default time is 1 day
- -E: Encryption; Options include DES, 3DES, AES, AES-GCM, etc.

IKE Phase 2:

-Occurs after main mode and the IKE Phase 1 tunnel has been established

- -IKE Phase 2 is also referred to as Quick Mode or IPsec SA

-The goal of Phase 2 is to establish a communication channel to pass data plane traffic either symmetrically or asymmetrically

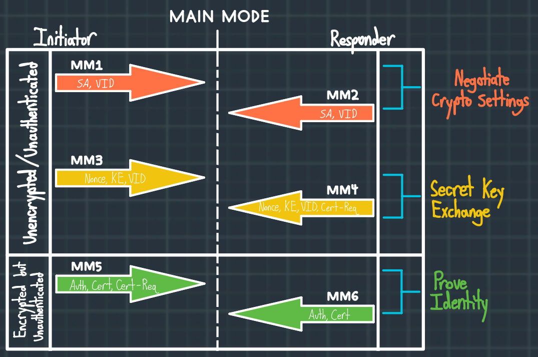
-In Phase 2 additional SAs are negotiated on behalf of IPsec services that need Key material or parameter negotiation

-By default the IPsec session Keys are derived from the initial Keying material obtained in the Phase 1 DH Key exchange

- -Optionally the IPsec session Keys can be derived from independent new DH Keying material
  - -This achieves Perfect Forward Secrecy (PFS) across the IPsec SA

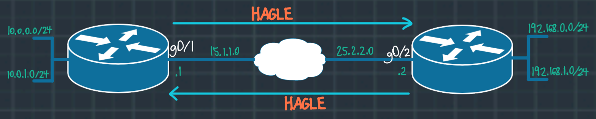
-The IKE Phase 2 tunnel does not get established/come online unless interesting traffic is passed over the tunnel

- -Interesting traffic is matched based on Access Control Lists (ACLs) applied to crypto maps

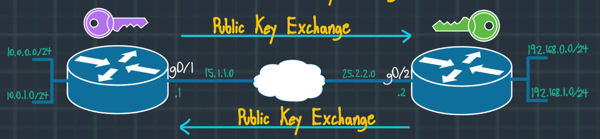


Phase 1 complete: Encrypted & Authenticated

MM1 & MM2: HAGLE information is shared

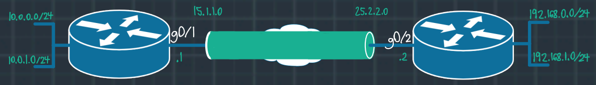


MM3 & MM4: DH Key Exchange

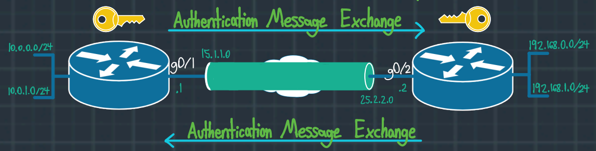


NAT-D is performed in MM3 & MM4

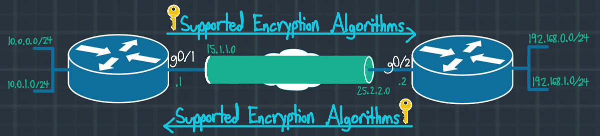
Phase 1 tunnel is established

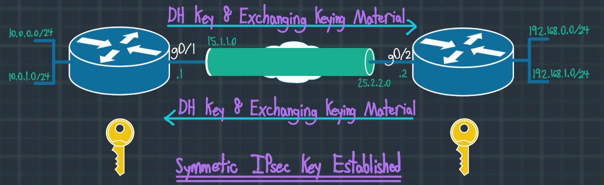


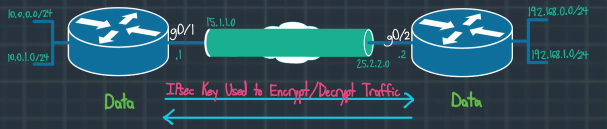
MM5 & MM6: Verifies Peer Identity



Symmetric Key is established here and both sides are encrypted and authenticated




DH Key & Exchanging Keying Material
10.0.0.0/24
10.0.1.0/24
g0/1
.1
15.1.1.0
25.2.2.0
g0/2
.2
192.168.0.0/24
192.168.1.0/24
DH Key & Exchanging Keying Material
Symmetic IPsec Key Established


10.0.0.0/24
10.0.1.0/24
g0/1
.1
15.1.1.0
25.2.2.0
g0/2
.2
192.168.0.0/24
192.168.1.0/24
Data
IPsec Key Used to Encrypt/Decrypt Traffic
Data