CISSP® Common Body of Knowledge Review:

Telecommunications & Network Security Domain – Part 2

Version: 5.9.2

Learning Objectives
Telecommunications & Network Security Domain – Part 2

The Telecommunications and Network Security domain encompasses the structures, techniques, transport protocols, and security measures used to provide integrity, availability, confidentiality, and authentication for transmissions over private and public communication networks.

The candidate is expected to demonstrate an understanding of communications and network security as it relates to data communications in local area and wide area networks, remote access, internet/intranet/extranet configurations. Candidates should be knowledgeable with network equipment such as switches, bridges, and routers, as well as networking protocols (e.g., TCP/IP, IPSec,) and VPNs.

Reference: *CISSP CIB*, January 2012 (Rev. 5)

Topics

Telecommunications & Network Security Domain – Part 2

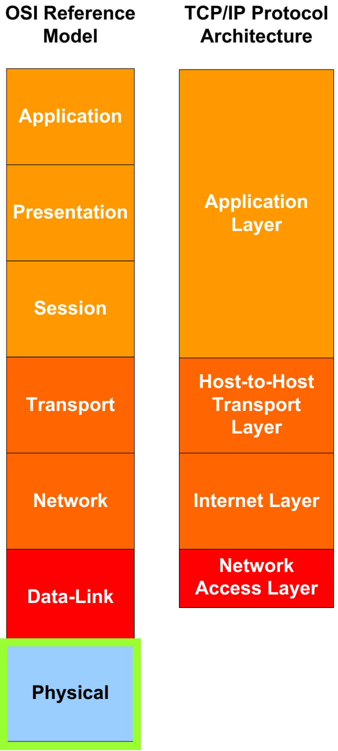
- Security Countermeasures and Controls
  - Physical Layer
  - Data-Link Layer
  - IP Network Layer
  - Transport Layer
  - Application Layer
- VPN
- NAS

Memorization	OSI Reference Model	TCP/IP Protocol Architecture
Away	Application	Application Layer
Pizza	Presentation	
Sausage	Session	
Throw	Transport	Host-to-Host Transport Layer
Not	Network	Internet Layer
Do	Data-Link	Network Access Layer
People	Physical	

Security of Physical Layer – Review

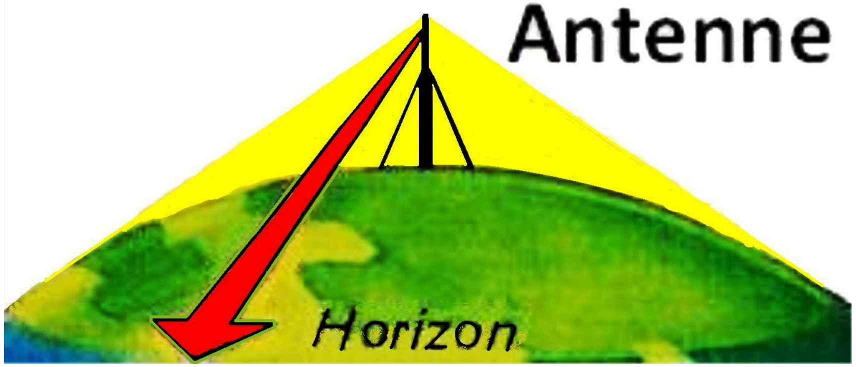
Transport Media

- Cables
  - LAN: Twisted Pair (Shield, Un-shield), Coaxial, Fiber Optics (Single-mode, Multi-mode)
  - WAN: SONET
- Radio Frequency (RF)
  - LAN: 2.4GHz, 5GHz, UWB (3.1GHz – 10.6GHz)
  - WAN: Microwave (VHF, UHF, HF) (300MHz – 300GHz)
- Optical
  - LAN: Infrared
  - WAN: LASER (medium: fiber, air)



Transport Media

- Physical protection of transport media
  - Cables/Fibers: Casings (Concrete, Steel pipe, Plastic, etc.)
  - RF: Allocation of radio spectrum, power of RF, selection of line-of-sight (LOS), protection from element (rain, ice, air)
  - Optical: Selection of transport medium, light wave spectrum (multi-mode), LOS and strength of light beam (e.g. single-mode)
- Path Diversity of transport media
  - Cables / Fibers: Geographic diversity
  - RF: Utilization of radio channels, coverage area
  - Optical: Multi-mode



Transport Interfaces (I/Fs)

- Physical protection of transport I/Fs
  - Access control of network equipment
    - Telecommunication Room
    - Data Center / Server Room
    - Network Closet
- Logical protection of transport I/Fs
  - Disable All Interfaces Not In-Use
  - Enable Interface only when Ready-To-Use
  - Designate specific I/Fs for management
  - Designate specific I/Fs for monitor

Network Equipment

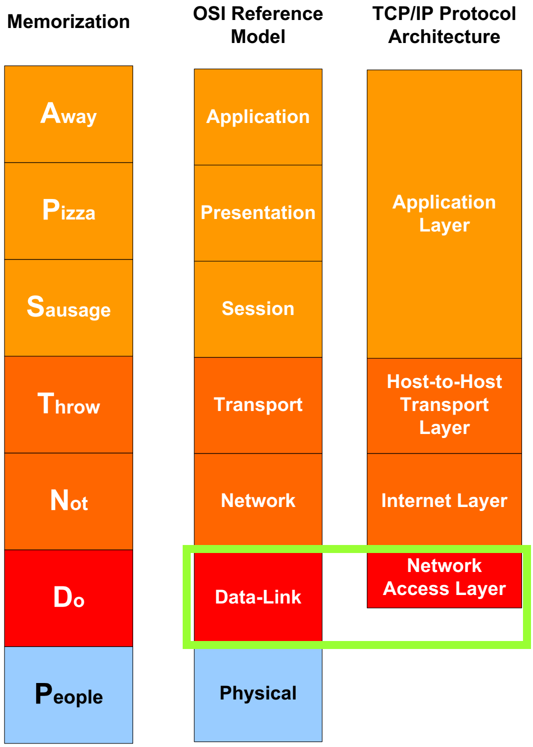
- Enable `service password-encryption` on all routers (global config mode). This command obscures all clear-text passwords in the configuration using a Vigenere cipher. Almost impossible to break
- Use `enable secret` (encrypts the password) command and not with the `enable password` (password in plain text) command (show running-config)
- Each router shall have different enable and user password
- Access routers only from "secured or trusted" server or console

Reference: DISA FSO *Network STIG*

Topics

Telecommunications & Network Security Domain – Part 2

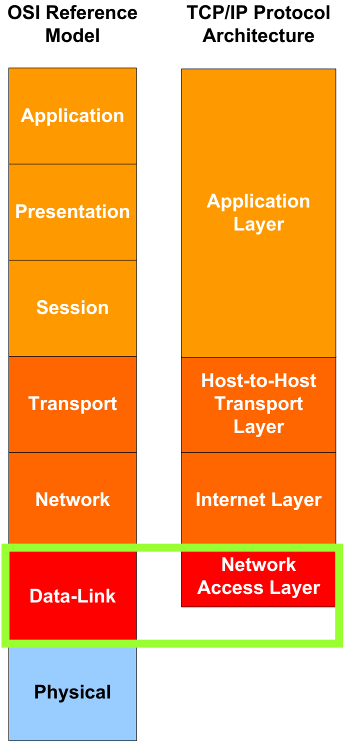
- Security Countermeasures and Controls
  - Physical Layer
  - Data-Link Layer
  - IP Network Layer
  - Transport Layer
  - Application Layer
- VPN
- NAS



Memorization	OSI Reference Model	TCP/IP Protocol Architecture
Away	Application	Application Layer
Pizza	Presentation	
Sausage	Session	
Throw	Transport	Host-to-Host Transport Layer
Not	Network	Internet Layer
Do	Data-Link	Network Access Layer
People	Physical	

Security of Data-Link Layer – Review

- Data-Link Layer
  - MAC (LAN & WAN)
  - LLC (LAN)
- LAN Data-Link Layer Protocols
  - Ethernet (CSMA/CD)
  - Token Ring (Token Passing)
  - IEEE 802.11 a/b/g (CSMA/CA)
- WAN Data-Link Layer Protocols
  - X.25
  - Frame Relay
  - SMDS (Switched Multi-gigabit Data Services)
  - ISDN (Integrated Services Digital Network)
  - HDLC (High-level Data Link Control)
  - ATM (Asynchronous Transfer Mode)



Security of Data-Link Layer

Confidentiality and Integrity of Data-Link Layer

- SLIP (Serial Line Internet Protocol)
- PPP (Point-to-Point Protocol)

RF:

- LAN: WEP (Wired Equivalent Privacy), EAP (Extensible Authentication Protocol), IEEE 802.1X

Serial Line Internet Protocol (SLIP)

- SLIP (Serial Line Internet Protocol) is a packet framing protocol that encapsulates IP packets on a serial line
- Runs over variety of network media:
  - LAN: Token Ring
  - WAN: X.25, Satellite links, and serial lines
- Supports only one network protocol at a time.
- No error correction
- No security

Point-to-Point Protocol (PPP)

- PPP (Point-to-Point Protocol) is a encapsulation mechanism for transporting multi-protocol packets across Layer 2 point-to-point links. (RFC 1661)
- PPP replaces SLIP because:
  - Support multiple network protocols (IP, AppleTalk, IPX, etc.) in a session
  - Options for authentication
- Security features:
  - PAP (Password Authentication Protocol)
  - CHAP (Challenge Handshake Authentication Protocol)
  - EAP (Extensible Authentication Protocol)

Point-to-Point Protocol (PPP)

- PAP (Password Authentication Protocol) (RFC 1334)
  - Authentication process is in plaintext
- CHAP (Challenge Handshake Authentication Protocol) (RFC 1994, replaces RFC 1334)
  - Protection against playback/replay attack (a valid data transmission is maliciously repeated) by using 3-way handshake:
    1. After link established, authenticator sends a “challenge” message to the peer
    2. Peer response with a value calculated using a “one-way hash” (with password)
    3. Authenticator calculate the expected hash value and match against the response (verify the password)
  - CHAP requires that the “secret” key be available in plaintext form. But the “secret” key is NOT send over the link

Point-to-Point Protocol (PPP)

- EAP (Extensible Authentication Protocol) (RFC 2284) supports multiple authentication mechanisms
- It provides some common functions and negotiation of authentication methods called EAP methods:
  - MD5-Challenge
  - One-Time Password (OTP)
  - Generic Token Card
- Protection against playback attack by using 3-way handshake:
  1. After link established, authenticator sends a authentication request message to the peer
  2. Peer send response with a set of values that matches authentication mechanism of the authenticator
  3. Authenticator calculates the expected value and match against the response

Address Resolution Protocol (ARP) & Reverse ARP (RARP)

- ARP (Address Resolution Protocol) maps IP addresses (logical addresses) to MAC addresses (physical addresses) (RFC 826)
- RARP (Reverse ARP), opposite of ARP, maps MAC addresses to IP addresses. (RFC 903)
- Preserving integrity of ARP table is the key to security of switching topology.

Address Resolution Protocol (ARP) & Reverse ARP (RARP)

ARP Table is vulnerable to…

- Man-in-the Middle Attack
  - A hacker can exploit ARP Cache Poisoning to intercept network traffic between two devices in your network.
- MAC Flooding Attack
  - *MAC Flooding* is an ARP Cache Poisoning technique aimed at network switches. By flooding a switch's MAC-Port table with a ton of spoofed ARP replies, a hacker can overload network switch and put it in “hub” mode. Then the hacker can packet sniff your network while the switch is in "hub" mode.

Reference: DISA FSO *Network STIG*

Address Resolution Protocol (ARP) & Reverse ARP (RARP)

To preserve integrity of ARP table…

- Logical Access Control:
  - Static ARP table. Not scalable, but very effective.
  - Enable port security using sticky MAC address. Write the dynamically learned MAC addresses into memory of device. It will be the same after reboot.
- Physical Access Control:
  - Disable all Interfaces Not In-Use.
  - Enable Interface only when Ready-To-Use.

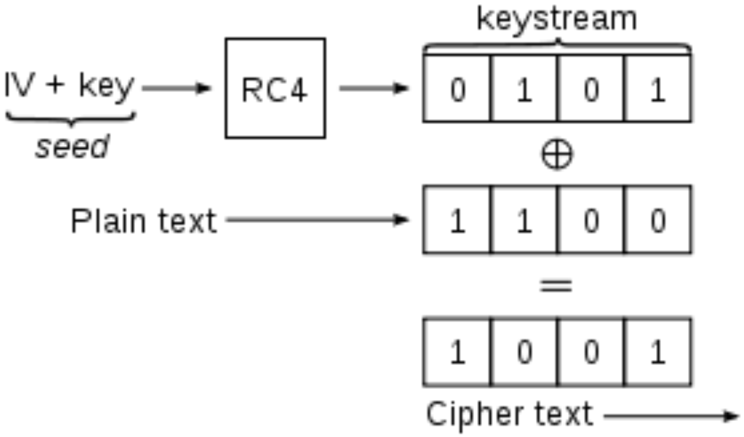
Reference: DISA FSO *Network STIG*

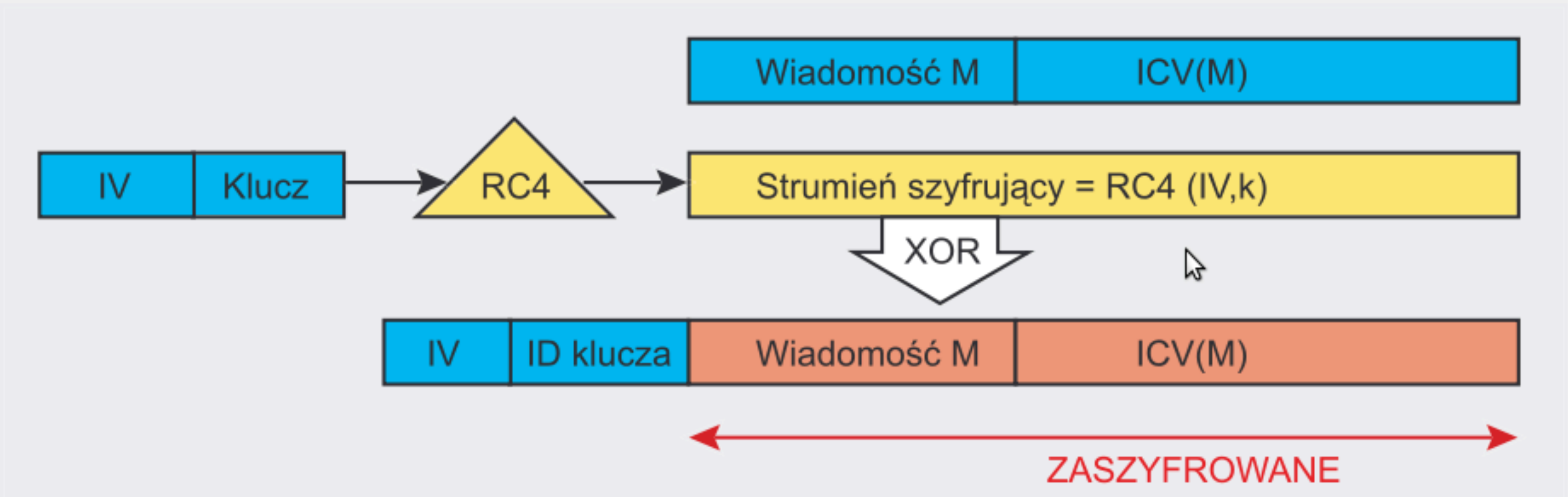
Wired Equivalent Privacy (WEP)

- WEP (Wired Equivalent Privacy) is an optional IEEE 802.11 encryption standard.
  - Implemented at the MAC sub-layer
  - Use RSA's RC4 stream cipher with variable key-size
  - Shared symmetric key, 40-bit! (104-bit is not a standard!) with 24-bit IV (Initialization Vector)
  - Use the same static key to encrypt all communications
- Security issue with WEP…
  - Size of IV (24-bit) +
  - Shared static symmetric key (40-bit or 104-bit)
  - Hacker can collect enough frames in same IV and find out the symmetric key (i.e. related key attack)
- Mitigation:
  - IPsec over 802.11
  - IEEE 802.11i and IEEE 802.1X

Reference: http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

WEP - scheme





C = [M || ICV(M)] + [RC4(K || IV)]

WPA (Wi-Fi Protection Access)

- WPA is an improvement over WEP in that it does not use the same static key to encrypt all communications. Instead, it negotiates a unique key set with each host. The key is randomly changend from the defined set of keys for the host.

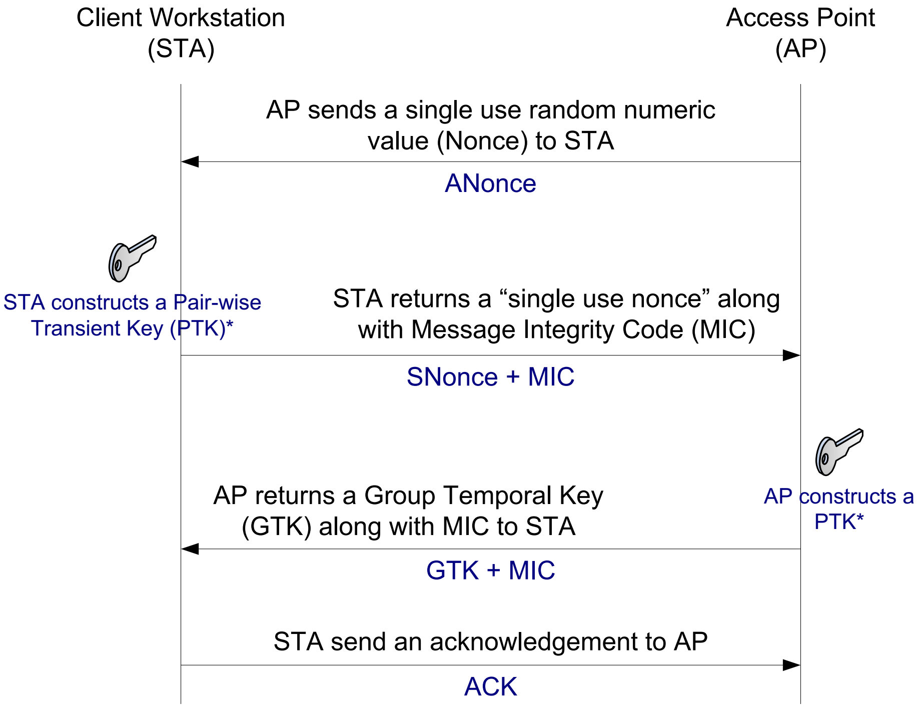
- Use TKIP/RC4 for encryption

Modes:

1. Enterprise – EAP, 802.1X, Radius
2. Personal - PSK (*Pre-Shared Key)*

WPA2 - IEEE 802.11i

- IEEE 802.11i (WPA2) standard
- Uses IEEE 802.1X (i.e. EAP) for authentication.
- Uses 4-way handshake for key management.
- Uses AES-based CCMP (Counter-mode Cipher-block-chaining Message authentication code Protocol).

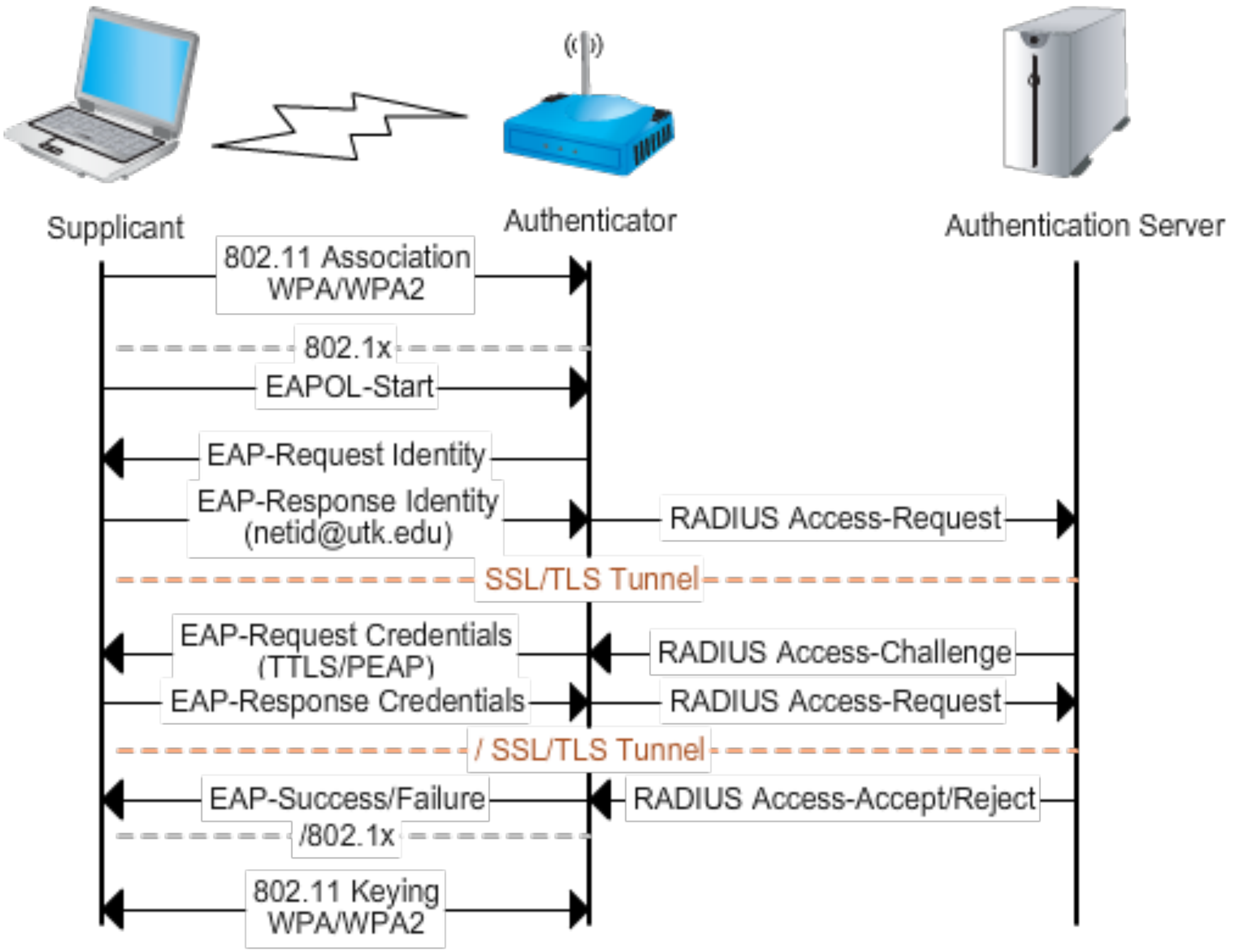

Client Workstation (STA)
Access Point (AP)
AP sends a single use random numeric value (Nonce) to STA
ANonce
STA constructs a Pair-wise Transient Key (PTK)*
STA returns a “single use nonce” along with Message Integrity Code (MIC)
SNonce + MIC
AP constructs a PTK*
AP returns a Group Temporal Key (GTK) along with MIC to STA
GTK + MIC
STA send an acknowledgement to AP
ACK

* As soon as the PTK is obtained it is divided into 3 separate keys:

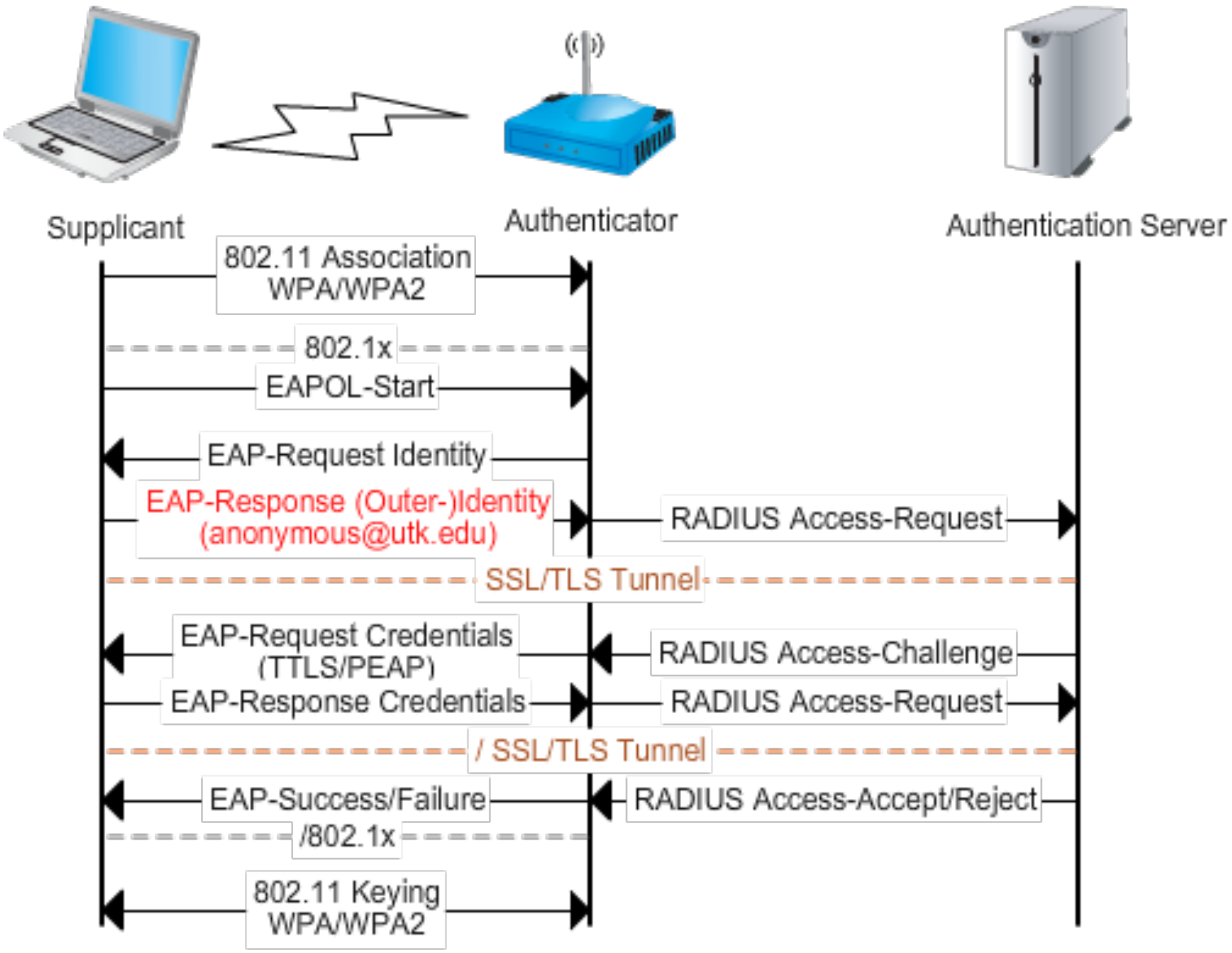
- EAP-KCK (Extended Authentication Protocol-Key Confirmation Key)
- EAP-KEK (Key Encryption Key)
- TK (Temporal Key) – The key used to encrypt the wireless traffic.

Reference:
- Q&A, Wi-Fi Protected Access, WPA2 and IEEE 802.11i, Cisco Systems
- http://en.wikipedia.org/wiki/IEEE_802.11i

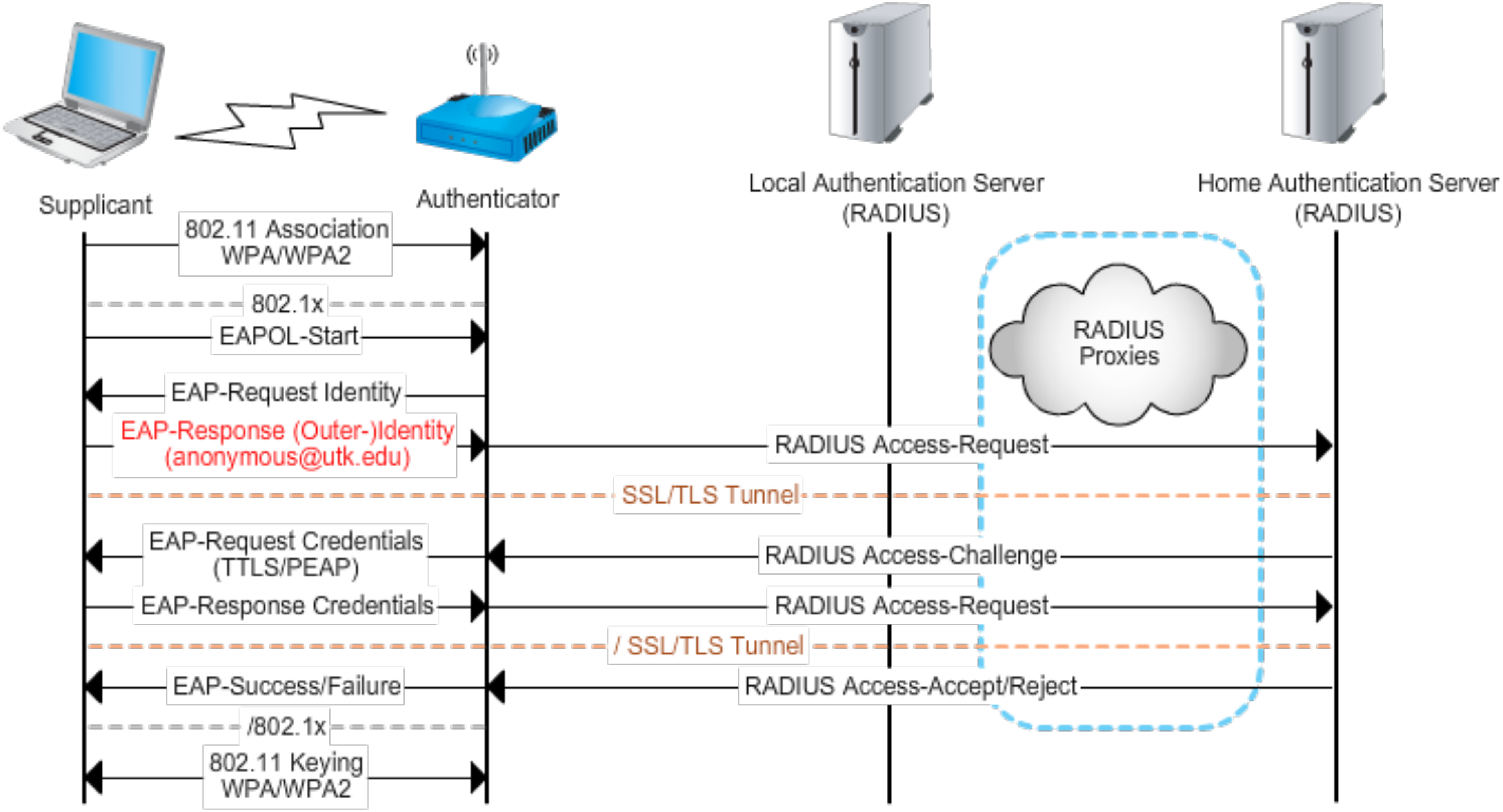
Authentication with 802.1x over 802.11 with EAP details



Authentication with 802.1x over 802.11 with an anonymous outer-identity

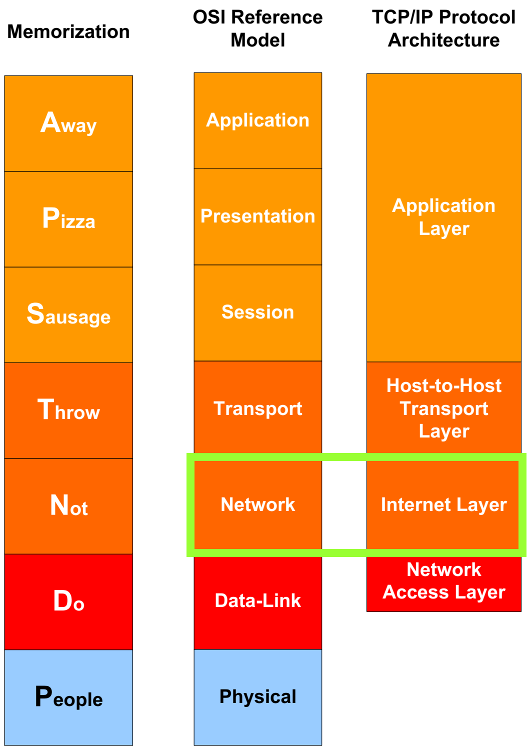


Authentication with 802.1x over 802.11 with RADIUS proxying



Telecommunications & Network Security Domain – Part 2

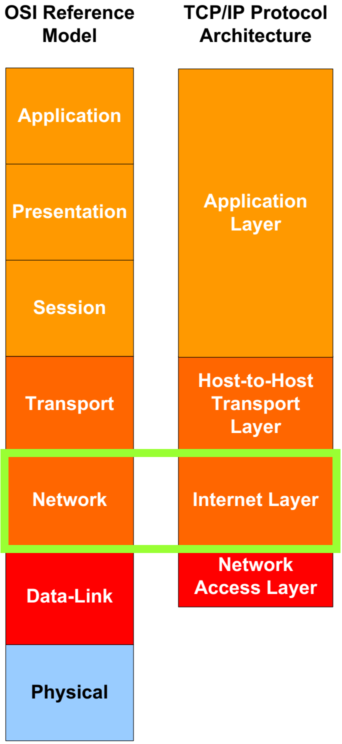
- Security Countermeasures and Controls
  - Physical Layer
  - Data-Link Layer
  - IP Network Layer
  - Transport Layer
  - Application Layer
- VPN
- NAS



Memorization	OSI Reference Model	TCP/IP Protocol Architecture
Away	Application	Application Layer
Pizza	Presentation	
Sausage	Session	
Throw	Transport	Host-to-Host Transport Layer
Not	Network	Internet Layer
Do	Data-Link	Network Access Layer
People	Physical	

Security of Network Layer – Review

- Logical Addressing (IP address)
- Controls: ICMP, ARP, RARP
- Routing: Static, Dynamic
- Routing Protocols:
  - Interior Gateway Protocols (IGP's)
  - Exterior Gateway Protocols (EGP's)



Network Address Translation (NAT)

NAT (Network Address Translation) is a method of connecting multiple computers to the Internet (or any other IP network) using one IP address.

- The increased use of NAT comes from several factors:
  - Shortage of IP addresses
  - Security needs
  - Ease and flexibility of network administration
- RFC 1918 reserves the following private IP addresses for NAT
  - Class A: 10.0.0.0 – 10.255.255.255
  - Class B: 172.16.0.0 – 172.31.255.255
  - Class C: 192.168.0.0 – 192.168.255.255

Reference: http://www.ietf.org/rfc/rfc1918.txt

Routing: Static vs. Dynamic

Preserving integrity of route table is the key to security of routing topology.

- Static routing is the most secure routing configuration. However, scalability is a major drawback.
  - Static Route Table, no automatic updates.
- Dynamic routing is scalable, but need to establish security policy to preserve integrity of route table
  - Automatic updates.
  - Need to set thresholds.
  - Authenticate neighbors and peers.

Dynamic Routing

There are two types of routing protocols:

- Interior Gateway Protocols (IGPs)
  - Routing Information Protocols (RIP)
  - Interior Gateway Routing Protocol (IGRP)
  - Enhanced IGRP (EIGRP, Cisco proprietary)
  - Open Shortest Path First (OSPF)
  - Intermediate System to Intermediate System (IS-IS)
- Exterior Gateway Protocols (EGPs)
  - Exterior Gateway Protocol (EGP, RFC 827). EGP is no longer in use for Internet
  - Border Gateway Protocol (BGP). BGP is the standard routing protocol for Internet

MD5 Authentication

- You can configure MD5 authentication between two peers, meaning that each segment sent on the TCP connection between the peers is verified.

- MD5 authentication must be configured with the same password on both peers; otherwise, the connection between them will not be made.

- Configuring MD5 authentication causes the Cisco IOS software to generate and check the MD5 digest of every segment sent on the TCP connection.

Security of Network Equipment

- Physical Access Control
  - Dedicated access ports for management
    - Console Port, Auxiliary Port, VTY (Virtual TTY) Port.
  - Dedicated monitoring I/Fs for SNMP
    - Use SNMPv3: default community strings, provides message integrity/authentication by using an MD5 or SHA-1 HMAC using the password as the key
    - SNMPv3 packets are encrypted using either the Data Encryption Standard (DES) or the Advanced Encryption Standard (AES)
    - SNMPv2c: community strings as “password” transmitted in plain text, no encryption.
- Logical Access Control
  - Set password & privilege levels.
  - Implement AAA (Authentication, Authorization & Accountability).
  - Implement centralized authentication & authorization mechanism: TACACS+ or RADIUS.

Reference: DISA FSO *Network STIG*

Security of Network Equipment

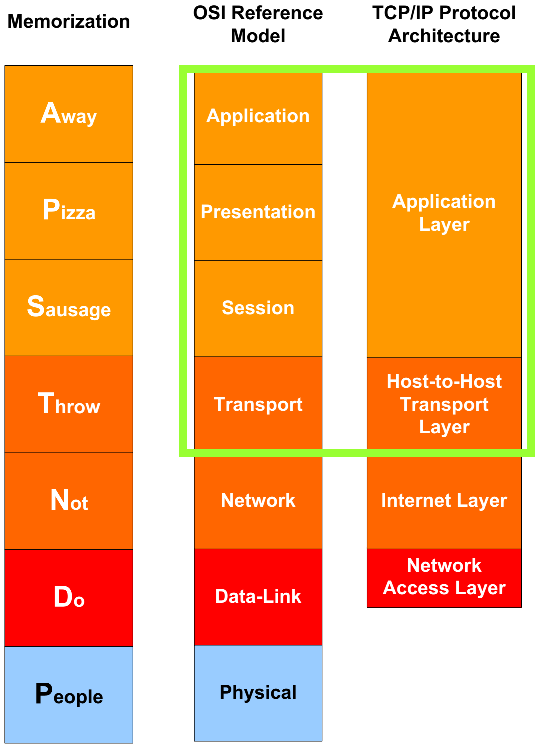
- Time synchronization
  - Use multiple time sources.
  - Use NTP for all Layer 3 equipment to synchronize their time.
  - Use NTP authentication between clients, servers, and peers to ensure that time is synchronized to approved servers only.
- Event Logging
  - Configure key ACLs to record access violations.
  - Example: Anti-spoofing violations, VTY access attempts, Router filter violations, ICMP, HTTP, SNMP…etc.

Reference: DISA FSO *Network STIG*

Topics

Telecommunications & Network Security Domain – Part 2

- Security Countermeasures and Controls
  - Physical Layer
  - Data-Link Layer
  - IP Network Layer
  - Transport Layer
  - Application Layer
- VPN
- NAS

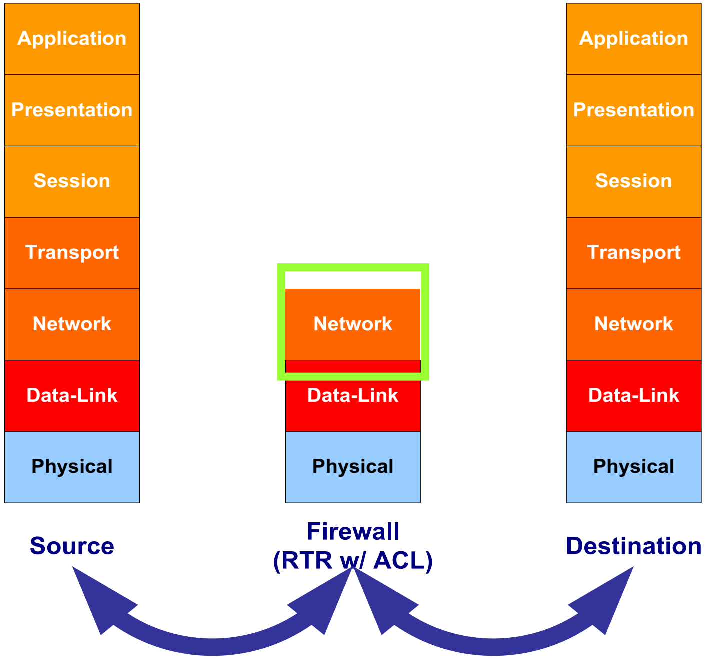


Firewalls

1. Static Packet-filtering firewall
2. Stateful inspection firewall (Dynamic packet filtering firewall)
3. Proxy firewall (Application-level gateway firewall)

Static Packet-filtering firewall

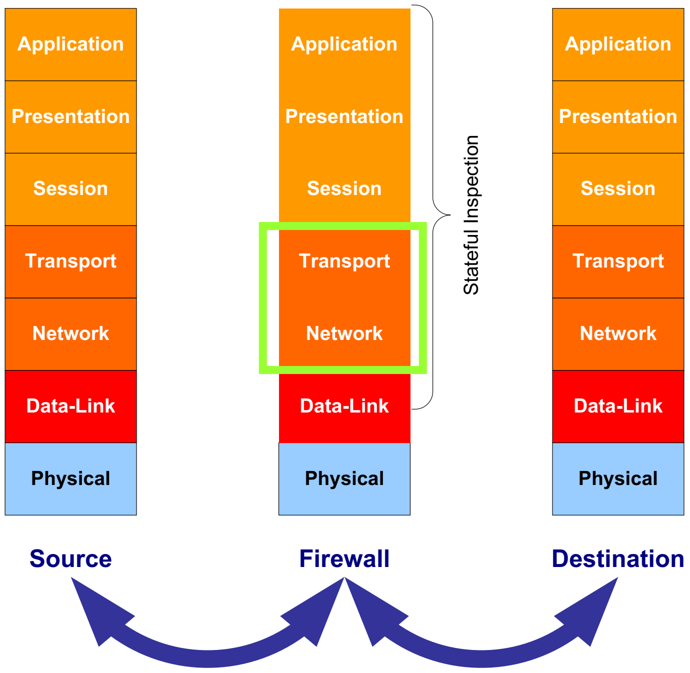
- Router ACL's ~ Packet-filter firewall
- Do not examine Layer 4-7 data. Therefore it cannot prevent application-specific attacks
- Firewall Policy: Deny by default, Permit by exception
  - Understand the data-flow (i.e. source, destination, protocols, and routing methods), so the security engineer knows how to apply IP filtering
  - Knows the specific inbound and outbound I/F's
  - Disable all un-necessary protocols & services



Source: DISA FSO *Network STIG*

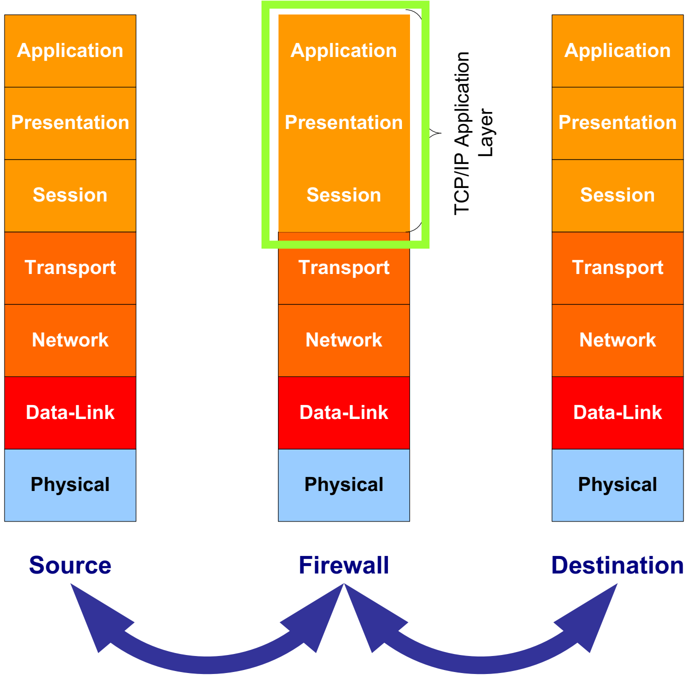
Stateful inspection firewalls (Dynamic packet filtering firewall)

- Layer 3-4 of OSI model
- Evaluate the state or the context of network traffic
- It’s faster than proxy firewall and more flexible because it examines TCP/IP protocols not the data
- Unlike proxy firewall, it does not rewrite every packets and does not “talk” on application server’s behalf



Proxy firewalls (Application-level gateway firewall)

- examining packets at the application layer
- Able to analyze application commands inside the payload (datagram)
- Do not allow any direct connections
- copies packets from one network into another; the copy process also changes the source and destination addresses to protect the identity
- This type of firewall negatively affects network performance because each packet must be examined and processed as it passes through the firewall between internal and external computing hosts
- Supports user-level authentications. Able to keep a comprehensive logs of traffic and specific user activities

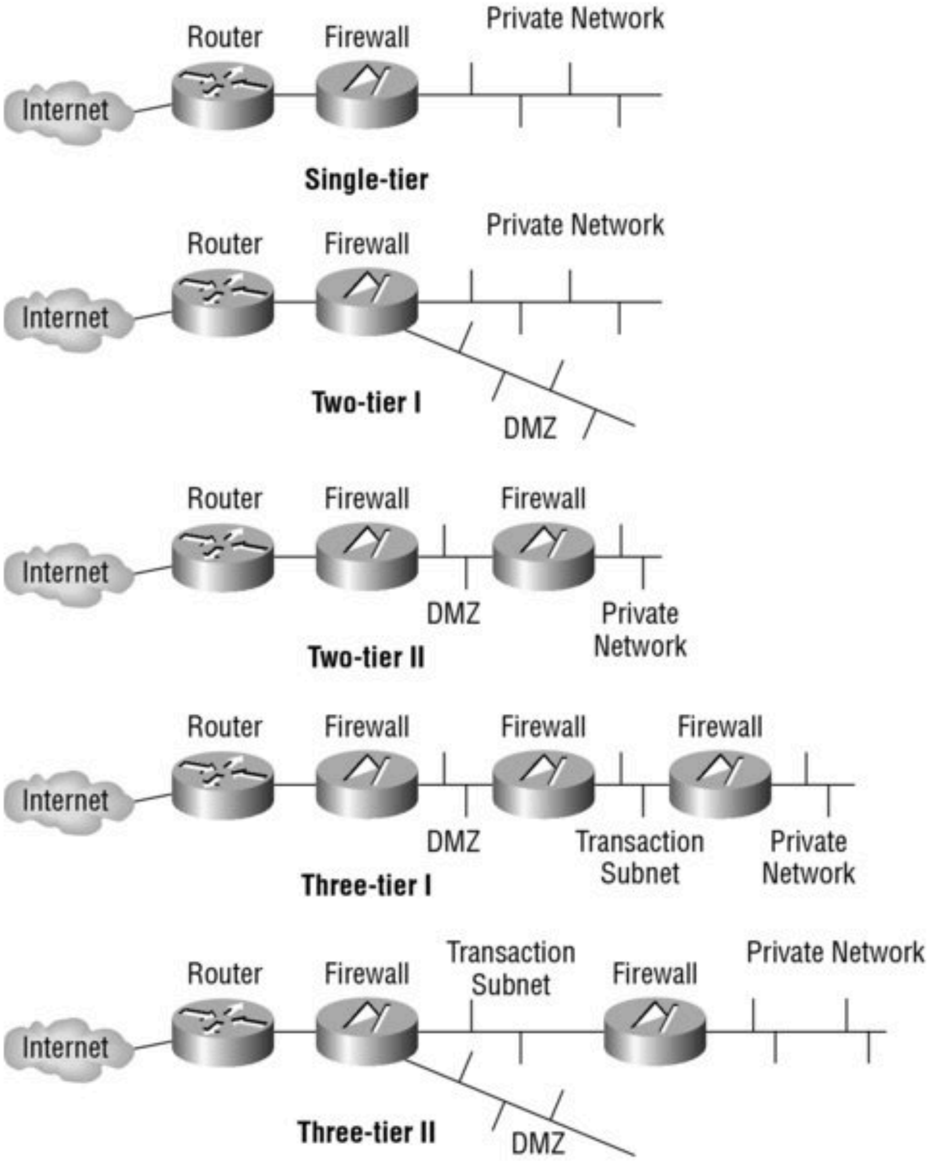


Firewall Deployment Architectures

- There are three commonly recognized firewall deployment architectures: single tier, two tier, and three tier
- Single tier: private network behind a firewall (useful for generic attack only, minimum protection)
- Two tier I: Firewall with three or more interfaces
- Two tier II: Two Firewalls in a series.

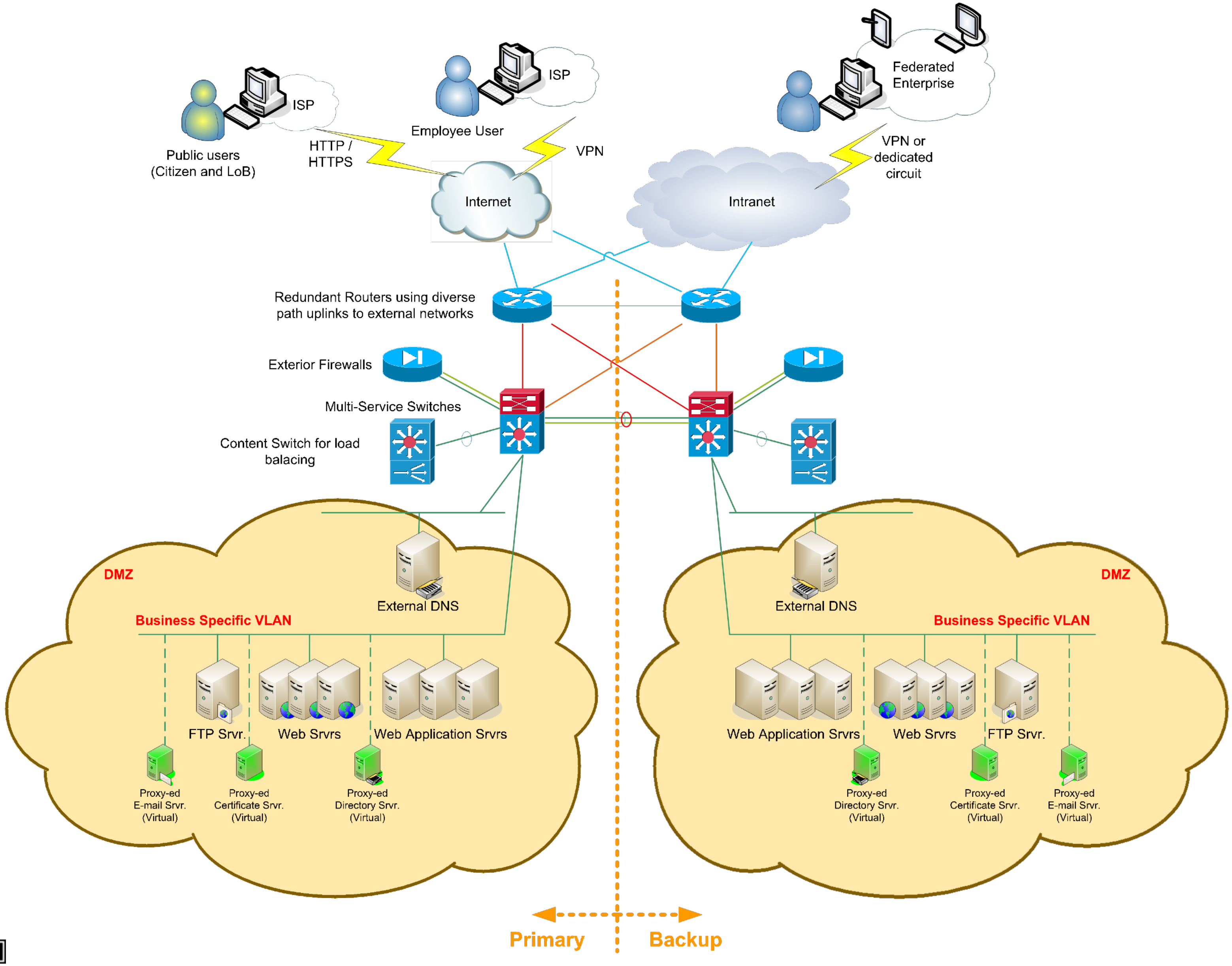
  DMZ – demilitarized zone (is designed to systems like web servers that must be accessible from both the internal and external networks – private network and Internet)
- Three tier - is the deployment of multiple subnets between the private network and the Internet separated by firewalls.
  - A middle subnet can serve as a transaction subnet where systems needed to support complex web applications in the DMZ reside.
  - The third, or back-end, subnet can support the private network.
  - the most secure; however, it is also the most complex to design, implement, and manage.

Firewall Deployment Architectures



Security of Transport & Application Layers

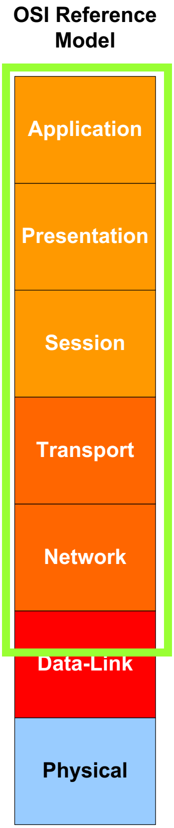
Network Design with Firewalls



Firewall Policy

In principal, firewall performs three actions:

- *Accept*: where the firewall passes the IP packets through the firewall as matched by the specific rule
- *Deny/Reject*: where the firewall drops the IP packets when not matched by the specific rule and return an error message to the source system. (log entries are generated)
- *Discard/Drop*: where the firewall drops the IP packets, and not return an error message to the source system. (i.e., Like a "black hole")



Intrusion Detection System (IDS) & Intrusion Prevention System (IPS)

- Network-IDS (Intrusion Detection System) is a “passive” device
  - To detect attacks and other security violations
  - To detect and deal with pre-ambles to attacks (i.e., probing / scanning)
  - To document the threat to a network, and improve diagnosis, recovery and correction of an unauthorized intrusion
  - Passive method - Notifications can be sent to administrators via email, text or pager messages, or pop-up messages.

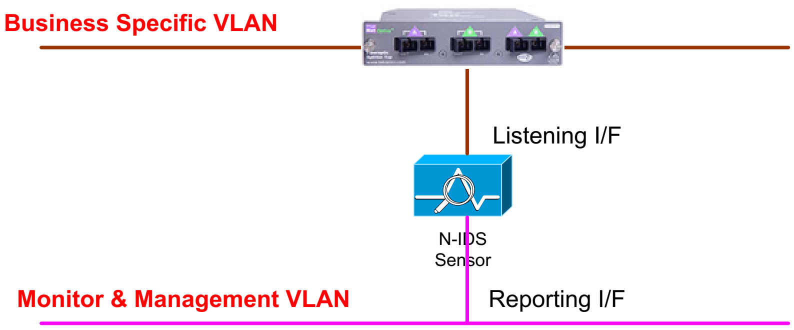
- Network-IPS (Intrusion Prevention System) is a “in-line” device
  - Has all the same service features of a N-IDS, plus
  - Inference the internetworking “behavior” to PREVENT further damage to internetworking services
  - Active responses can modify the environment using several different methods

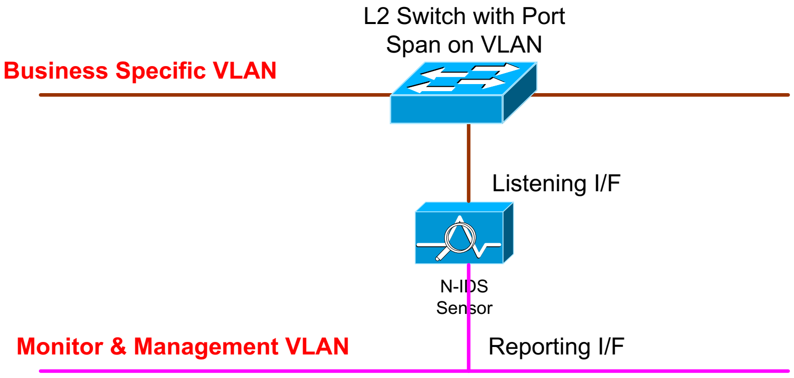
Intrusion Detection System (IDS) & Intrusion Prevention System (IPS)

- Knowledge-based method ("signature-based") methodology to detect intrusions
  - Uses a database of known attacks and vulnerabilities called signatures
  - Only as good as the last signature update
  - Can be difficult to tune – false positives, acceptable behavior.
- Behavior-based methodology to detect and prevent intrusions.
  - Learns normal network or host behavior
  - Alerts when behavior deviates from the norm such as malformed packets, abnormal network utilization, or memory usage

Network-based Intrusion Detection System (N-IDS)

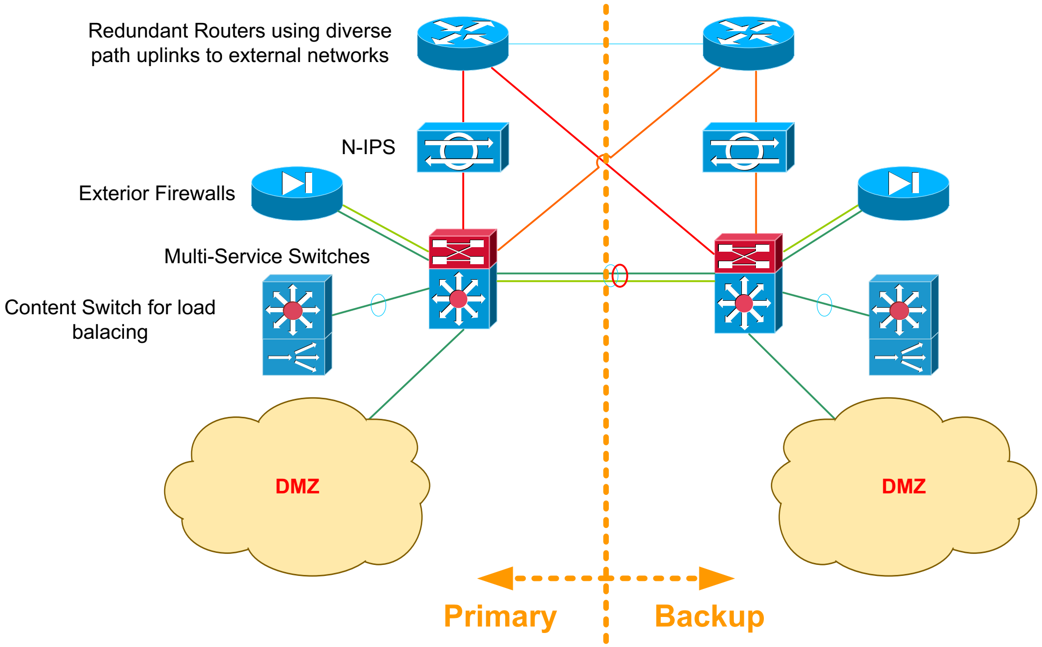
- Network-IDS (intrusion detection system) – deployment architecture
  - There are two way to setup the listening interfaces: Network TAP (hardware device between two points) and VLAN Port Spanning on L2 switch





Network-based Intrusion Prevention System (N-IPS)

- Network-IPS (intrusion prevention system) is an “in-line”- deployment architecture
  - it may block some “normal” enterprise internetworking LAN traffic. So, it’s best to use it between the edge router and exterior perimeter firewall


Redundant Routers using diverse path uplinks to external networks
N-IPS
Exterior Firewalls
Multi-Service Switches
Content Switch for load balacing
DMZ
DMZ
Primary
Backup

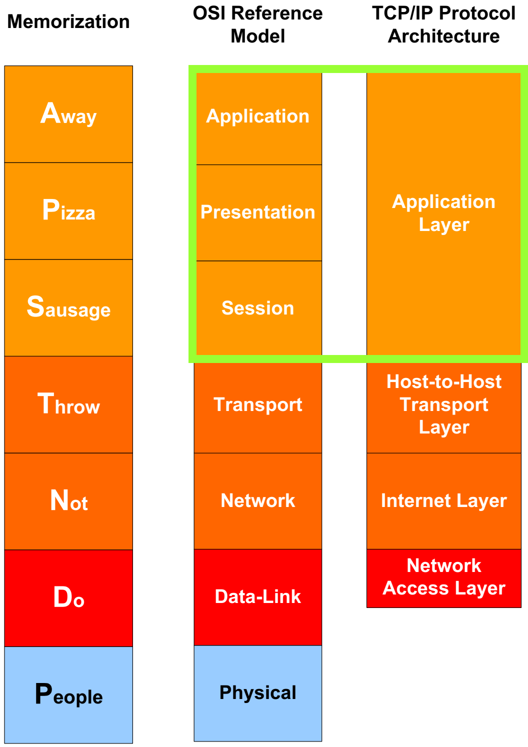
Honeypots/ Honeynets

- Honeypots are individual computers created as a trap for intruders.
- Honeynet is two or more networked honeypots used together to simulate a network.
- They look and act like legitimate systems, but they do not host data of any real value for an attacker.
- Administrators often configure honeypots with vulnerabilities to tempt intruders into attacking them.
- The goal is grab the attention of intruders and keep the intruders away from the legitimate network that is hosting valuable resources.
- The longer the attacker spends with the honeypot, the more time an administrator has to investigate the attack and potentially identify the intruder

Topics

Telecommunications & Network Security Domain – Part 2

- Security Countermeasures and Controls
  - Physical Layer
  - Data-Link Layer
  - IP Network Layer
  - Transport Layer
  - Application Layer
- VPN
- NAS



Memorization	OSI Reference Model	TCP/IP Protocol Architecture
Away	Application	Application Layer
Pizza	Presentation	
Sausage	Session	
Throw	Transport	Host-to-Host Transport Layer
Not	Network	Internet Layer
Do	Data-Link	Network Access Layer
People	Physical	

Security of Application Layers – Computing Hosts

Protection of servers (network focused)…

- Be specific on service functions
  - Limit services, minimize potential exposures
  - Focus on a single function…

Web Server	Web Pages
DNS Server	DNS
E-mail Server	E-mail
DB Server	DB Services

- Install Host-IDS
- Install Anti-Virus
- Disable all processes/services not in use
- Enforce strict access control
  - Network I/Fs
  - OS / Applications

Security of Application Layers – S-HTTP vs. HTTPS

- S-HTTP (Secure HTTP) (RFC 2660) is an experimental protocol designed for use in conjunction with HTTP
  - S-HTTP is a Message-oriented secure communication protocol

- HTTPS is HTTP over SSL (Secure Socket Layer).
  - SSL works at the Transport Layer level
  - HTTP message is encapsulated within the SSL

Security of Application Layers – DNS

- Domain Name System (DNS) translates hostnames to IP addresses. BIND (Berkeley Internet Name Domain) is the most commonly used DNS server on the Internet
  - DNS server. It supplies domain name to IP address conversion
  - DNS resolver. When it can not resolve DNS request. It send a DNS query to another known DNS server
- Security issues with DNS:
  - HOSTS poisoning (static DNS) - If an attacker is able to plant false information into the HOSTS file
  - Caching DNS server attacks – A caching DNS server is any DNS system deployed to cache DNS information from other DNS servers.
  - DNS lookup address changing - sending an alternate IP address to the client to be used as the DNS server the client uses for resolving queries. Once the client has the wrong DNS server, they will be sending their queries to a hacker-controlled DNS server
  - DNS query spoofing, where the attacker spoofs the DNS server's answer with it's own IP address in source-address field
- Countermeasures:
  - Install HIDS, NIDS – watch DNS attack
  - Setup multiple DNS servers (External, internal)
  - Keep your BIND and OS up to date
  - Regularly review the logs of your DNS and DHCP system

Technical Countermeasures in IATF v3.1

Defense-In-Depth	Security Mechanism	Security Services
Defending the Network & Infrastructure	Redundant & Diverse Comm. Links	Availability
	Encryptors	Confidentiality, Integrity
	Routers	Access Control
Defending the Enclave Boundary	Firewalls	Access Control, Integrity
	Multi-Service & Layer 2 Switches	Access Control
Defending the Computing Environment	Network-based & Host-based IDS's	Integrity
	Hardened OS	Access Control, Integrity
	Anti-Virus Software	Access Control, Integrity
Supporting the Infrastructure	PKI (X.509-based Messaging: DMS)	Confidentiality: Access Control, Identification, Authentication, Integrity, Non-Repudiation

Security Services Spectrum:

- Access Control
- Confidentiality
- Integrity
- Availability
- Non-Repudiation

Reference & Guidelines:

- *Information Assurance Technical Framework (IATF), Release 3.1*
- DoDI 8500.2 *Information Assurance (IA) Implementation*

Topics

Telecommunications & Network Security Domain – Part 2

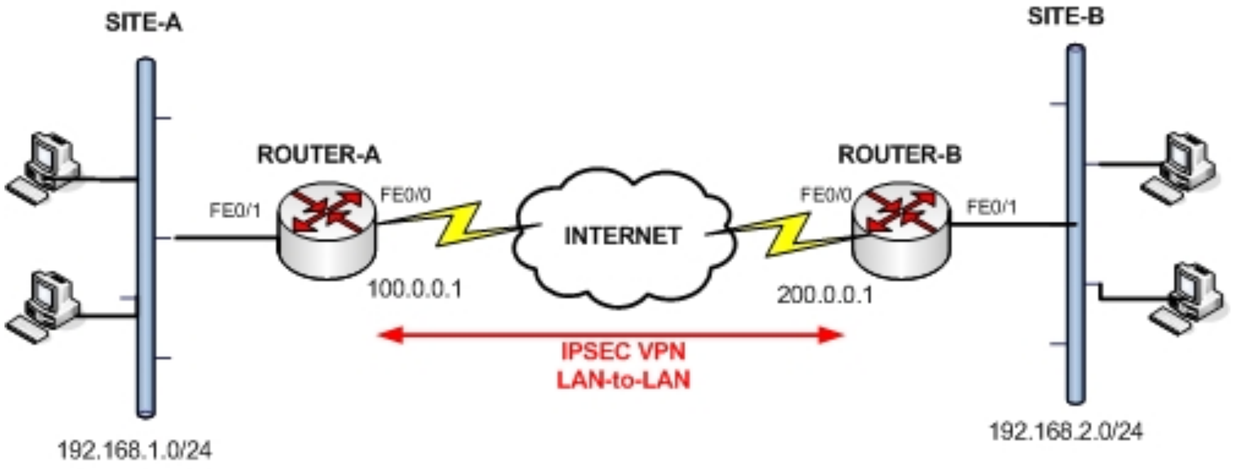
- Security Principles & Network Architecture
- Security Countermeasures and Controls
  - Physical Layer
  - Data-Link Layer
  - IP Network Layer
  - Transport Layer
  - Application Layer
- ➡ VPN
- NAS

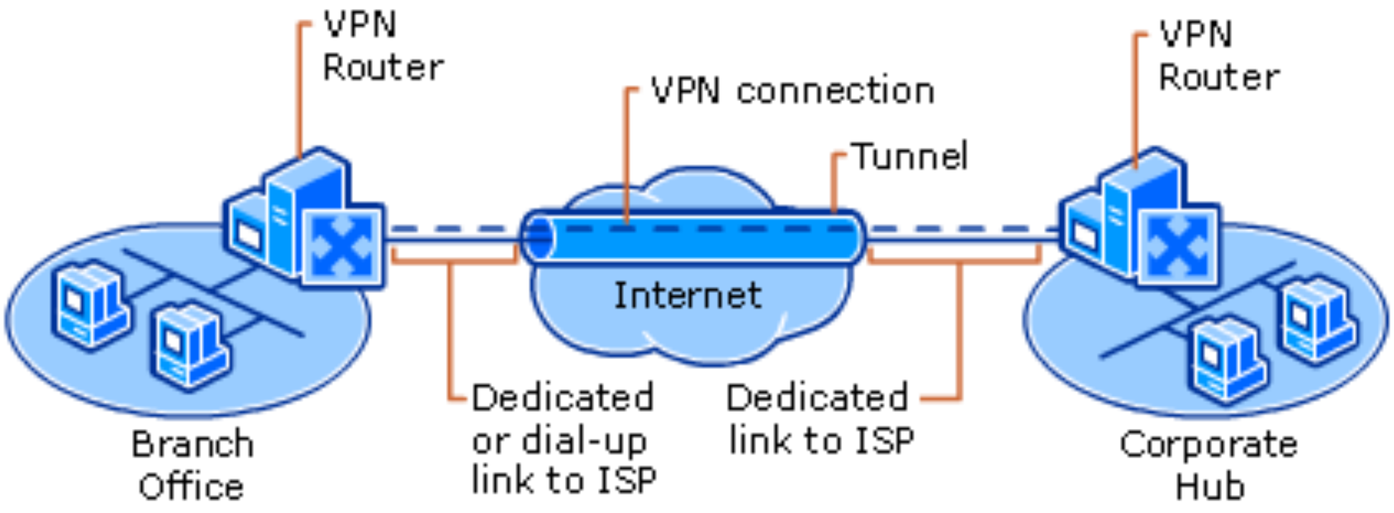
Virtual Private Network (VPN) & Tunneling

- Tunneling is used to "package/encapsulate" packets and transport them INSIDE of another packets from one internetworking domain to another.
- VPN enables the shared internetworking resources to be used as private or dedicated circuits. (i.e. Access Control)
  - Types of VPN:
    - LAN-to-LAN
    - Host-to-LAN
    - Host-to-Host
  - Example:
    - PPTP (Point-to-Point Tunneling Protocol)
    - L2TP (Layer 2 Tunneling Protocol)
    - MPLS (Multi-Protocol Label Switching)
    - GRE (Generic Routing Encapsulation)
    - IPsec (Internet Protocol Security)
    - SSH (Secure Shell)

Virtual Private Network (VPN) & Tunneling

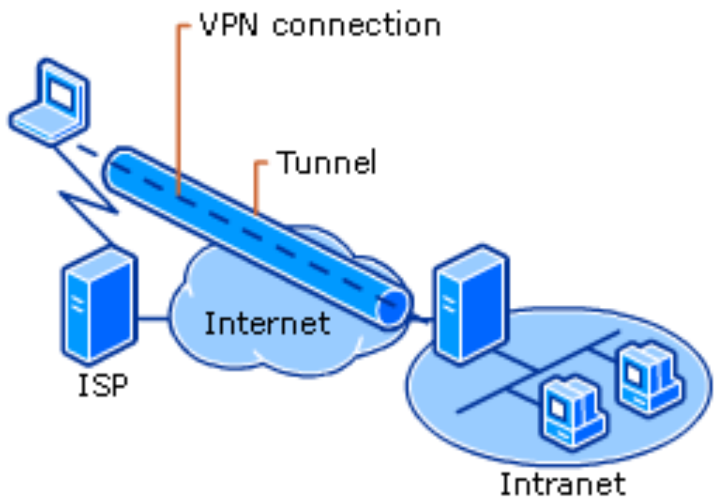
VPN Connecting Two Remote Sites Across the Internet



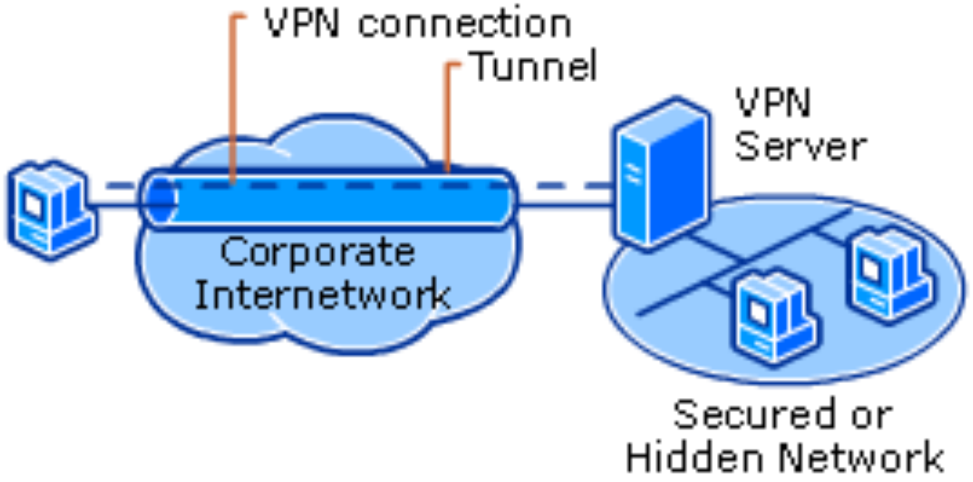


Virtual Private Network (VPN) & Tunneling

VPN Connecting a Remote Client to a Private Intranet



VPN Connection Allowing Remote Access to a Secured Network over an Intranet



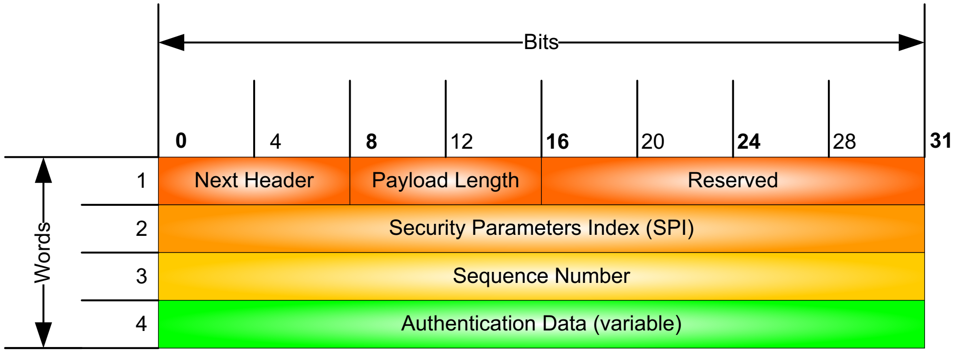
IPsec... (1/6)

IPsec is a protocol suite (RFC ~~2401~~ 4301, 2411).

- Transport Layer:
  - AH (IP Authentication Header) provides connection-less integrity, data origin authentication.
  - ESP (Encapsulating Security Payload) provides confidentiality through encryption and optionally authentication
- Application Layer: (RFC 4306)
  - IKE (Internet Key Exchange) is performed using ISAKMP (Internet Security Association and Key Management Protocol).

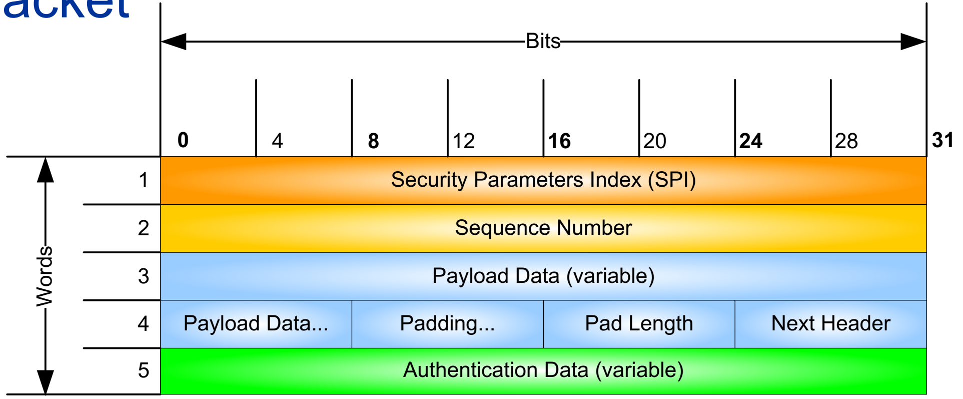
IPsec… (2/6)

- Authentication Header (AH) (RFC 4302)
  - AH follows right after IP header
  - Next Header: Identifies the protocol of transferred data
  - Payload Length: Size of AH packet
  - SPI: Identifies the security parameters, which in combination with the IP address, identify the security association implemented with this packet
  - Sequence Number: Used to prevent replay attacks
  - Authentication Data: Contains the integrity check value (ICV) to authenticate the packet



IPsec… (3/6)

- Encapsulating Security Payload (ESP) (RFC 4303)
  - ESP operates directly on top of IP header
  - SPI: Identifies the security parameters in combination with the IP address
  - Sequence Number: Used to prevent replay attacks
  - Payload Data: The encapsulated data
  - Padding: Used to pad the data for block cipher (addding 100……….0 – as required)
  - Pad Length: Necessary to indicate the size of padding
  - Next Header: Identifies the protocol of the transferred data
  - Authentication Data: Contains the integrity check value (ICV) to authenticate the packet



1	Security Parameters Index (SPI)			
2	Sequence Number			
3	Payload Data (variable)			
4	Payload Data...	Padding...	Pad Length	Next Header
5	Authentication Data (variable)			

IPsec... (4/6)

IPsec imposes computational performance costs on the host or security gateways.

- Memory needed for IPSec code and data structures
- Computation of integrity check values.
- Encryption and decryption.
- Use of SA/key management protocols, especially those that employ public key cryptography, also adds computational costs to use of IPSec

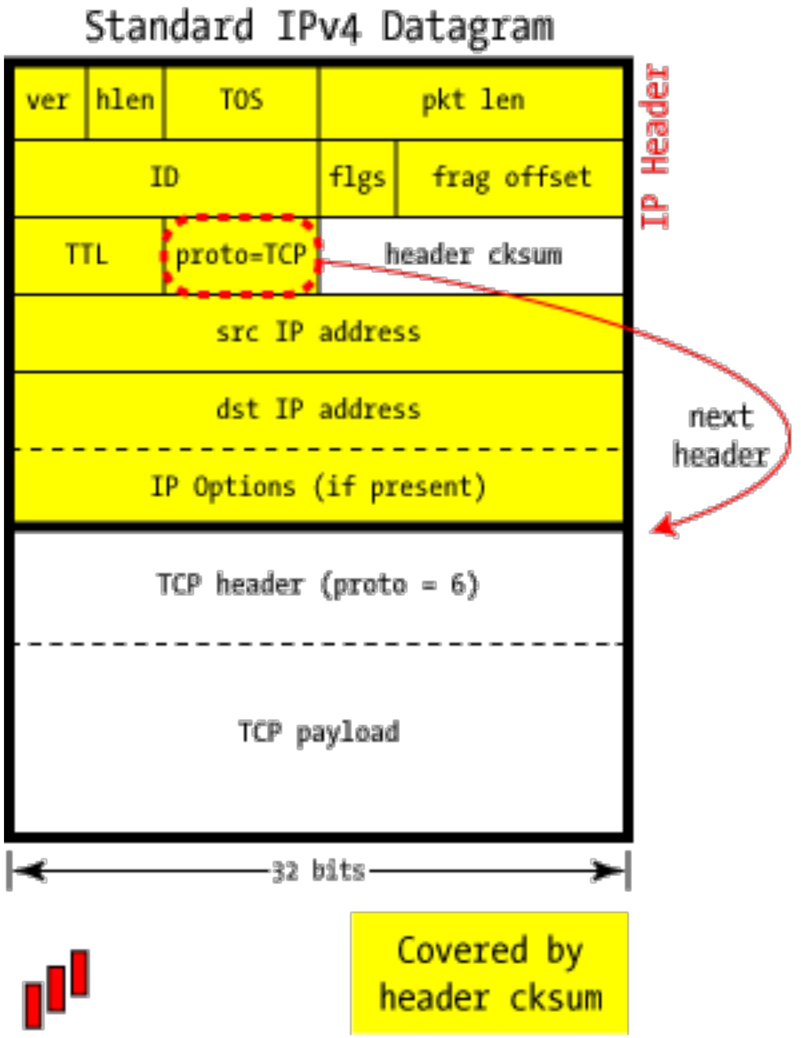
Reference: http://tools.ietf.org/html/rfc2411

IPsec… (5/6)

IPsec operates in two modes:

- Transport mode:
  - Only the payload is protected (i.e., encryption & hash)
  - IP headers are not encrypted
  - If AH is used then IP address can not be translated (i.e., NAT)
  - For host-to-host communications only
- Tunnel mode:
  - The payload and IP header are protected (i.e., encryption & hash)
  - Used for network-to-network, host-to-network, and host-to-host communications

Reference: http://en.wikipedia.org/wiki/IPsec



Standard IPv4 Datagram

ver | hlen | TOS | pkt len

ID | flgs | frag offset

TTL | proto=TCP | header cksum

src IP address

dst IP address

IP Options (if present)

IP Header

next header

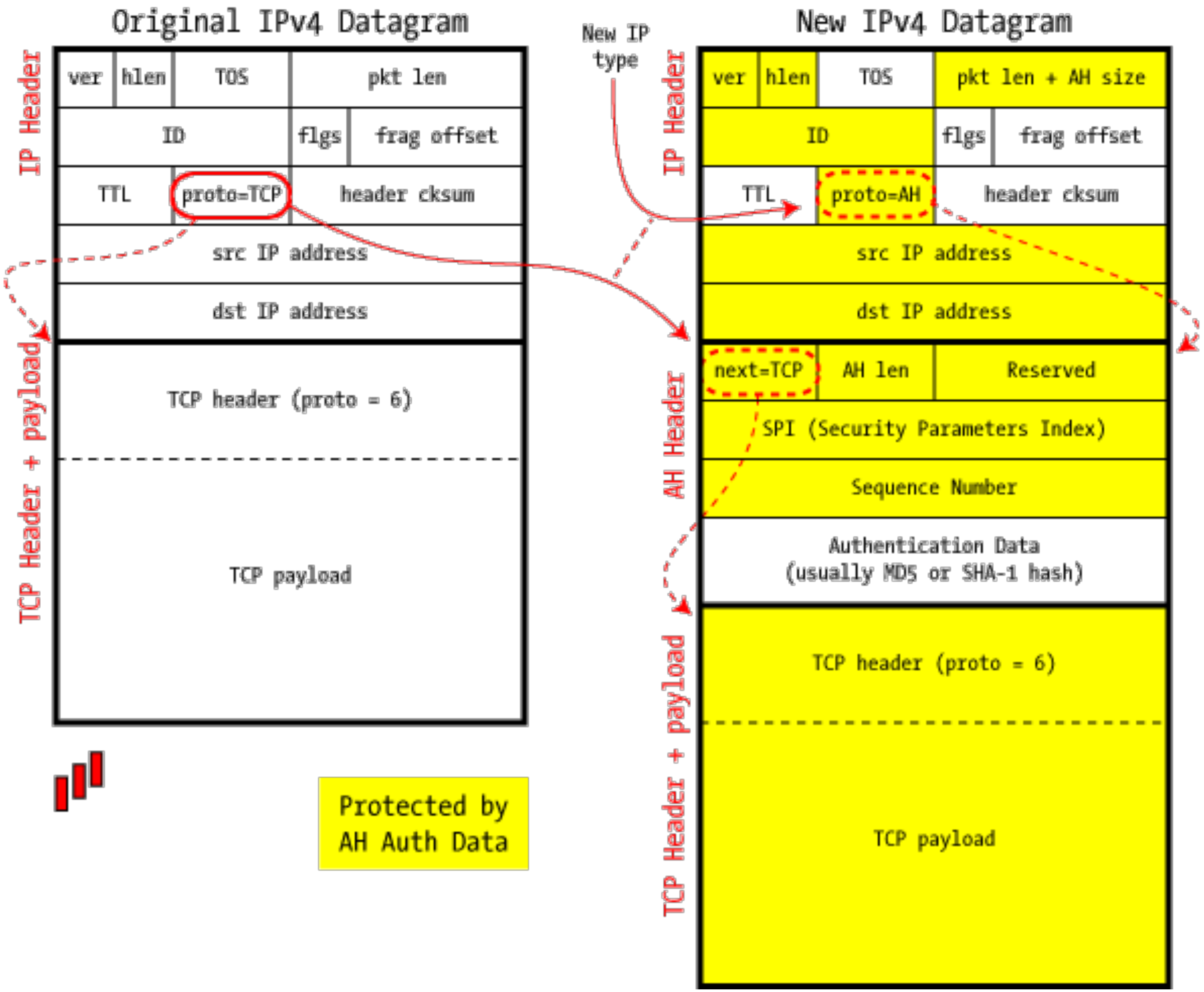
TCP header (proto = 6)

TCP payload

32 bits

Covered by header cksum

IPSec in AH Transport Mode



Original IPv4 Datagram

IP Header

ver | hlen | TOS | pkt len

ID | flgs | frag offset

TTL | proto=TCP | header cksum

src IP address

dst IP address

TCP Header + payload

TCP header (proto = 6)

TCP payload

New IP type

New IPv4 Datagram

IP Header

ver | hlen | TOS | pkt len + AH size

ID | flgs | frag offset

TTL | proto=AH | header cksum

src IP address

dst IP address

AH Header

next=TCP | AH len | Reserved

SPI (Security Parameters Index)

Sequence Number

Authentication Data
(usually MD5 or SHA-1 hash)

TCP Header + payload

TCP header (proto = 6)

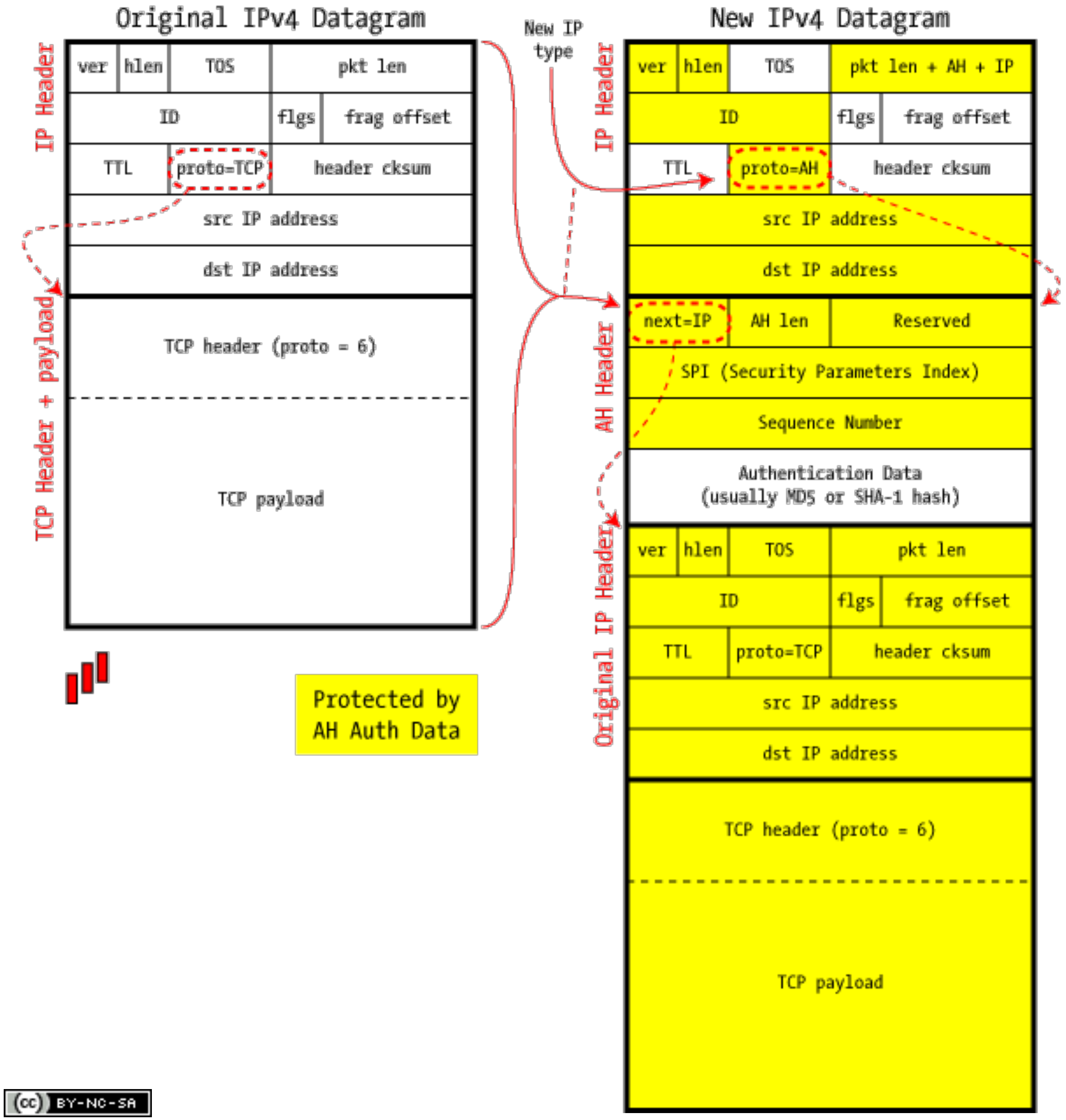
TCP payload

Protected by
AH Auth Data

Transport Mode, which is used to protect an end-to-end conversation between two hosts.

the IP packet is modified only slightly to include the new AH header between the IP header and the protocol payload (TCP, UDP, etc.)

IPSec in AH Tunnel Mode



Original IPv4 Datagram

IP Header

ver | hlen | TOS | pkt len

ID | flgs | frag offset

TTL | proto=TCP | header cksum

src IP address

dst IP address

TCP Header + payload

TCP header (proto = 6)

TCP payload

New IP type

New IPv4 Datagram

IP Header

ver | hlen | TOS | pkt len + AH + IP

ID | flgs | frag offset

TTL | proto=AH | header cksum

src IP address

dst IP address

AH Header

next=IP | AH len | Reserved

SPI (Security Parameters Index)

Sequence Number

Authentication Data (usually MD5 or SHA-1 hash)

Original IP Header

ver | hlen | TOS | pkt len

ID | flgs | frag offset

TTL | proto=TCP | header cksum

src IP address

dst IP address

TCP header (proto = 6)

TCP payload

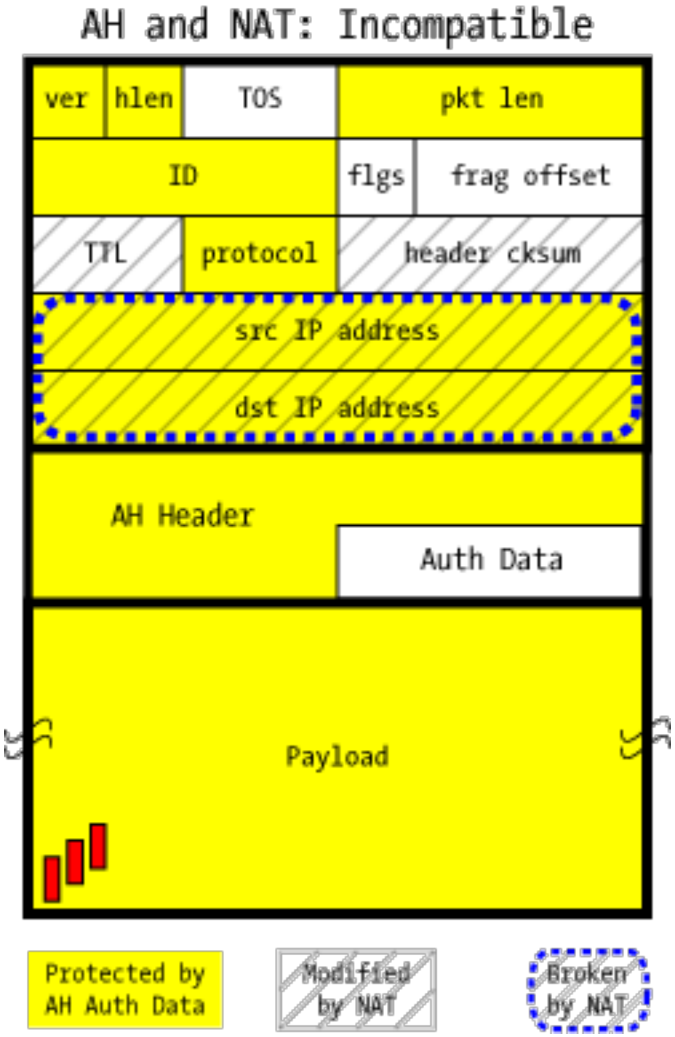
Protected by AH Auth Data

Entire IP packets are encapsulated inside another and delivered to the destination

This allows the source and destination addresses to be different from those of the encompassing packet:
This allows formation of a tunnel.

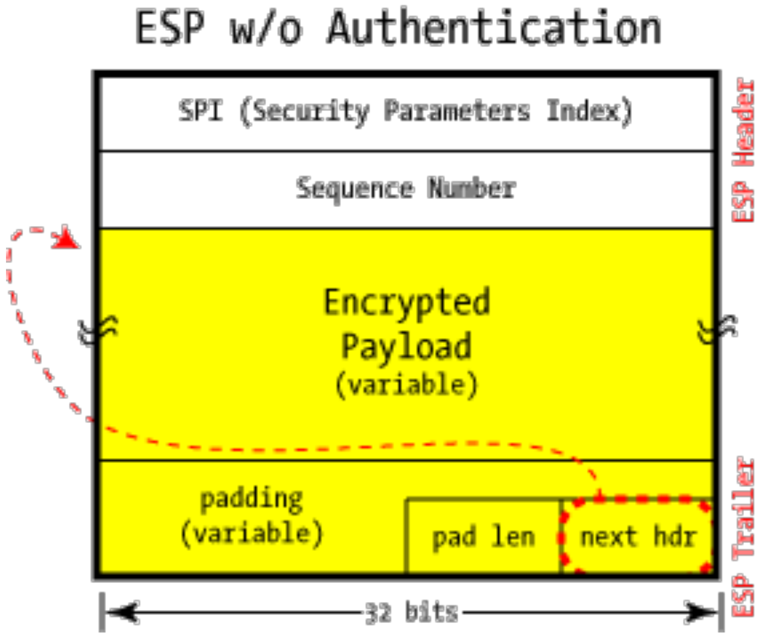
The reconstituted packet could be delivered to the local machine or routed elsewhere (according to the destination IP address found in the encapsulated packet), though in any case is no longer subject to the protections of IPsec. At this point, it's just a regular IP datagram.

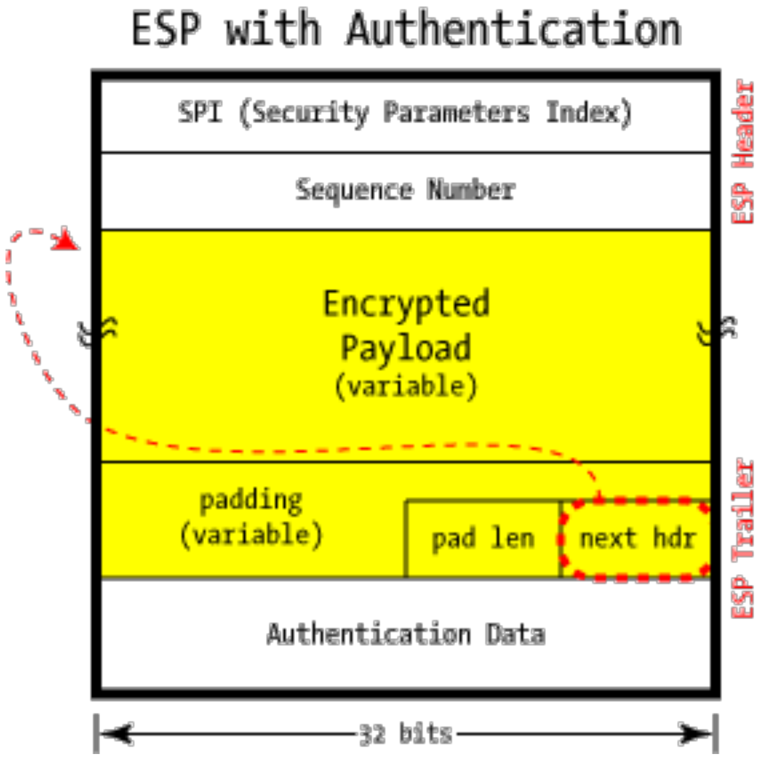
Tunnel mode is more typically used between gateways (routers, firewalls, or standalone VPN devices) to provide a Virtual Private Network (VPN).



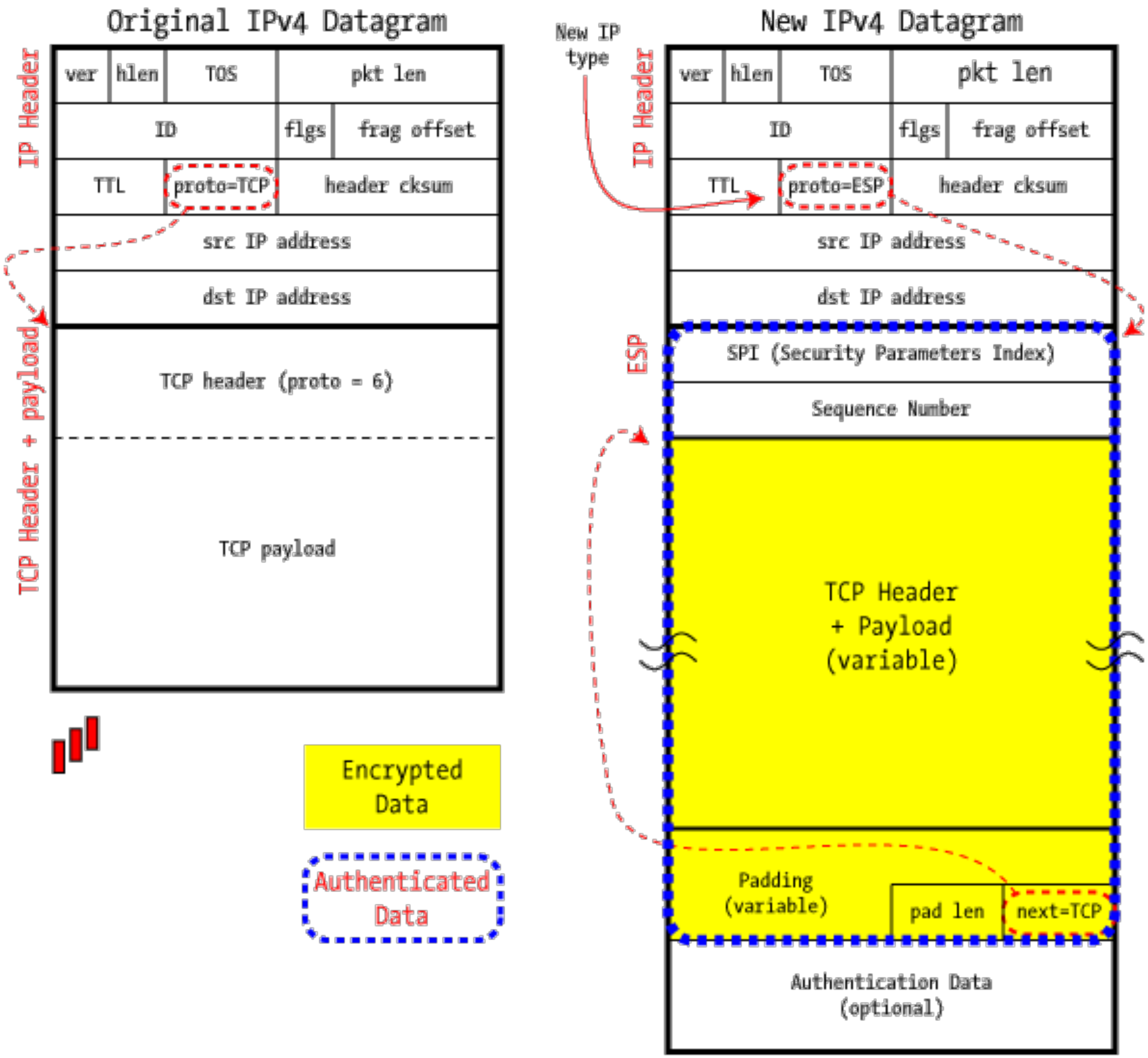
When the appropriate source or header IP address is changed, it forces a recalculation of the header checksum. This has to be done anyway, because the NAT device typically serves as one "hop" in the path from source to destination, and this requires the decrement of the TTL (Time To Live) field.

Because the TTL and header checksum fields are *always* modified in flight, AH knows to excludes them from coverage, but this does not apply to the IP addresses.
These are *included* in the Integrity Check Value, and any modification will cause the check to fail when verified by the recipient.
Because the ICV incorporates a secret key which is unknown by intermediate parties,
the NAT router is not able to recompute the ICV.


ESP w/o Authentication

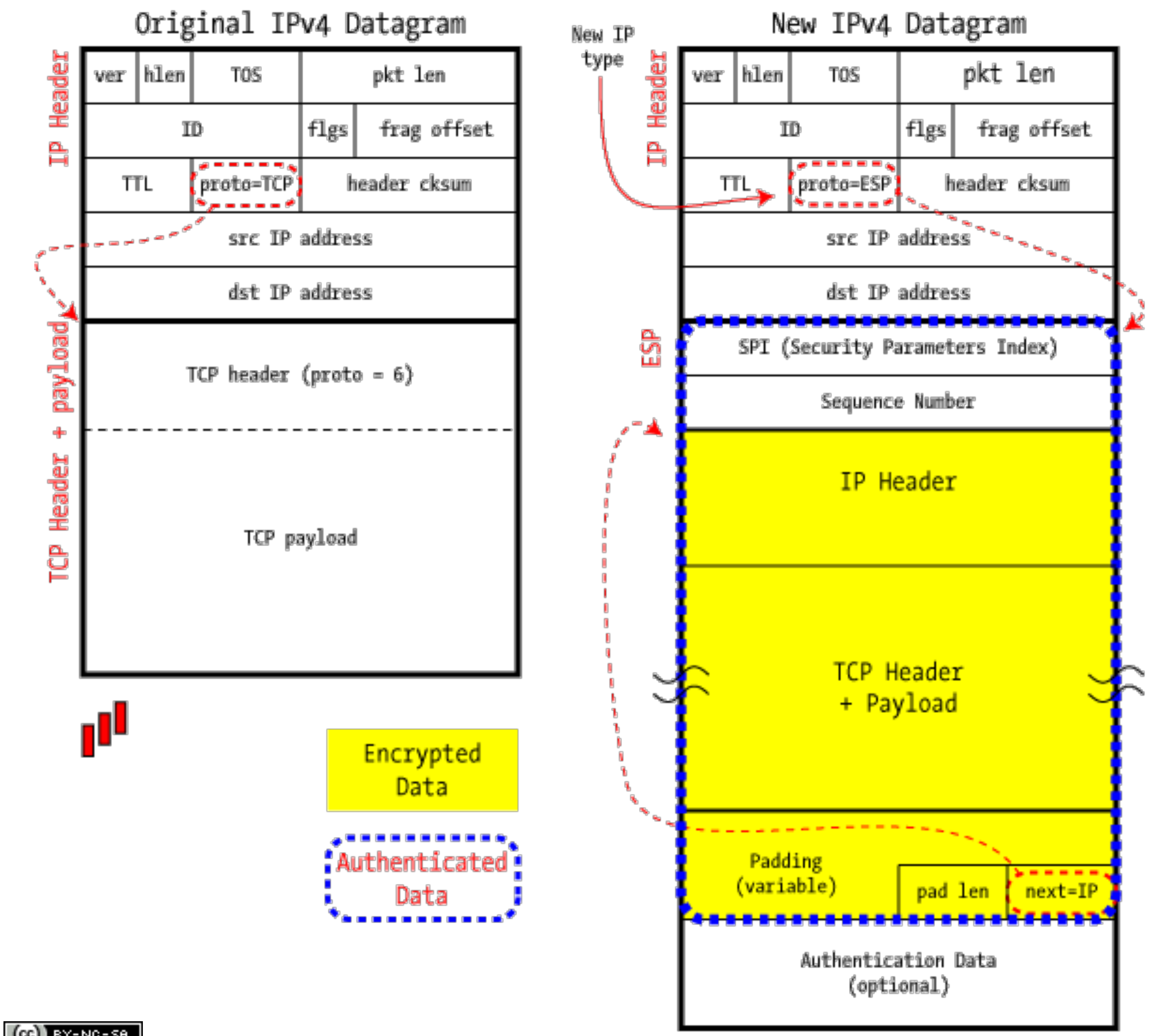

ESP with Authentication

IPSec in ESP Transport Mode



As with AH, Transport Mode encapsulates just the datagram's payload and is designed strictly for host-to-host communications.

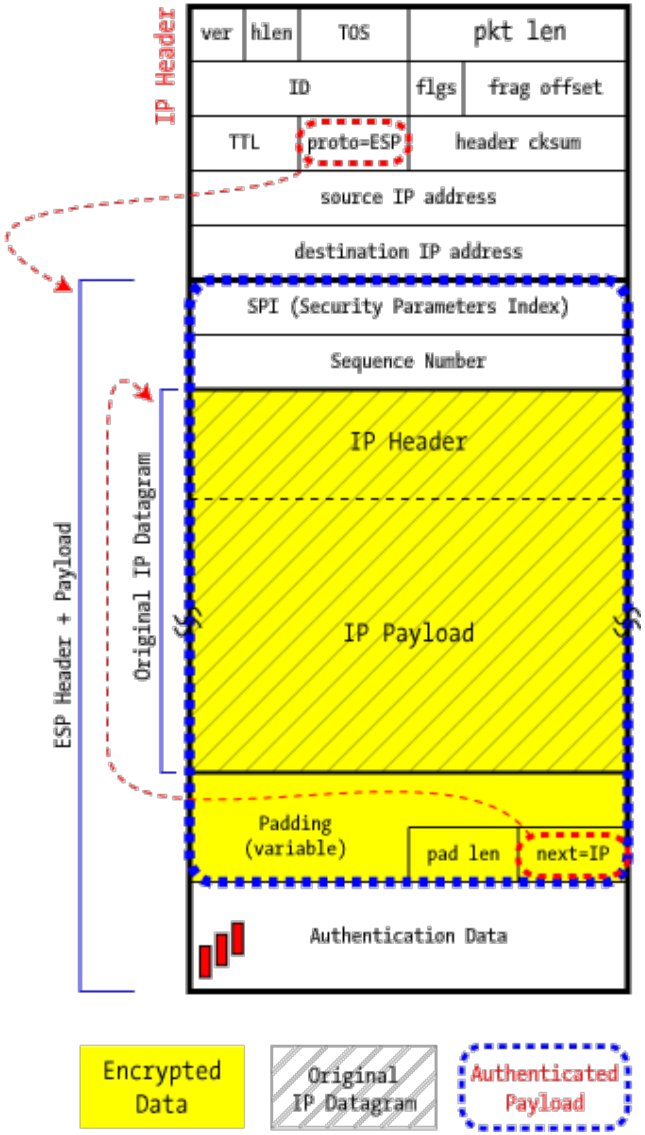
IPSec in ESP Tunnel Mode



Entire IP packets are encapsulated inside another and delivered to the destination

This allows the source and Destination addresses to be different from those of the encompassing packet: This allows formation of a tunnel.

ESP+Auth+Tunnel Mode
- Traditional VPN



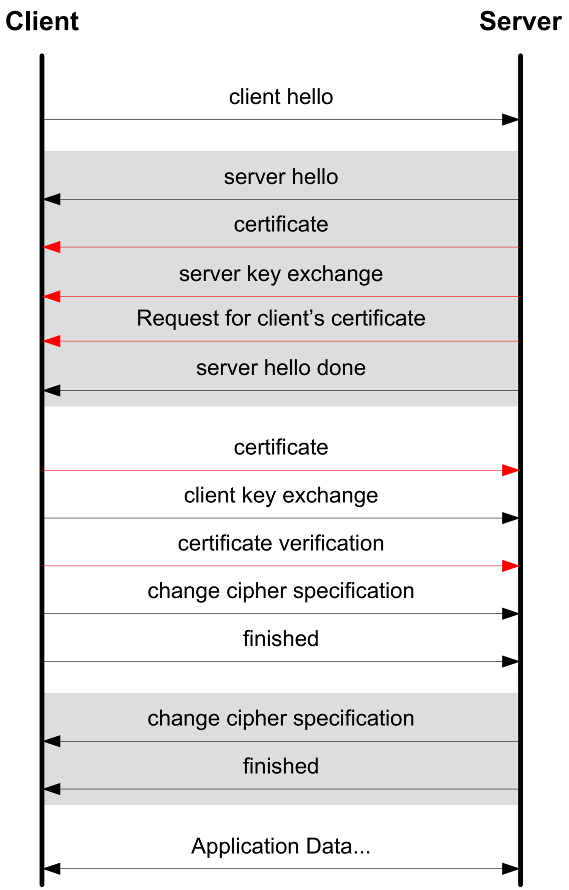
Clearly, a secure VPN requires both authentication *and* encryption. We know that ESP is the only way to provide encryption, but ESP and AH both can provide authentication: which one do we use?

ESP+Auth is used in Tunnel mode to fully encapsulate the traffic on its way across an untrusted network, protected by both encryption and authentication in the same thing.

Secure Sockets Layer (SSL)

SSL (Secure Sockets Layer)

- Runs between the Application Layer (HTTP, SMTP, NNTP, etc) and Transport Layer (TCP)
- Supports client/server's negotiation of cryptographic algorithms:
  - Public-key cryptography: RSA, Diffie-Hellman, DSA or Fortezza
  - Symmetric ciphers: RC2, IDEA, DES, 3DES or AES
  - One-way hash functions: MD5 or SHA



Reference: http://wp.netscape.com/eng/ssl3/

SSL/TLS handshake – (1/5)

Client Hello message content in SSL/TLS

- **SSL VERSION NUMBER** : the client sends a list of ssl version it supports. And priority is given to the highest version it supports

- **Random Data Number** : Its made up of 32 bytes. 4 byte number made up from client's date & time plus 28 byte randomly generated number (this will be used with server's random value made of date & time for generating the "master secret", from which encryption key will be derived).

- **SESSION ID:** In order to enable client's resuming capabilities this session ID is included.
- **CIPHER SUITS:** RSA algorithm is used for the initial key exchange which will be done using public key cryptography. And SHA is used for MAC and hashing. And also sends the encrption algo's supported by the client like DES for example.
- **Compression Algorithm:** this will include compression algorithms details, if used.

SSL/TLS handshake – (2/5)

Server Hello message in SSL/TLS

- **Version Number:** Server selects an ssl version thats supported by both the server and the client, and is the highest version supported by both of them

- **Random Data**: the server also generates a random value using the server's date and time plus a random number of 28bytes. Client will use this random value and its own random value to generate the "master key”

- **Sesssion ID:** There are three possiblities, with regard to the session id. It all depends on the type of client-hello message. If the client requires to resume a previously created session, then both the client and server will use the same session ID. But, if the client is initiating a new session, the server will send a new session ID. Sometimes a null session ID is also used, where server will never support resuming the session, so no session id's are used at all.

- **Cipher Suits:** Similar to the version number selected by the server, the server will select the best cipher suite version supported by both of them.

SSL/TLS handshake – (3/5)

- **Certificate**: The server also sends a certificate, which is signed and verified by a Certificate Authority, along with the public key(Content encrypted with public key can only be opened with a corresponding private key. In this case, only the server can unlock it because, the server has the private key for its public key).

- **Server Key Exchange:** this step is taken by the server, only when there is no public key shared along with the certificate. If this key is used, this will be used to encrypt the "Client Key Exchange Method"

- **Client Certificate request:** This is seldom used, because this is only used, when the client also needs to get authenticated, by a client certificate.

- **Server Hello Done:** this message from the server will tell the client, that the server has finished sending its hello message, and is waiting for a response from the client.

SSL/TLS handshake – (4/5)

Response from the client to server's hello message:

- **Client Certificate:** The client sends a client certificate back to the server. This step is only used when a client certificate is requested by the server(through the server hello message).
- **Client Key Exchange:** This message is only sent, after the client calculates, the premaster secret with the help of the random values of both the server and the client(Which was shared by both the server and the client through the hello message). **"Client Key exchange"** message, is sent by encrypting it with the server's public key, which was shared through the hello message. This message can only be decrypted with the server's private key. If successful, the server is authenticated.

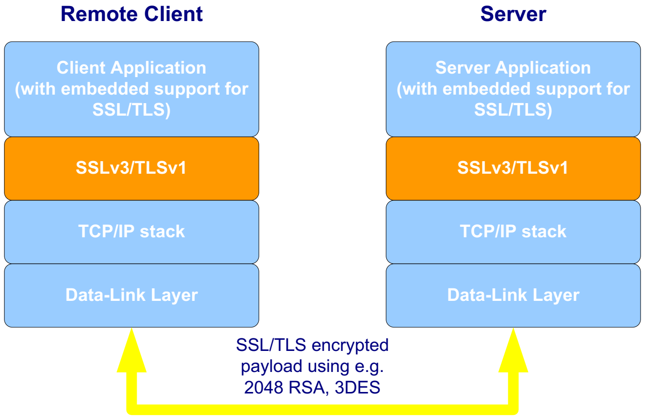
SSL/TLS handshake – (5/5)

- **Certificate verify -** This message is used to provide explicit verification of a client certificate. This message is only sent following a client certificate that has signing capability

- **Change cipher spec protocol** - The change cipher spec message is sent by both the client and server to notify the receiving party that subsequent records will be protected under the newly negotiated CipherSpec and keys.

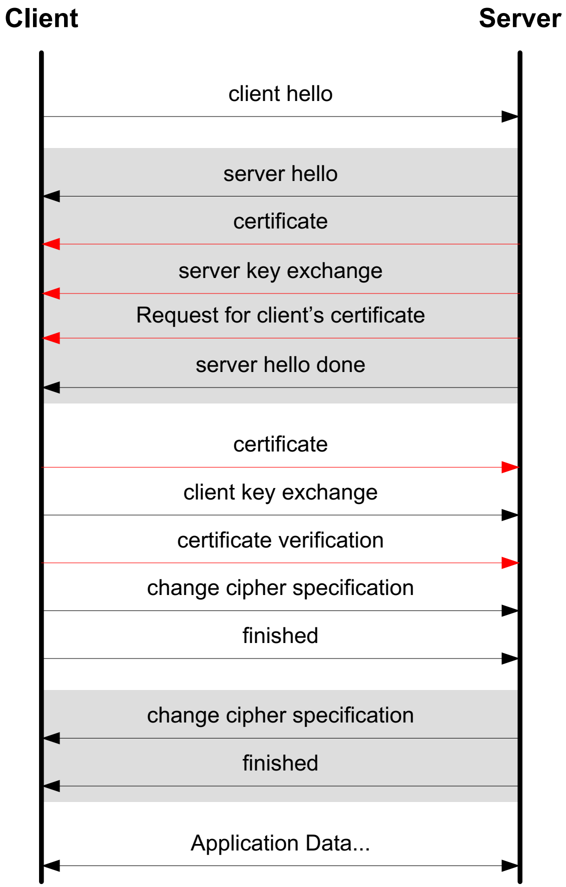
Secure Sockets Layer (SSL)

- SSL works in two modes:
  - Application embedded. i.e. HTTPS
  - SSL Tunnel or SSL VPN (e.g. OpenVPN)
- SSL VPN is less complex than IPsec…
  - Unlike IPsec, SSL protocol sits on top of Transport Layer stack.
  - OpenVPN because unlike IPsec, it operates out side of OS kernel.
  - SSL is more flexible in supporting multiple cryptographic algorithms


Remote Client
Server
Client Application (with embedded support for SSL/TLS)
Server Application (with embedded support for SSL/TLS)
SSLv3/TLSv1
SSLv3/TLSv1
TCP/IP stack
TCP/IP stack
Data-Link Layer
Data-Link Layer
SSL/TLS encrypted payload using e.g. 2048 RSA, 3DES

Transport Layer Security (TLS)

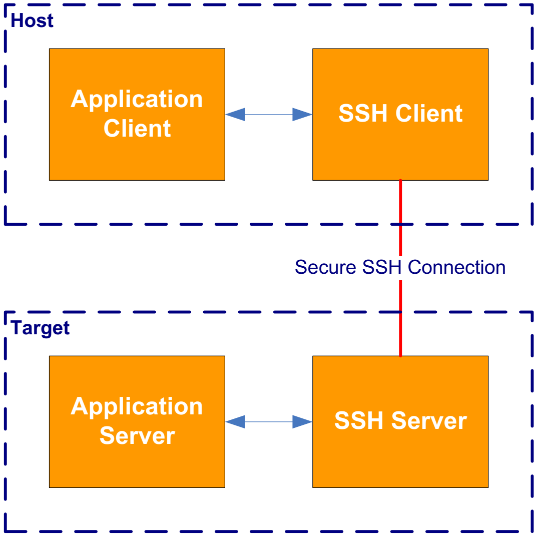
- TLS 1.0 (Transport Layer Security) (RFC 2246) is defined base on SSL 3.0
- TLS and SSL protocols are not interchangeable (during a client/server session)
- The selection of TLS or SSL is negotiated between client/server at the "hello".



Reference: http://www.ietf.org/rfc/rfc2246.txt

Secure Shell (SSH)

- SSH (Secure Shell) is a secure replacement for the r* programs (rlogin, rsh, rcp, rexec, etc.)
- SSH uses public-key to authenticate users, and supports variety of cryptography algorithms: Blowfish, 3DES, IDEA, etc.
- SSH protects:
  - Eavesdropping of data transmitted over the network.
  - Manipulation of data at intermediate elements in the network (e.g. routers).
  - IP address spoofing where an attack hosts pretends to be a trusted host by sending packets with the source address of the trusted host.
  - DNS spoofing of trusted host names/IP addresses.



Reference: http://www.ietf.org/rfc/rfc4251.txt

Topics

Telecommunications & Network Security Domain – Part 2

- Security Principles & Network Architecture
- Security Countermeasures and Controls
  - Physical Layer
  - Data-Link Layer
  - IP Network Layer
  - Transport Layer
  - Application Layer
- VPN
- NAS

Network Access Servers (NAS)

- NAS (Network Access Server) provides centralized Access Control of AAA (Authentication, Authorization, Accounting) services
  - A distributed (client/server) security model
  - Authenticated transactions
  - Flexible authentication mechanisms
- Versions of NAS:
  - TACACS+ (Terminal Access Controller Access Control System) (Cisco proprietary).
  - RADIUS (Remote Authentication Dial-In User Service) (Open source).

Reference:

- RADIUS: http://www.ietf.org/rfc/rfc3579.txt
- DIAMETER: http://www.ietf.org/rfc/rfc4005.txt

Authentication Servers – RADIUS

RADIUS (Remote Authentication Dial-In User Service)

- RADIUS Server stores UserID, Password, and Authorization parameter (ACL) centrally.
- Unlike TACACS, RADIUS does support authentication proxies, so the user authentication information or schema is scalable.
- Uses CHAP (Challenge Handshake Authentication Protocol) to authenticate user.
- Client/Server uses shared secret stored in configuration file for encryption and decryption of CHAP, but not data packets.
- Uses a single UDP packet design for speed and performance.

Reference:

- RADIUS: http://www.ietf.org/rfc/rfc3579.txt
- DIAMETER: http://www.ietf.org/rfc/rfc4005.txt

Authentication Servers – TACACS+

TACACS (Terminal Access Controller Access Control System) (RFC 1492)

- TACACS+ is a significant improvement of old version. Unlike RADIUS, TACACS is stateful, TCP-based.
- TACACS is not supported by all vendors. In addition, TACACS protocol does not support authentication proxies, which means user authentication can only be stored centrally in a Cisco ACS.
- Unlike RADIUS, TACACS encrypts entire TCP packet, not just the authentication messages.

Reference:

- http://www.cisco.com/warp/public/480/10.html
- http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a0080094eb0.shtml