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)

Question:

- Name the seven layers of OSI reference model?

    –

    –

    –

    –

    –

    –

    –

Hint: “People do not throw sausage pizza away”

Question:

- Name the seven layers of OSI reference model?
  - Physical (people)
  - Data-Link (do)
  - Network (not)
  - Transport (throw)
  - Session (sausage)
  - Presentation (pizza)
  - Application (away)

Topics

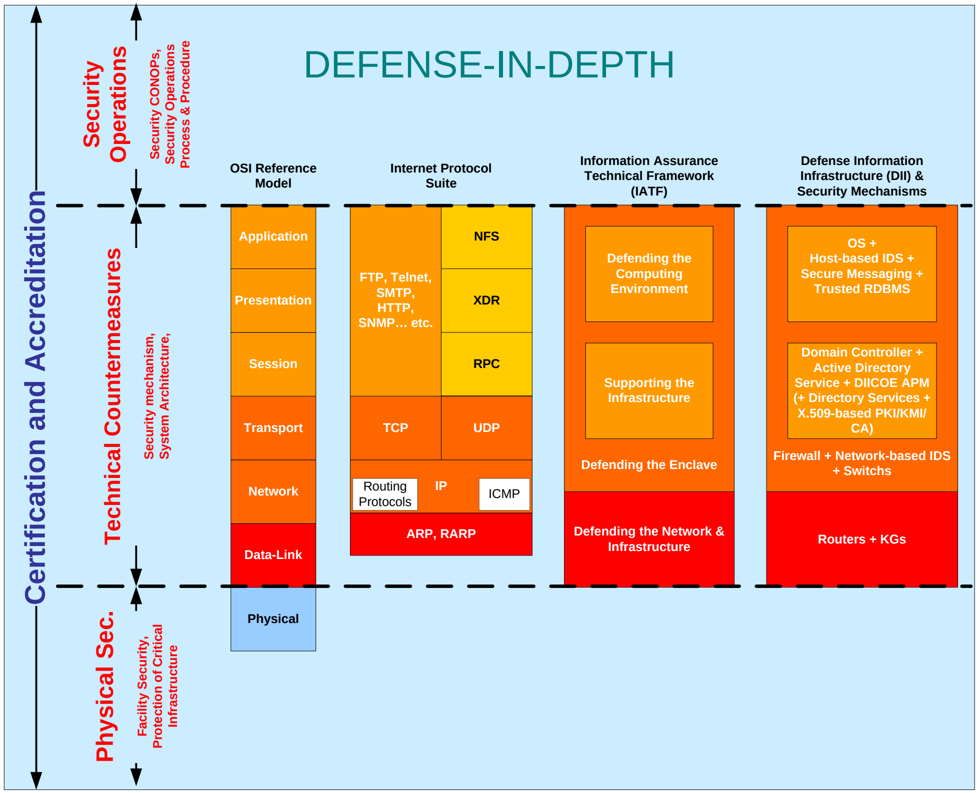
Telecommunications & Network Security Domain – Part 2

➡ Security Countermeasures and Controls

- Physical Layer
- Data-Link Layer
- IP Network Layer
- Transport Layer
- Application Layer

- VPN
- NAS

Implementation of Technical Countermeasures



DEFENSE-IN-DEPTH

Certification and Accreditation

Security Operations — Security CONOPs, Security Operations Process & Procedure

Technical Countermeasures — Security mechanism, System Architecture,

Physical Sec. — Facility Security, Protection of Critical Infrastructure

OSI Reference Model: Application, Presentation, Session, Transport, Network, Data-Link, Physical

Internet Protocol Suite: FTP, Telnet, SMTP, HTTP, SNMP… etc.; NFS; XDR; RPC; TCP; UDP; Routing Protocols; IP; ICMP; ARP, RARP

Information Assurance Technical Framework (IATF): Defending the Computing Environment; Supporting the Infrastructure; Defending the Enclave; Defending the Network & Infrastructure

Defense Information Infrastructure (DII) & Security Mechanisms: OS + Host-based IDS + Secure Messaging + Trusted RDBMS; Domain Controller + Active Directory Service + DIICOE APM (+ Directory Services + X.509-based PKI/KMI/ CA); Firewall + Network-based IDS + Switchs; Routers + KGs

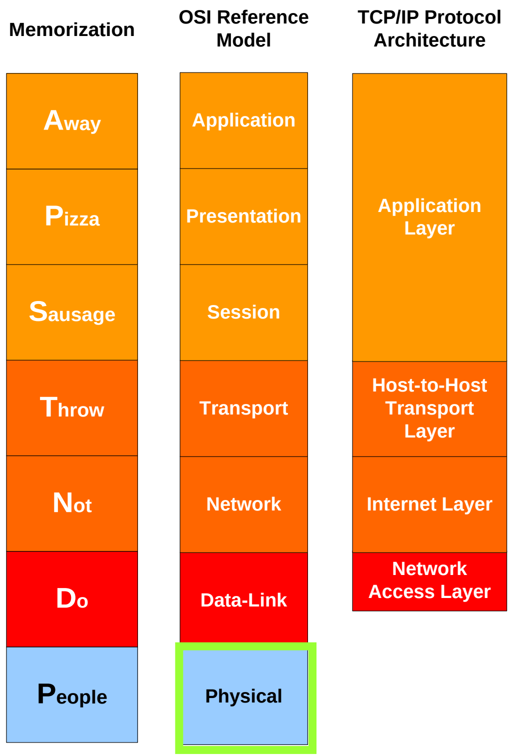
Example implementation of technical countermeasures in Network and Internetworking Services:

- Routers
- Switches
- Encryptors
- Firewalls
- Intrusion Detection System (IDS)
- Intrusion Prevention Systems (IPS)
- Operating Systems (OS)

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

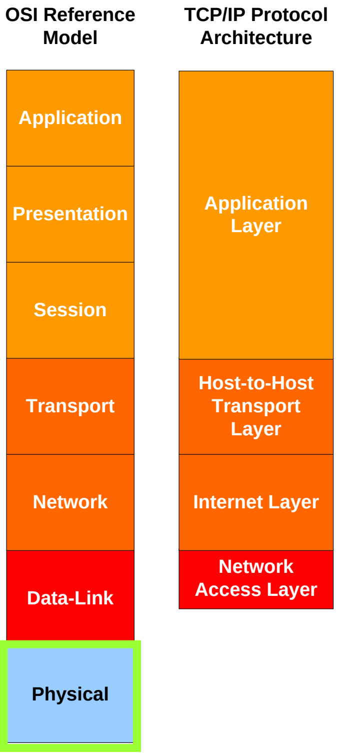


Memorization	OSI Reference Model	TCP/IP Protocol Architecture
Away	Application	Application Layer
Pizza	Presentation	
Sausage	Session	
Throw	Transport	Host-to-Host Transport Layer
Not	Network	Internet Layer
Do	Data-Link	Network Access Layer
People	Physical	

Security of Physical Layer – Review

Transport Medium

- Cables
  - LAN: Twisted Pair (Shield, Un-shield), Coaxial, Fiber Optics (Single-mode, Multi-mode)
  - WAN: SONET, X.21-bis, HSSI, SMDS
- Radio Frequency (RF)
  - LAN: 2.4GHz, 5GHz, UWB (3.1GHz – 10.6GHz)
  - WAN: Microwave (VHF, UHF, HF) (300MHz – 300GHz)
- Light
  - 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. LASER, single-mode)
- Path Diversity of transport media
  - Cables / Fibers: Geographic diversity
  - RF: Utilization of radio channels, coverage area
  - Optical: Multi-mode

Transport Media

Security considerations for transport media…

- EMI (Electromagnetic Interference)
  - Crosstalk
  - HEMP (High-altitude Electromagnetic Pulse)
- RFI (Radio Frequency Interference)
  - UWB (Ultra Wide Band): > 500MHz, FCC authorizes the unlicensed use in 3.1 – 10.6GHz
  - Household microwave oven: 2.45GHz
- Transient. Disturbance of power traveling across transport medium
- Attenuation. Loss of signal strength over distance

Transport Interfaces (I/Fs)

- Physical protection of transport I/Fs
  - Access control of network equipment
    - Telco Demarcation / 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.
- Use `enable secret` command and not with the `enable password` command
- Each router shall have different enable and user password
- Access routers only from "secured or trusted" server or console
- Reconfigure the *connect*, *telnet*, *rlogin*, *show ip access-lists*, and *show logging* command to privilege level 15 (*secret*)
- Add Warning Banner

Reference: DISA FSO *Network STIG*

Questions:

- Why household microwave oven may interfere with your Wi-Fi (IEEE 802.11b/g)?
  - –

- Loss of signal strength over distance is?
  - –

- Disturbance of power traveling across a transport medium is?
  - –

Answers:

- Why household microwave oven may interfere with your Wi-Fi (IEEE 802.11b/g)?
  - The microwave oven operates in 2.45GHz and Wi-Fi operates in 2.4GHz

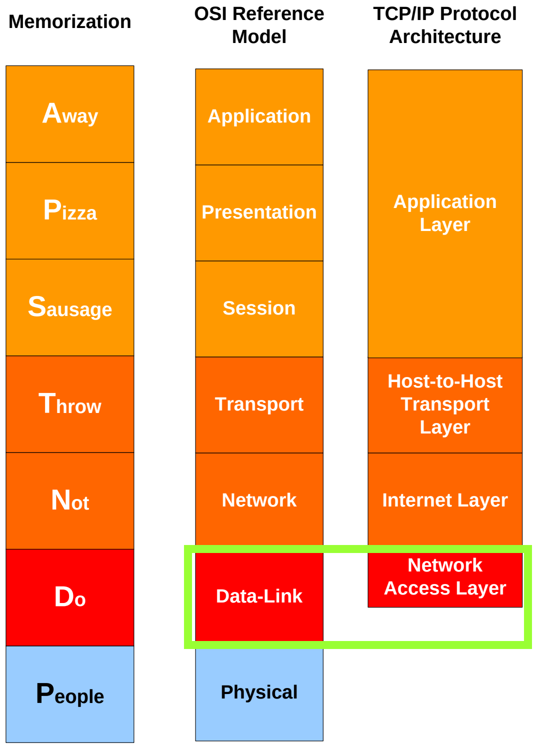
- Loss of signal strength over distance is?
  - Attenuation

- Disturbance of power traveling across a transport medium is?
  - Transient

Topics

Telecommunications & Network Security Domain – Part 2

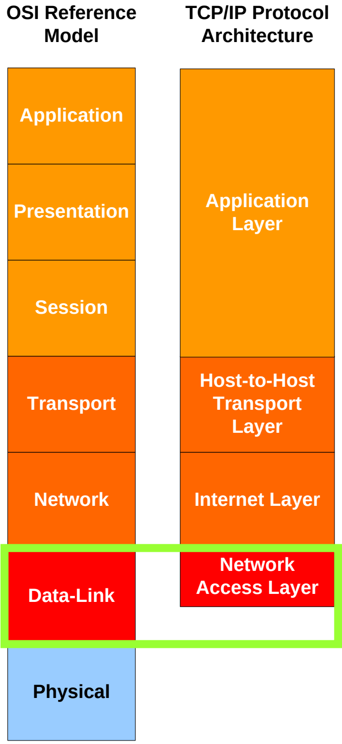
- Security Countermeasures and Controls
  - Physical Layer
  - Data-Link Layer
  - IP Network Layer
  - Transport Layer
  - Application Layer
- VPN
- NAS



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)
- L2TP (Layer 2 Tunnel Protocol)
- Link Encryption (i.e. Link / Bulk Encryptor) : ISDN, Frame Relay, ATM
- RF:
  - LAN: WEP (Wired Equivalent Privacy), EAP (Extensible Authentication Protocol), IEEE 802.1X
  - WAN: AN/PSC-5 Radio (w/ embedded encryption for SATCOM, DAMA, LOS communications), TADIL-J (Link-16) (w/ embedded encryption for LOS communications)

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: Ethernet, 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)
  - ISDN, Frame Relay, ATM, etc.
- 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)

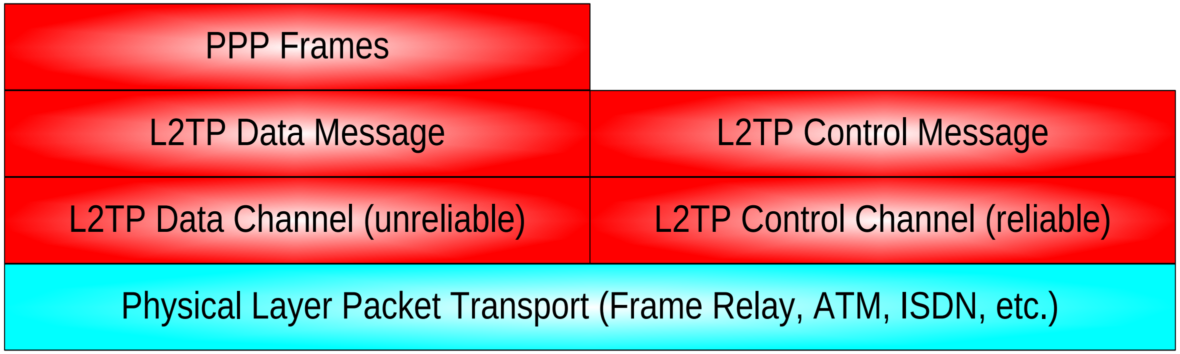
- PAP (Password Authentication Protocol) (RFC 1334)
  - Authentication process is in plaintext, and it is send over the established link
- CHAP (Challenge Handshake Authentication Protocol) (RFC 1994, replaces RFC 1334)
  - Protection against playback attack by using 3-way handshake:
    1. After link established, authenticator sends a "challenge" message to the peer
    2. Peer response with a value calculated using a "one-way hash"
    3. Authenticator calculate the expected hash value and match against the response
  - 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:
  - 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

Layer 2 Tunnel Protocol (L2TP)

- L2TP (Layer 2 Tunnel Protocol) (RFC 2661) extends the PPP model by allowing the L2 and PPP endpoints to reside on different devices (e.g. workstation to router) interconnected by a packet-switched network



PPP Frames

L2TP Data Message

L2TP Control Message

L2TP Data Channel (unreliable)

L2TP Control Channel (reliable)

Physical Layer Packet Transport (Frame Relay, ATM, ISDN, etc.)

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)
- 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

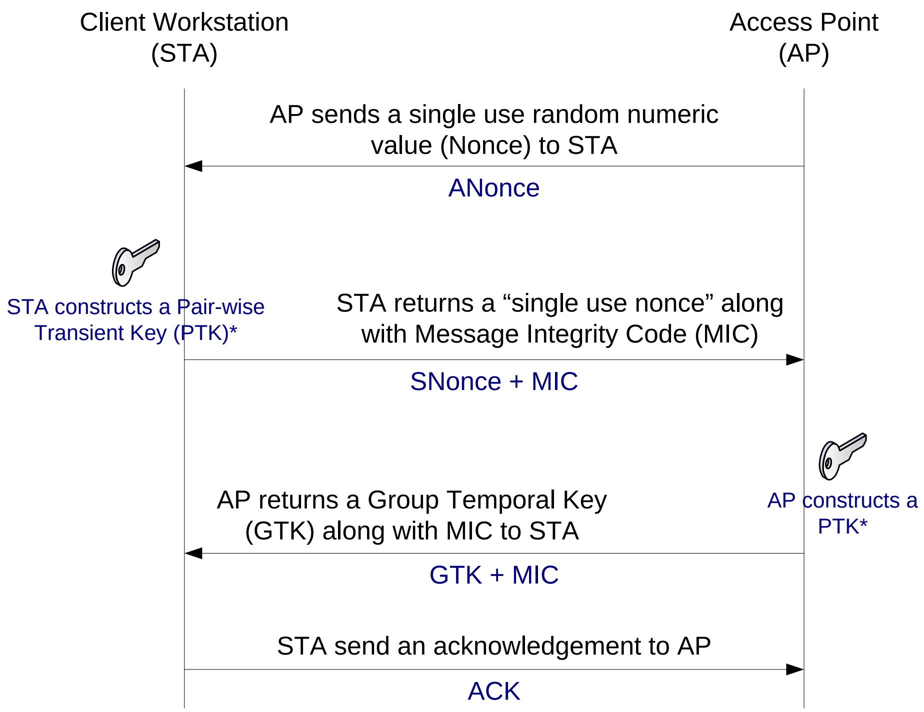
IEEE 802.1X

- IEEE 802.1X uses EAP (Extensible Authentication Protocol)
  - 802.1X is an interoperability standard **NOT** a security standard!
- Uses 3-way handshake, in state machine model:
  1. Unauthorized State: After link established, authenticator (access point) sends a authentication request message to the peer.
  2. Unauthorized State: Peer send response with a set of values that matches authentication mechanism of the authenticator.
  3. Unauthorized State: Authenticator calculates the expected value and match against the response.
  4. Authorized State: Exchange encrypted data message.

Reference: http://standards.ieee.org/getieee802/download/802.1X-2004.pdf.

IEEE 802.11i

- IEEE 802.11i standard has been ratified on 6/24/2004.
  - FIPS 140-2 certified by NIST.
  - A.k.a. WPA2 (Wi-Fi Protected Access version 2)
- Uses IEEE 802.1X (i.e. EAP) for authentication.
- Uses 4-way handshake.
- 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

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…

- Denial-of-Services (DoS) Attack
  - A hacker can easily associate an operationally significant IP address to a false MAC address. Then your router begin to send packets into a non-existing I/F.
- 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 ARP 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.
  - Disable all un-necessary protocols & services.
- Physical Access Control:
  - 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.

Reference: DISA FSO *Network STIG*

Questions:

- Why Point-to-point protocol (PPP) is better than Serial Line Internet Protocol (SLIP)?
  - –
  - –

- Both Challenge handshake authentication protocol (CHAP) and Extensible authentication protocol (EAP) uses 3-way handshake. What is the advantage using EAP instead of CHAP?
  - –

Answers:

- Why Point-to-point protocol (PPP) is better than Serial Line Internet Protocol (SLIP)?
  - PPP supports multiple internetworking protocols in a session
  - SLIP has no security feature

- Both Challenge handshake authentication protocol (CHAP) and Extensible authentication protocol (EAP) uses 3-way handshake. What is the advantage using EAP instead of CHAP?
  - EAP supports multiple authentication mechanisms: MD5, One-time password (OTP), and Token card.

Questions:

- What is the size of the shared static symmetric key for 128-bit Wired Equivalent Privacy (WEP)?
  -

- What is the relationship between IEEE 802.1X and IEEE 802.11i?
  -

- Is IEEE 802.1X a security standard?
  -

- What is the primary security issue for Layer 2 switches?
  -

Answers:

- What is the size of the shared static symmetric key for 128-bit Wired Equivalent Privacy (WEP)?
  - 104-bit. 24-bit of Initialization vector (IV)

- What is the relationship between IEEE 802.1X and IEEE 802.11i?
  - IEEE 802.11i uses IEEE 802.1X for EAP authentication

- Is IEEE 802.1X a security standard?
  - No. IEEE 802.1X is an interoperability standard

- What is the primary security issue for Layer 2 switches?
  - Preserving the integrity of ARP table

Topics

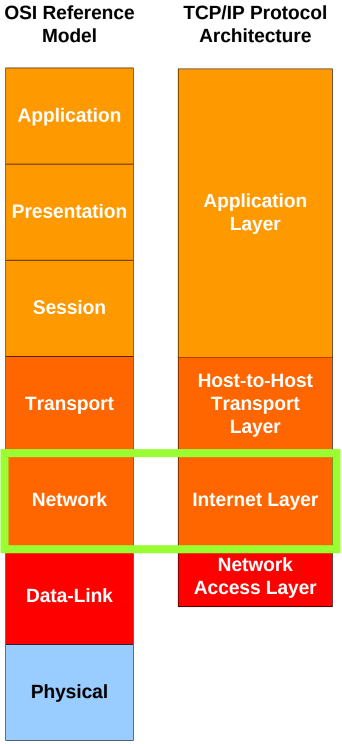
Telecommunications & Network Security Domain – Part 2

- 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 Network Layer – Review

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



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

Virtual IP Address (VIP)

VIP (Virtual IP Address) is a method that maps a virtual internetworking entity into many computing hosts.

- One-to-Many:
  - Used for Load-Balance / Sharing
  - Used limit exposure of multiple IP addresses or multiple network I/Fs. (one-to-many)
- Many-to-one:
  - One network I/F to many IP addresses.
  - Used for Application sharing

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

Dynamic Routing: Interior Gateway Protocols (IGPs)

- Router uses distance vector routing protocols mathematically compare routes using some measurement of distance (or # of hops) and send all or a portion of route table in a routing update message at regular intervals to each of neighbor routers.
  - RIP (Routing Information Protocol)
  - IGRP (Interior Gateway Routing Protocol)
  - EIGRP (Enhanced IGRP, Cisco proprietary)
- Security issues:
  - Integrity of routing tables: Automatic distribution of route table updates.
  - Operational stability: The routing updates create chain-reaction of route table recalculations to every neighbor routers.

Reference: *Routing TCP/IP Volume I*, by J. Doyle, et. al., Cisco Press

Dynamic Routing: Interior Gateway Protocols (IGPs)

- To preserve integrity of route table: Use MD-5 authentication between neighbor routers.
  - Do not use RIPv1, because it does not support MD-5 authentication.
- To improve operational stability of routers running distance vector IGP’s:
  - Use Split horizons with poison-reverse updates. It prevents routing loops by preventing a router from updating adjacent neighbors of any routing changes that it originally learned from those neighbors.
  - Use Hold downs (for IGRP & EIGRP). It prevents IGRP’s interval updates from wrongly reinstating an invalid route.

Reference: *Routing TCP/IP Volume I*, by J. Doyle, et. al., Cisco Press

Dynamic Routing: Interior Gateway Protocols (IGPs)

- Router uses link-state routing protocols sends only link-state advertisements (LSAs) to each of its neighbor routers.
  - OSPF (Open Shortest Path First)
  - IS-IS (Integrated intermediate system-to-intermediate system)
- Security issues:
  - Integrity of routing tables: Automatic distribution of LSAs.
  - Operational stability: After the adjacencies are established, the router may begin sending out LSAs. the LSAs create chain-reaction of recalculations of route paths to every neighbor routers (i.e. Link-state Flooding).

Reference: *Routing TCP/IP Volume I*, by J. Doyle, et. al., Cisco Press

Dynamic Routing: Interior Gateway Protocols (IGPs)

- To preserve integrity of route table: Use MD-5 authentication between neighbor routers.
- To improve operational stability of routers running link-state IGP's:
  - Set sequence number for each link-state advertisement (LSA). The sequence numbers are stored along with the LSAs, so when a router receives the same LSA that is already in the database and the sequence number is the same, the received information is discarded.

Reference: *Routing TCP/IP Volume I*, by J. Doyle, et. al., Cisco Press

Dynamic Routing: Exterior Gateway Protocols (EGPs)

- Exterior gateway protocols are design for routing between multiple AS' (Autonomous Systems).
  - EGP (Exterior Gateway Protocol).
  - BGP (Border Gateway Protocol).

  BGP is THE routing protocol for Internet. BGP peers exchange full routing information when a new peer is introduced, then send only updates for route change. BGP is a path vector routing protocol, because the router does its own path calculation, and advertises only the optimal path to a destination network.
- Security issues:
  - Integrity of routing tables: Automatic distribution of route table updates.
  - Operational stability: The router running BGP is vulnerable to "route-flap". Where a unstable routing path to an unreachable network may cause dynamic updates to all peering routers and this impacts performance of entire Internet!

Dynamic Routing: Exterior Gateway Protocols (EGPs)

- To preserve integrity of route table: Use MD-5 authentication between peering routers.
- To preserve operational stability of edge routers running BGP:
  - Enable BGP route-flap damping on all edge routers. For example:

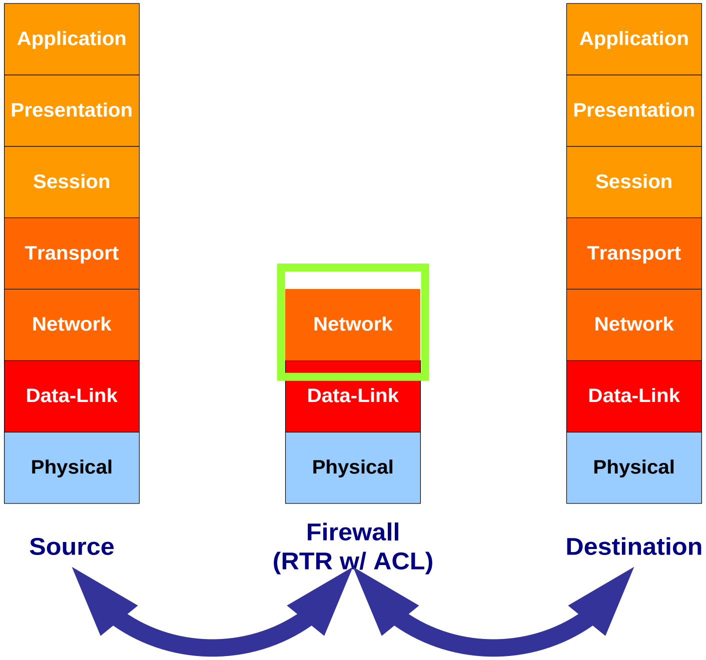
Prefix length:	/24	/19	/16
Suppress time:	3hr.	45-60min.	<30min.

  - Set ACL to deny all “Bogon” IP addresses. For Edge routers peering on Internet.

Note: “Bogon” IP addresses are the un-used or not been assigned IP addresses on the Internet. The list can be obtained at http://www.cymru.com/Documents/bogon-list.html.

Packet-filtering Firewall

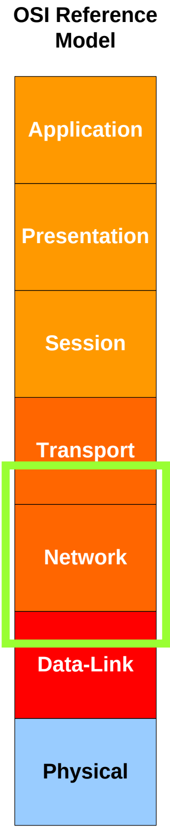
- Router ACL's = Packet-filtering firewall
- Firewall Policy: Deny by default, Permit by exception.
  - Understand the data-flow (i.e. source, destination, protocols, and routing methods), so the security engineer knows how to apply IP filtering.
  - Knows the specific inbound and outbound I/F's
  - Disable all un-necessary protocols & services.



Reference: DISA FSO *Network STIG*

Packet-filtering Firewall

- Use `distribute-list <ACL>` *`out`* to control outbound routing information.
- Use `distribute-list <ACL>` *`in`* to control inbound routing information.
- Global Filtering:
  1. Create ACLs that defines what network information is allowed in/out.
  2. Configure `distribute-list` in the appropriate direction under the router's routing protocol configuration.
- Per-interface Filtering:
  – Apply `distribute-list <ACL> <in/out>` to a `<specific interface>`



Reference: DISA FSO *Network STIG*

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, or SNMPv2c, no default community strings
    - For SNMPv2c, treat community strings as “password”.
- 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*

Questions:

- What are the two primary security issues associated with the use of dynamic routing protocols?
  - –
  - –

- What is the difference between Interior gateway protocols (IGPs) and Exterior gateway protocols (EGPs)?
  - –

Answers:

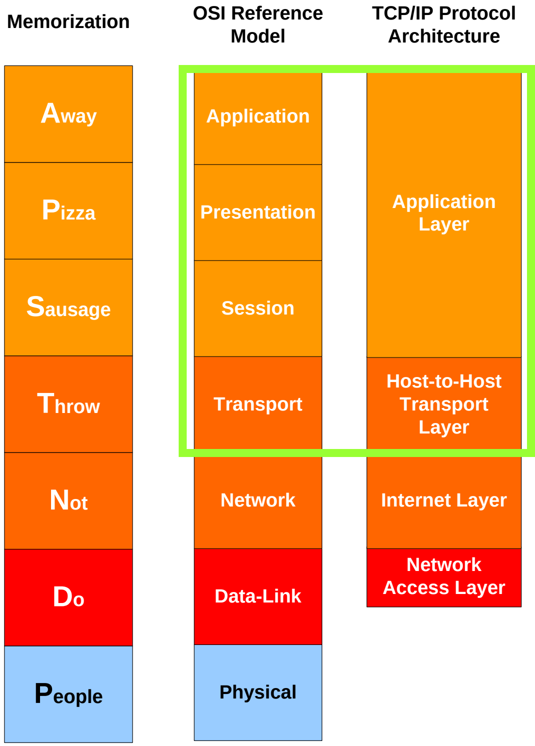
- What are the two primary security issues associated with the use of dynamic routing protocols?
  - Integrity of routing tables
  - Operational stability

- What is the difference between Interior gateway protocols (IGPs) and Exterior gateway protocols (EGPs)?
  - IGPs are used within autonomous systems. EGPs are used between autonomous systems

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	

Firewalls

- Packet-filtering firewall (i.e. Router ACLs)
  - Do not examine Layer 4-7 data. Therefore it cannot prevent application-specific attacks
- Proxy firewall
  - It supports selected IP protocols (I.e. DNS, Finger, FTP, HTTP, LDAP, NNTP, SMTP, Telnet). For multicast protocols (PIM, IGMP…etc) must be **TUNNEL** through the firewall
- Stateful inspection firewall
  - 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

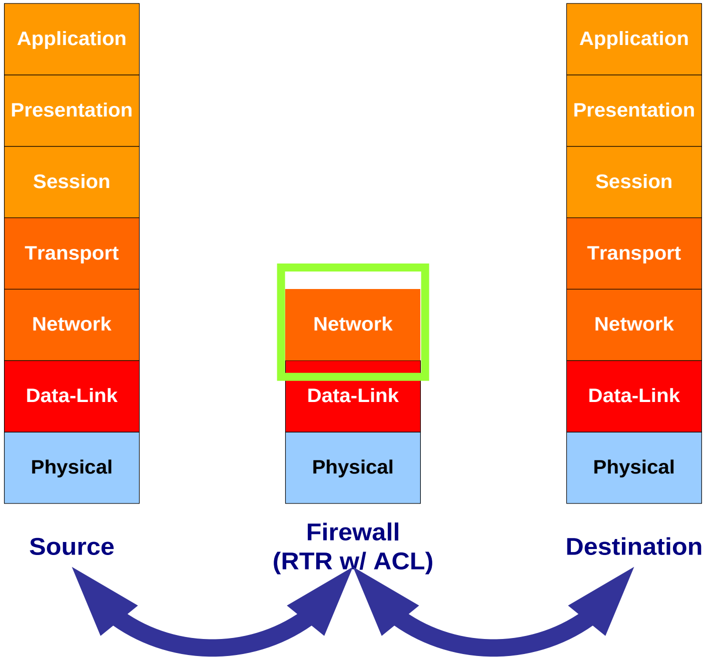
Firewalls

Hybrid Firewalls…

- Circuit-level proxy firewall
  - IETF created SOCKS proxy protocol (RFC 1928) for secure communications
  - SOCKS creates a circuit between client and server without requiring knowledge about the internetworking service. (No application specific controls)
  - It supports user authentication
- Application proxy firewall
  - Application proxy + Stateful inspection
  - A different proxy is needed for each service
  - It supports user authentication for each supported services.
  - e.g. Checkpoint Firewall-1 NG

Packet-filtering firewalls

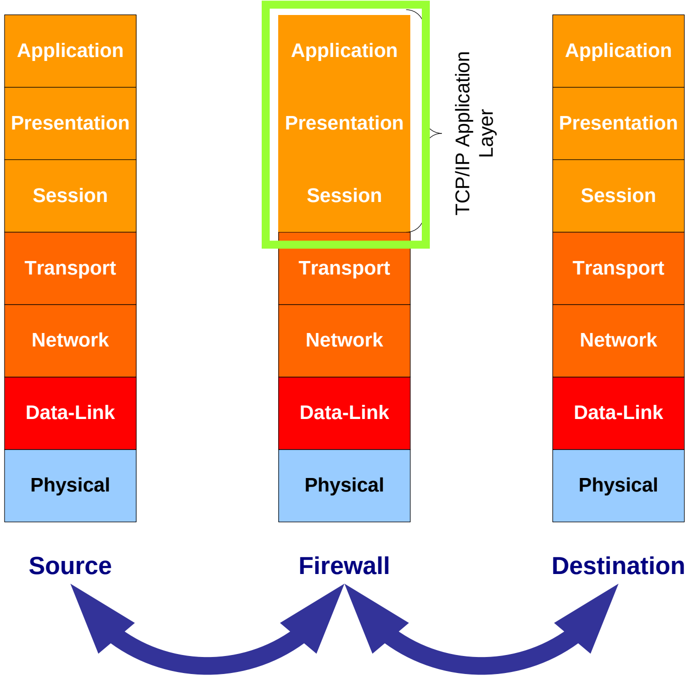
- Router ACL's ~ Packet-filter firewall
- Firewall Policy: Deny by default, Permit by exception
  - Understand the data-flow (i.e. source, destination, protocols, and routing methods), so the security engineer knows how to apply IP filtering
  - Knows the specific inbound and outbound I/F's
  - Disable all un-necessary protocols & services



Source: DISA FSO *Network STIG*

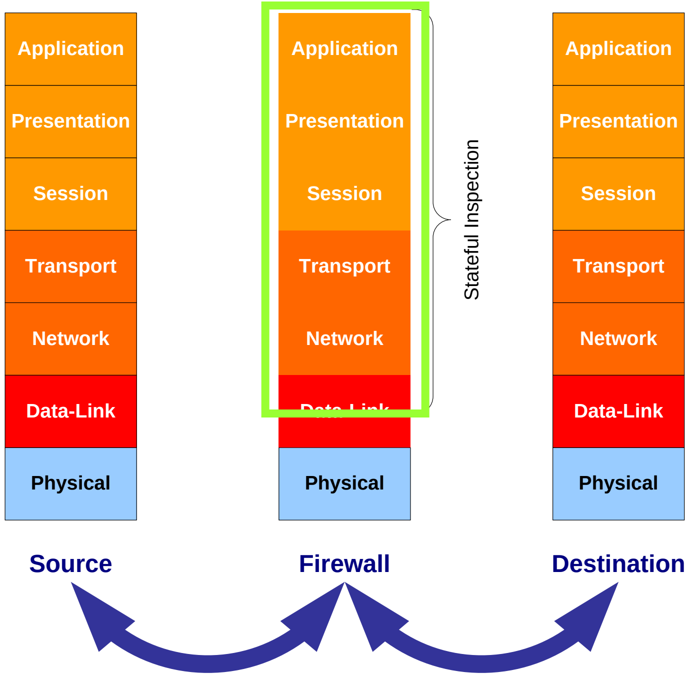
Proxy firewalls

- Do not allow any direct connections between internal and external computing hosts
- Able to analyze application commands inside the payload (datagram)
- Supports user-level authentications. Able to keep a comprehensive logs of traffic and specific user activities



Stateful inspection firewalls

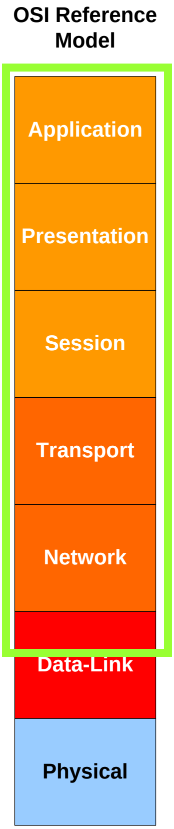
- Supports all TCP/IP-based services, including UDP (by some)
- Inspects TCP/IP packets and keep track of states of each packets. Low overhead and high throughput
- Allows direct TCP/IP sessions between internal computing hosts and external clients
- Offers no user authentication



Firewall Policy

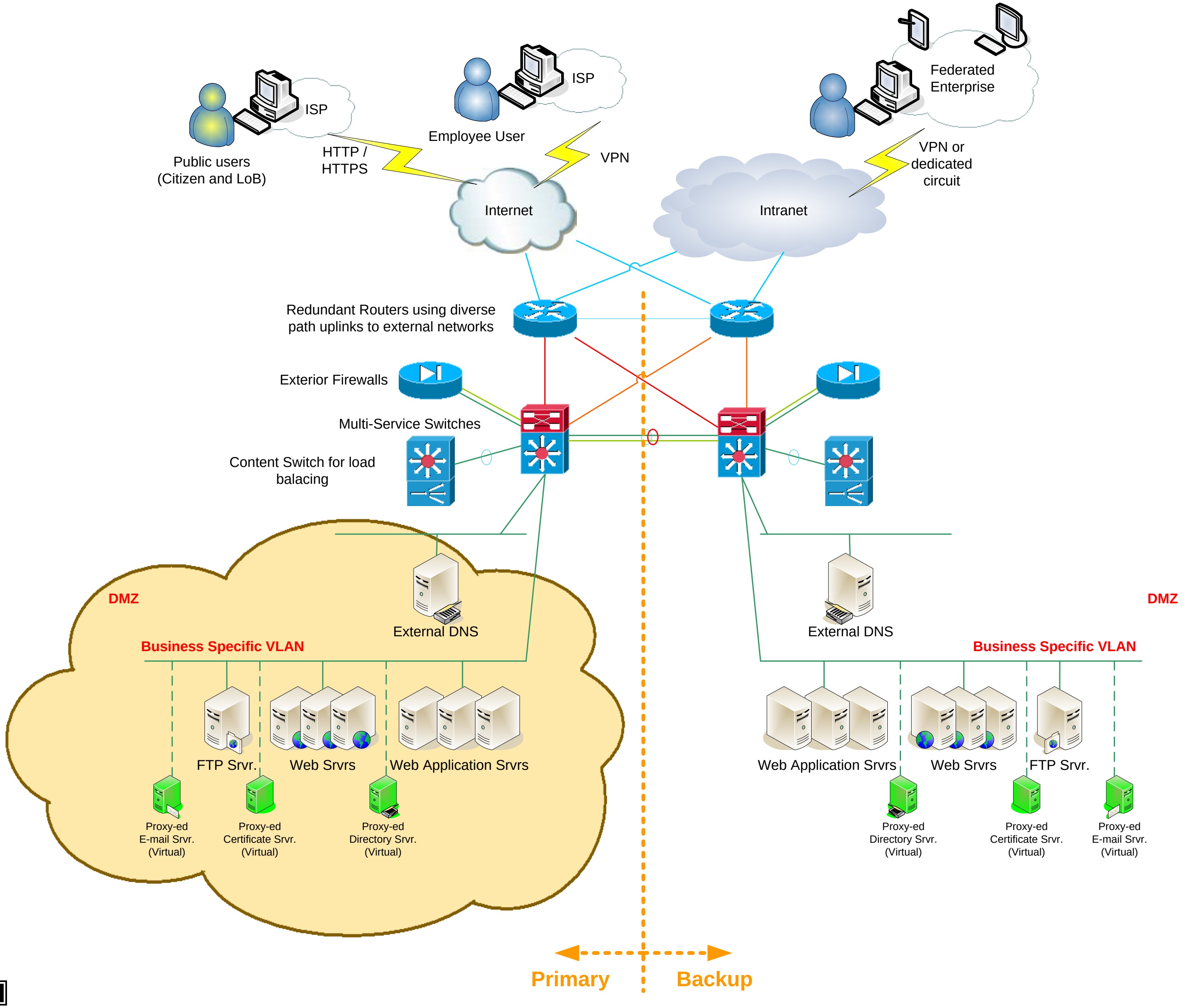
In principal, firewall performs three actions:

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



Security of Transport & Application Layers

Network Design with Firewalls



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

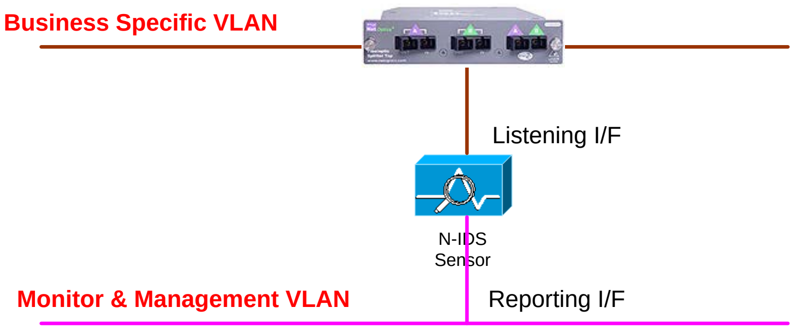
- Network-IDS (Intrusion Detection System) is a "passive" device
  - To detect attacks and other security violations
  - To detect and deal with pre-ambles to attacks (i.e., "doorknob rattling"/ probing / scanning)
  - To document the threat to a network, and improve diagnosis, recovery and correction of an unauthorized intrusion
- 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

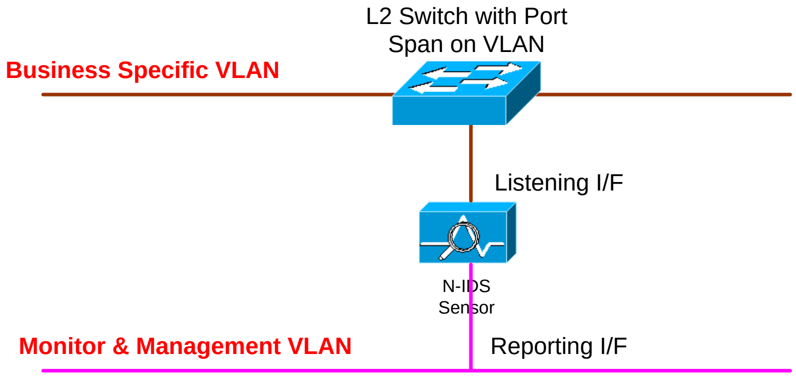
Intrusion Detection System (IDS) & Intrusion Prevention System (IPS)

- N-IDS (and Host-IDS) use “knowledge-based” (a.k.a. “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.
- N-IPS uses “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)

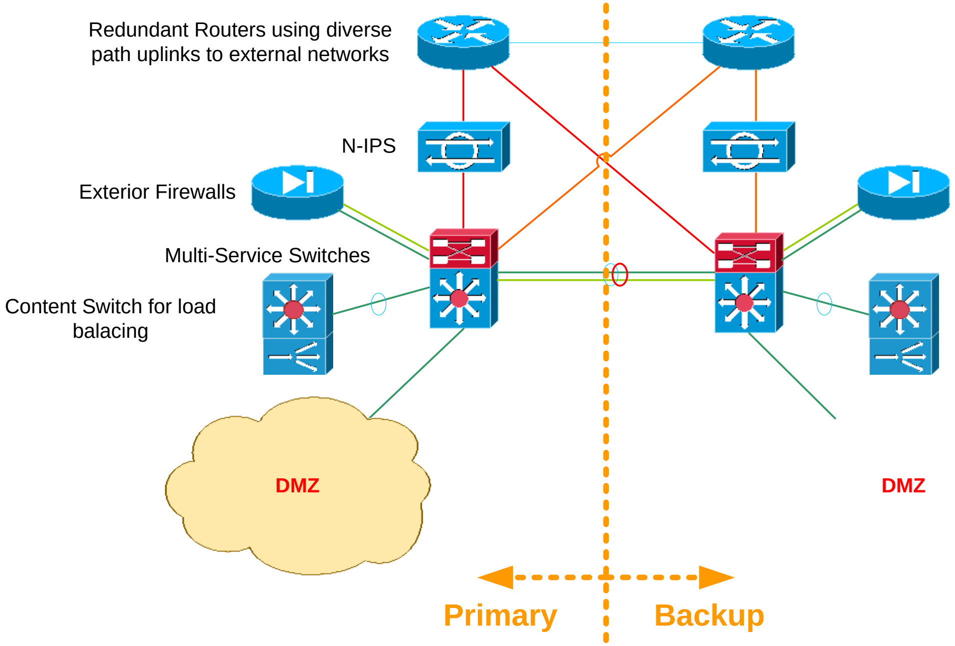
- Network-IDS (intrusion detection system) is a "passive" device
  - There are two way to setup the listening interfaces: Network TAP and VLAN Port Spanning on L2 switch
  - N-IDS is composted of two components: Pre-processor (Sensor) and Event Collector/Analyzer
    - Pre-processor assembles the packets and match them against a pre-defined signature database
    - Event Collector/Analyzer collects the events from all the sensors, correlate and present intrusion pattern





Network-based Intrusion Prevention System (N-IPS)

- Network-IPS (intrusion prevention system) is an "in-line" device
  - Examines network traffic and automatically blocks inappropriate or malicious traffic
  - However, 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

Questions:

- What are the five common types of firewall?
  –
  –
  –
  –
  –

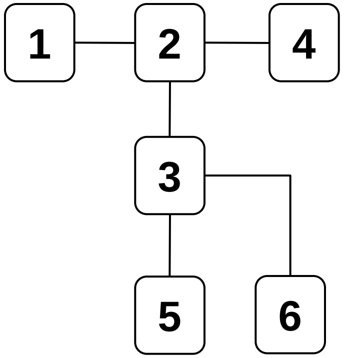
- What are the three policy actions a firewall can take?
  –
  –
  –

Answers:

- What are the five common types of firewall?
  - Packet filtering
  - Proxy
  - Stateful inspection
  - Circuit-level proxy (i.e., SOCKS)
  - Application proxy

- What are the three policy actions a firewall can take?
  - Accept
  - Deny
  - Discard

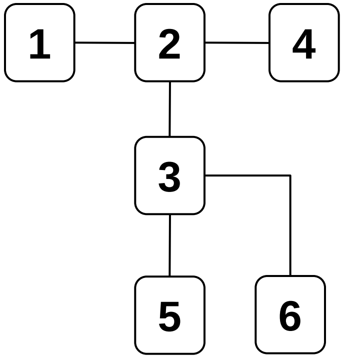
Questions:



- If **1** is a router, **4** is located in a DMZ. What is **2**?
  -

- If **3** is a switch, **5** is a N-IDS, and **6** is a computing platform. What does one have to do to the switch ports connected to **5** and **6**?
  -

Answers:



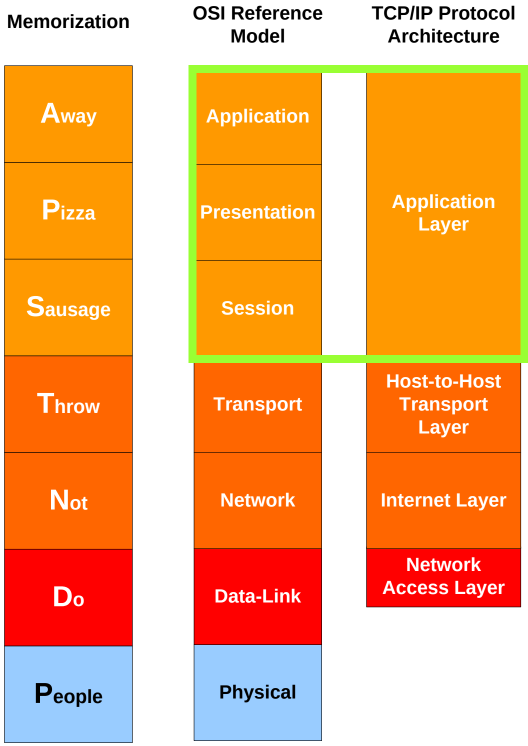
- If **1** is a router, **4** is located in a DMZ. What is **2**?
  - Firewall

- If **3** is a switch, **5** is a N-IDS, and **6** is a computing platform. What does one have to do to the switch ports connnected to **5** and **6**?
  - Provision a port span

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 – 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 – SET

Secure Electronic Transaction (SET) is a system for ensuring the security of financial transactions on the Internet. It was supported initially by MasterCard, Visa, Microsoft, Netscape, and others

- A user is given an *electronic wallet* (digital certificate) and a transaction is conducted and verified using a combination of digital certificates and digital signature among the purchaser, a merchant, and the purchaser's bank in a way that ensures privacy and confidentiality
- SET uses Netscape's SSL, Microsoft's STT (Secure Transaction Technology), and Terisa System's S-HTTP
- SET uses some but not all aspects of a PKI

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:
  - DNS cache poisoning, where the legitimate IP addresses are replaced
  - DNS spoofing, where the attacker spoofs the DNS server's answer with it's own IP address in source-address field
- Countermeasures:
  - Forbid recursive queries to prevent spoofing
  - Setup multiple DNS servers (External, internal)
  - Keep your BIND up to date

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

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
  - Enforce CM and Change Control
- Install Anti-Virus
- Disable all processes/services not in use
- Enforce strict access control
  - Network I/Fs
  - OS / Applications

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
    - Remote Client Access
    - Client-less Remote Access
  - 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)

Point-to-Point Tunneling Protocol (PPTP)

PPTP (Point-to-Point Tunneling Protocol) operates at Layer 2. (RFC 2637)

- A protocol which allows PPP (Point-to-Point Protocol) to be tunneled through an IP-based network.
  - PPTP packages data within PPP packets, then encapsulates the PPP packets within IP packets for transmission through an Internet-based VPN tunnel
- PPTP supports data encryption and compression
- PPTP also uses a form of GRE to get data to and from its final destination

Layer 2 Tunneling Protocol (L2TP)

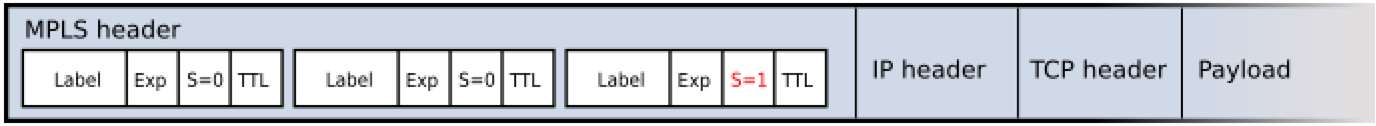
L2TP (Layer 2 Tunneling Protocol) operates at Layer 2. (RFC 2661)

- A protocol which allows PPP (Point-to-Point Protocol) to be tunneled through an IP-based network.
- It is a hybrid of PPTP and L2F can support multiple protocols
- Often combined with IPsec for security

Multi-Protocol Label Switching (MPLS)

MPLS (Multi-Protocol Label Switching) (a.k.a. Tag Switching), operates at Layer 2

- a data-carrying mechanism, operating at data-link layer. It was designed to provide a unified data-carrying service for both circuit-based clients and packet-switching clients which provide a datagram service model
- It can be used to carry many different kinds of traffic, including both voice telephone traffic and IP packets.
- It does not rely on encapsulation and encryption to maintain high-level of security



Generic Routing Encapsulation (GRE)

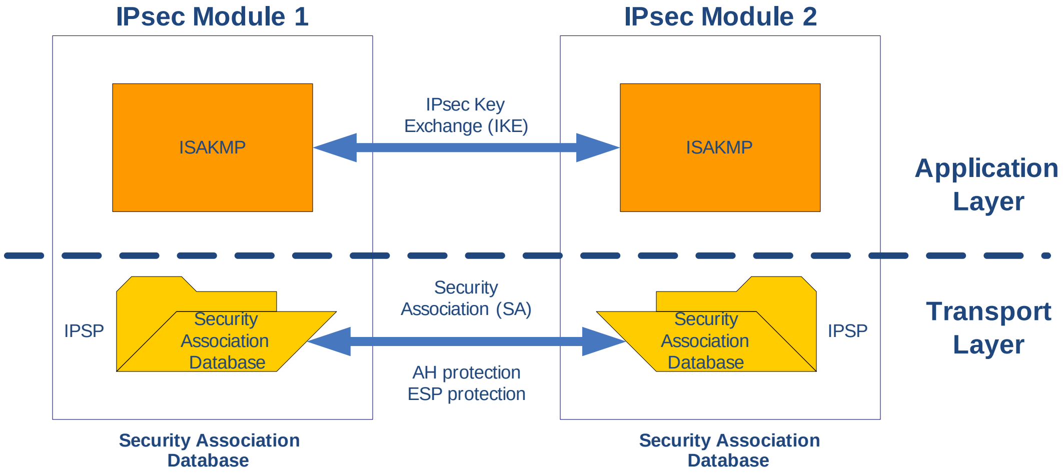
GRE (Generic Routing Encapsulation) (RFC 2784)

- GRE is a Network Layer tunnel that allows any network protocol to be transmitted over a network running some other protocol such as:
  - Transmitting multicast datagrams over a unicast network.
  - Transmitting non-TCP/IP routing protocols such as: AppleTalk, IPX, etc.
- GRE can be a security issue (i.e. packet-filtering), so recommended that GRE be created in front of a firewall.

IPsec... (1/6)

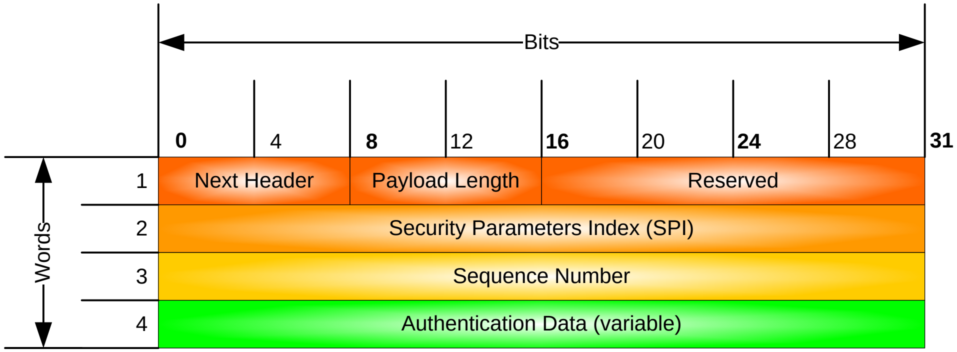
IPsec is a protocol suite (RFC ~~2401~~ 4301, 2411).

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


IPsec Module 1
IPsec Module 2
ISAKMP
IPsec Key Exchange (IKE)
ISAKMP
Application Layer
IPSP
Security Association Database
Security Association (SA)
Security Association Database
IPSP
Transport Layer
AH protection
ESP protection
Security Association Database
Security Association Database

IPsec… (2/6)

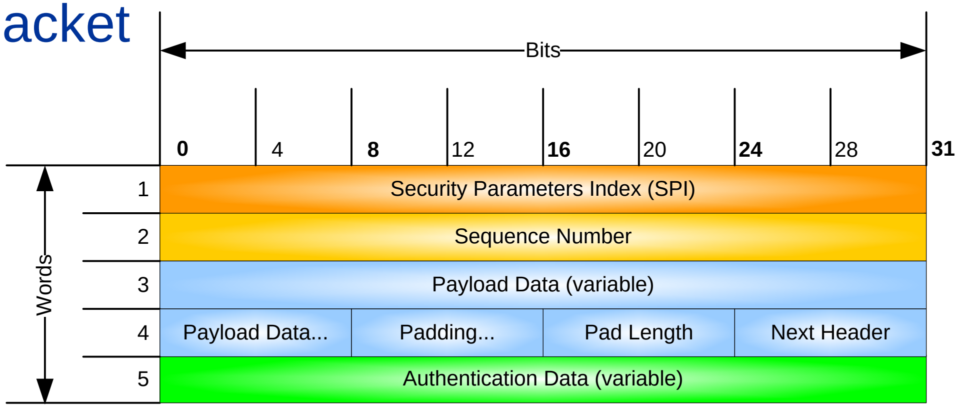
- Authentication Header (AH) (RFC 4302)
  - AH follows right after IP header
  - Next Header: Identifies the protocol of transferred data
  - Payload Length: Size of AH packet
  - SPI: Identifies the security parameters, which in combination with the IP address, identify the security association implemented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



Words	0–7	8–15	16–31
1	Next Header	Payload Length	Reserved
2	Security Parameters Index (SPI)		
3	Sequence Number		
4	Authentication Data (variable)		

IPsec... (3/6)

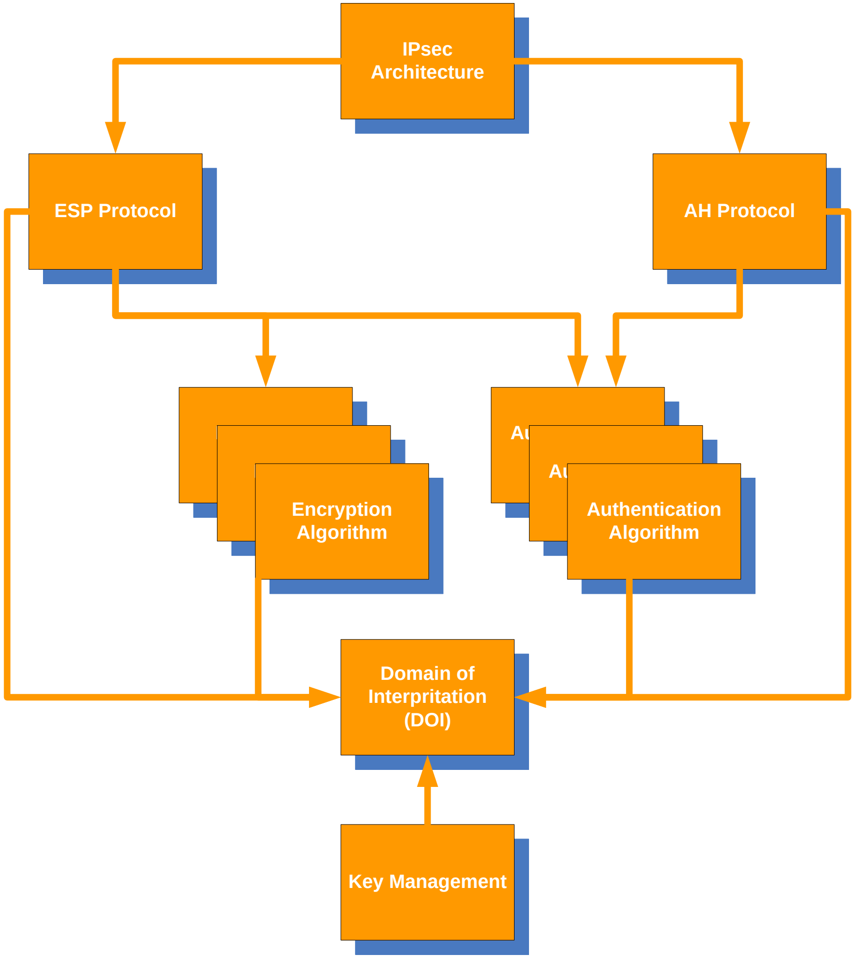
- Encapsulating Security Payload (ESP) (RFC 4303)
  - ESP operates directly on top of IP header
  - SPI: Identifies the security parameters in combination with the IP address
  - Sequence Number: Used to prevent replay attacks
  - Payload Data: The encapsulated data
  - Padding: Used to pad the data for block cipher
  - 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



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.
- Added per-packet handling- manifested by increased latency and possibly, reduced throughput
- 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 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

IPsec... (6/6)

IPsec is implemented in the following "popular" ways…

- Network-to-Network
  - IPsec tunnel between two security gateways
  - GRE/IPsec in established Layer 3 tunnel
  - L2TP/IPsec in established Layer 2 tunnel
- Host-to-Network
  - L2TP/IPsec in established Layer 2 tunnel via VPN client on remote client (i.e. your laptop or PC)
  - IPsec tunnel between VPN client to security gateway
- Host-to-Host
  - IPsec in transport mode or tunnel mode between two computing machines

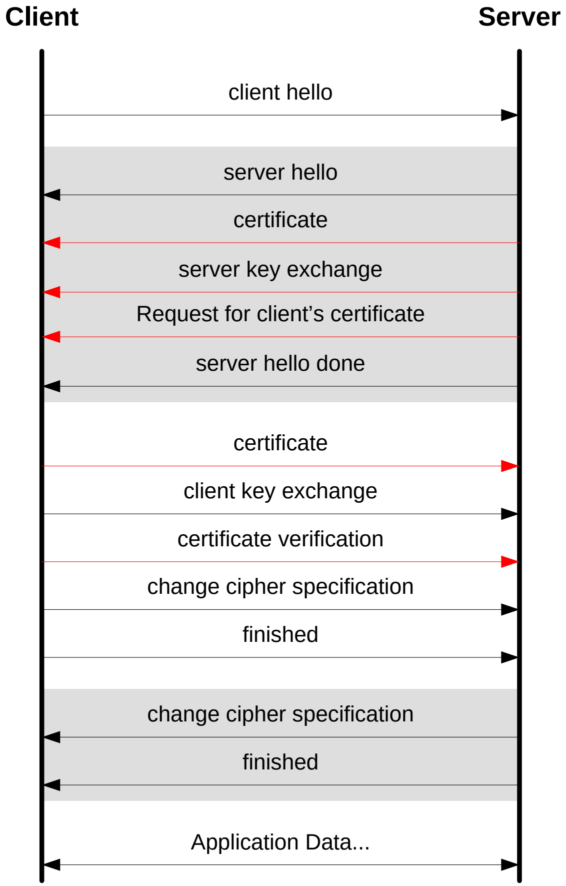
Reference:

- http://en.wikipedia.org/wiki/IPsec
- http://en.wikipedia.org/wiki/L2TP
- http://www.cisco.com/en/US/tech/tk583/tk372/tech_configuration_examples_list.html
- http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt4/scipsec.htm
- RFC 4301, *Security Architecture for the Internet Protocol* (http://tools.ietf.org/html/rfc4301)

Secure Sockets Layer (SSL)

SSL (Secure Sockets Layer)

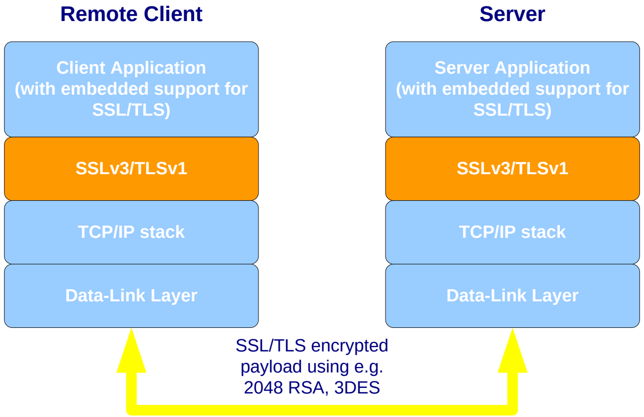
- Runs between the Application Layer (HTTP, SMTP, NNTP, etc) and Transport Layer (TCP)
- Supports client/server's negotiation of cryptographic algorithms:
  - Public-key cryptography: RSA, Diffie-Hellman, DSA or Fortezza
  - Symmetric ciphers: RC2, IDEA, DES, 3DES or AES
  - One-way hash functions: MD5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

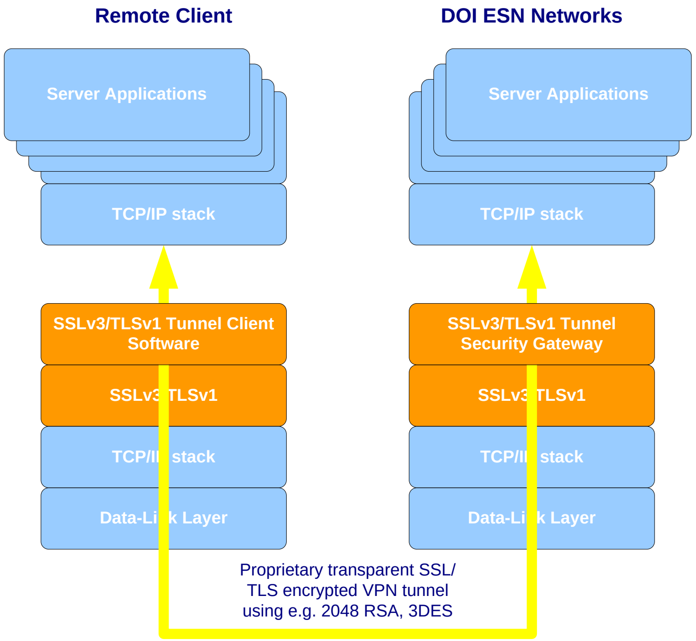


Reference: http://wp.netscape.com/eng/ssl3/

Secure Sockets Layer (SSL)

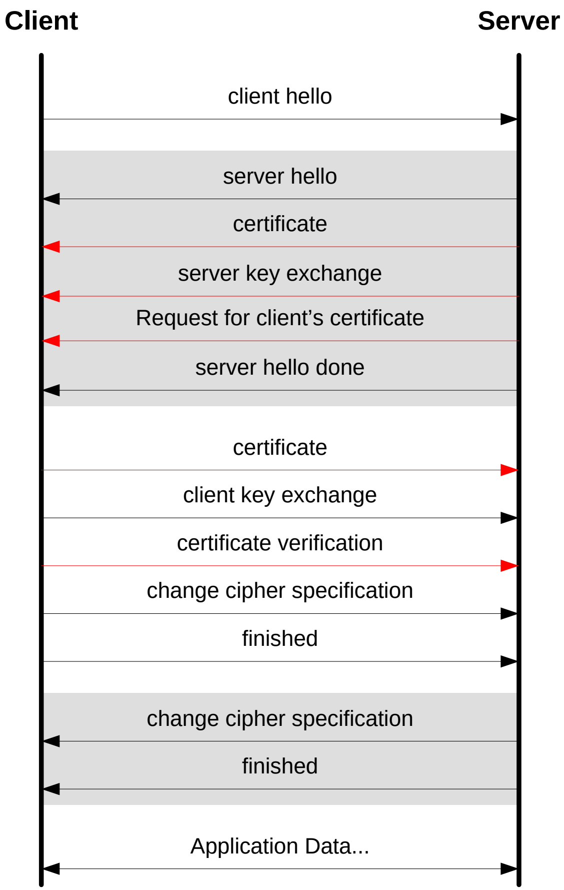
- SSL works in two modes:
  - Application embedded. i.e. HTTPS
  - SSL Tunnel or SSL VPN (e.g. OpenVPN)
- SSL VPN is less complex than IPsec…
  - Unlike IPsec, SSL protocol sits on top of Transport Layer stack.
  - OpenVPN (a.k.a. user-space VPN) because unlike IPsec, it operates out side of OS kernel.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

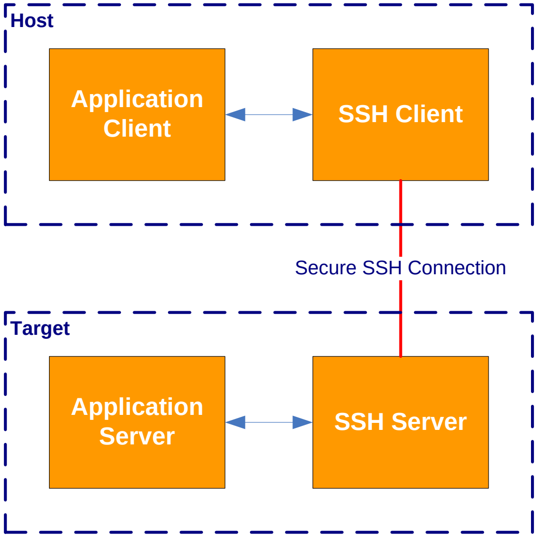
- TLS 1.0 (Transport Layer Security) (RFC 2246) is defined base on SSL 3.0
- TLS and SSL protocols are not interchangeable. (during a client/server session)
- The selection of TLS or SSL is negotiated between client/server at the “hello”.



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.
  - IP source routing



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

Questions:

- Why PPP can utilize PPTP and L2TP?
  –

- What are the two primary purposes to use GRE?
  –

  –

- What are the two operating modes for IPsec?
  –

  –

Answers:

- Why PPP can utilize PPTP and L2TP?
  - Because PPP allows multiple protocols per session

- What are the two primary purposes to use GRE?
  - Transmission of non-TCP/IP routing protocols (e.g., AppleTalk or IPX)
  - Transmission of multicast datagrams over a unicast network

- What are the two operating modes for IPsec?
  - Transport mode
  - Tunnel mode

Questions:

- Why IPsec requires AH protocol and ESP protocol?

  –

- SSL uses which three cryptosystems?

  –

  –

  –

- What are the two operating modes for SSL?

  –

  –

Answers:

- Why IPsec requires AH protocol and ESP protocol?
  - AH for authentication and ESP for encryption

- SSL uses which three cryptosystems?
  - Public-key (Asymmetric) (RSA, Diffie-Hellman, DSA or Fortezza)
  - Symmetric (RC2, IDEA, DES, 3DES or AES)
  - Hash function (MD5 or SHA)

- What are the two operating modes for SSL?
  - Application embedded
  - Tunnel mode

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).
  - DIAMETER.

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. (However, Cisco ACS does support authentication proxy to both UNIX and Windows servers.)
- 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

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 scale able.
- 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 – Diameter

Diameter (RFC 3588) is designed based on RADIUS that supports "Mobile-IP" services.

- Diameter protocol supports NAS, Mobile-IP, ROAMOPS (Roaming Operations), and EAP.
- Operates peer-to-peer (instead of client/server), supports multiple authentication proxy and broker models.
- Diameter supports both IPsec (mandatory) and TLS (optional).

Reference:

- RADIUS: http://www.ietf.org/rfc/rfc3579.txt
- Diameter:
  - http://tools.ietf.org/html/rfc4005 http://tools.ietf.org/html/rfc3588

Validation Time… ☺

1. Class Exercise

2. Review Answers

Exercise #1: VPN

- Please provide explanations for the following:
  - If you are running WPA2 (IEEE 802.11i) at home, why would you need to run IPsec to MITRE?
  - Why is running “split tunnel” bad?
  - How is “MITRE WiFi” WPA2 different than your home wireless network running WPA2? (Hint: IEEE 802.1X)

Exercise #2: Layers of Perimeter Security

- Please provide examples of network-based perimeter security controls and provide rationale:
  - For boundary protection at the edge?
  - For DMZ?
  - For enclave protection at the core (/ interior)?