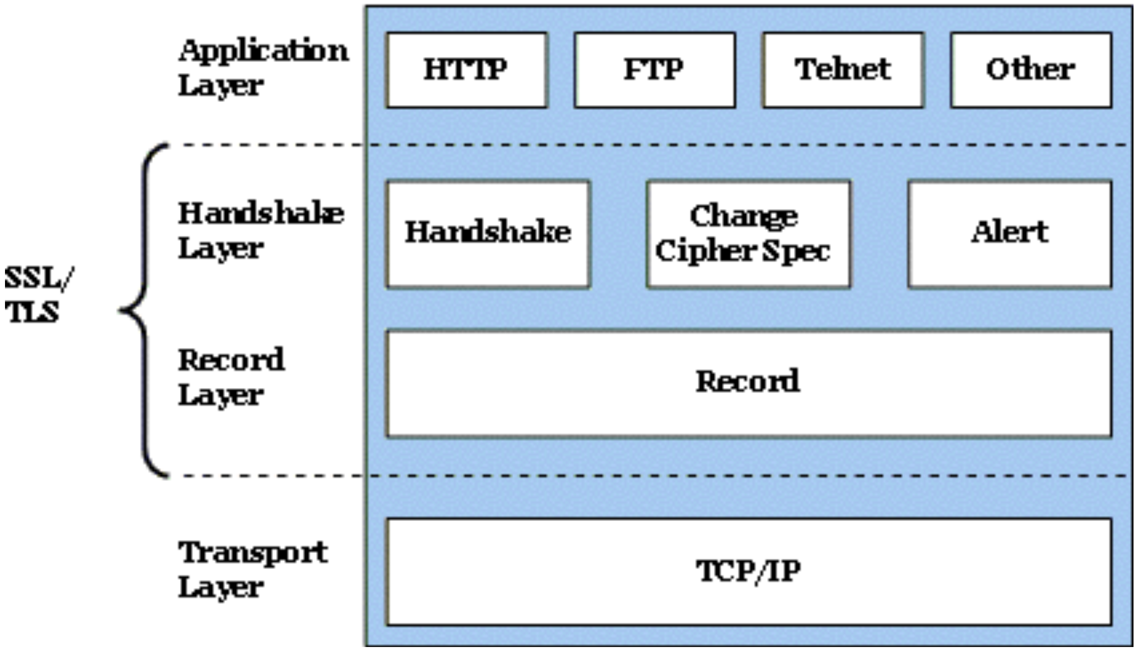
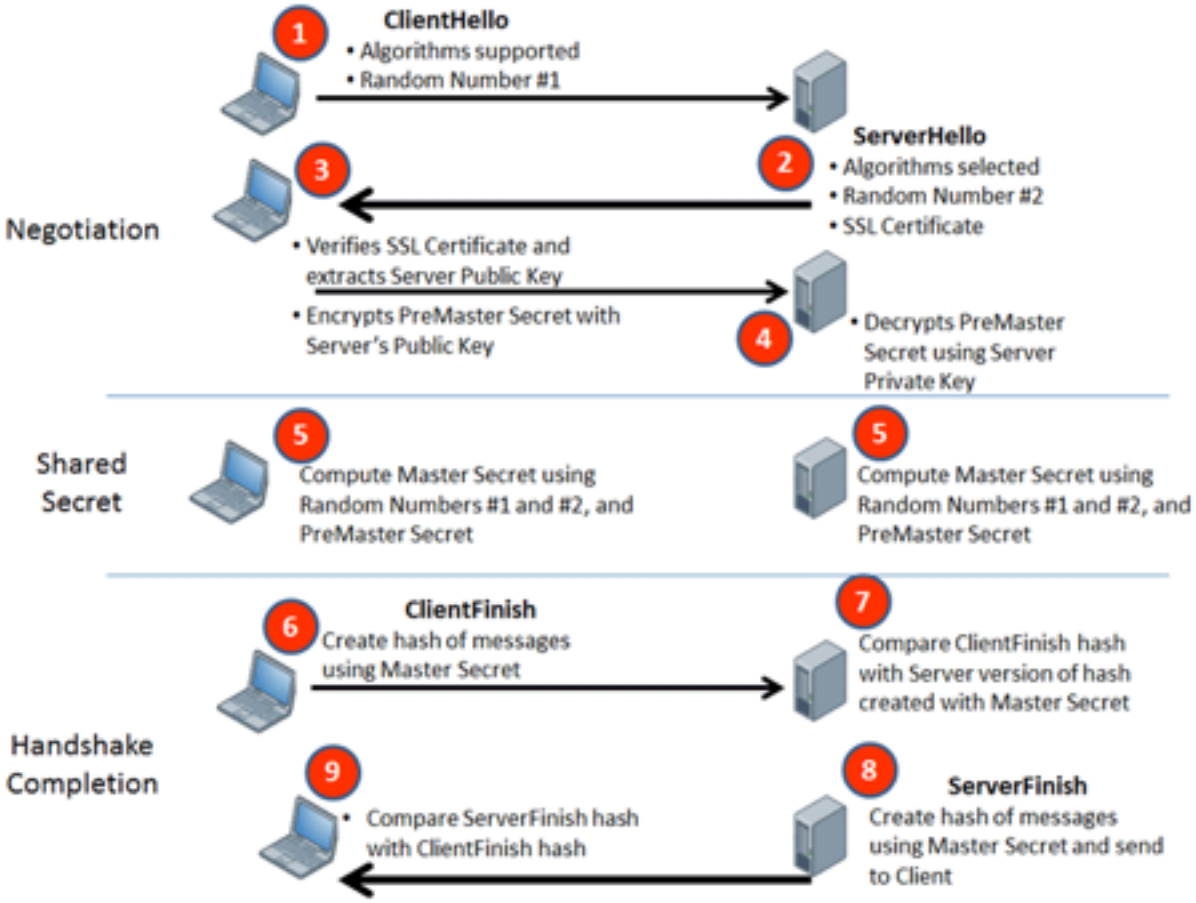
Q: What is SSL hand-shake protocols?

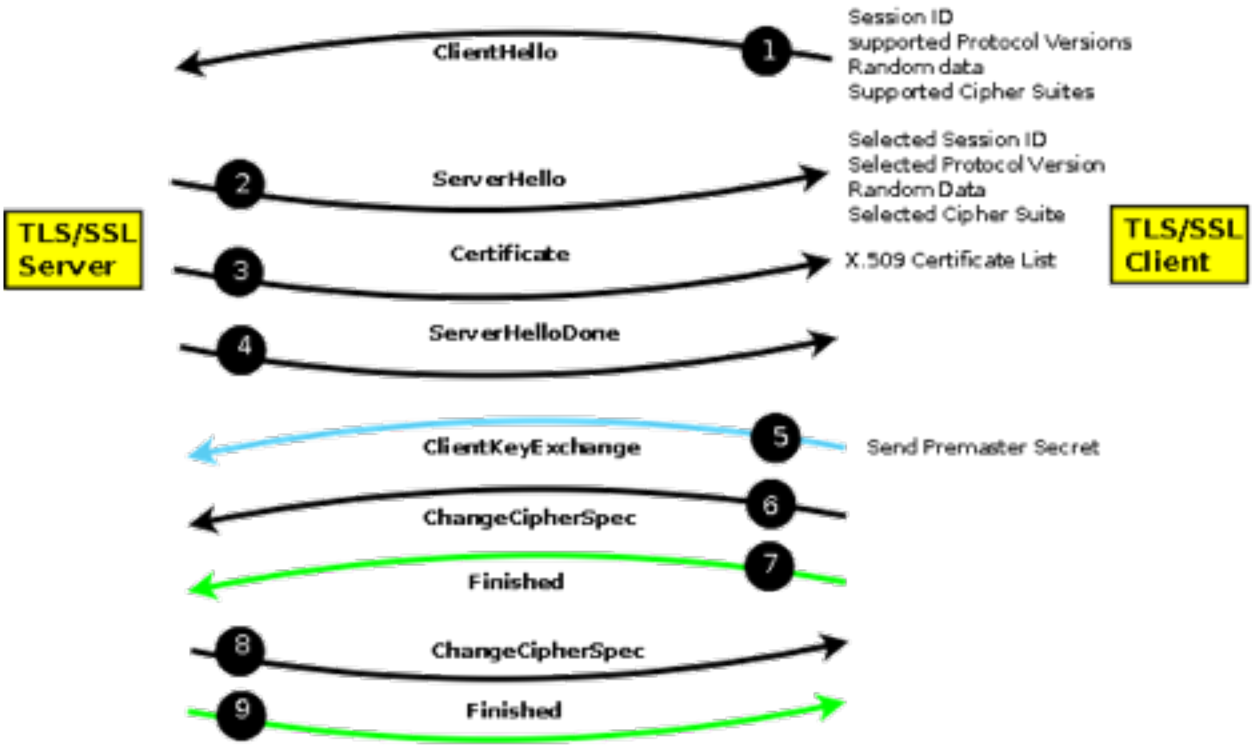
SSL/TLS Protocol Layers



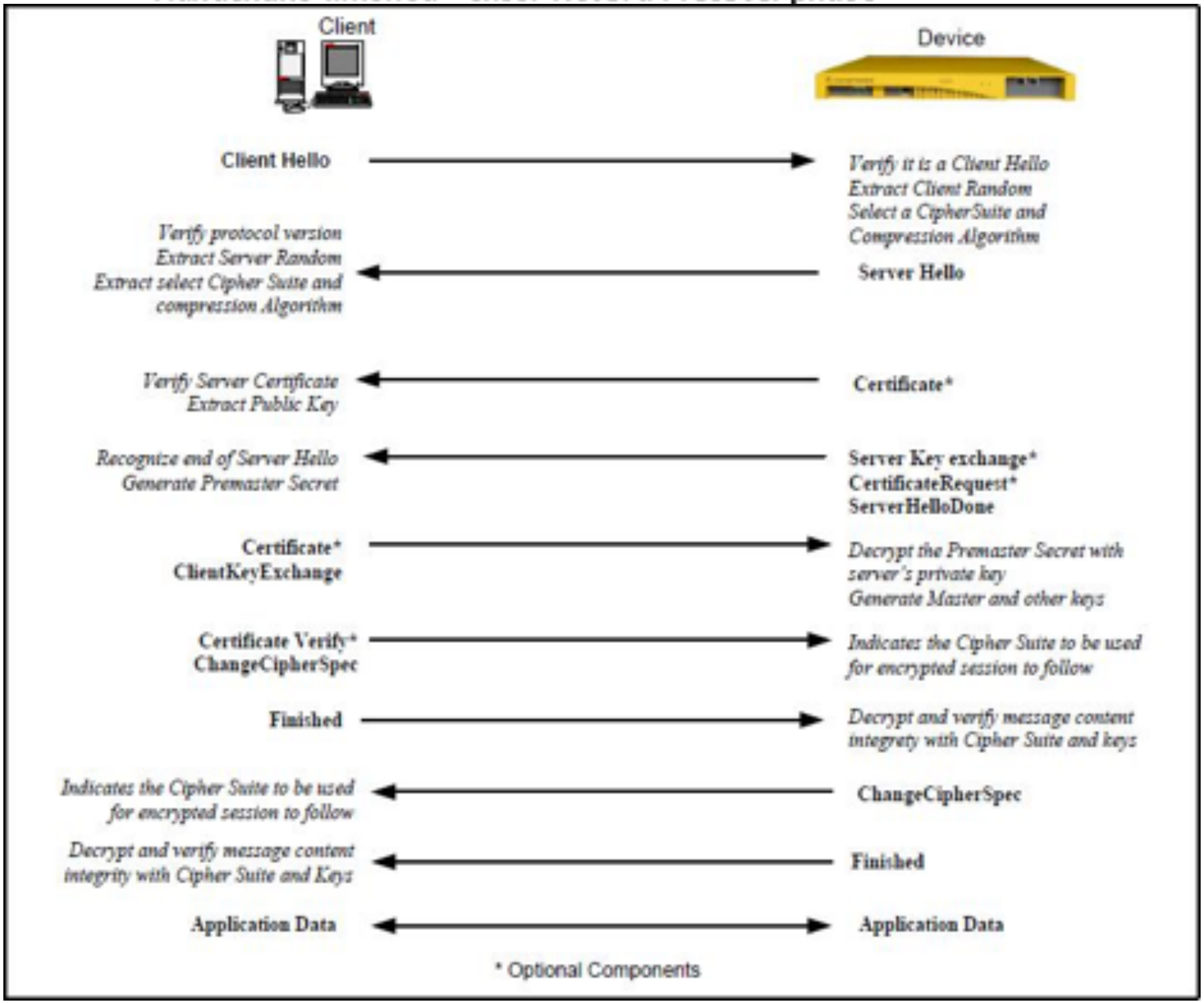

1
ClientHello
• Algorithms supported
• Random Number #1
2
ServerHello
• Algorithms selected
• Random Number #2
• SSL Certificate
Negotiation
3
• Verifies SSL Certificate and extracts Server Public Key
• Encrypts PreMaster Secret with Server's Public Key
4
• Decrypts PreMaster Secret using Server Private Key
Shared Secret
5
Compute Master Secret using Random Numbers #1 and #2, and PreMaster Secret
5
Compute Master Secret using Random Numbers #1 and #2, and PreMaster Secret
Handshake Completion
6
ClientFinish
Create hash of messages using Master Secret
7
Compare ClientFinish hash with Server version of hash created with Master Secret
8
ServerFinish
Create hash of messages using Master Secret and send to Client
9
• Compare ServerFinish hash with ClientFinish hash

TLS/SSL Protocol Sequences

Handshake Protocol



Handshake finished - enter Record Protocol phase


Client
Device
Client Hello
Verify it is a Client Hello
Extract Client Random
Select a CipherSuite and
Compression Algorithm
Verify protocol version
Extract Server Random
Extract select Cipher Suite and
compression Algorithm
Server Hello
Verify Server Certificate
Extract Public Key
Certificate*
Recognize end of Server Hello
Generate Premaster Secret
Server Key exchange*
CertificateRequest*
ServerHelloDone
Certificate*
ClientKeyExchange
Decrypt the Premaster Secret with
server's private key
Generate Master and other keys
Certificate Verify*
ChangeCipherSpec
Indicates the Cipher Suite to be used
for encrypted session to follow
Finished
Decrypt and verify message content
integrety with Cipher Suite and keys
Indicates the Cipher Suite to be used
for encrypted session to follow
ChangeCipherSpec
Decrypt and verify message content
integrity with Cipher Suite and Keys
Finished
Application Data
Application Data
* Optional Components

SSL/TLS are protocols used for encrypting information between two points. It is usually between server and client, but there are times when server to server and client to client encryption are needed. For the purpose of this blog, I will focus only on the negotiation between server and client.

For SSL/TLS negotiation to take place, the system administrator must prepare the minimum of 2 files: **Private Key and Certificate**. When requesting from a Certificate Authority such as Symantec Trust Services, an additional file must be created. This file is called **Certificate Signing Request**, generated from the Private Key. The process for generating the files are dependent on the software that will be using the files for encryption.

For a list of the server softwares Symantec has, have a look at: Symantec CSR Generation

Note that although certificates requested from Certificate Authorities such as Symantec are inherently trusted by most clients, additional certificates called Intermediate Certificate Authority Certificates and Certificate Authority Root Certificates may need to be installed on the server. This is again server software dependent. There is usually no need to install the Intermediate and Root CA files on the client applications or browsers.

Once the files are ready and correctly installed, just start the SSL/TLS negotiation by using the secured protocol. On browser applications it is usually https://www.yourwebsite.com.

Remember to use **your** secured website address. Above is just a sample address.

That will start the SSL/TLS negotiation:

Keys and Secrets during RSA SSL negotiation

The following is a standard SSL handshake when RSA key exchange algorithm is used:

1 **Client Hello**
- Information that the server needs to communicate with the client using SSL.
- Including SSL version number, cipher settings, session-specific data.
- Send a random number #1 to server

2. **Server Hello**
- Information that the client needs to communicate with the server using SSL.
- Including SSL version number, cipher settings, session-specific data.
- Including Server’s Certificate (Public Key)
- Send a random number #2 to client

3. **Authentication and Pre-Master Secret**
- Client **authenticates** the server certificate. (e.g. Common Name / Date / Issuer)
- Client (depending on the cipher) creates the pre-master secret for the session,
- **Encrypts** with the server's public key and sends the encrypted pre-master secret to the server.

4. **Decryption and Master Secret**
- Server uses its private key to **decrypt** the pre-master secret,
- Both Server and Client perform steps to generate the master secret with the agreed cipher using: random number #1, random number #2 and pre-master secret.

5. **Generate Session Keys**
- Both the client and the server use the master secret to generate the session keys, which are symmetric keys used to encrypt and decrypt information exchanged during the SSL session

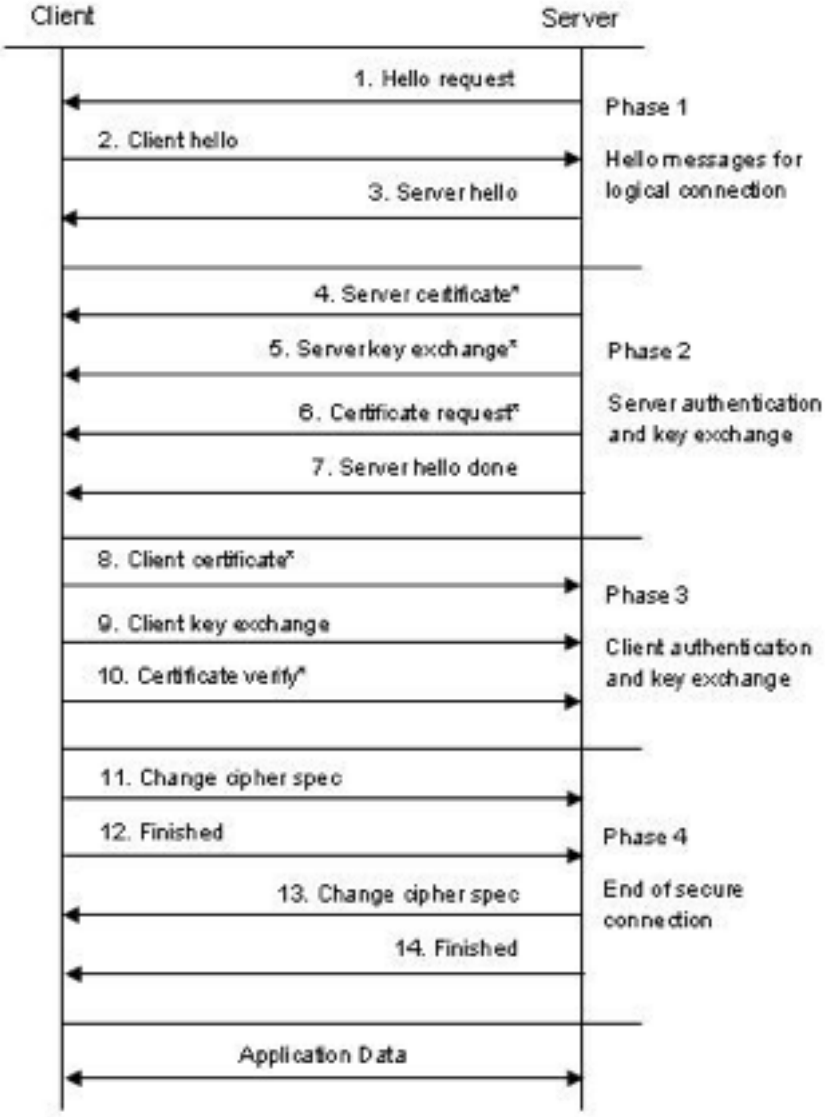
6. **Encryption with Session Key**
- Both client and server exchange messages to inform that future messages will be encrypted.

Tools such as OpenSSL can be used check the SSL/TLS negotiations:

```
OpenSSL s_client -connect www.symantec.com:443 -state -ssl3
Loading 'screen' into random state - done
CONNECTED(000001C0)
SSL_connect:before/connect initialization
SSL_connect:SSLv3 write client hello A
SSL_connect:SSLv3 read server hello A
depth=2 C = US, O = "VeriSign, Inc.", OU = VeriSign Trust Network, OU = "(c) 2006 VeriSign, Inc. - For authorized use only", CN = VeriSign Class 3 Public Primary Certification Authority - G5
```

```
SSL_connect:SSLv3 read server certificate A
SSL_connect:SSLv3 read server done A
SSL_connect:SSLv3 write client key exchange A
SSL_connect:SSLv3 write change cipher spec A
SSL_connect:SSLv3 write finished A
SSL_connect:SSLv3 flush data
SSL_connect:SSLv3 read finished A
---
Certificate chain
 0 s:/1.3.6.1.4.1.311.60.2.1.3=US/1.3.6.1.4.1.311.60.2.1.2=Delaware/businessCategory=Private
Organization/serialNumber=2158113/C=US/postalCode=94043/ST=California/L=Mountain View/
street=350 Ellis Street/O=Symantec Corporation/OU=Corp Mktg & Comms - Online Exp/
CN=www.symantec.com
```

There it is. SSL and SSL Negotiation summarized. Mission complete.



Asterisk (*) are optional or situation dependent messages that are not always sent.

Sumber : Rhee, M.Y. 2003. *Internet Security: Cryptographic Principles, Algorithms and Protocols*.

Q: What are some of the open source SSL tools?
Openssl

Q. Why you change jobs frequently last 6-7 years?

1. First, in the last few years, I have been looking for a growing sector in networking industry, but very few bright spots obvious have surfaced. If you have worked at network infrastructure like MPLS/Routign/Switching which have been very mature, then you probably would anxiously look for something that still have space to grow for quite a while. Many of my colleagues from Cisco moved to areas like storage, DCN, wireless, carrier ethernet etc. After a while, I have seen cloud/cyber security will be something could potentially grow very fast and could just got started for the another decade. And that is something people in silicon valley would like to work for.
2. Secondly, when you worked for companies that has either international background such as Huawei, or companies that went through changes like privatization such as Dell, they tend to be not stable in business due to regulation such as Huawei, or layoff such as Dell. That can be proved or well-known.
3. Also if you work as contractor like I did at AT&T, you tend to change after a while to work as employee.
4. Maybe sometimes it is just part of the nature of job, there is involuntary situation where you got involved into some complexity where the the whole team left the company and you don't want to be the only one left behind.

The bottom line is if you have the opportunity to work for a fast growing sector, a company in leadership like Palo Alto, and you know what you want to do and you want to catch up opportunities, then there is no reason to turn over easily.

Q. Can you recall a customer's RFP requirements?
- A major carrier customer in south America
- Replacement of existing wired network infrastructure.
- Data center inter-connect, IP/MPLS core, also they are looking at core Data Center.
- 1G Ethernet to upgrade to 10G/now, and 40/100G ethernet soon: customer wanted to know where we were heading in the future, we were calling that out through our solution development.

Key Objectives in RFP:
- Reduce network support costs(Total Cost of Ownership): technology front/solution front/management front. We didn't stay away from management too. Imperative to stress management tool. HP is leading at management capability.
- Enhance network availability and performance: hammer home our message and take advantage all the great technologies we can bring to the table, such as VSS like, vPC like, MCEC, a lot standard based technologies and the enhancement we added in Huawei and support for the emerging standards.
- Simplify network deployment: falling into the same category of lowering TCO.
- Provide support for emerging standards during the 7-10 years life cycle of the proposed solution

Q: What is the strategy to present solution to customer.

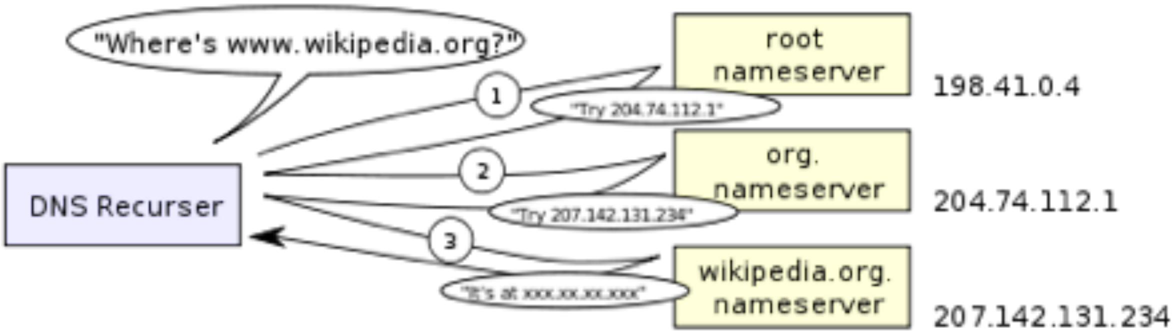
1. Understand customer key requirement to address the that with key messages/theme we pick out: Performance, availability, support for emerging standards, specially something being standard as opposed to being proprietary. what that means to customer which is important to customer.

Q: What happens when you type in a URL into a browser?

1. browser checks cache; if requested object is in cache and is fresh, skip to #9
2. browser asks OS for server's IP address
3. OS makes a DNS lookup and replies the IP address to the browser:

- **Browser cache** – The browser caches DNS records for some time. Interestingly, the OS does not tell the browser the time-to-live for each DNS record, and so the browser caches them for a fixed duration (varies between browsers, 2 – 30 minutes).
- **OS cache** – If the browser cache does not contain the desired record, the browser makes a system call (gethostbyname in Windows). The OS has its own cache.
- **Router cache** – The request continues on to your router, which typically has its own DNS cache. (??)
- **ISP DNS cache** – The next place checked is the cache ISP's DNS server. With a cache, naturally.
- **ISP Recursive search** – Your ISP's DNS server begins a recursive search, from the root nameserver, through the .com top-level nameserver, to Facebook's nameserver. Normally, the DNS server will have names of the .com nameservers in cache, and so a hit to the root nameserver will not be necessary.

Here is a diagram of what a recursive DNS search looks like:



Here is a more descriptive steps:

- Request a record You begin by asking your computer to resolve a hostname, such as visiting 'http://www.google.com' in a web browser. The first place your computer looks is its local DNS cache, which stores DNS information that the computer has recently retrieved.
- Ask the Recursive DNS servers If the records are not stored locally, your computer queries (or contacts) your ISP's recursive DNS servers. These

machines perform the legwork of DNS queries on behalf of their customers. The recursive DNS servers have their own caches, which they check before continuing with the query.

-Ask the Root DNS servers If the recursive DNS servers do not have the record cached, they contact the root name servers. These thirteen name servers contain pointers for all of the Top-Level Domains (TLDs), such as '.com', '.net' and '.org'. If you are looking for 'www.google.com.', the root name servers look at the TLD for the domain - 'www.google.com'- and direct the query to the TLD DNS name servers responsible for all '.com' pointers.

- Ask the TLD DNS servers The TLD DNS servers do not store the DNS records for individual domains; instead, they keep track of the authoritative nameservers for all the domains within their TLD. The TLD DNS servers look at the next part of the query from right to left - 'www.google.com' - then direct the query to the authoritative nameservers for ‘google.com'

- Ask the Authoritative DNS servers Authoritative nameservers contain all of the DNS records for a given domain, such as host records (which store IP addresses), MX records (which identify nameservers for a domain), and so on. Since you are looking for the IP address of 'www.google.com', the recursive server queries the authoritative nameservers and asks for the host record for ‘www.google.com'.

- Retrieving the record The recursive DNS server receives the host record for 'www.google.com' from the authoritative nameservers, and stores the record in i its local cache. If anyone else requests the host record for 'www.google.com', the recursive servers will already have the answer, and will not need to go through the lookup process again until the record expires from cache.

-The Answer! Finally, the recursive server gives the host record back to your computer. Your computer stores the record in its cache, reads the IP address from the record, then passes this information to the web browser. Your browser then opens a connection to the IP address '72.14.207.99' on port 80 (for HTTP), and our webserver passes the web page to your browser, which displays Google.

4 browser opens a TCP connection to server (this step is much more complex with HTTPS): The following is the OS software activities for constructing the first TCP packet.

- Lookup the local routing table for default gateway as the next hop if the destination IP address is not at the same subnet.
- Lookup the ARP table for the default-gateway’s MAC address. Mostly it has already exists. If not, broadcast ARP request: whoever has the IP address of x.x.x.x please tell me your MAC address.   the default-gateway respond with its MAC address.
- Construct the first TCP packet with the destination MAC as the gateway’s.

5 browser sends the HTTP request through TCP connection

6 browser receives HTTP response and may close the TCP connection, or reuse it for another request

7 browser checks if the response is a redirect or a conditional response (3xx result status codes), authorization request (401), error (4xx and 5xx), etc.; these are handled differently from normal responses (2xx)

8 if cacheable, response is stored in cache

9 browser decodes response (e.g. if it's gzipped)

10 browser determines what to do with response (e.g. is it a HTML page, is it an image, is it a sound clip?)

11 browser renders response, or offers a download dialog for unrecognized types. Assuming the response HTML and not an image or data file, then the browser parses the HTML to render the page. Part of this parsing and rendering process may be the discovery that the web page includes images or other embedded content that is not part of the HTML document. The browser will then send off further requests (either to the original web server or different ones, as appropriate) to fetch the embedded content, which will then be rendered into the document as well.

Q: What is loop guard?

When a none-designated port doesn't receive BPDU, without loop guard enabled, this port will transform into designated port and eventually in forwarding state. If you know in advanced that the network would potentially have a loop and configure loop guard at this port, not receiving BPDU on this port will not make this port a designated port and not ultimately put into forwarding state.

Q: What is Cisco APIC?

The Cisco Application Policy Infrastructure Controller (Cisco APIC) is the unifying point of automation and management for the Application Centric Infrastructure (ACI) fabric. The Cisco APIC provides centralized access to all fabric information, optimizes the application lifecycle for scale and performance, and supports flexible application provisioning across physical and virtual resources.

A little specifically, Cisco APIC also provides policy authority and resolution mechanisms. Cisco ACI policies define connectivity, security, and networking requirements for agile and scalable application deployments.

Q: What is Palo Alto Networks Eco System?

Partners:

StarLink (January 2015): Sell and support the offering through its network of channel partners in the GCC region

- Agari (November 2014): Provide email-based threat intelligence data; the enhanced threat prevention of malware and advanced persistent threats

- Easynet (September 2014): Simplify its security solutions with new portfolio of security services

- Skyhigh Networks (September 2014): Partnership to deliver enhanced data governance capabilities for cloud-based services

- Westcon (August 2014): Expands distribution agreement to span 40 countries during the next few years

- VMware (February 2014): Extends partnership and announced the VM-Series support for VMware virtual cloud infrastructure

- Citrix (February 2014): Delivers consolidated, multi-tenant network security for public and private clouds

Acquisition:

Cyvera (March 2014) and Morta Security (January 2014) will strengthen the enterprise security portfolio

Q. What is the five common types of Security Attacks?

Cyber attack No. 1: Socially engineered Trojans
Browse a trusted website and then got warning for malware, for a need of installing a new software, or for a need of defragment etc. The ultimate goal for such warning is prompt the user to install some form of software. After the software is installed, attacker's mission is completed.

Cyber attack No. 2: Unpatched software
Coming in a distant second is software with known, but unpatched exploits. The most common unpatched and exploited programs are Java, Adobe Reader, and Adobe Flash.

Cyber attack No. 3: Phishing attacks

I think of an effective phishing email as a corrupted work of art: Everything looks great; it even warns the reader not to fall for fraudulent emails. The only thing that gives them away is the rogue link asking for confidential information.

Cyber attack No. 4: Network-traveling worms
Today, if you say computer viruses aren't much of a threat anymore, but their cousins which are network-traveling worms cousins are more of a threat. I am not a virus expert but I can only remember a couple of names that most organizations have had to fight like Conficker and Zeus. We don't see the massive outbreaks of the past with email attachment worms, but the network-traveling variety is able to hide far better than its email relatives.

Cyber attack No. 5: Advanced persistent threats (APT)
Lastly, APTs usually gain a foothold using socially engineered Trojans or phishing attacks.

A very popular method is for APT attackers to send a very specific phishing campaign -- known as spearphishing -- to multiple employee email addresses. The phishing email contains a Trojan attachment, which at least one employee is tricked into running. After the initial execution and first computer takeover, APT attackers can compromise an entire enterprise in a matter of hours. It's easy to accomplish, but it is pain to clean up.

Q. Can you describe easy VPN negotiation?

- Clients starts ISAKMP Phase I with Server
  - Client sends Group name along with Phase 1 parameters
  - Authentication of Group determines Client's policy
- If successful, Server pushes options to clients
  - E.g. Tunnel IP, DNS, WINS, Split ACL settings etc.
  - Considered ISAKMP Phase 1.5
- ISAKMP Phase 1.5 made up of two portions
  - Mode Configuration (Mode CFG)
    - Extension to ISAKMP message exchange
    - CFG_REQUEST/CFG_REPLY
    - CFG_SET/CFG_ACK
    - Used to request/set various attributes, e.g. allow client to request a VPN IP address
  - Extended Authentication (Xauth)
    - ISAKMP authenticates only the device, i.e. Group authentication
    - Xauth implements two-factor authentication, i.e. per-user authentication
    - Supports various methods of authentication, i.e. CHAP username/password, RSA Secure ID, etc.
  - Easy VPN Remote (Initator) supports tow Modes of operation
    - Client mode
      - Easy VPN Server assigns new IP address to Client
      - Client run PAT to the Easy VPN IP
    - Network Extension Mode (NEM)
      - No IP address assigned by Server
      - No NAT/PAT performed on the client
      - Sometimes called Hardware Client

- Remote subnets are visible to the headend and remote resources can be accessed by their native IP.

- Network Extension Plus Mode:

- Identical to Network Extension Mode but with IP address assigned from the configured VPN pool, potentially used for troubleshooting purpose

Q. What is stateful failover in firewall?

A: Every time a session is created for a flow of traffic on the primary node, it is synced to the secondary node. When the primary node fails, sessions continue to pass traffic through the secondary node without having to re-establish.

Q. What is VPN and describe IPsec VPN

A: Virtual Private Network (VPN) creates a secure network connection over a public network such as the internet.

IPsec VPN means VPN over IP Security allows two or more users to communicate in a secure manner by authenticating and encrypting each IP packet of a communication session.

Q. What is Site to Site and remote access VPN?

A: A site-to-site VPN allows offices in multiple locations to establish secure connections with each other over a public network such as the Internet. Site-to-site VPN is different from remote-access VPN as it eliminates the need for each computer to run VPN client software as if it were on a remote-access VPN.

Q. How do you check the status of the tunnel's phase 1 & 2 ?

A: Use following commands to check the status of tunnel phases:

Phase 1 : show crypto isakmp and State : MM_ACTIVE

Phase 2 : show crypto ipsec sa

Note: if you have lot of tunnels and the output is confusing use a 'show crypto ipsec sa peer 12.12.12.12' command instead.

Q. What is SSL VPN? How it is different from IPsec VPN?

A: SSL VPN provides remote access connectivity from almost any internet enabled location without any special client software at a remote site. You only need a standard web browser and its native SSL encryption.

IPsec is a dedicated point-to-point fixed VPN connection where SSL VPNs provides anywhere connectivity without any configuration or special software at remote site.

Q. What is GRE and why is it required?

A: Generic Routing Encapsulation (GRE) is a protocol that encapsulates packets in order to route other protocols over IP networks.

GRE enables a wrapper to be placed around a packet during transmission of the data. A receiving GRE removes the wrapper, enabling the original packet to be processed by the receiving stack.

Advantages of GRE tunnels include the following:

GRE tunnels connect discontinuous sub-networks.
GRE tunnels allow VPNs across wide area networks (WANs).
GRE tunnels encase multiple protocols over a single-protocol backbone.
GRE tunnels provide workarounds for networks with limited hops.

Q. Firewalls work at what layer? Define firewall generations and their roles.

A: Firewalls work at layer 3, 4 & 7. First generation firewalls provide packet filtering and they generally operate at layer 3 (Network Layer). Second generation firewalls operate up to the Transport layer (layer 4) and records all connections passing through it and determines whether a packet is the start of a new connection, a part of an existing connection, or not part of any connection. Second generation firewall is mainly used for Stateful Inspection.

Third generation firewalls operate at layer 7. The key benefit of application layer filtering is that it can “understand” certain applications and protocols (such as File Transfer Protocol (FTP), Domain Name System (DNS), or Hypertext Transfer Protocol (HTTP)).

Q. What is DoS attack? How can it be prevented?

A: DoS (Denial of Service) attack can be generated by sending a flood of data or requests to a target system resulting in a consume/crash of the target system’s resources. The attacker often uses ip spoofing to conceal his identity when launching a DoS attack.

Q. What is IP Spoofing?

A: An IP spoofing attack enables an attacker to replace its identity as trusted for attacking host. For example, if an attacker convinces a host that he is a trusted client, he might gain privileged access to a host.

Q. What are the security-levels in cisco ASA?

A: ASA uses security levels to determine the parameters of trust given to a network attached to the respective interface. The security level can be configured between 0 to 100 where higher number are more trusted than lower. By default, the ASA allows packets from a higher (trusted) security interface to a lower (untrusted) security interface without the need for an ACL explicitly allowing the packets.

Q. What is AAA?

A: AAA stands for authentication, authorization and accounting, used to control user’s rights to access network resources and to keep track of the activity of users over a network. The current standard by which devices or applications communicate with an AAA server is the Remote Authentication Dial-In User Service (RADIUS).

Q. What is IPS? How does it work?

A: An Intrusion Prevention System (IPS) is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits. An Intrusion Prevention System can play a good role to protect against various network security attacks such as brute force attacks, Denial of Service (DoS) attacks, and vulnerability detection. Moreover, an IPS also ensures prevention against protocol exploits.

Intrusion Prevention System uses four types of approaches to secure the network from intrusions which include:

Signature-Based
Anomaly-Based
Policy-Based
Protocol-Analysis-Based

Q: What is SSL?

- SSL is an application layer (Layer 7) cryptographic protocol that provides secure communications over the Internet for web browsing, e-mail, instant messaging, and other data traffic.
- SSL, which was originally developed by Netscape and released in 1996, later served as the foundation for the IETF standard—Transport Layer Security (TLS) protocol.
- Although SSL and TLS vary in some respects and are not interoperable, the protocol architecture largely remains the same. The primary objective of both protocols is to provide data privacy and data integrity, thereby providing secure communications between applications. By default, SSL uses TCP port 443.

Q: What is SSL VPN?

- SSL VPN offers remote access solution using native SSL encryption of a web browser.
- SSL is flexible and low-cost without any special-purpose and pre-installed client software.
- SSL VPN can be used on any internet connected PC with web browser.
- SSL VPN allows optional client-server application to be downloaded dynamically with different files such as Java, ActiveX, or .exe

Q: What is SSL VPN Access mode?

- Clientless mode (Layer 7): Clientless mode provides secure access to web resources and access to web- based content. This mode is useful for accessing content that can be accessed in a web browser, such as Internet access, databases, and online web-based tools. Clientless mode can also offer remote file sharing by using the common Internet file system (CIFS) that provides a list of file server links in the web portal page, thereby allowing the remote user to browse listings of domains, servers, and directory folders, download a file, create a new file/directory, and so on. Clientless mode is limited to web-based content only.

- Thin Client mode (Layer 7, also known as port forwarding): Thin-Client SSL VPN technology can be used to allow secure access for applications that use static ports. Examples are Telnet (23), SSH (22), POP3 (110), IMAP4 (143), and SMTP (25). The Thin-Client can be user-driven, policy-driven, or both. A remote client must download a small, Java-based applet for secure access of TCP applications that use static port numbers. UDP is not supported. Examples include access to POP3, SMTP, IMAP, SSH, and Telnet. The user needs local administrative privileges because changes are made to files on the local machine. This method of SSL VPN does not work with applications that use dynamic port assignments, for example, several FTP applications.
- Thick Client mode (Layer 3, also known as tunnel mode or full tunneling client): delivered dynamically by downloading SSL VPN Client (SVC) software or the Cisco AnyConnect VPN client software from the VPN server appliance. This mode delivers a lightweight, centrally configured, and easy-to-support SSL VPN tunneling client that provides full network layer (Layer 3) access to virtually any application.

Q: What is IPSec?

- A set of security protocols and algorithms used to secure IP data at the network layer
- IPSec provides data confidentiality (encryption), integrity (hash), authentication (signature/certificates) of IP packets while maintaining the ability to route them through existing IP networks

Q: What is IKE?

- IKE is a “meta” protocol comprising:

  - Oakley (RFC 2412)
  - ISAKMP (Internet Security Association and Key Management Protocol)
  - SKEME (Secure Key Exchange Mechanism)
- Negotiating various IPSec options.
- Authenticating both sides.
- Exchange public keys
- Managing sessions keys after exchange.
- Negotiating various IPSec options.
- Authenticating both sides.
- Exchange public keys
- Managing sessions keys after exchange.
- IKE uses UDP port 500
- SKEME authenticates both sides of the IKE SA using public key encryption
- Oakley is Mode Based Mechanism used to derive encryption key for the session.

- ISAKMP is the message exchange architecture to define message format and state transition
- Protocol structure is difficult to implement and scale. IKE v2 is under way

Q: What is IKE Phase I and II?

- Phase I uses Main Mode or Aggressive Mode. End Goal is to establish IKE or ISAKMP SA.

  - Negotiate parameters

  - Exchange and generate keys

  - Authenticate both side

- Phase II uses Quick Mode. End Goal is to establish IPsec SA.

  - Agreeing on parameters for IPsec SA

  - In Perfect Forward Secrecy (PFS), redo DH exchange

Q: Can you describe what does IKE phase I do?

- Establish ISAKMP
- Main mode: six-way packet exchange
- Aggressive mode: three-way packet exchange, at dialup environment
- **Negotiate IKE policies** (message types 1 and 2): Diffie-Hellman group, encryption algorithm such as 3DES, Hashing such as MD5, and authentication mechanism such as Preshared etc.
- **Performs authenticated DH exchange** (messages 3 and 4):
  1)Exchange DH public key and a random number.

  2) Calculate a set of common session keys. Totally 3 keys are generated.

  - key 1 to calculate other keys

  - key 2 to provide data integrity and authentication

  - key 3 to encrypt Messages 5 & 6

- **Authenticate IKE peers' identity** (messages 5 and 6) --- 2 peers authenticate each other by sending its identity payload (IP address and hostname) as well as the hashed identity payload value for authentication purpose. Messages 5 and 6 are encrypted using the agreed upon encryption methods by message 1 and 2.

Q: Can you describe what does IKE phase II do?

- Establish **IPSec SA** using the existing IKE SA (notice the difference between IPSec SA and IKE SA)
- Called IKE Quick Mode
- Peers were already authenticated in Phase I so only two messages are needed

- Establish IPSec security parameters.
- SA Lifetime
- Proxy Identities
  - Defines what traffic will be protected
  - Also called Proxy ACL
- Periodically **renegotiate IPSec SA**
  - **Encapsulation protocol, encryption & authentication methods and modes:**
    - **ESP vs AH**
    - **MD5(128bit), SHA(160bit), SHA256, SHA384, SHA512**
    - **DES vs. 3DES vs. AES/AES-GCM/AES-GMAC(128bit,192bit,256bit)**
    - **Tunnel vs Transport mode**
- Optional additional Diffie-Hellman exchange.
- PFS (Perfect Forward Secrecy): a property that forces the peers to generate a new DH secret during the quick mode exchange, and this new DH secret in turn is used to generate a new encryption key.
- Message Type I: authenticate both sides again, select a random number, IPsec SA proposal payload provide a public key. The IPSec SA parameters could be:

 - Encapsulation: ESP

 - Integrity checking: SHA-HMAC

 - DH group: 2

 - Mode: Tunnel/Transport

- Message Type II: responding party generate a hash, authenticate itself, select a random number, accepts the SA by the initiating peer.
- Message Type III: acknowledge information from the initiator to the responder.

Q: What is Diffie-Hellman(DH) group?

- Oakley uses DH algorithm to negotiate a session key to encrypt IKE information.
- Only exchange public key and a random number. No secret key needs to exchange
- Each side calculates the “shared” secret key
- DH is vulnerable to man-in-the-middle attacks. SKEME is used to authenticate DH peer.

- Different DH groups mean different number bits being used. Group 1 uses 768-bit, Group II uses 1024-bit and Group 5 uses 1536 bit.

Q: What is Perfect Forward Secrecy(PFS)?

- A mechanism to generate new sessions keys when new negotiation of ISAKMP and IPsec SAs occurs.
- When enabled, PFS guarantees an independent keys from the previous session keys will be generated.
- PFS is based on DH and its strength depends on the DH group to generate primes with different sizes. Group 1,2,5 is used.
- PFS is configured at IPsec crypto map.

Q: What Encryption options will IPSec use?

- DES (Data Encryption Standard)

  - 1977 standards. Should not be used
  - 56 bits DES ciphertext was cracked in 22 hours.
- 3DES

  - Encrypt 3 times with 3 different 56-bit keys.
  - Used in most IPsec and VPN
- AES (Advanced Encryption Standard)

  - Ratified by the U.S. National Institute of Standards and Technology
  - Support 128, 192, and 256 bitss.
  - Defined in Federal Information Processing Standards (FIPS) publication 197.
  - Should make sure vendors support it soon.

Q: What is Authentication Header(AH)?

- Authentication option for IPsec
- Provide connectionless integrity and data origin authentication and optional against replays
- IP port 51
- “Next header” field in AH decides Tunnel/Transport mode

  - Tunnel mode: next header = 4
  - Transport mode: next header = TCP/UDP
- RFC 2402
- No Encryption (Data confidentiality)
- Authentication (Data integrity) --- Yes.
- Data origin authentication – Authentication data. HMAC-MD5-96 & HMAC-SHA-1-96

- Replay detection -- sequence number
- SPI --- arbitrary 32-bit value, in combination with destination IP, uniquely identify and SA for this datagram.
- IP header protection – Yes, both at transport mode and tunnel mode. Except some fields such as TTL, CRC, TOS and Fragment, it encrypts the whole IP packet header and data excluding some the fields such as IP header CRC , TTL, TOS, Flag and Offset

- AH is used for authentication only, NOT encryption.
- AH Header is 16 bytes long.
- *Authentication is performed by hashing over nearly all the fields of the IP packet (excluding those which might be modified in transit, such as TTL or the header checksum), and stores this in a newly-added AH header and sent to the other end.*
- **next hdr:** This identifies the protocol type of the following payload, and it's the original packet type being encapsulated: this is how the IPsec header(s) are linked together.AH lenThis defines the length, in 32-bit words, of the whole AH header, minus two words (this "minus two words" proviso springs from the format of IPv6's RFC 1883 Extension Headers, of which AH is one).
- **Authentication Data: This is the Integrity Check Value calculated over the entire**
- **Security Parameters Index (SPI): opaque 32-bit identifier identify a SA.**

Q: What is Encapsulating Security Payload(ESP)?

Supports authentication, encryption and anti-replay.

- IP port 50
- RFC 2406
- Encryption (Confidentiality) --- DES and 3DES to encrypt IP data
- Authentication (Data integrity) --- Authentication data with an Integrity Check Value (ICV) at packet tail. HMAC-MD5-96 & HMAC-SHA-1-96. Only authenticate ESP header + encrypted data, NO IP header.
- Data origin authentication – Authentication data at packet tail. HMAC-MD5-96 & HMAC-SHA-1-96
- Replay detection -- sequence number
- SPI --- arbitrary 32-bit value, in combination with destination IP, uniquely identify and SA for this datagram.
- IP header protection --- No, only encrypt IP data, not headers. The details:

  - Tunnel mode: The new IP header is not protected. The original IP packet including IP header is encrypted.

  - Transport mode: The original IP header is not protected. Only the data portion of the IP packet is encrypted.

- ESP has variable length because of encrypted data.
- ESP header is 8 bytes long followed ESP payload.
- Encrypted payload has variable length
- Optional authentication data at the end of the ESP encapsulation.

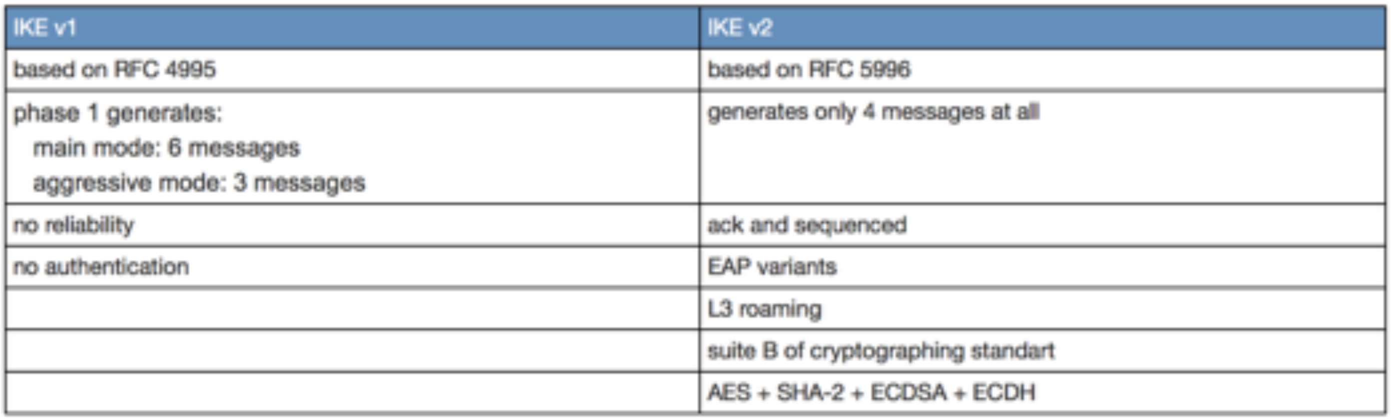
Q: What is the difference between IKEv1 an IKEv2?
1.IKEv2 does not consume as much bandwidth as IKEv1.
2.IKEv2 supports EAP authentication while IKEv1 doesn't.
3.IKEv2 supports MOBIKE while IKEv1 doesn't.
4.IKEv2 has built-in NAT traversal while IKEv1 doesn't.
5.IKEv2 can detect whether a tunnel is still alive while IKEv1 cannot.

An IKEv2 child SA is known as a Phase 2 SA in IKEv1. The child SA differs in behavior from the Phase 2 SA in the following ways:

- IKE and child SA rekeying—In IKEv2, a child security association (SA) cannot exist without the underlying IKE SA. If a child SA is required, it will be rekeyed; however, if the child SAs are currently active, the corresponding IKE SA will be rekeyed.

IKE Properties

- Negotiate SA attributes
- Generate and refresh keys using DH
- authenticate peer devices using many attributes (like IP, FQDN, LDAP DN and more). Note: LDAP stands for Lightweight Directory Access Protocol. It is an application protocol used over an IP network to manage and access the distributed directory information service.
- It has two phases
  1 determine transforms, hashing and more
    - ○ main mode
    - ○ aggressive mode
  2 ISAKMP negotiates SA for IPSEC



IKE v1	IKE v2
based on RFC 4995	based on RFC 5996
phase 1 generates: main mode: 6 messages aggressive mode: 3 messages	generates only 4 messages at all
no reliability	ack and sequenced
no authentication	EAP variants
	L3 roaming
	suite B of cryptographing standart
	AES + SHA-2 + ECDSA + ECDH

        - quick mode
        - sdoi mode

Q: What is the IPSec Tunnel Mode and Transport Mode?

- **Tunnel Mode:** The original IP header is not used to transport the packet. Instead, a new IP header is tagged in front of the ESP or AH header. The new IP header contains the IP addresses of the two IPsec peers as the source and destination IP addresses. Good for RFC 1918 private addresses. The most widely used mode in IPsec deployment.
- **Transport Mode:** The original IP header is being used to transport the packet, an additional header for ESP or AH is inserted between the IP header and pay load.
- Tunnel mode is preferred everywhere.

- private addressing is allowed

- big range of connectivity options

- required in site-to-site VPNs and remote VPNs.

- NAT works only with Tunnel mode
- Transport mode is used in combination with GRE for the purpose of encapsulation efficiency.

Q: What is IPSec NAT Traversal?

- IPSec NAT Traversal (NAT-T) feature introduces support for IPSec traffic to travel through NAT points in the network.
- There are three parts to NAT Traversal.
- The first is to determine if the remote peer supports NAT Traversal. The second is to detect the presence of a NAT function along the path between the peers.
- The third is to determine how to deal with NAT using UDP encapsulation.
- Support is negotiated in first two IKE messages. Both peers need to support it. Most device supports NAT-T
- NAT-T requirement detected in IKEv1 messages 3 and 4. Receiver detects that by looking at the destination IP address and the identify address.
    - If NAT-T is required, IKEv1 messages 5&6 change to UDP 4500
    - If NAT-T is required, Phase 2 change to UDP 4500

Q: What is Transparent Tunneling ?

- Negotiate a customer UDP port when going through stateful firewall. This is not for NAT.
- Stateful firewall doesn't support inspection of ESP.

Q: What ports does IPSec Control plane use?

-UDP 500 (default)

- UDP 4500 (If NAT is used)
- TCP customer port (only if gateway is ASA). IKEv1 payload inside TCP

Q: What is Oakley in IPSec protocol stack?

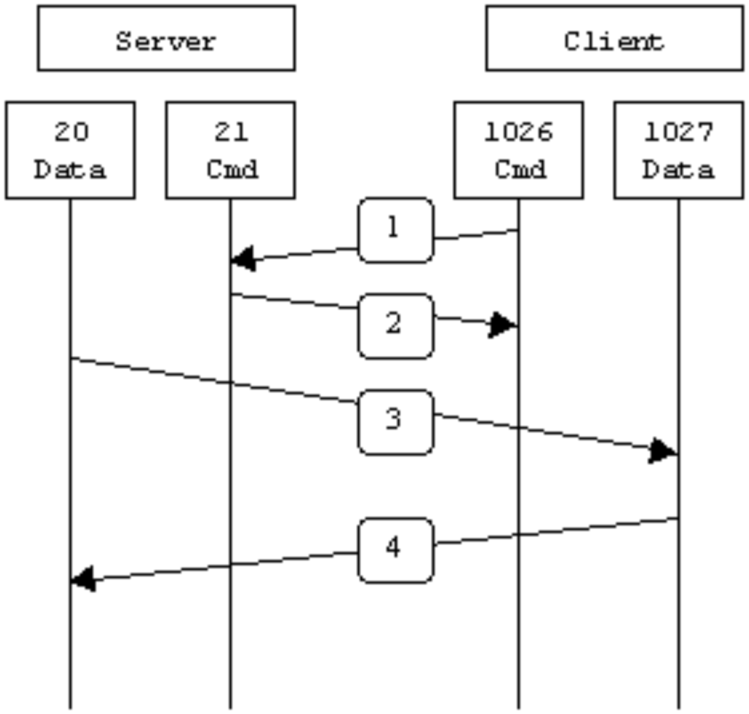
Oakley is used along side ISAKMP, and is now commonly known as IKE (Internet Key Exchange). Basically Oakley is a protocol to carry out the key exchange negotiation process for both peers, in which both ends after being authenticated can agree on secure and secret keying material. Oakley is based on the Diffie-Hellman key algorithm in which two gateways can agree on a key without the need to encrypt.

Q: What is FTP Active and Passive Mode?

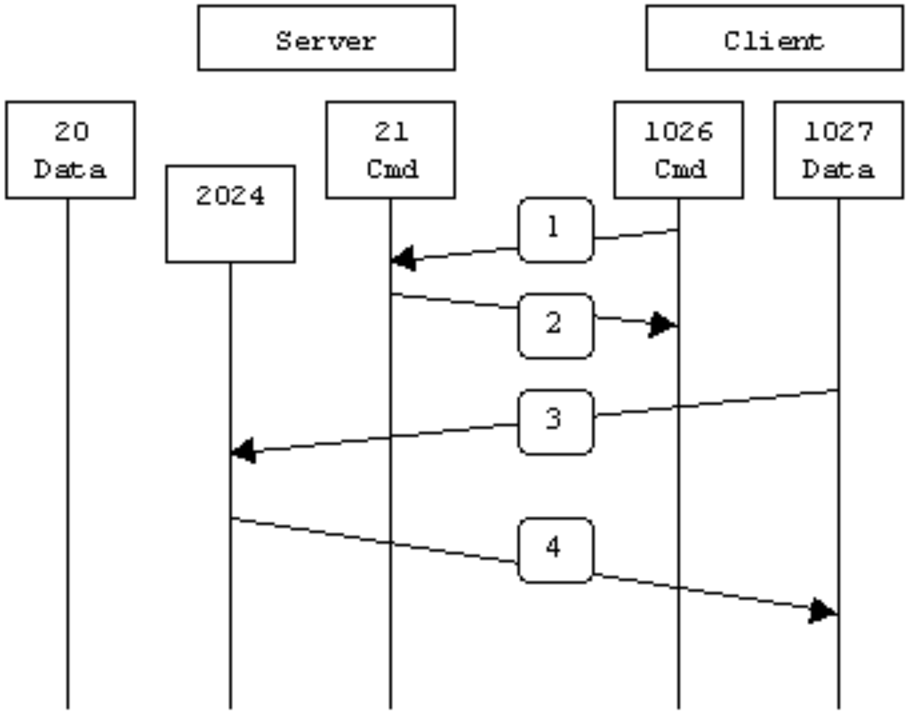
1. Normal Mode or Active Mode

To start an FTP session in normal mode, a client first allocates two TCP ports for itself, each of them with a port number above 1024. It uses the first to open the command channel connection to the server and then issues FTP's PORT command to tell the server of the second port number, which the client wants to use for the data channel. The server then opens the data channel connection. This data channel connection is backwards from most protocols, which open connections from the client to the server.

This backwards open complicates things for sites that are attempting to do start-of-connection packet filtering to ensure that all TCP connections are initiated from the inside, because external FTP servers will attempt to initiate data connections to internal clients, in response to command connections opened from those internal clients. Furthermore, these connections will be going to ports known to be in an unsafe range.



Passive Mode



To start a connection in passive mode, an FTP client allocates two TCP ports for its own use and uses the first port(21) to contact the FTP server, just as when using normal mode. However, instead of issuing the PORT command to tell the server the client's second port, the client issues the PASV command. This causes the server to allocate a second port of its own for the data channel (for architectural reasons, servers use random ports above 1023 for this, not port 20 as in normal mode; you couldn't have two servers on the same machine simultaneously listening for incoming PASV-mode data connections on port 20) and tell the client the number of that port. The client then opens the data connection from its port to the data port the server has just told it about.

Passive mode is useful because it allows you to avoid start-of-connection filtering problems. In passive mode, all connections will be opened from the inside, by the client. Or In passive mode, only the server is required to open up ports for incoming traffic.

Summary

The following chart should help admins remember how each FTP mode works:

```
 Active FTP :
     command : client >1023 -> server 21
     data    : client >1024 <- server 20

 Passive FTP :
     command : client >1023 -> server 21
     data    : client >1024 -> server >1023
```

A quick summary of the pros and cons of active vs. passive FTP is also in order:

Active FTP is beneficial to the FTP server admin, but detrimental to the client side admin. The FTP server attempts to make connections to random high ports on the client, which would almost certainly be blocked by a firewall on the client side. Passive FTP is beneficial to the client, but detrimental to the FTP server admin. The client will make both connections to the server, but one of them will be to a random high port, which would almost certainly be blocked by a firewall on the server side.

Luckily, there is somewhat of a compromise. Since admins running FTP servers will need to make their servers accessible to the greatest number of clients, they will almost certainly need to support passive FTP. The exposure of high level ports on the server can be minimized by specifying a limited port range for the FTP server to use. Thus, everything except for this range of ports can be firewalled on the server side. While this doesn't eliminate all risk to the server, it decreases it tremendously. See Appendix 1 for more information.

Q: What is Adaptive Security Algorithm(ASA)?

Adaptive Security Algorithm (ASA) is a Cisco algorithm for managing stateful connections for PIX Firewalls. ASA controls all traffic flow through the PIX firewall, performs stateful inspection of packets, and creates remembered entries in connection and translations tables. These entries are referenced every time when traffic tries to flow back through from lower security levels to higher security levels. If a match is found, the traffic is allowed through. Finally, the ASA provides an extra level of security by randomizing the TCP sequence numbers of outgoing packets in an effort to make them more difficult to predict by hackers

Q: Can you describe ASA security levels?

- ASA classifies the level of “trust” of an interface by its security-level (0-100)
- 100 is the most trusted interface
  - Assigned to interface “inside” by default
- 0 is the most untrusted interface
  - Assigned to all other interfaces by default
- ASA interfaces can only pass traffic if nameif and security-level are defined.

Q: What is CASB?

Cloud Access Security Brokers are on-premses or cloud-hosted software that act as a control point to support continuous visibility, compliance, threat protection, and security for cloud services.

four pillars of CASB (visibility, compliance, threat prevention and data security)

Gartner predicted at 2014, “By 2017, 50% of CASB vendors will either be acquired or evolve to support a broader set of cloud security requirements”

Q: What is Secure Web Gateway(SWG)?

Secure Web gateway solutions protects Web-surfing PCs from infection and enforce company policies. A secure Web gateway is a solution that filters unwanted software/malware from user-initiated Web/Internet traffic and enforces corporate and regulatory policy compliance. The gateways must at a minimum, include URL filtering, malicious-code detection and filtering, and application controls for popular Web-based applications, such as instant messaging(IM) and Skype. Native or integrated data leak prevention is also increasingly included.

Q(SQL): What are the technical specification of MySQL?

MySQL has the following technical specifications -

- Flexible structure
- High performance
- Manageable and easy to use
- Replication and high availability
- Security and storage management

Q(SQL). How can we get the number of rows affected by query?

Number of rows can be obtained by:

```
SELECT COUNT (user_id) FROM users;
```

Q(SQL) What are the different tables present in MySQL?

Total 5 types of tables are present:

- MyISAM
- Heap
- Merge
- INNO DB
- ISAM

MyISAM is the default storage engine as of MySQL .

Q(SQL) What is ISAM?

ISAM is abbreviated as Indexed Sequential Access Method.It was developed by IBM to store and retrieve data on secondary storage systems like tapes.

Q(SQL) What is InnoDB?

InnoDB is a transaction safe storage engine developed by Innobase Oy which is a Oracle Corporation now.

Q: How to display nth highest record in a table for example? How to display 4th highest (salary) record from customer table?

```
SELECT DISTINCT SALARY FROM TABLENAME ORDER BY DESC SALARY
LIMIT 3,1;
```

Q(SQL) How to display top 50 rows?

In MySql, top 50 rows are displayed by using this following query:

```
SELECT * FROM
LIMIT 0,50;
```

Q(SQL) What is the difference between Primary Key and Unique Key?
Answer : Both Primary and Unique Key is implemented for Uniqueness of the column. Primary Key creates a clustered index of column where as an Unique creates unclustered index of column. Moreover, Primary Key doesn't allow NULL value, however Unique Key does allows one NULL value.

Q(SQL) What are indexes in a Database. What are the types of indexes?
Answer : Indexes are the quick references for fast data retrieval of data from a database. There are two different kinds of indexes.

Clustered Index

Only one per table.

Faster to read than non clustered as data is physically stored in index order.

Nonclustered Index

Can be used many times per table.

Quicker for insert and update operations than a clustered index.

Q(SQL) What is BLOB?

- BLOB stands for binary large object.
- It that can hold a variable amount of data.

There are four types of BLOB based on the maximum length of values they can hold:

- TINYBLOB
- BLOB
- MEDIUMBLOB
- LONGBLOB

Q(SQL): What is TEXT?
TEXT is case-insensitive BLOB. The four types of TEXT are:

- TINYTEXT
- TEXT
- MEDIUMTEXT

- LONGTEXT

Q(SQL): What is the default port for MySQL Server?
- 3306

Q(SQL): want to find out all databases starting with ‘test’, I have access to?
- SHOW DATABASES LIKE ‘test%’;

Q(SQL): What is a trigger in MySQL?
A trigger is a set of codes that executes in response to some events.

Q(SQL): How many Triggers are possible in MySQL?
There are only six Triggers allowed to use in MySQL database.
1 Before Insert
2 After Insert
3 Before Update
4 After Update
5 Before Delete
6 After Delete

Q(SQL): What is heap table?
Tables that are present in memory is known as HEAP tables. When you create a heap table in MySQL, you should need to specify the TYPE as HEAP. These tables are commonly known as memory tables. They are used for high speed storage on temporary basis. They do not allow BLOB or TEXT fields.

Q(SQL): What are the advantages of MySQL in comparison to Oracle?
1 MySQL is a free, fast, reliable, open source relational database while Oracle is expensive, although they have provided Oracle free edition to attract MySQL users.
2 MySQL uses only just under 1 MB of RAM on your laptop while Oracle 9i installation uses 128 MB.
3 MySQL is great for database enabled websites while Oracle is made for enterprises.
4 MySQL is portable.

Q(SQL): What are the disadvantages of MySQL?

1. MySQL is not so efficient for large scale databases.
2. It does not support COMMIT and STORED PROCEDURES functions version less than 5.0.
3. <li>Level of support of open source databases like MySQL is not so powerful as close source databases.</li>
4. Transactions are not handled very efficiently.

Q(SQL): What is the difference between CHAR and VARCHAR?

1) CHAR and VARCHAR are differ in storage and retrieval.
2) CHAR column length is fixed while VARCHAR length is variable.
3) The maximum no. of character CHAR data type can hold is 255 character while VARCHAR can hold up to 4000 character.
4) CHAR is 50% faster than VARCHAR.
5) CHAR uses static memory allocation while VARCHAR uses dynamic memory allocation.

Q(SQL): How do you backup a database in MySQl?

It is easy to backing up data with phpMyAdmin. Select the database you want to backup by clicking the database name in the left hand navigation bar. Then click the export button and make sure that all tables are highlighted that you want to backup. Then specify the option you want under export and save the output.

Q(SQL): Can we you give one example how to use Python API to query MySQL DB?

```
▸ def cfm_sql_stats(self):
▸ ▸ dut = self.dut
▸ ▸ logger = dut.logger
▸ ▸ total = query_sql(dut,"select count(*) from CFM_SERVICES")
▸ ▸ total_down = query_sql(dut,"SELECT count(*) FROM CFM_SERVICES where CROSS_CON like \'%X%\' OR ERROR_CCM like \'%X%\' OR RMEP_ERR like \'%X%\'     OR PORT_STATUS like \'%X%\' OR RDI like \'%X%\' OR INSTABILITY like \'%X%\'")
▸ ▸ total_down_assoc = query_sql(dut,"SELECT count(*) FROM CFM_SERVICES where (SERVICE_NAME like \'%CFM-A%\') AND (CROSS_CON like \'%X%\' OR ERROR     _CCM like \'%X%\' OR RMEP_ERR like \'%X%\' OR PORT_STATUS like \'%X%\' OR RDI like \'%X%\' OR INSTABILITY like \'%X%\')")
▸ ▸ total_down_corout = total_down - total_down_assoc
```

```
        total_assoc = query_sql(dut,"SELECT count(*) FROM CFM_SERVICES where SERVICE_NAME like \'%CFM-A%\'")
        total_static = query_sql(dut,"SELECT count(*) FROM CFM_SERVICES where SERVICE_NAME like \'%VS-F%\'")
        cx = query_sql(dut,"SELECT count(*) FROM CFM_SERVICES where CROSS_CON like \'%X%\'")
        ccm = query_sql(dut,"SELECT count(*) FROM CFM_SERVICES where ERROR_CCM like \'%X%\'")
        rmep = query_sql(dut,"SELECT count(*) FROM CFM_SERVICES where RMEP_ERR like \'%X%\'")
        ports = query_sql(dut,"SELECT count(*) FROM CFM_SERVICES where PORT_STATUS like \'%X%\'")
        rdi = query_sql(dut,"SELECT count(*) FROM CFM_SERVICES where RDI like \'%X%\'")
        inst = query_sql(dut,"SELECT count(*) FROM CFM_SERVICES where INSTABILITY like \'%X%\'")

```

Q(SQL): If the value in the column is repeatable, how do you find out the unique values?

Use DISTINCT in the query, such as SELECT DISTINCT user_firstname FROM users; You can also ask for a number of distinct values by saying SELECT COUNT (DISTINCT user_firstname) FROM users;

Q(SQL): How do you return the a hundred books starting from 25th?

SELECT book_title FROM books LIMIT 25, 100.

The first number in LIMIT is the offset, the second is the number.

Q(SQL): How would you change a column from VARCHAR(10) to VARCHAR(50)?

ALTER TABLE techpreparation_questions CHANGE techpreparation_content techpreparation_CONTENT VARCHAR(50).

Q(SQL): How would you delete a column?

ALTER TABLE techpreparation_answers DROP answer_user_id.

Q(SQL): How do you start and stop MySQL on Windows?

net start MySQL, net stop MySQL

Q(SQL): How do you start MySQL on Linux?
/etc/init.d/mysql start

Q(SQL): Explain the difference between mysql and mysql interfaces in PHP?
mysqli is the object-oriented version of mysql library functions.