10- VPN Technologies and Cryptography Concepts

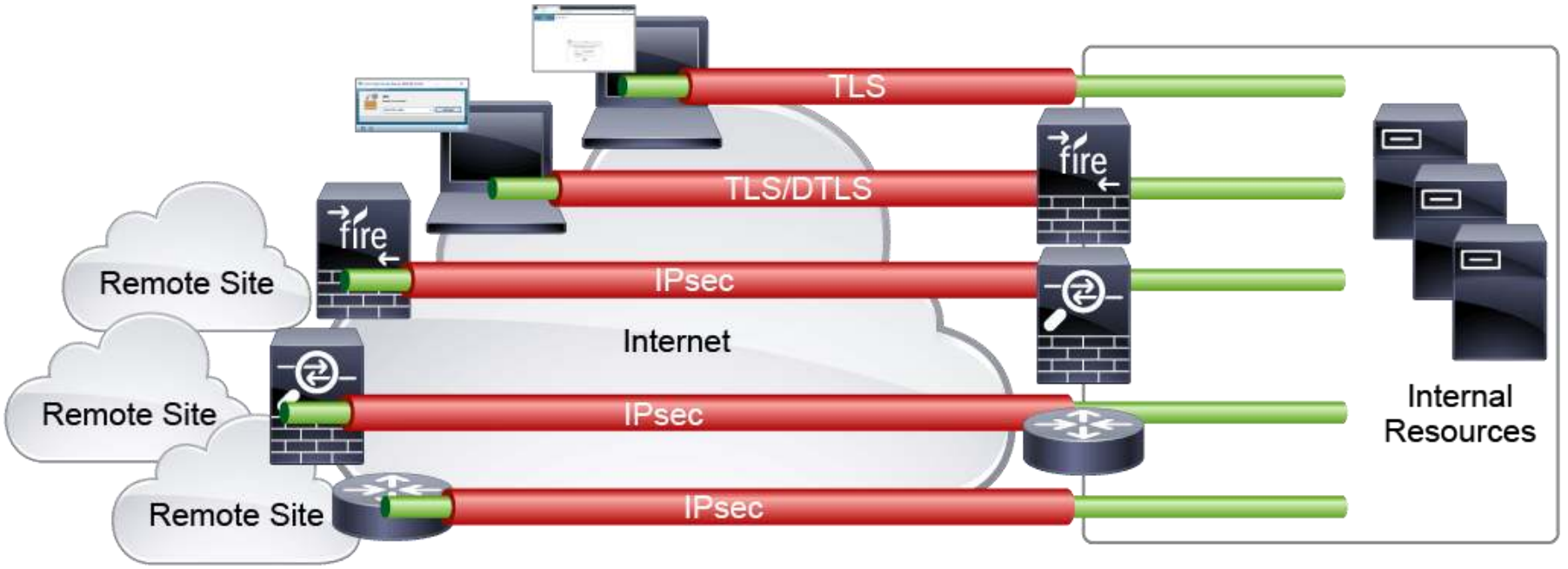
Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me/about

VPN Definition

- a VPN is "a computer network that is constructed from the system resources of a relatively public, physical (real) network, often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network.“
- A VPN carries private traffic over a public infrastructure (such as the Internet).
- VPNs protect data that is transmitted over a public or shared infrastructure such as the Internet from threats such as man-in-the-middle attacks.

© egyptnetriders.com

VPN Definition (cont.)



© egyptnetriders.com

VPN Definition (cont.)

VPNs have several benefits:

- **Cost savings:** VPNs enable organizations to use cost-effective third-party Internet transport to connect remote offices and remote users to the main corporate site.
- **Scalability:** VPNs enable corporations to use the Internet infrastructure within ISPs and devices, which makes it easy to add new users
- **Compatibility with broadband technology:** VPNs allow mobile workers, telecommuters, and people who want to extend their workday to take advantage of high-speed, broadband connectivity, such as DSL and cable, to gain access to their corporate networks, providing workers significant flexibility and efficiency.
- **Security:** VPNs provide the highest level of security by using advanced encryption and authentication protocols that protect data from unauthorized access.

VPN Types

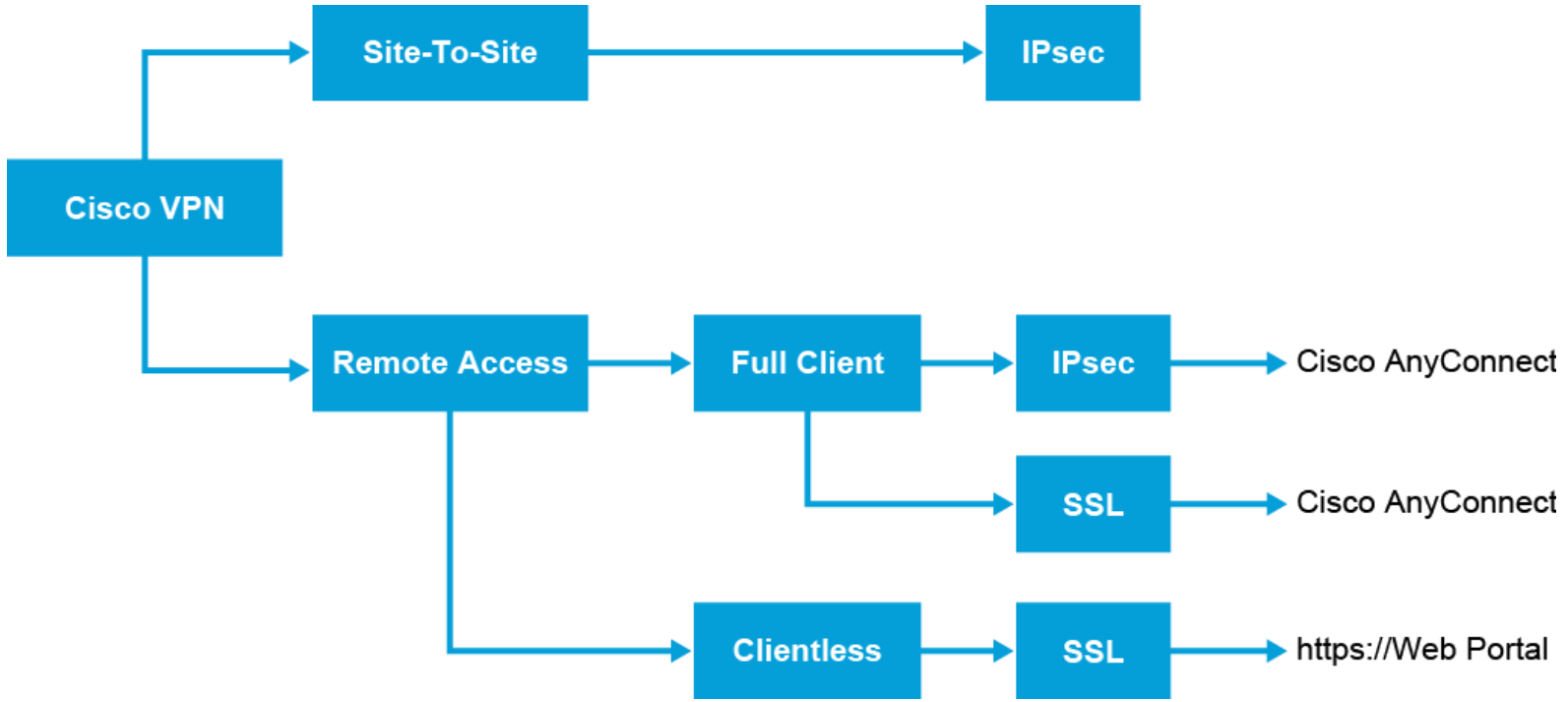
VPNs are classified according to the following criteria:

- **Based on deployment mode:** Site-to-site VPN and remote-access VPN
- **Based on OSI layer:** Layer 2 VPN (legacy protocols such as Frame Relay, and Layer 2 Multiprotocol Label Switching [MPLS] VPN, Layer 3 VPN Internet Protocol Security [IPsec] and MPLS Layer 3 VPN, and Layer 7 VPN Secure Sockets Layer [SSL] VPN)
- **Based on underlying technology:** IPsec VPN, SSL VPN, MPLS VPN, other Layer 2 technologies such as Frame Relay, and hybrid VPNs combining multiple technologies.

© egyptnetriders.com

VPN Types (cont.)

The two basic VPN deployment models typically use either IPsec or SSL technologies to keep the communications secure.

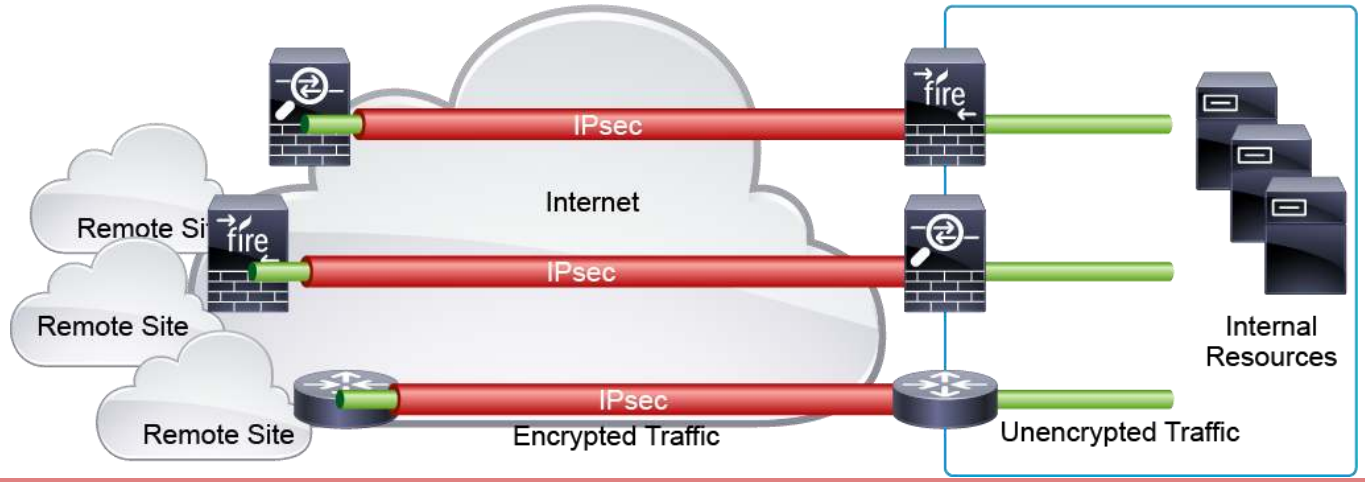


© egyptnetriders.com

VPN Types (cont.)

1- Site-to-Site VPN

- Site-to-site VPNs connect entire networks to each other; for example, they can connect a branch office network to a company headquarters network. In the past, a leased line or Frame Relay connection was required to connect sites, but because corporations now have Internet access, these connections can be replaced with site-to-site VPNs.



© egyptnetriders.com

VPN Types (cont.)

Site-to-Site VPN (cont.)

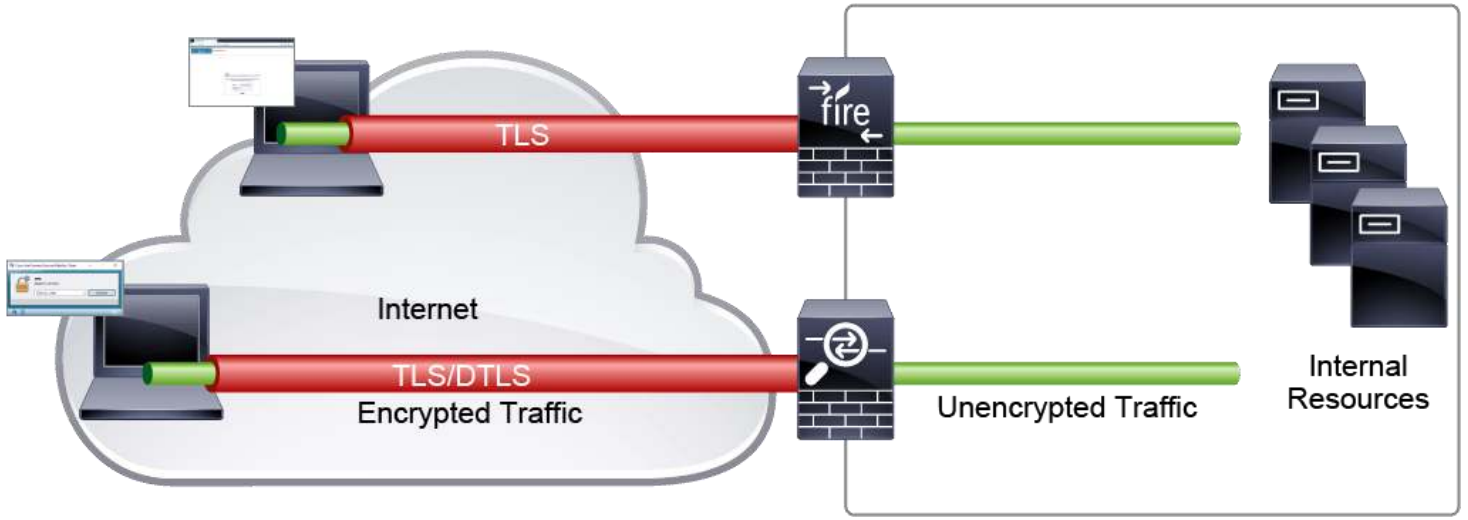
- In a site-to-site VPN, hosts do not have client software; they send and receive normal TCP/IP traffic through a VPN gateway, which could a **Cisco IOS XE router**, **Cisco ASA appliance**, **or Cisco FirePower NGFW firewall**.
- The VPN gateway is responsible for encapsulating and encrypting outbound traffic for all the traffic from a particular site and sending it through a VPN tunnel over the Internet to a peer VPN gateway at the target site.
- Upon receipt, the peer VPN gateway strips the headers, decrypts the content, and relays the packet toward the target host inside its private network.

© egyptnetriders.com

VPN Types (cont.)

2- Remote-access VPNs

- Remote-access VPNs connect individual hosts (telecommuters and mobile users)who must access their company network securely over the Internet.



© egyptnetriders.com

VPN Types (cont.)

2- Remote-access VPNs (cont.)

- Hosts in a remote-access VPN commonly have a VPN client installed, such as **Cisco AnyConnect Secure Mobility Client** or are using **clientless SSL VPN**.
- The Cisco AnyConnect uses a virtual network adapter in the host computer to send traffic back to the VPN gateway, such as **Cisco ASA appliance** or **Cisco FirePower NGFW**, back at the head office.
- The clientless SSL VPN lets users establish a secure, remote-access VPN tunnel to the VPN gateway using **a web browser**.
- There is no need for either a software or hardware client.
- Clientless SSL VPN provides easy access to a broad range of web resources and both web-enabled and legacy applications from almost any computer that can reach VPN gateway over HTTPS.

VPN Types (cont.)

2- Remote-access VPNs (cont.)

"**Clientless SSL VPN is only available on Cisco ASA appliances**, It is not available on **Cisco FirePower NGFW**, which only supports remote access SSL VPN using the Cisco AnyConnect Secure Mobility Client"

VPN Types (cont.)

VPN Components

- There are important components that are typically part of a VPN implementation.
- Not every VPN implementation will include any or all of these components.
- Based on the requirements listed in your security policy, you might not need all of these components.
- You need to examine security policy to determine which VPN implementation has the necessary components to meet security policy requirements.

© egyptnetriders.com

VPN Types (cont.)

VPN Components (cont.)

1. **Authentication:** It is important to verify the identity of a device or user before allowing it to establish a VPN connection to your network, Device authentication allows you to restrict VPN access to your network based on authentication information that a remote VPN device provides. There are two types of authentication typically used: preshared keys, or digital signature or certificate.

VPN Types (cont.)

VPN Components (cont.)

2. **Encapsulation Method:** a VPN must define an encapsulation method: how user information, such as data, is to be encapsulated and transported across a network, Encapsulation also defines which applications or protocols can be placed in the payload of a VPN packet.

3. **Data Encryption:** Data encryption is used to solve eavesdropping issues, Data encryption basically takes user data and a key value and runs it through an encryption algorithm, producing what looks like a random string of characters .. Only a device with the same key value can decrypt the information.

VPN Types (cont.)

VPN Components (cont.)

4. **Packet Integrity:** The sending and receiving systems have to first agree on the secret key along with the hashing function used to verify the data integrity of the communication between them.
5. **Key Management:** Management of keys is important with VPN connections. For example, how are keys derived? Are they statically configured or randomly generated? How often are keys regenerated to increase security?

Cryptographic Services

- Cryptography is the study of information hiding and verification.
- It includes the protocols, algorithms, and strategies to securely and consistently prevent or delay unauthorized access to sensitive information and enable verifiability of every component in a communication.
- With a cryptographic system, the confidentiality and integrity of information can be achieved by using various methods that employ cryptography, such as encryption and decryption techniques, hash functions, digital signatures, key management techniques, and various other systems.

Cryptographic Services (cont.)

The key services provided by cryptography are as follows:

1. **Confidentiality:** The assurance that no one can read a particular piece of data except the explicitly intended receivers.
2. **Integrity or data authentication:** The assurance that data has not been altered in transit, intentionally or unintentionally.
3. **Peer authentication:** The assurance that the other entity is who they claim to be.
4. **Nonrepudiation:** A proof of the integrity and origin of data. The sender cannot repudiate that he or she is the person who sent the data.
5. **Key management:** The generation, exchange, storage, safeguarding, use , and replacement of keys.

Cryptographic Services (cont.)

- VPN services use a combination of cryptographic technologies and algorithms to accomplish their goals.
- In the router-to-router VPN, also known as site-to-site VPN, IP packets use symmetric encryption algorithms to encrypt the payload, with keys negotiated by key management protocols.
- They also use asymmetric encryption algorithms to create digital signatures and authenticate the VPN peers, and use hashing functions to provide checksum-type integrity checks.

© egyptnetriders.com

Cryptographic Services (cont.)

- Encryption is the use of an algorithmic process that uses a secret key to transform plain data into a secret code, to prevent anyone except the intended recipient from accessing the information.
- Encryption obscures information to make it unreadable to unauthorized recipients.
- Encryption provides a means of secure communication over an insecure communications medium.

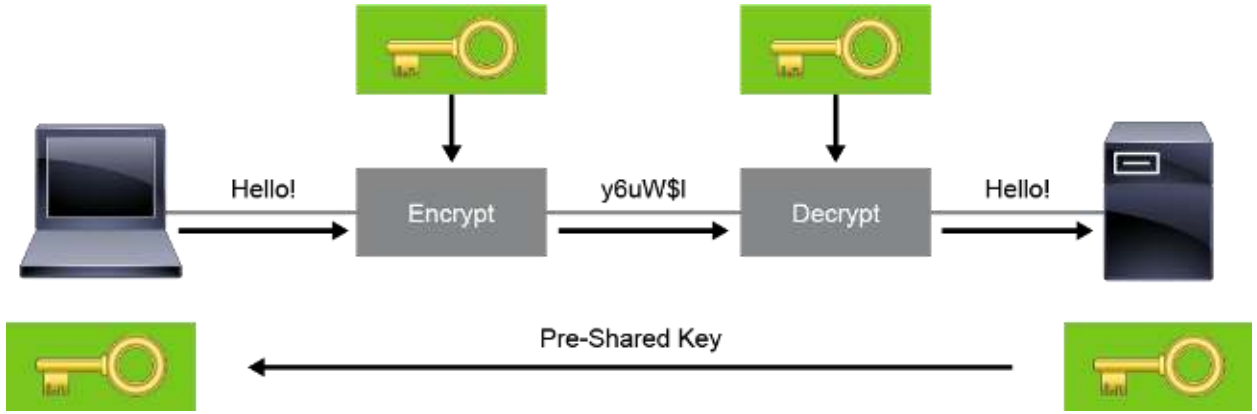
© egyptnetriders.com

Cryptographic Services (cont.)

Cryptographic algorithms can be divided into these three categories:

1. Symmetric key algorithms:

- ✓ Also known as **secret key** or **preshared key** cryptography, uses a single key for both the encryption and decryption process.
- ✓ Modern symmetric algorithms use key lengths that range from **40** to **256** bits.
- ✓ Examples include **3DES** and **AES**.



Cryptographic Services (cont.)

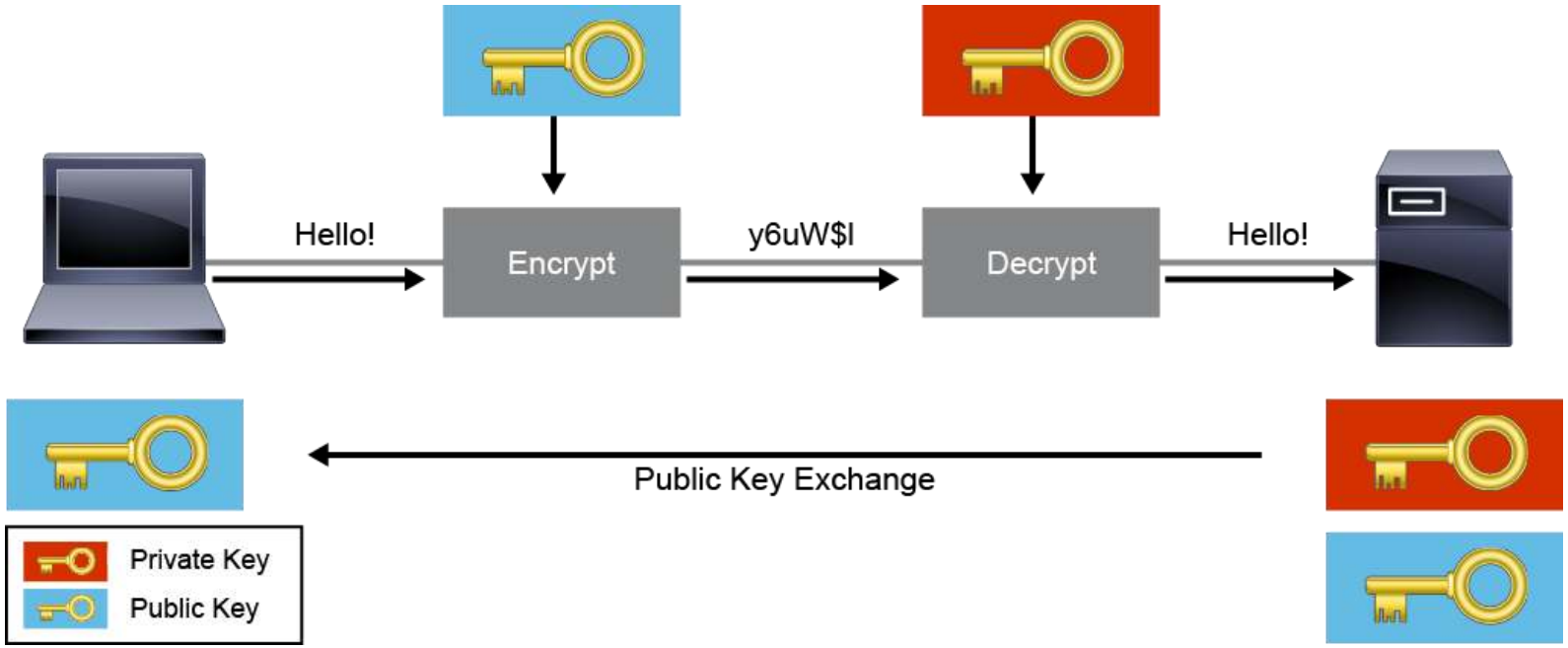
Cryptographic algorithms can be divided into these three categories (cont.)

2. Asymmetric/Public-Key algorithms:

- ✓ Also known as **public key** cryptography, uses a two-key pair, one key for the encryption and another for the decryption process.
- ✓ Asymmetric algorithms are substantially slower than symmetric algorithms.
- ✓ The typical key length range for asymmetric algorithms is **1024** to **4096** bits.
- ✓ Examples include Digital Signature Algorithm (**DSA**), **RSA**, **ElGamal**.

Cryptographic Services (cont.)

Cryptographic algorithms can be divided into these three categories (cont.)



© egyptnetriders.com

Cryptographic Services (cont.)

Cryptographic algorithms can be divided into these three categories (cont.)

- Server on the right generates the **private**/**public** key pair.
- Server on the right keeps the **private key** totally secret but publishes the **public key** so it is available to everyone.
- Workstation on the left got the **public key** from the server on the right.
- Workstation now encrypts data with the **public key** of the server and send encrypted data to the server.
- The server decrypts data with its **private key**.
- Only the **private key** that belongs to the **public key** can decrypt what was encrypted with the public key, providing confidentiality of data.

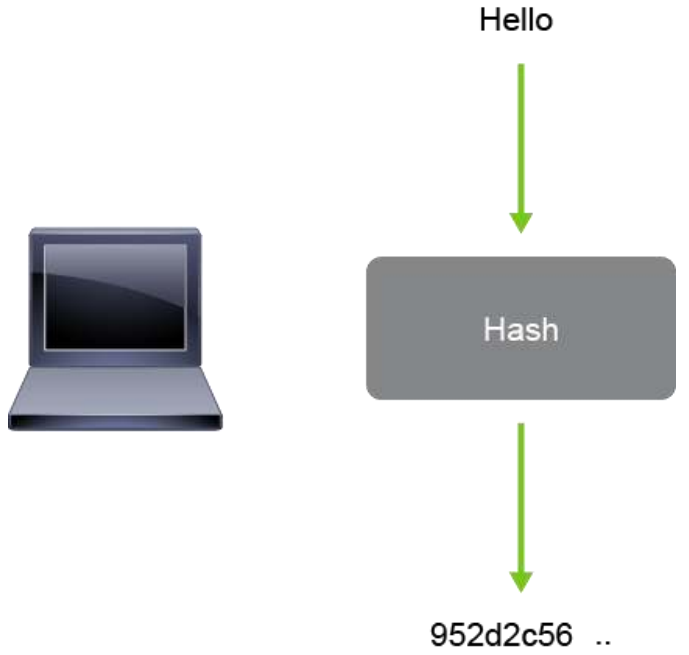
© egyptnetriders.com

Cryptographic Services (cont.)

Cryptographic algorithms can be divided into these three categories (cont.)

3. Hash algorithms:

- ✓ Provide a constant-sized output for any input.
- ✓ Hash algorithms are also called digital fingerprinting algorithms.
- ✓ Examples of hash functions are **SHA-1** and **SHA-2**.
- ✓ Message-digest5 (**MD5**) is a hash function that is insecure and should be avoided.



© egyptnetriders.com

Site-to-Site VPN Topologies

The three typical logical VPN topologies that are used in site-to-site VPNs are:

1. Individual point-to-point VPN connection:

- ✓ Two sites interconnect using a secure VPN path.
- ✓ The network may include a few such individual point-to-point VPN connections that connect sites that require mutual connectivity.

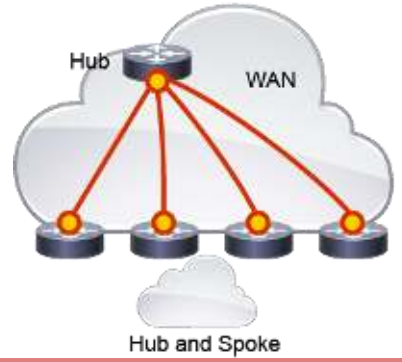
© egyptnetriders.com

Site-to-Site VPN Topologies (cont.)

The three typical logical VPN topologies that are used in site-to-site VPNs are (cont.)

2. Hub-and-spoke network:

- ✓ One central site is considered a hub and all other sites (spokes) peer exclusively with the central site devices.
- ✓ Typically, most of the user traffic flows between the spoke network and the hub network.

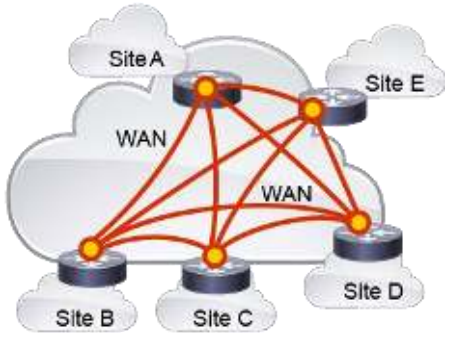


Site-to-Site VPN Topologies (cont.)

The three typical logical VPN topologies that are used in site-to-site VPNs are (cont.)

3. Fully meshed network:

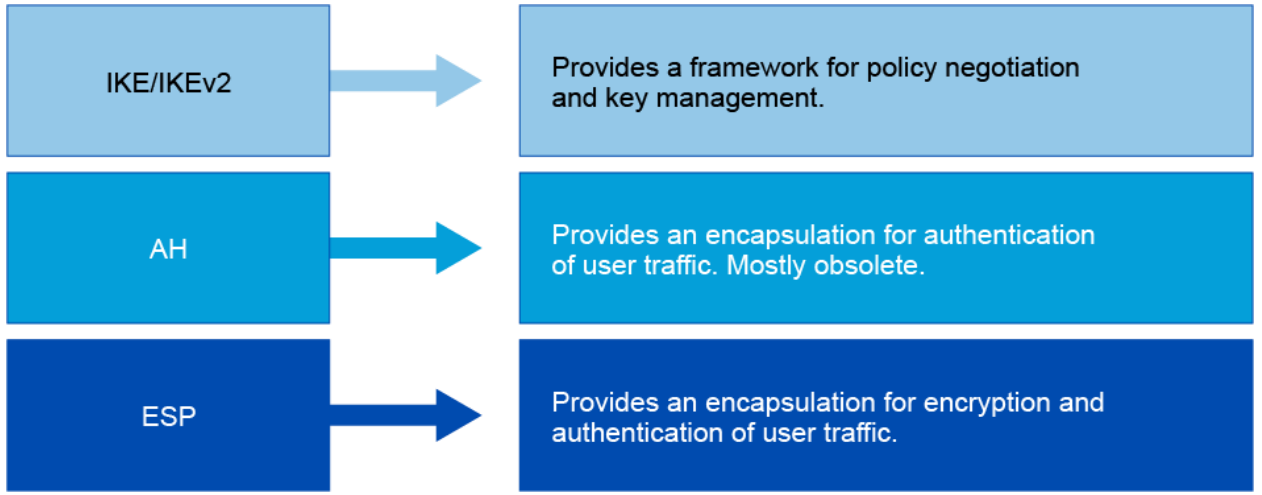
- ✓ Every network device is connected to every other network device.
- ✓ This topology enables any-to-any communication; provides the most optimal, direct paths in the network; and provides the greatest flexibility to network users.



Full Mesh

IPsec VPN Overview

- Ipsec offers access control, connectionless integrity, data origin authentication, protection against replays, confidentiality, and limited traffic flow confidentiality.
- These services are provided at the network layer and offer protection for IP and upper-layer protocols.
- IPsec combines the following security protocols:



Remote Access VPN Technologies

- Remote access VPNs provide a solution to connect individual remote users to a set of protected resources in the enterprise internal network over the Internet in a secured and protected way.
- The Cisco ASA firewall and Cisco Firepower NGFW can both be implemented as VPN gateways for accepting remote access VPNs.
- Either Cisco AnyConnect or clientless VPN connections can be initiated by the users.
- Based on the VPN solution used, each user will typically have a VPN client software installed or will use a web-based client.
- The VPN components required for the VPN implementation will also depend on the VPN type used between the users and the VPN gateways.

© egyptnetriders.com

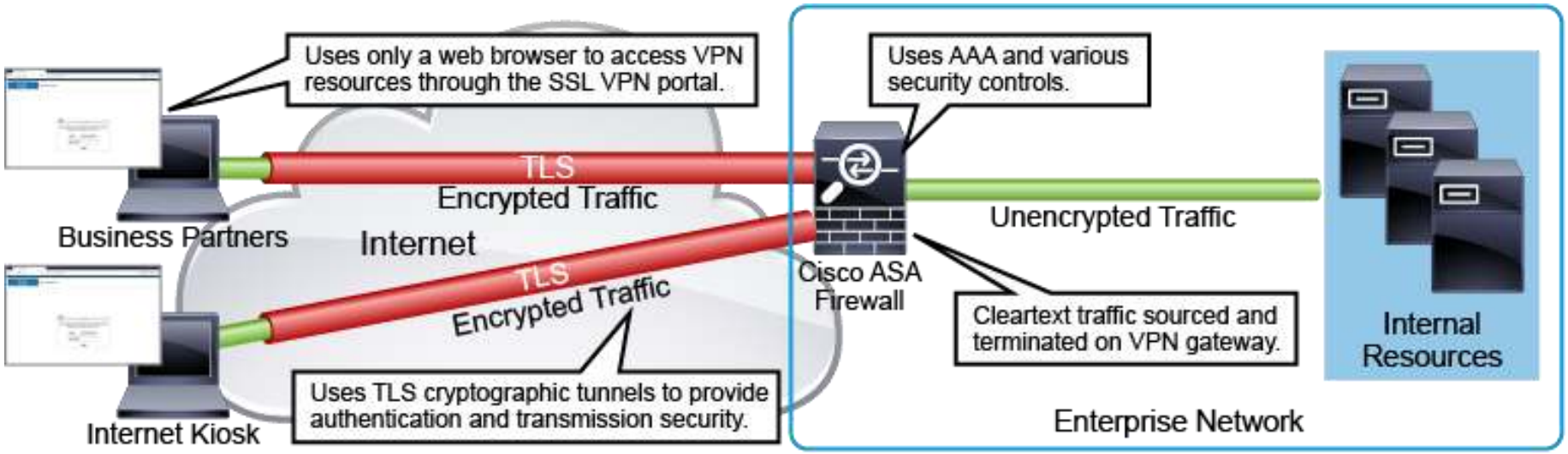
Remote Access VPN Technologies (cont.)

1- Cisco Clientless SSL VPN

- Cisco clientless SSL VPN solutions provide a browser-based access to resources behind the Cisco ASA.
- In clientless SSL VPNs, users can access resources without any special client software.
- Users can access web-based applications, Common Internet File System (CIFS) file shares, and FTP servers when using clientless SSL VPNs.
- In addition, by using application plug-ins and smart tunnels, clientless SSL VPNs allows users to access almost any application that uses static TCP ports.

Remote Access VPN Technologies (cont.)

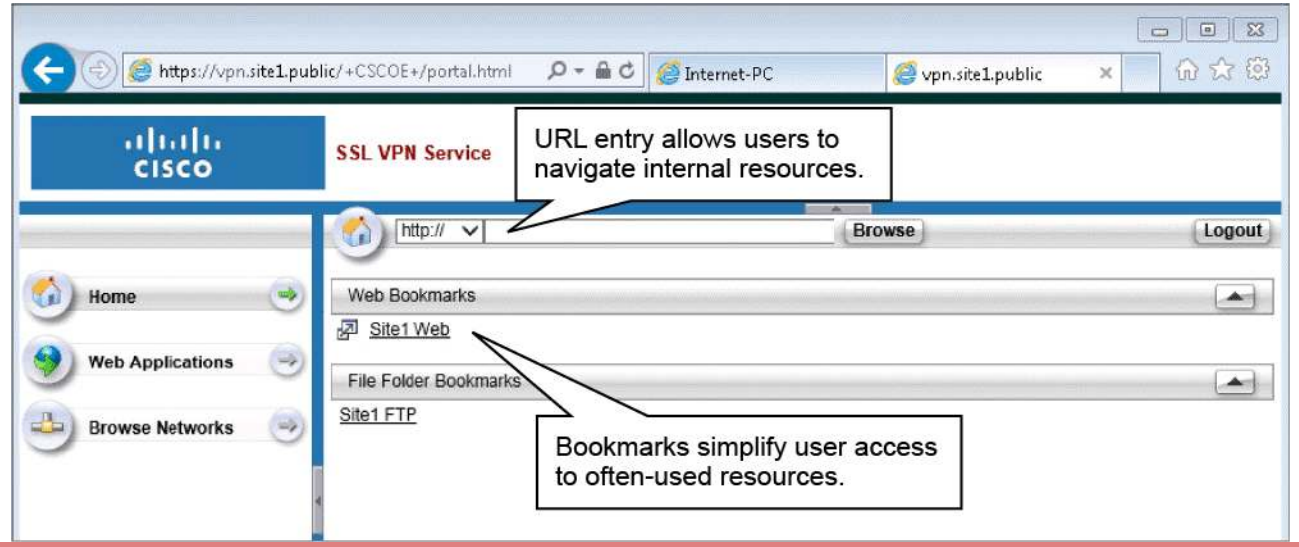
1- Cisco Clientless SSL VPN (cont.)



Remote Access VPN Technologies (cont.)

1- Cisco Clientless SSL VPN (cont.)

- The clientless SSL VPN solution is often a perfect fit for business partners, contractors, or users connecting from internet kiosks who should only have access to a very limited set of resources in the organization's network.



Remote Access VPN Technologies (cont.)

2- Cisco AnyConnect VPN

- The Cisco AnyConnect VPN provides users with flexible, client-based access to sensitive resources over a remote access VPN gateway, which can be implemented on the Cisco ASA or Cisco Firepower NGFW.
- When you combine the Cisco AnyConnect VPN client with the Cisco ASA or Cisco Firepower NGFW appliances that can be configured as VPN gateways, you can provide full-tunnel SSL VPN services to remote users.
- The Ipsec and TLS technologies can all be used as part of the Cisco

Remote Access VPN Technologies (cont.)

2- Cisco AnyConnect VPN (Cont.)