System and Network Administration

A · P · U
ASIA PACIFIC UNIVERSITY
OF TECHNOLOGY & INNOVATION

SSL/TLS and Tunnels

Secure Systems

1. Security policy
   - **What needs to be protected**
   - **Kinds / level of protection**
   - **Responsibilities**
   - **Auditing policy**

2. Security environment
   - **Physical environment**
   - **Physical security**
   - **Hardware, operating system**
   - **firewalls, etc**

3. Security mechanisms
   - **cryptography**
   - **authentication**
   - **security protocols**

4. Monitoring and auditing procedures
   - **monitor access**
   - **audit trails**
   - **feedback on failures, security breaches**
   - **containment & recovery**

Security Protocols

In practice, no single mechanism is adequate to address all goals, so a mix of mechanisms will be required to enforce security policies.

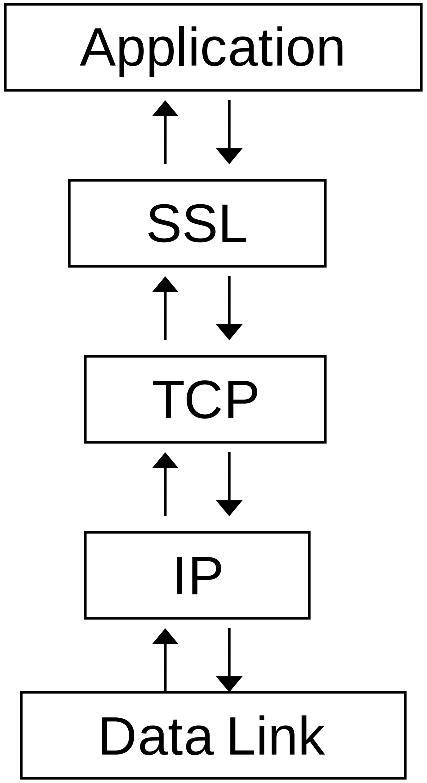
A protocol is an orderly sequence of steps that two or more parties follow in order to accomplish some joint task

e.g. protocols for

- authentication of participants in an exchange of messages
- data integrity checks

Encryption is a mechanism that can be incorporated into security protocols

Secure Sockets Layer (SSL)
Transport Layer Security (TLS)



SSL is a commonly-used protocol for managing the security of message transmission.

TLS is the IETF standard version of SSL.

SSL is a layer between the application and TCP layers

Symmetric vs Asymmetric Key

Symmetric key	**Asymmetric key**
Typically both share same key	Two separate keys: a public and a private key
Typically faster x100!	Typically slower
Examples: DES, IDEA, RC5, AES, …	Examples: RSA, ElGamal Encryption, ECC…

Mechanisms to Protocols: Session Keys

- Public Key Algorithms are ‘computationally intensive’
  - 1000 times slower on average than symmetric systems.
- Conventional Algorithms require secure key exchange
  - If the key is intercepted, confidentiality will be compromised

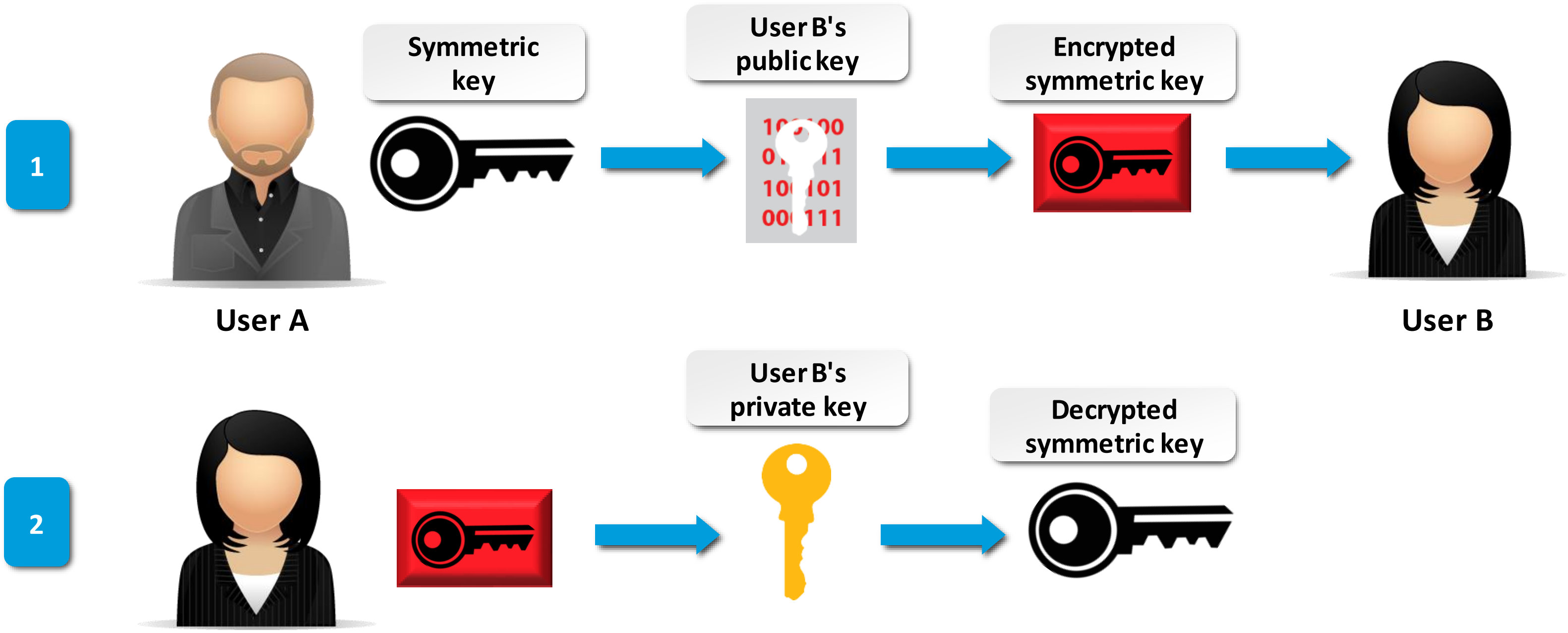
SO ...

- Generate a symmetric ‘session key’
  - Used only for this communication session
  - Random number
- Use public key to encrypt
- Then use the session key to exchange data

Session Keys

A single-use symmetric key used for encrypting all messages in a single series of related communications.

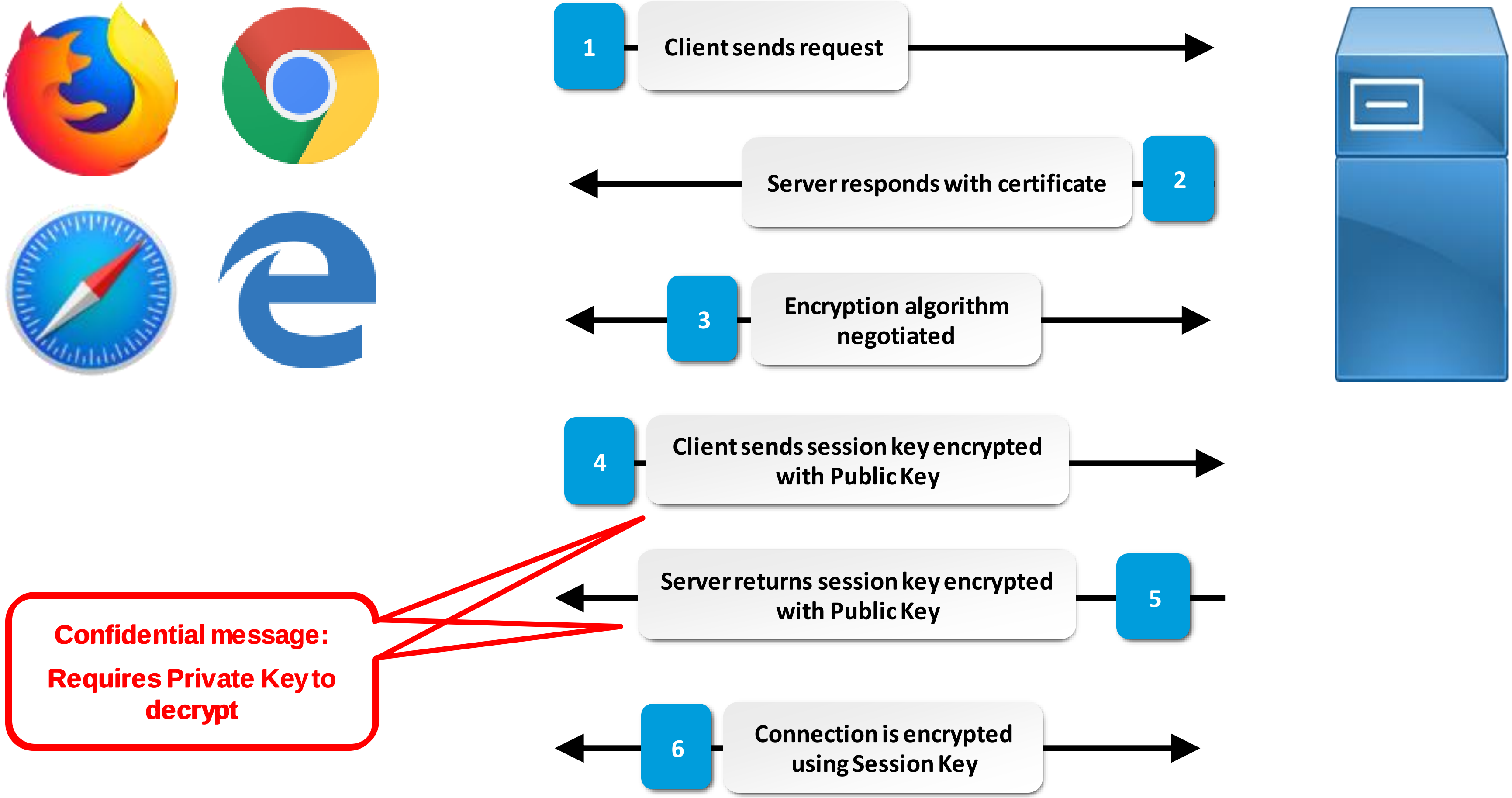
- Limits the amount of data encrypted with a key to reduce the effectiveness of analysis.
- Can be faster and more efficient than asymmetric encryption alone.



SSL / TLS

- HTTP using SSL (**HTTPS://** in a URL) is now the standard mechanism for protecting data sent to and from websites across the Internet
- Browsers have a collection of Certificates from various certificate authorities to use to authenticate websites
- Sites can also generate “Self-Signed” Certificates that can be accepted by the user
- Must use **https://** in the URL request to signal the server that the browser wants to initiate a secure connection

The SSL/TLS Connection Process



1 Client sends request

2 Server responds with certificate

3 Encryption algorithm negotiated

4 Client sends session key encrypted with Public Key

5 Server returns session key encrypted with Public Key

6 Connection is encrypted using Session Key

Confidential message:

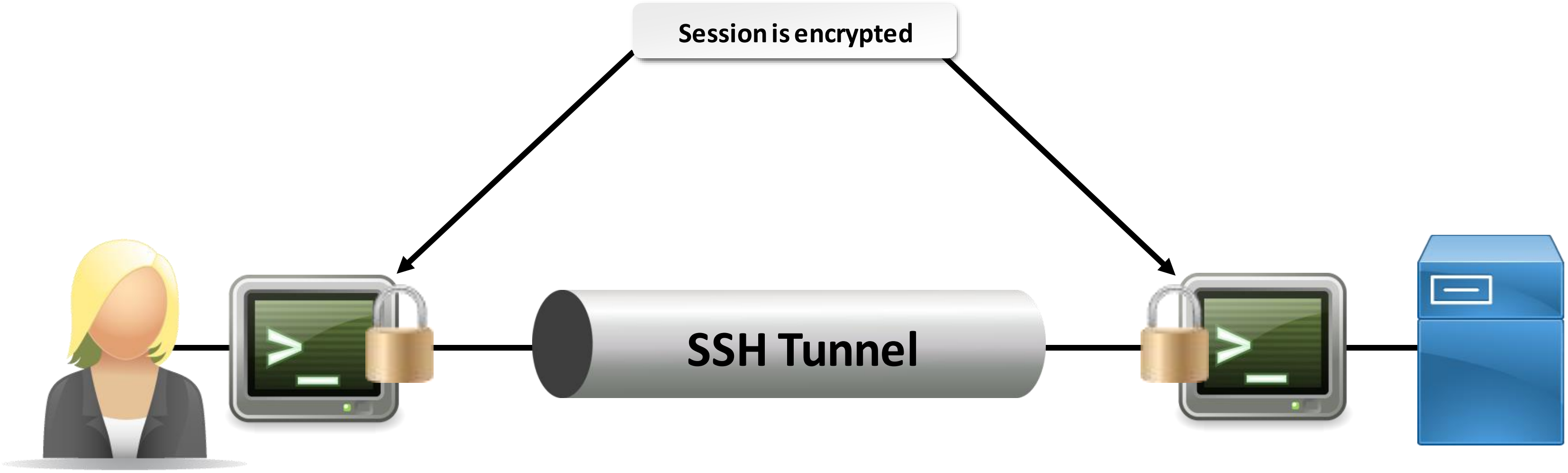
Requires Private Key to decrypt

Secure Shell (ssh, scp, sftp)

A protocol used for secure remote access and secure transfer of data.

- Consists of a client and server.
- ssh for remote login sessions.
- Provides secure copy (scp) and file transfer (sftp)
- Entire session is encrypted.

Similar to using telnet / ftp / tftp with stunnel



CompTIA

Ports and Port Ranges

Port: The endpoint of a logical network connection.

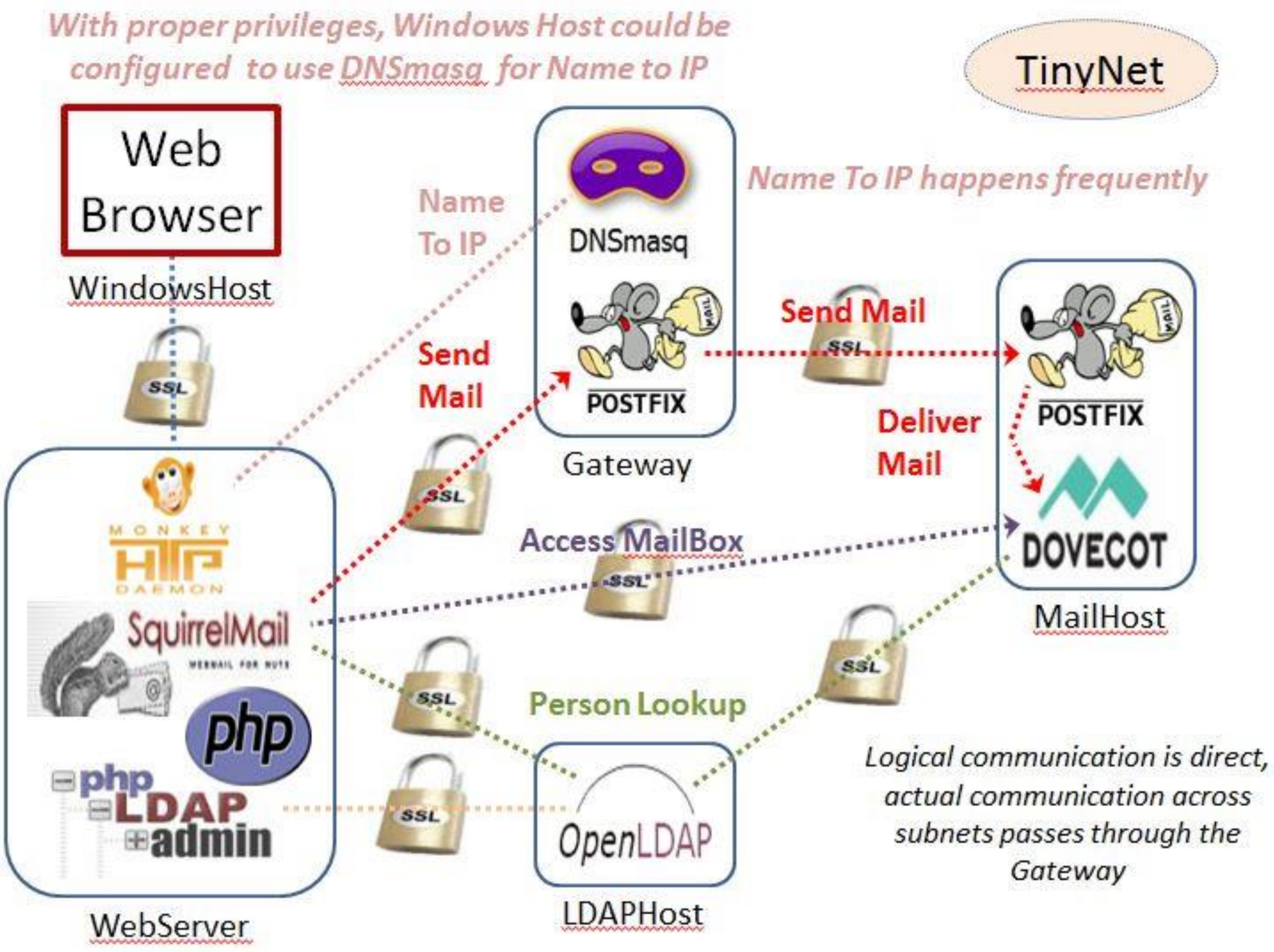
- Client computers connect to server programs through a designated port.
- Port is a “Layer 4” concept – TCP header
- All ports assigned are between the numbers 0 and 65535.

Port	Service	Secure	Port
20	Telnet	SSH	**22**
25	SMTP	SMTPS	**465**
80	HTTP	HTTPS	**443**
143	IMAP	IMAPS	**993**
389	LDAP	LDAPS	**636**

Port	Service
53	DNS
67	DHCP (server)
68	DHCP (client)
587	Submission

Q
&
A
dreamstime.com

Configure Security



Logical communication is direct, actual communication across subnets passes through the Gateway

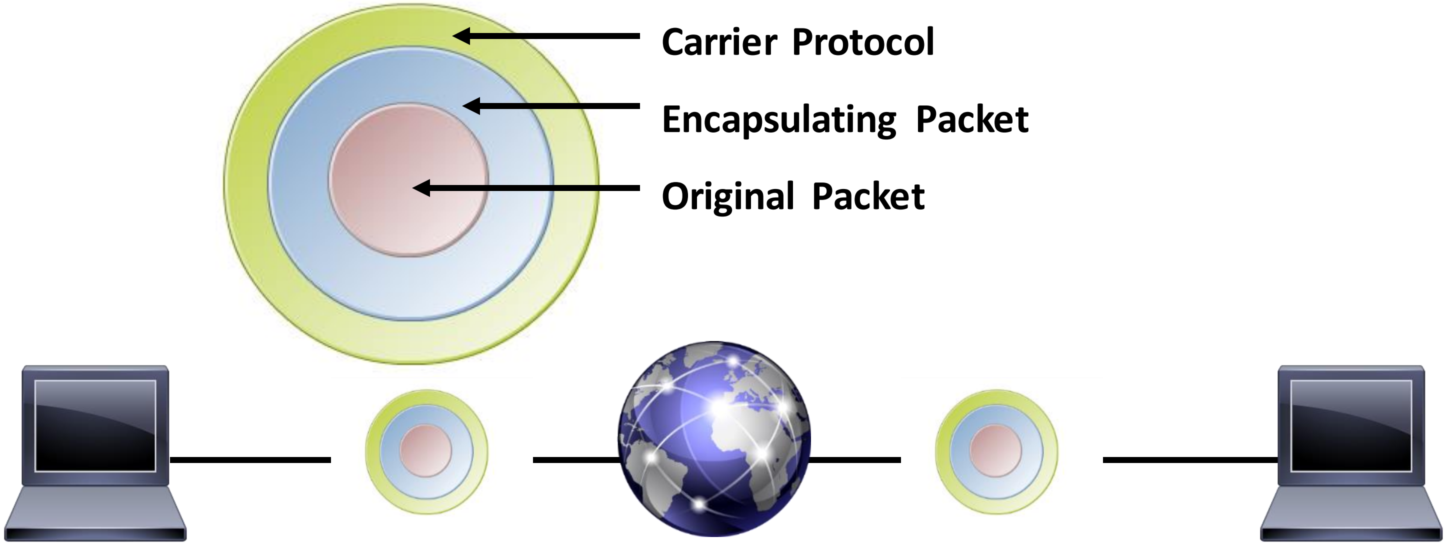
stunnel

- We use stunnel rather than the native SSL capabilities of postfix, dovecot, and ldap because it is simpler to have one configuration and adapt it rather than munging all of the config files ...
- and it demonstrates the concept of port forwarding.

Tunneling

A data-transport technique in which a data packet is encrypted and encapsulated in another data packet.

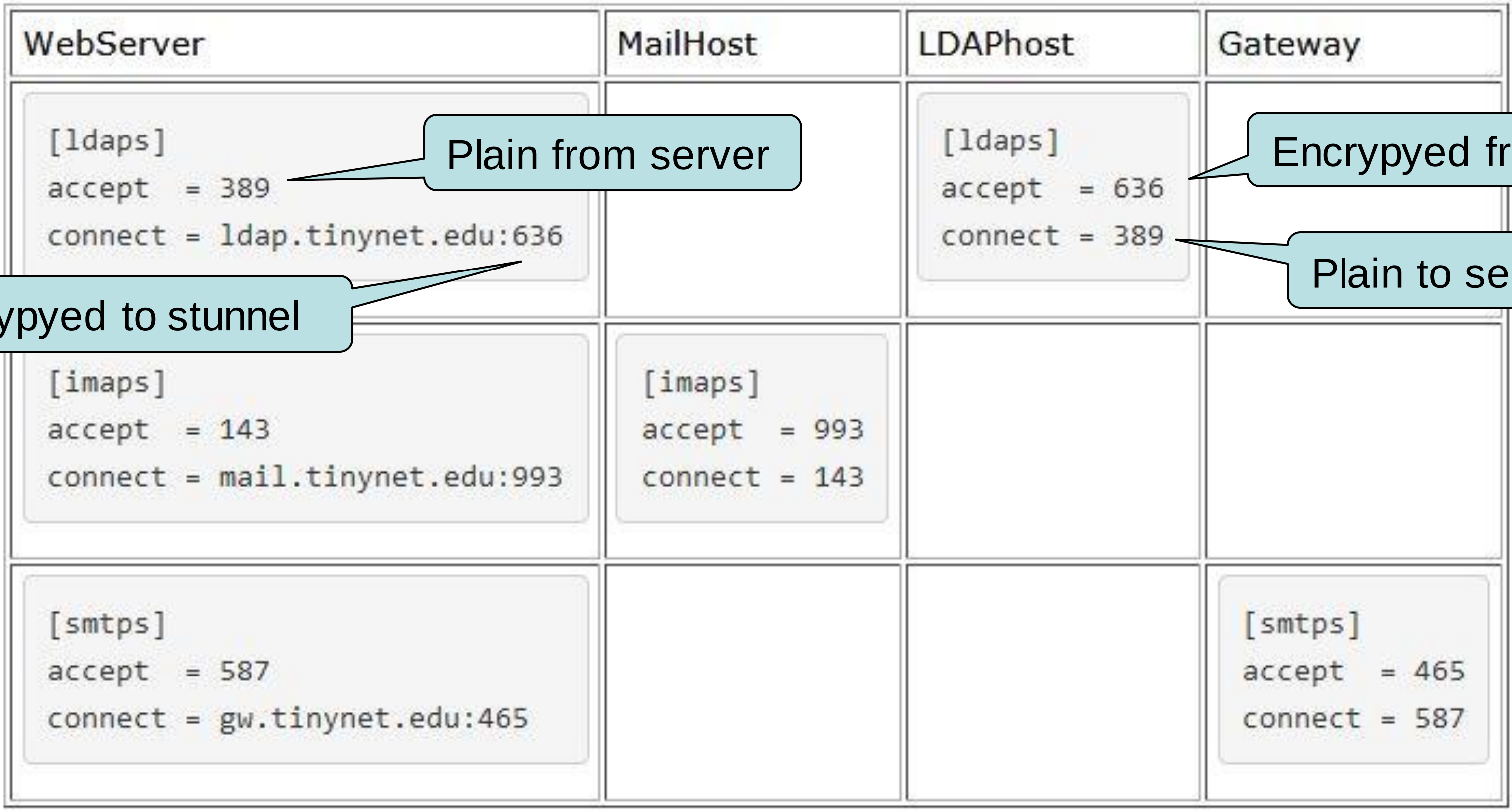
- Tunneling conceals information of the inside packet.
- Hides user-encrypted data from carrier network.
- Used in remote access protocols, typically in VPN.



Encapsulation

- Network devices at both ends of the tunnel, called *tunnel interfaces*, encrypt and encapsulate outgoing packets and reopen and decrypt incoming packets.
- Routers along the way do not parse the payload (the inner packet); they only parse the outer packet as they forward it towards the tunnel endpoint.
- Upon reaching the tunnel endpoint, encapsulation is removed and the payload is passed along to its ultimate destination.

Our port forwarding scheme is simple. We just need to configure the listening (*accept*) port and the forwarding (*connect*) port for each service, depending on the role as a client or server.



WebServer	MailHost	LDAPhost	Gateway
[ldaps] accept = 389 connect = ldap.tinynet.edu:636		[ldaps] accept = 636 connect = 389	
[imaps] accept = 143 connect = mail.tinynet.edu:993	[imaps] accept = 993 connect = 143		
[smtps] accept = 587 connect = gw.tinynet.edu:465			[smtps] accept = 465 connect = 587

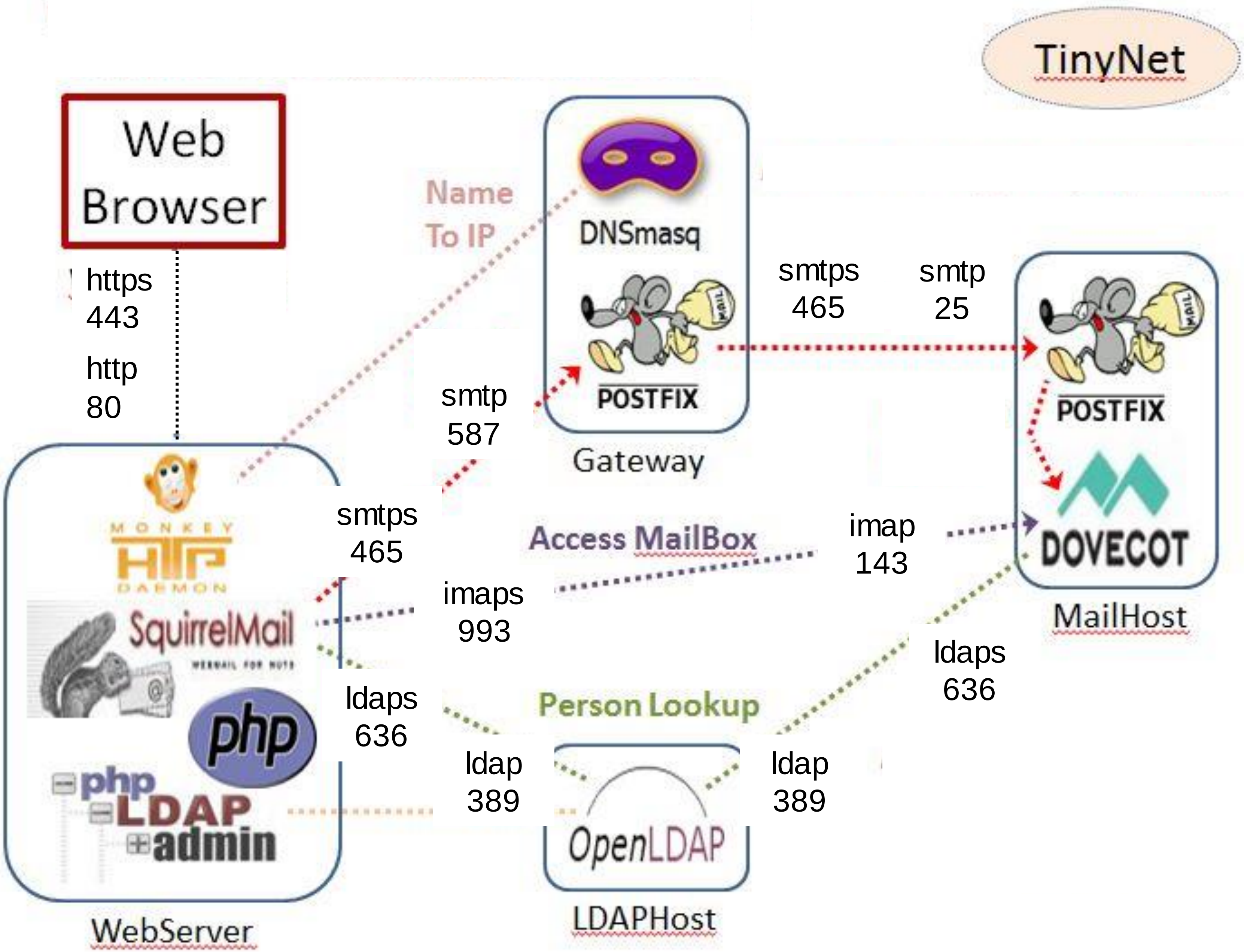
Plain from server

Encrypyed to stunnel

Encrypyed from stunnel

Plain to server

So, to check our mail [imaps], the request is received by the client-side stunnel on port 143, stunnel does the encryption, and then sends it off to the MailServer. The server-side stunnel receives the request on port 993, unencrypts it, and passes it to Dovecot via port 143. Responses work the same way, in reverse.



TinyNet
Web Browser
https 443
http 80
Name To IP
DNSmasq
POSTFIX
Gateway
smtps 465
smtp 25
POSTFIX
DOVECOT
MailHost
smtp 587
smtps 465
Access MailBox
imap 143
imaps 993
MONKEY HTTP DAEMON
SquirrelMail
WEBMAIL FOR NUTS
php
phpLDAPadmin
ldaps 636
Person Lookup
ldaps 636
ldap 389
ldap 389
OpenLDAP
LDAPHost
WebServer

stunnel

- Our stunnel configuration is low-security, in the sense that it does not check the validity of the key
- Any key is good for encryption ... But not every key can be trusted
  - there is a good discussion of trust vs. security at https://security.stackexchange.com/questions/112768/why-are-self-signed-certificates-not-trusted-and-is-there-a-way-to-make-them-tru
- We use the same key on every server, because it is all within the site – **More Convenience**, Less Security

‘‘ A self-signed certificate is like making a gold-colored badge looking thing in your home and then going around showing it to people saying you're a police officer. Maybe you can pull that trick with members of your family who accept that you're in charge, but if you want to be a real, public, law enforcement official, you have to be trusted by a central authority that everyone else trusts, like the government of your town or city or state. Otherwise, you're just impersonating a police officer and people would be wise to distrust you.’’
– Todd Wilcox Feb 4 '16 at 16:41

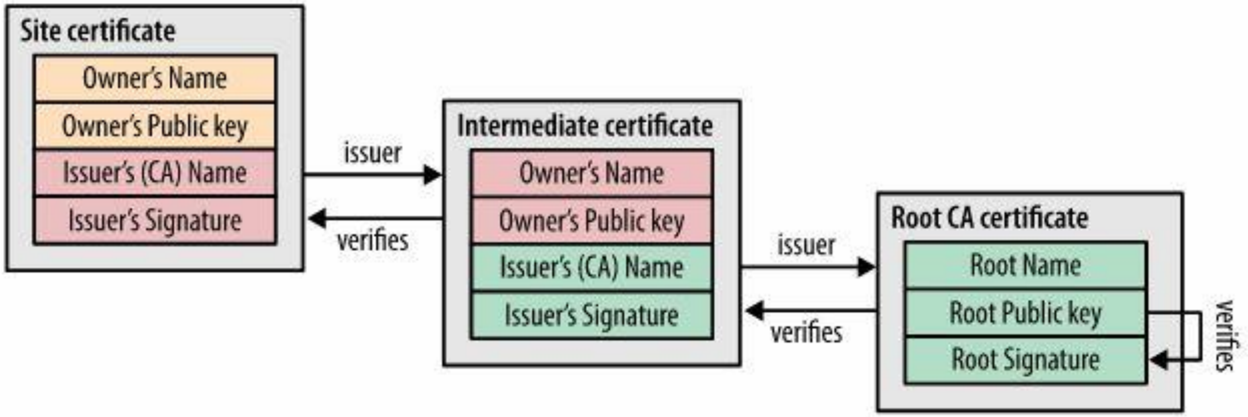


Figure 4-5. CA signing of digital certificates

https://hpbn.co/transport-layer-security-tls/

Q
&
A

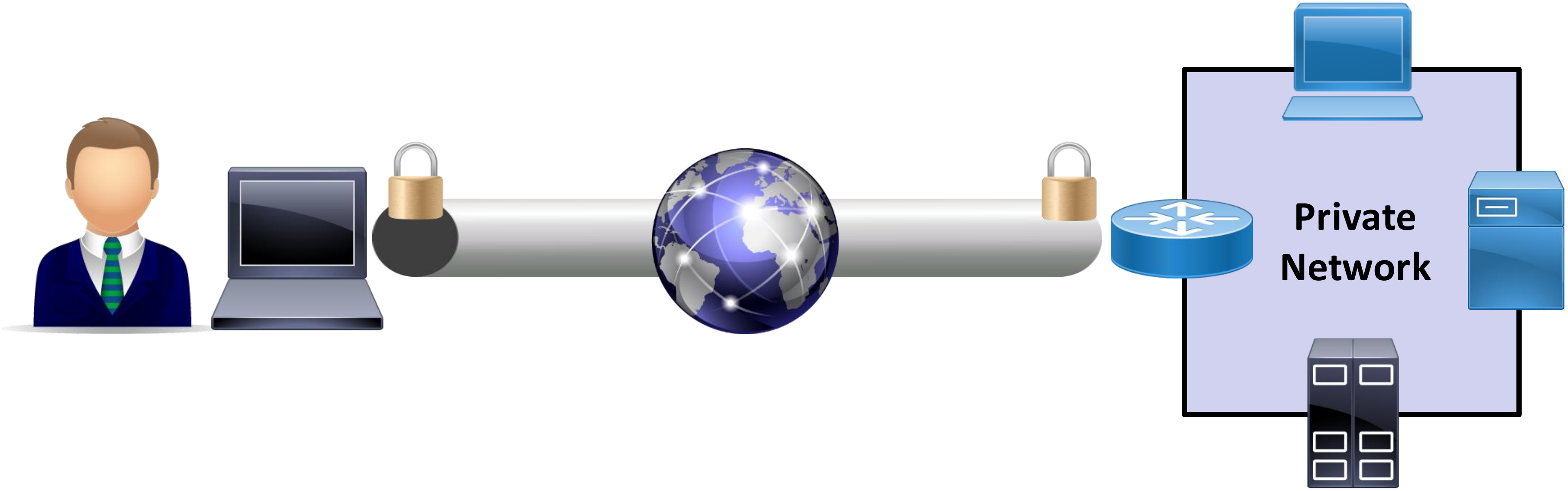
Virtual Private Networks

- stunnel and native capabilities are fine for per-service security, but what if we want to secure all communications between clients and servers?
- What if we need to provide secure remote access to a lot of different applications?
- Best answer: a “Virtual Private Network” (VPN)

Virtual Private Networks

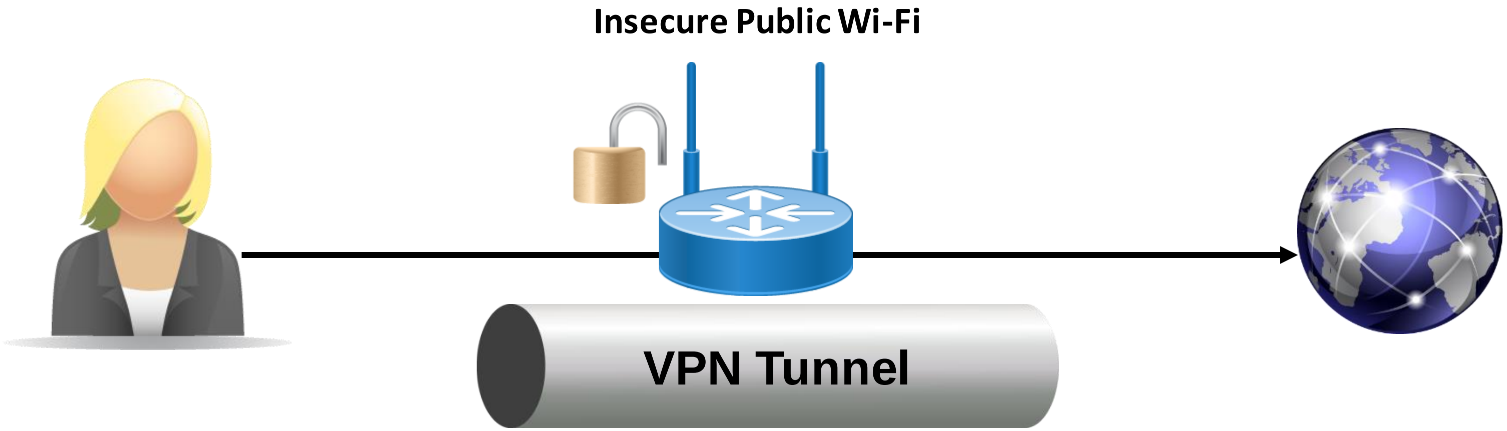
A method of extending a private network by tunneling through a public network like the Internet.

- Provides secure connections between endpoints.
- Encapsulates and encrypts data through the tunnel.
- VPN protocols provide tunneling and encryption services.



VPNs and Wireless

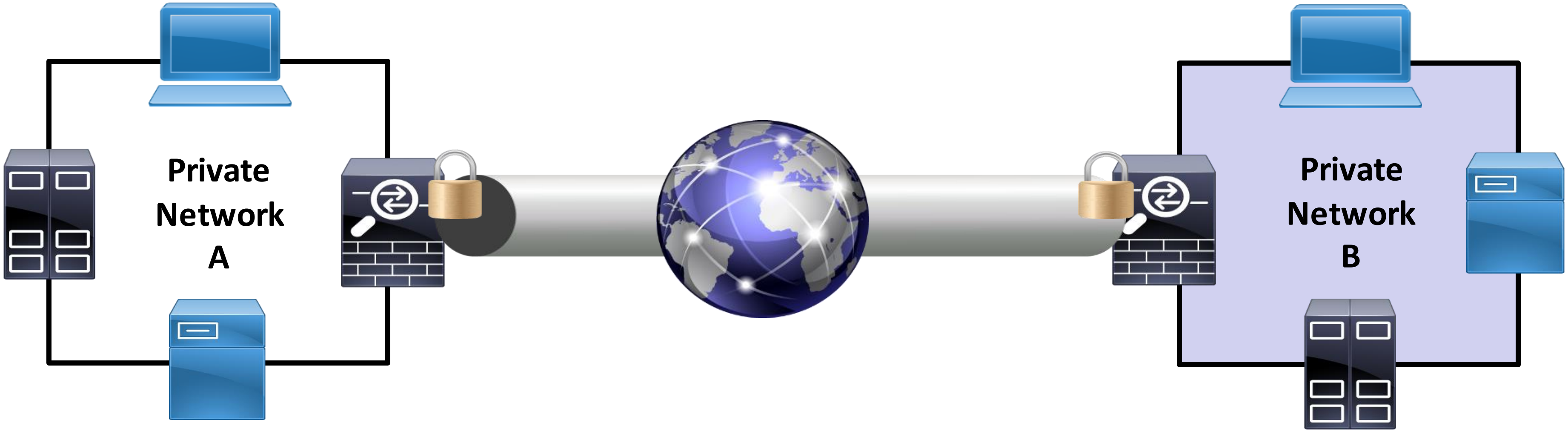
- Open wireless networks are a major risk.
- Attackers can compromise communications.
- If forced to use open wireless, tunnel through with a VPN.
  - Can encrypt data even when using an insecure wireless hotspot.
  - Use a strong tunneling protocol like IPSec.



VPN Concentrators

A single device that incorporates encryption and authentication to handle a large number of VPN tunnels.

- Can accommodate remote access or site-to-site.
- Common tunneling protocols:
  - IPSec (site-to-site)
  - SSL/TLS (remote access)



IPSec

- A "kernel space" VPN uses the secure version of IP (IPSec) to encrypt the data in every packet before it is sent. This works for both IPv4 and IPv6 networks.
- IPSec actually consists of three main protocols:
  - IPsec Authentication Header (AH),
  - IPsec Encapsulating Security Payload (ESP), and the
  - IPsec Internet Key Exchange (IKE).
- which are described in RFC4301 to RFC4309, plus 27 additional RFCs to clarify and update.

OpenVPN

- OpenVPN is a full-featured SSL VPN which can accomodate a wide range of configurations
- IP packets are encrypted and encapsulated in UDP, and sent through a TUN or TAP device to a matching device on a remote host.
- The remote host receives, decrypts, authenticates, and de-encapsulates the packets, pumping the payload of the UDP packet into the stack
- You can apply firewall rules to tun and tap interfaces in the same way that you can apply them to ethernet interfaces.

VPN Configuration

The two major techniques for VPN networking are **routing** (**tun** device) and **bridging** (**tap** device).

- The VPN essentially links a local **tun** or **tap** device with a remote one of the same type.
- Rather being connected to a wire, the driver connects to “user space”, where a program can open the device just like a file and read and write packets from and to it.

tun or tap interface?

- **Routing** uses separate subnets and setting up routes between them.
- A **tun** interface is a device driver that that looks like point-to-point network hardware to the operating system
- Routes must be set up linking each subnet.
- Better scalability

tun or tap interface?

- **Bridging** is a technique for creating a virtual, wide-area ethernet LAN, running on a single subnet.
- A **tap** interface emulates ethernet rather than point-to-point.
  - Allows software that depends on LAN broadcasts such as Windows NetBIOS file sharing and printer sharing to work.
- Less efficient than routing (all that broadcast traffic)
- Does not scale well.

TLS or Static Key mode?

- **TLS** mode allows an OpenVPN server to allocate addresses from a pool to clients similar to a DHCP server
- The tradeoff here is that every client needs to have its own certificate – **Less IP management**, More CA duties
- In **Static-Key** mode two OpenVPN **peers** share the same key
  - We need xinetd to establish a client/server relationship
- The tradeoff here is **Less CA duties**, More IP management
  - CA duties require planning and control - can be time consuming

Q&A