Lesson 11

Implementing Secure Network Protocols

CompTIA®

Topic 11A

Implement Secure Network Operations Protocols

Syllabus Objectives Covered

- 1.4 Given a scenario, analyze potential indicators associated with network attacks
- 3.1 Given a scenario, implement secure protocols

Network Address Allocation

```
msf auxiliary(dhcp) > set dhcpipend 10.1.0.210
dhcpipend => 10.1.0.210
msf auxiliary(dhcp) > set netmask 255.255.255.0
netmask => 255.255.255.0
msf auxiliary(dhcp) > set dnsserver 10.1.0.192
dnsserver => 10.1.0.192
msf auxiliary(dhcp) > set router 10.1.0.192
router => 10.1.0.192
msf auxiliary(dhcp) > set srvhost 10.1.0.192
srvhost => 10.1.0.192
msf auxiliary(dhcp) > show options

Module options (auxiliary/server/dhcp):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   BROADCAST                      no        The broadcast address to send to
   DHCPIPEND     10.1.0.210       no        The last IP to give out
   DHCPIPSTART   10.1.0.200       no        The first IP to give out
   DNSSERVER     10.1.0.192       no        The DNS server IP address
   DOMAINNAME                     no        The optional domain name to assign
   FILENAME                       no        The optional filename of a tftp boot
server
   HOSTNAME                       no        The optional hostname to assign
   HOSTSTART                      no        The optional host integer counter
   NETMASK       255.255.255.0    yes       The netmask of the local subnet
   ROUTER        10.1.0.192       no        The router IP address
   SRVHOST       10.1.0.192       yes       The IP of the DHCP server


Auxiliary action:

   Name     Description
   ----     -----------
   Service


msf auxiliary(dhcp) > run
[*] Auxiliary module execution completed

[*] Starting DHCP server...
msf auxiliary(dhcp) >
```

```
root@KALI:~# dnsspoof -i eth0 -f /root/phar
m.txt
dnsspoof: listening on eth0 [udp dst port 5
3 and not src 10.1.0.192]
```

```
[--->] DHCP_Discover
[--->] DHCP_Discover
[--->] DHCP_Discover
[--->] DHCP_Discover
[ -- ] timeout waiting on dhcp packet count
3
[--->] DHCP_Discover
[--->] DHCP_Discover
[ ?? ]                    waiting for DHCP poo
l exhaustion...
[--->] DHCP_Discover
[--->] DHCP_Discover
[--->] DHCP_Discover
[--->] DHCP_Discover
[--->] DHCP_Discover
[ -- ] timeout waiting on dhcp packet count
4
[ ?? ]                    waiting for DHCP poo
l exhaustion...
[ -- ] [DONE] DHCP pool exhausted!

root@KALI:~#
```

- Dynamic versus static IP address assignment
- Dynamic Host Configuration Protocol (DHCP)
- Prevent rogue DHCP servers
- Prevent DoS attacks (starvation) by rogue clients
- Secure administration interface

Domain Name Resolution

- System for resolving host names and domain labels to IP addresses
- Domain hijacking
  - Gain control of domain registration
  - whois
- Uniform Resource Locator (URL) redirection
  - Abuse of HTTP redirects and .htaccess redirects
- Domain reputation
  - Monitor blocklists/reputation lists for abuse of your domain

https://trusted.foo/login.php
?url="https://tru5ted.foo"

DNS Poisoning

- Man in the Middle
  - Rogue DNS server intercepts queries
- DNS client cache poisoning
  - HOSTS file
- DNS server cache poisoning
  - Corrupt cached records on DNS servers
  - Spoof responses to queries by exploiting weak transaction ID generation
  - DNS authoritative name server impersonation

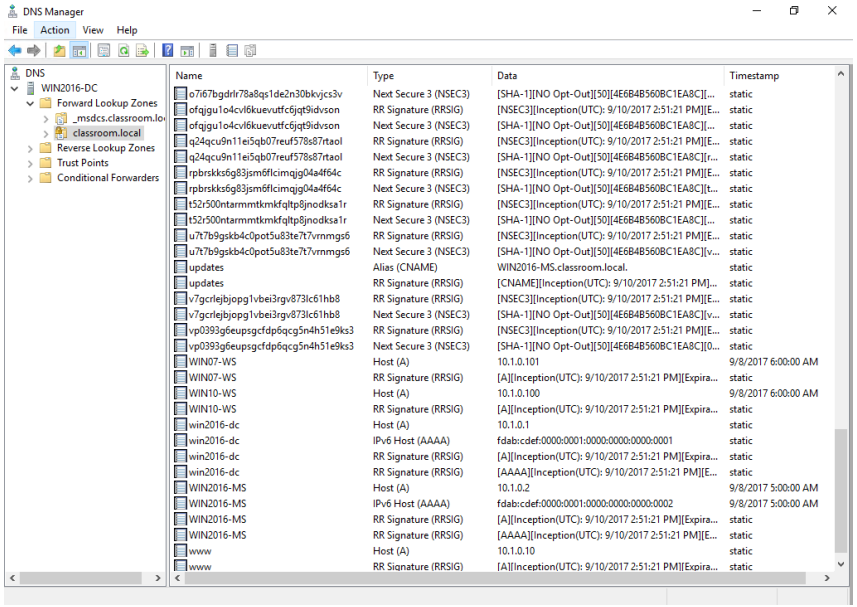
```
   HOSTNAME   www.web.local    yes       Hostname to hijack
   INTERFACE                   no        The name of the interface
   NEWADDR    192.168.2.192    yes       New address for hostname
   RECONS     192.168.2.254    yes       The nameserver used for reconnaissance
   RHOST      192.168.1.1      yes       The target address
   SNAPLEN    65535            yes       The number of bytes to capture
   SRCADDR    Real             yes       The source address to use for sending t
he queries (Accepted: Real, Random)
   SRCPORT    0                yes       The target server's source query port (
0 for automatic)
   TIMEOUT    500              yes       The number of seconds to wait for new d
ata
   TTL        46348            yes       The TTL for the malicious host entry
   XIDS       0                yes       The number of XIDs to try for each quer
y (0 for automatic)

msf auxiliary(bailiwicked_host) > run

[-] Failure: This hostname is already in the target cache: www.web.local
[-]          Cache entry expires on 2017-09-17 09:08:17 -0700... sleeping.
^C[-] Auxiliary interrupted by the console user
[*] Auxiliary module execution completed
msf auxiliary(bailiwicked_host) > set hostname updates.web.local
hostname => updates.web.local
msf auxiliary(bailiwicked_host) > run

[*] Targeting nameserver 192.168.1.1 for injection of updates.web.local. as 192.
168.2.192
[*] Querying recon nameserver for web.local.'s nameservers...
[*]  Got an NS record: web.local.              604800  IN      NS      ns.web.lo
cal.
[*]   Querying recon nameserver for address of ns.web.local....
[*]    Got an A record: ns.web.local.           604800  IN      A       192.168.
1.1
[*]     Checking Authoritativeness: Querying 192.168.1.1 for web.local....
[*]     ns.web.local. is authoritative for web.local., adding to list of nameser
vers to spoof as
[*] Calculating the number of spoofed replies to send per query...
[*]   race calc: 100 queries | min/max/avg time: 0.0/0.0/0.0 | min/max/avg repli
es: 0/1/0
[*] The server did not reply, giving up.
[*] Auxiliary module execution completed
msf auxiliary(bailiwicked_host) >
```

DNS Security



Screenshot used with permission from Microsoft.

- DNS server security
  - Fault tolerance
  - Authenticated recursive requests only
  - Access control
  - Patch management
  - Prevent footprinting
- DNS Security Extensions (DNSSEC)
  - RRset
  - Zone Signing Key
  - Key Signing Key
  - Root of Trust

Secure Directory Services

- Directory services and Lightweight Directory Access Protocol (LDAP)
- Binding methods
  - None
  - Simple authentication
  - Simple Authentication and Security Layer (SASL)
  - LDAPS (TLS over TCP port 636)
- Access control policy
  - Read-only
  - Read/write

Time Synchronization

- Time critical services
  - Authentication
  - Logging
  - Task scheduling/backup
  - …
- Network Time Protocol (NTP)
  - Stratum 1 servers
  - Stratum 2 servers
  - Simple NTP (clients)

Simple Network Management Protocol Security

- Simple Network Management Protocol (SNMP)
  - Agent runs on devices and maintains management information base (MIB)
  - Agent notifies SNMP monitor of events (traps)
- SNMP v1 and v2 feature no or weak authentication and no privacy
- SNMP v3 encryption and authentication

Topic 11B

Implement Secure Application Protocols

Syllabus Objectives Covered

- 2.1 Explain the importance of security concepts in an enterprise environment
- 3.1 Given a scenario, implement secure protocols

HyperText Transport Protocol and Web Services

- HTTP headers and payload
- Web services/applications
  - Forms mechanism allows client to upload data to the server
  - Stateless protocol but expanded with cookies and scripting

Transport Layer Security

- Secure Sockets Layer (SSL)/Transport Layer Security (TLS)
  - Communications secured using host certificates
- SSL/TLS versions
- Cipher suites
  - Key exchange – authentication – confidentiality - HMAC

    ECDHE-RSA-AES128-GCM-SHA256
  - TLS 1.3 uses shortened suites

    TLS_AES_256_GCM_SHA384

Screenshot used with permission from Wireshark.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.106	172.217.20.132	TCP	66	53476 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
2	0.016952	172.217.20.132	192.168.0.106	TCP	66	443 → 53476 [SYN, ACK] Seq=0 Ack=1 Win=60720 Len=
3	0.017028	192.168.0.106	172.217.20.132	TCP	54	53476 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
4	0.018272	192.168.0.106	172.217.20.132	TLSv1.3	688	Client Hello
5	0.036762	172.217.20.132	192.168.0.106	TCP	60	443 → 53476 [ACK] Seq=1 Ack=635 Win=62208 Len=0
6	0.036763	172.217.20.132	192.168.0.106	TLSv1.3	266	Server Hello, Change Cipher Spec, Application Dat
7	0.037274	192.168.0.106	172.217.20.132	TLSv1.3	118	Change Cipher Spec, Application Data
8	0.038669	192.168.0.106	172.217.20.132	TLSv1.3	224	Application Data

```
> Frame 6: 266 bytes on wire (2128 bits), 266 bytes captured (2128 bits) on interface \Device\NPF_{DC478856-D898-4
> Ethernet II, Src: Tp-LinkT_cf:ea:cb (60:e3:27:cf:ea:cb), Dst: Tp-LinkT_15:af:e4 (c4:e9:84:15:af:e4)
> Internet Protocol Version 4, Src: 172.217.20.132, Dst: 192.168.0.106
> Transmission Control Protocol, Src Port: 443, Dst Port: 53476, Seq: 1, Ack: 635, Len: 212
v Transport Layer Security
  v TLSv1.3 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 128
    v Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 124
        Version: TLS 1.2 (0x0303)
        Random: dba516a7b5f5b3d4f95453c6bbdfe85d73a1db4632640372…
        Session ID Length: 32
        Session ID: 011fa8811607e422d8a3d92ecdd135e6da77498d8b64f75d…
        Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
        Compression Method: null (0)
        Extensions Length: 52
      > Extension: pre_shared_key (len=2)
      > Extension: key_share (len=36)
      v Extension: supported_versions (len=2)
          Type: supported_versions (43)
          Length: 2
          Supported Version: TLS 1.3 (0x0304)
```

API Considerations

```
POST /api/users HTTP/1.1
Content-Type: application/json
{
 "user": {
   "name": "James",
   "email": "jpengelly@comptia.org"
 }
}
```

- Application programming interface (API)
  - Makes web application or service accessible to automation by scripting
  - Passing parameters
- API keys
  - Static keys
  - Authentication and authorization via SAML/OAuth

Subscription Services

- News and information services
  - Market and financial intelligence and information
  - Security threat intelligence and information
  - Reference and training materials
  - Software applications and cloud services
- Provide secure access
- News feed security
  - Really Simple Syndication (RSS)
  - Atom
  - XML injection and exploits

File Transfer Services

- SSH FTP (SFTP)
  - Run FTP over SSH on port 22
- FTP over SSL (FTPS)
  - Explicit TLS (FTPES)—use the AUTH TLS command to upgrade an unsecure connection established over port 21 to a secure one
  - Implicit TLS (FTPS)—negotiate an SSL/TLS tunnel before the exchange of any FTP commands (port 990 for the control connection)

Email Services

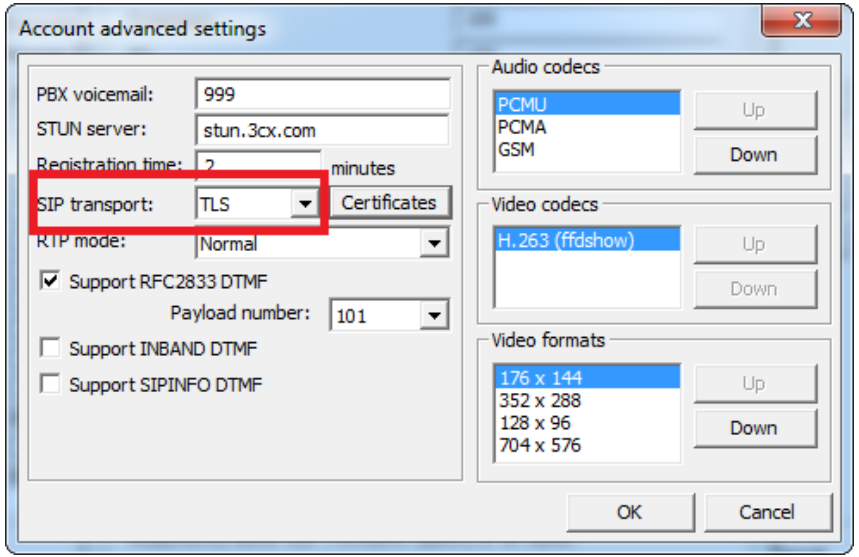
- Simple Mail Transfer Protocol (SMTP)
  - Route mail between servers
  - Security mechanisms
    - STARTTLS—explicit TLS
    - SMTPS—implicit TLS
    - Common port configurations
- Mailbox access protocols
  - Post Office Protocol (POP3)
  - Internet Message Access Protocol (IMAP)
    - Better mailbox management features than POP3
  - Secure ports
    - POP3S TCP port 995
    - IMAPS TCP port 993

Secure/Multipurpose Internet Mail Extensions

- End-to-end encryption for message contents
- Authentication and confidentiality using PKI certificates
- Correspondents must exchange and trust certificates

Voice and Video Protocol Security

- Voice over IP (VoIP), web conferencing, and video teleconferencing (VTC)
  - Session control
  - Data transport
  - Quality of service (QoS)
- Session Initiation Protocol (SIP)
  - SIP addresses
  - Integration with external networks via gateways and private branch exchanges (PBX)
  - Secure port 5061 to authenticate callers and encrypt connection setup
- Secure Real-time Transport Protocol (SRTP)
  - Call data confidentiality



Screenshot used with permission from 3CX.

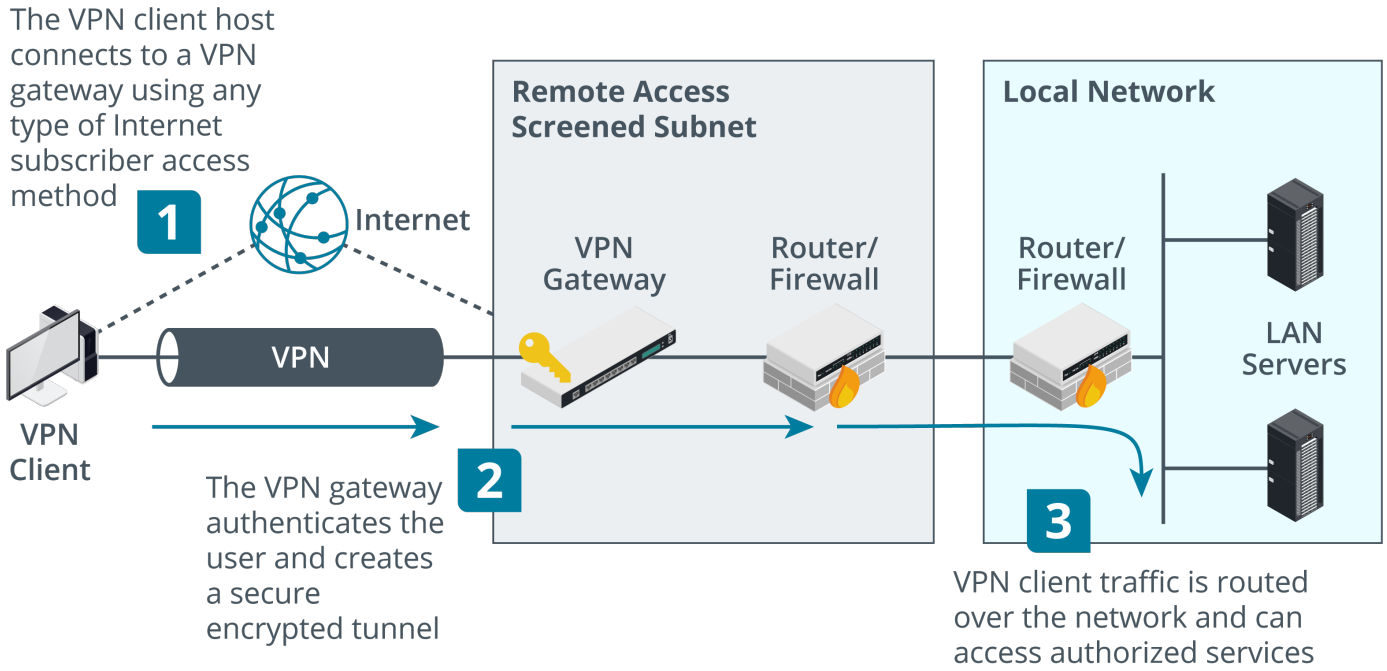
Topic 11C

Implement Secure Remote Access Protocols

Syllabus Objectives Covered

- 3.1 Given a scenario, implement secure protocols
- 3.3 Given a scenario, implement secure network designs
- 4.1 Given a scenario, use the appropriate tool to assess organizational security (SSH only)

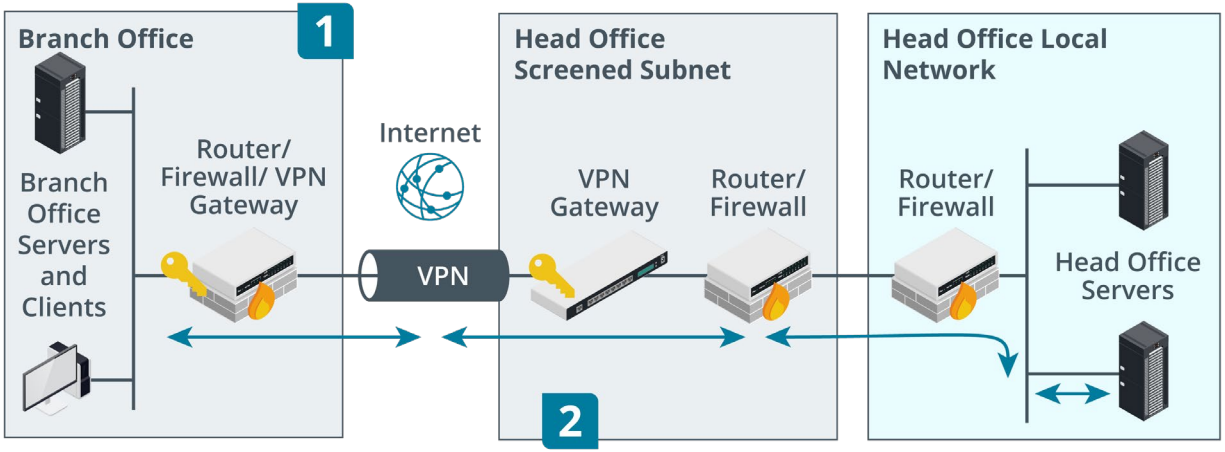
Remote Access Architecture (1)



Images © 123RF.com.

Remote Access Architecture (2)

The VPN gateway at a branch office establishes a VPN connection with the head office site

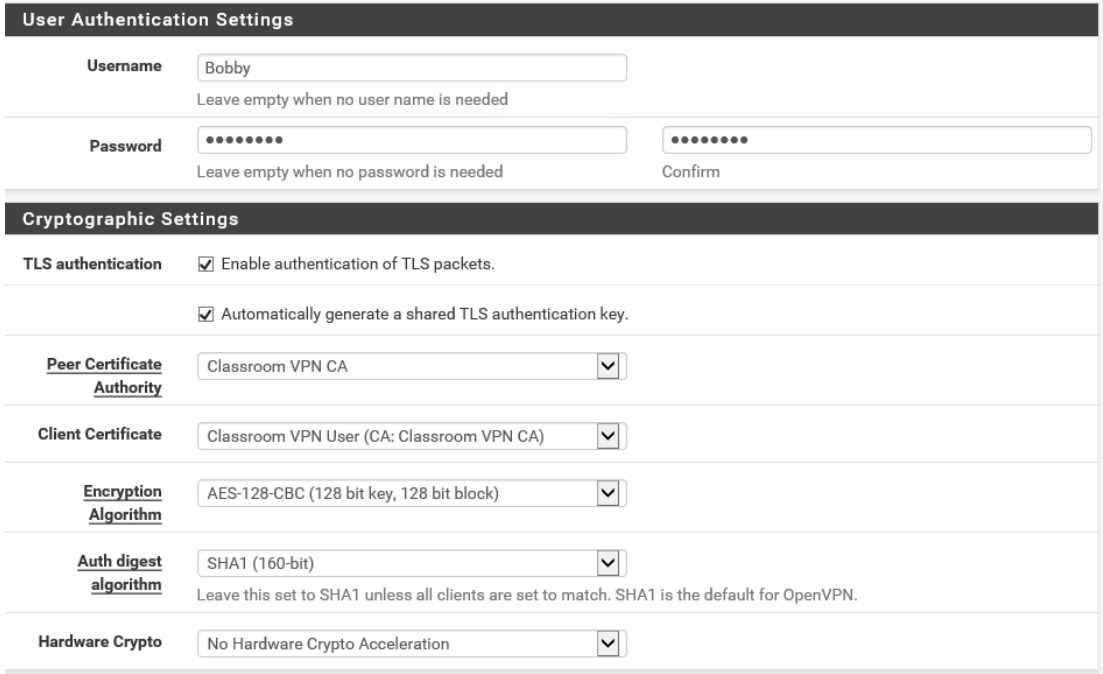


Traffic for a host at a remote site is automatically routed and tunneled over the VPN link

Images © 123RF.com.

Transport Layer Security VPN

- Use TLS to negotiate a secure connection, authenticated by PKI certificates
- Tunnel network traffic over TLS
- Can use TCP or UDP
- OpenVPN
  - TAP/bridged mode
  - TUN/routed mode
- Secure Sockets Tunneling Protocol (SSTP)
  - Secure tunnel for Point-to-Point Protocol encapsulated local network traffic



Screenshot used with permission from Rubicon Communications, LLC.

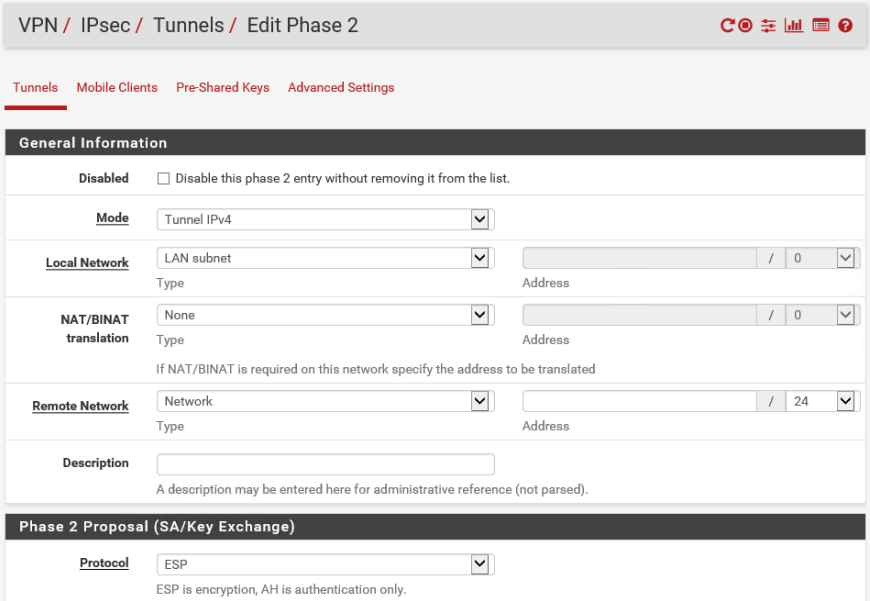
Internet Protocol Security (IPSec)

- Network layer security—application-independent
- Provides confidentiality and/or integrity
- Endpoints must be configured with an IPSec policy and at least one matching security method

- Authentication Header (AH)
  - Signs packet but does not encrypt payload
  - Provides authentication/integrity only
- Encapsulation Security Payload (ESP)
  - Provides confidentiality and/or authentication/integrity

IPSec Transport and Tunnel Modes

- Transport mode for host-to-host connections on a private network
- Tunnel mode between gateways across an unsecure network



Screenshot used with permission from Rubicon Communications, LLC.

Internet Key Exchange

Screenshot used with permission from Rubicon Communications, LLC.

- Internet Key Exchange (IKE)
- Security Association (SA)
- Endpoints must communicate a shared secret and confirm identity
- Phase I provides authentication
  - PKI/certificates
  - Pre-shared key
- Phase II establishes cipher suites and key sizes and use of AH or ESP

Layer 2 Tunneling Protocol and IKE v2

- Layer 2 Tunneling Protocol/IPSec VPN
  - Use IPSec for secure tunneling of Point-to-Point Protocol (PPP) frames
  - Allows user authentication via EAP or CHAP
- IKE v2
  - Makes IPSec a standalone remote access VPN protocol
  - Support for EAP user authentication methods
  - Reduces number of setup messages
  - Support multihoming on client device (switching between Wi-Fi and cellular data)

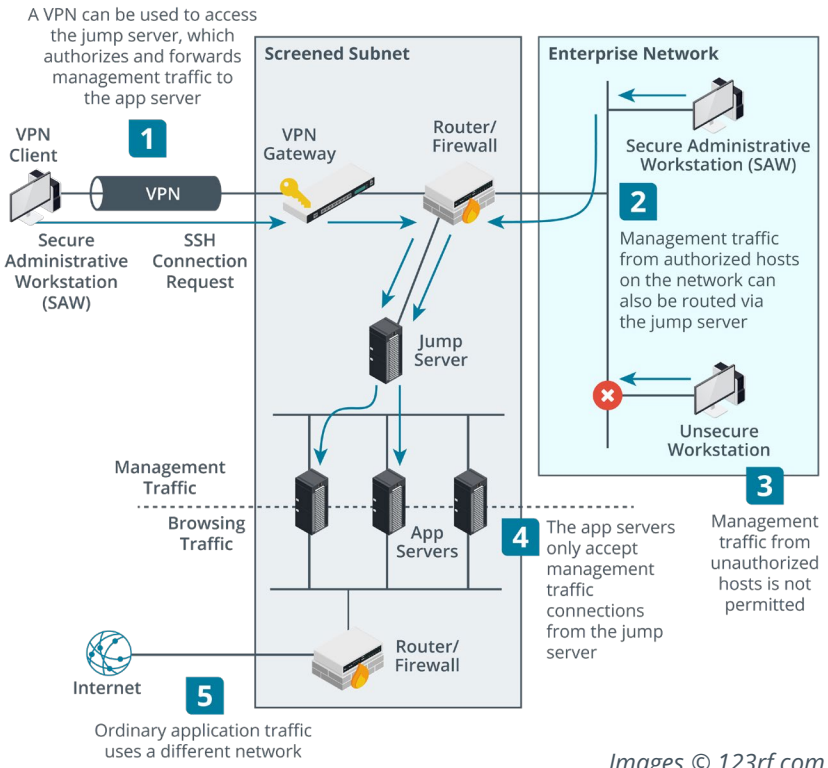
VPN Client Configuration

- Native VPN client or third-party software install
- Configuration
  - VPN gateway address
  - Security type and user credentials
  - Client certificate install
- Always-on VPN
  - Configure VPN to start automatically when trusted network link is detected
- Split tunnel
  - The client accesses the Internet directly using its "native" IP configuration and DNS servers
- Full tunnel
  - Internet access is mediated by the corporate network

Remote Desktop

- GUI-based remote terminal software
- Remote Desktop Protocol (RDP)
  - Connect to physical machines
  - RDP gateway to virtual desktops and apps
- HTML5/clientless
  - Access desktops and web applications from Internet via gateway to internal network
  - Browser support for canvas element plus WebSockets

Out-of-band Management and Jump Servers

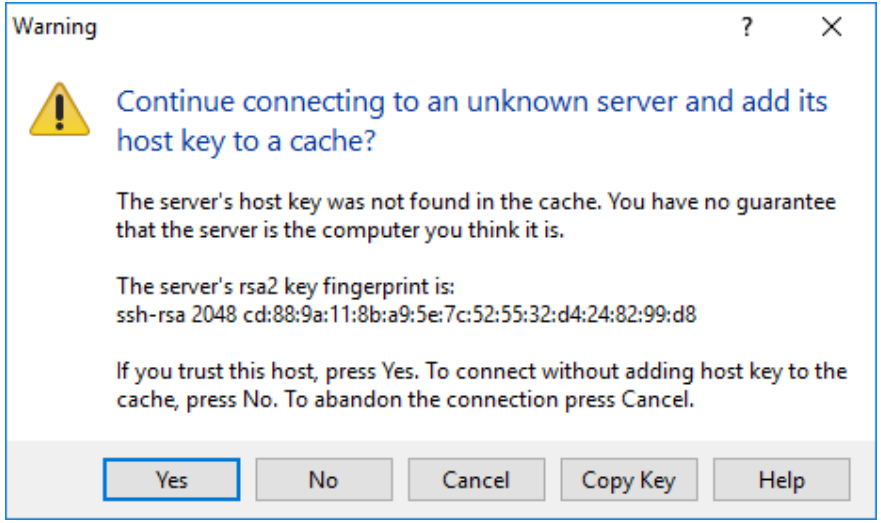


Images © 123rf.com.

- Secure admin workstations (SAWs)
- Out-of-band (OOB) management
  - Serial/modem/console port
  - Virtual terminal
  - Separate cabling or VLAN isolation
- Jump servers
  - Single host accepts SSH or RDP connections from SAWs
  - Forwards connections to app servers
  - App servers only accept connections from jump server

Secure Shell (SSH)

- Remote administration with public key cryptography security
- Host key identifies server
- Client authentication
  - Username/password
  - Public key authentication
  - Kerberos
- Key management
- SSH commands



Screenshot used with permission from PuTTY.

Lesson 11

Summary