

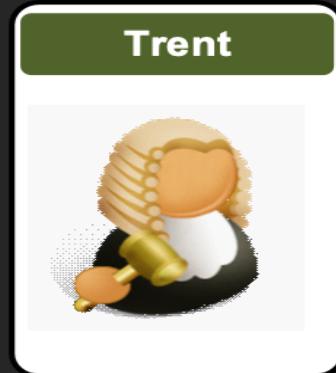
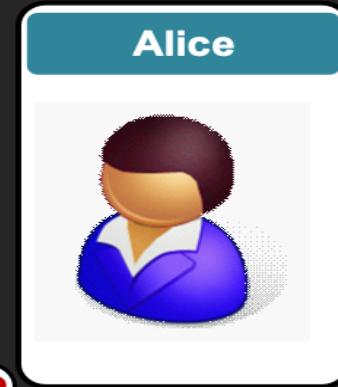
Advanced Crypto

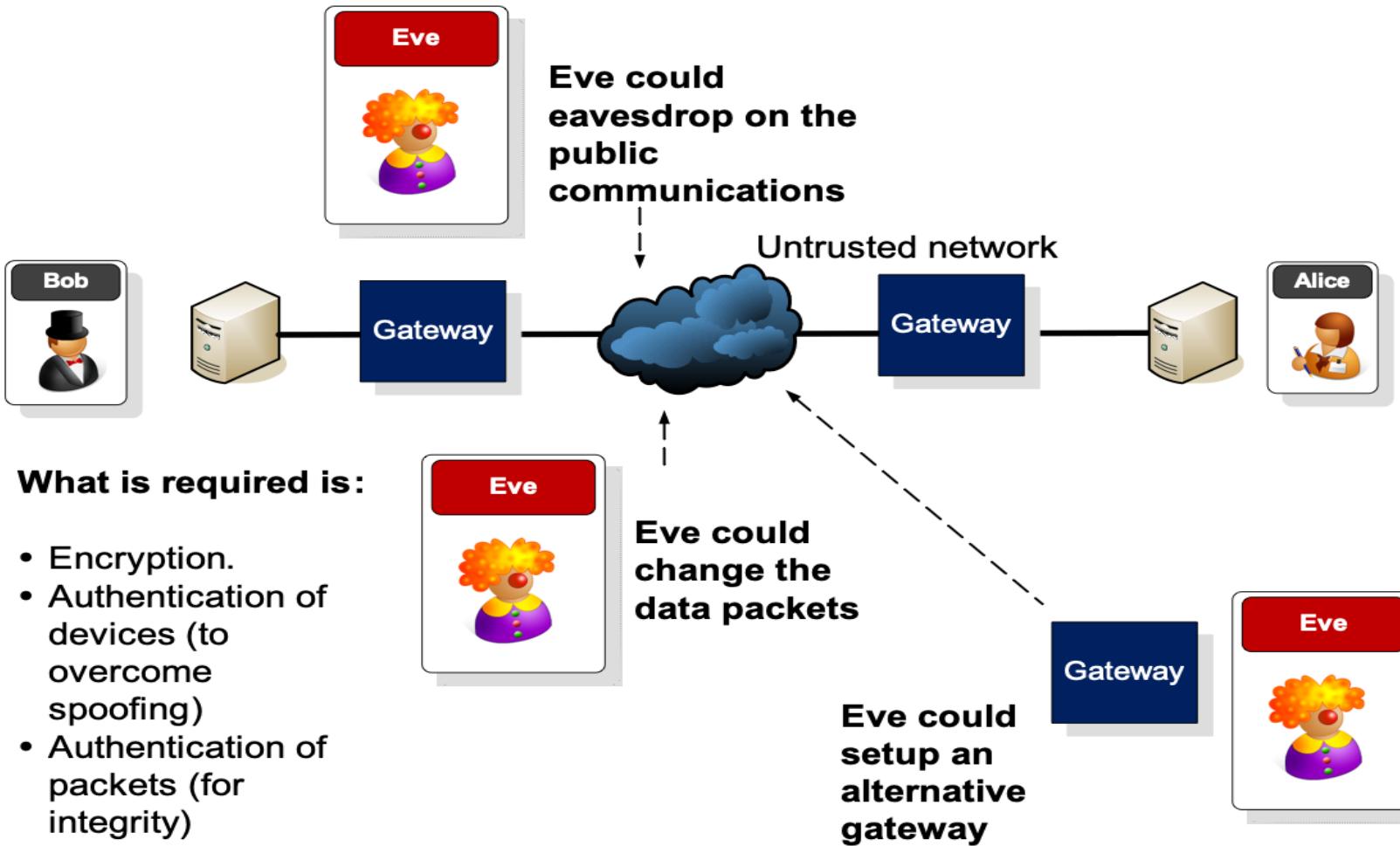
6. Tunnelling

Introduction

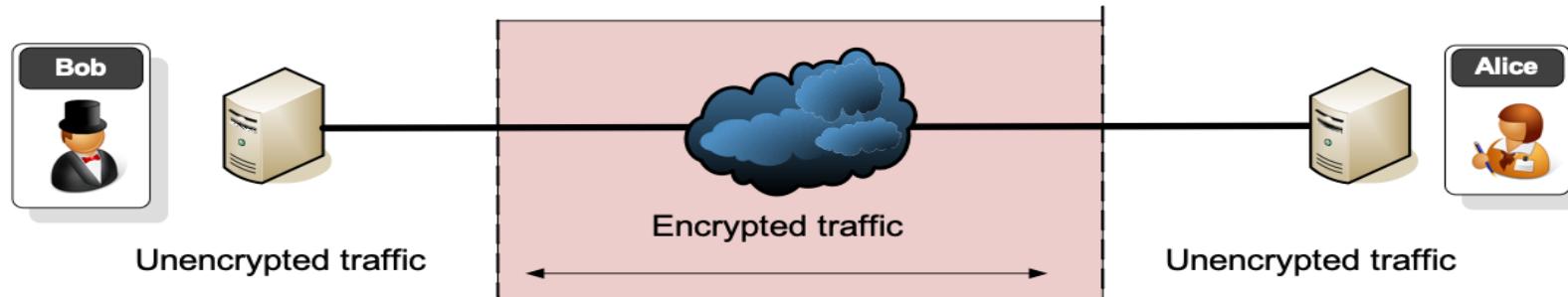
<http://asecuritysite.com/crypto>

Author: Prof Bill Buchanan

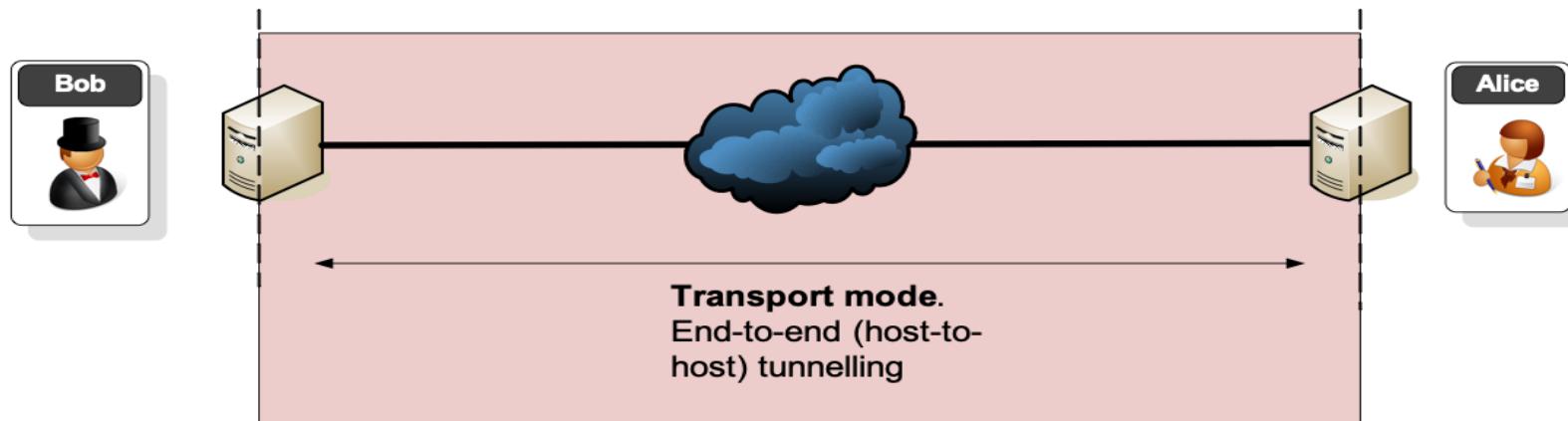


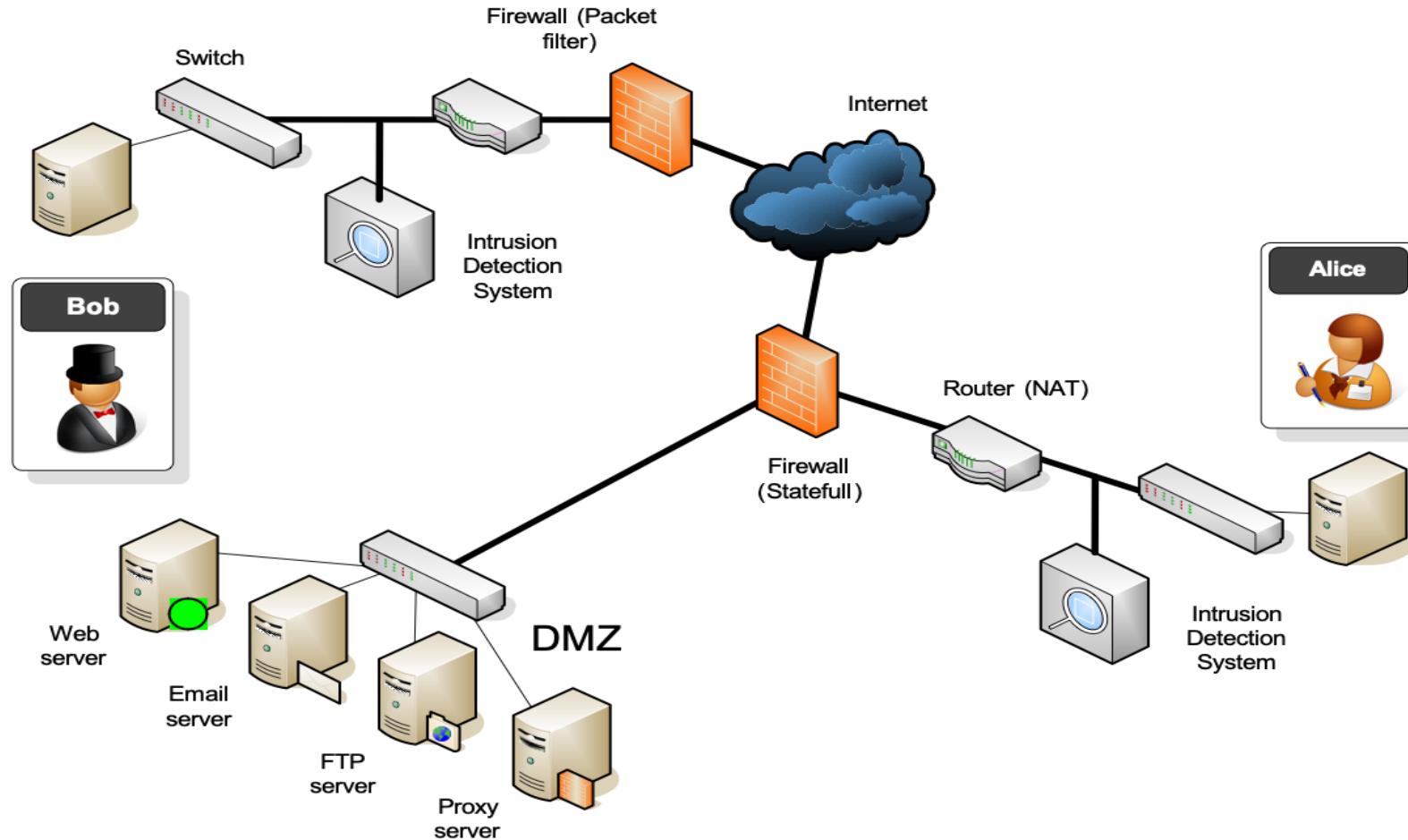


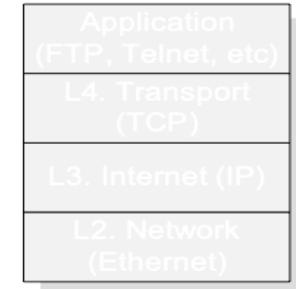
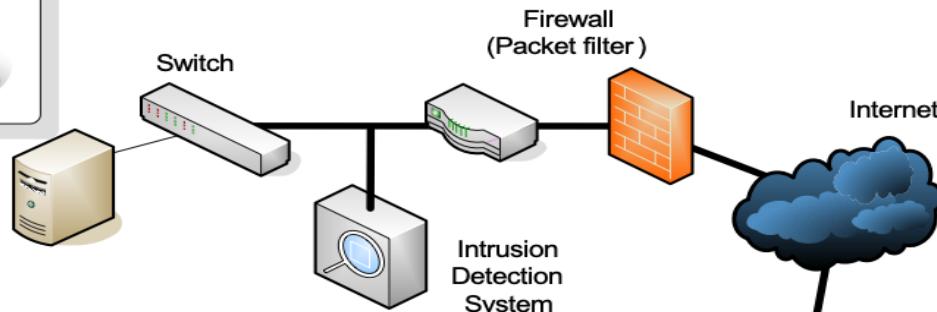
Traffic is encrypted over the untrusted network.



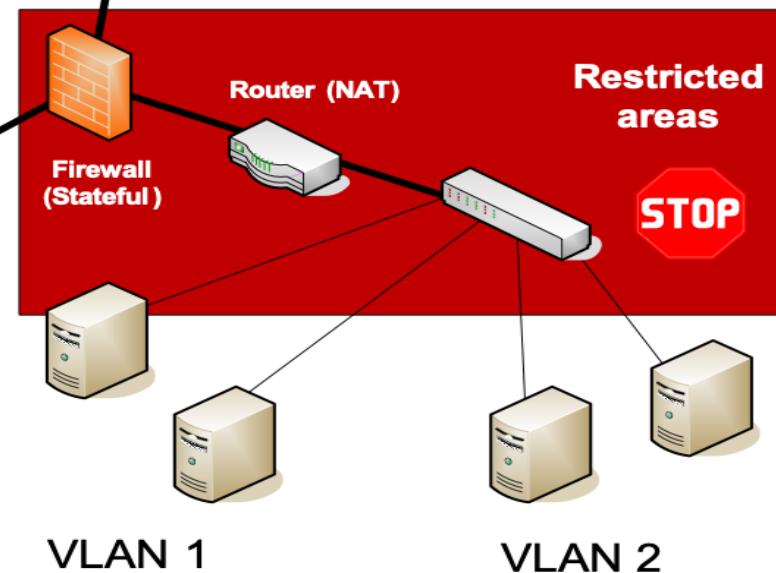
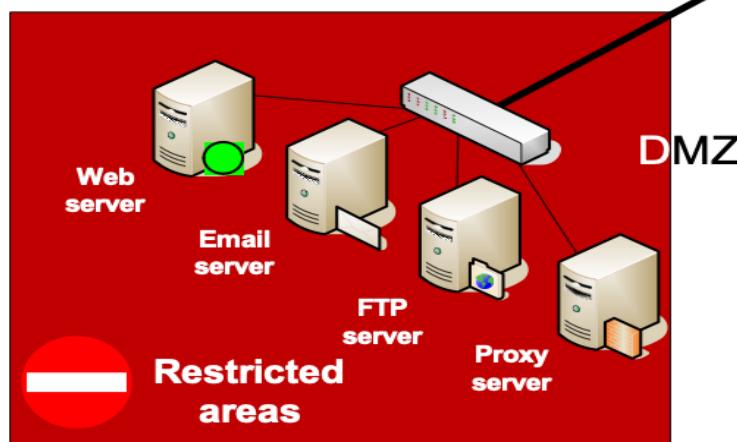
**Transport mode.
End-to-end (host-to-host) tunnelling**

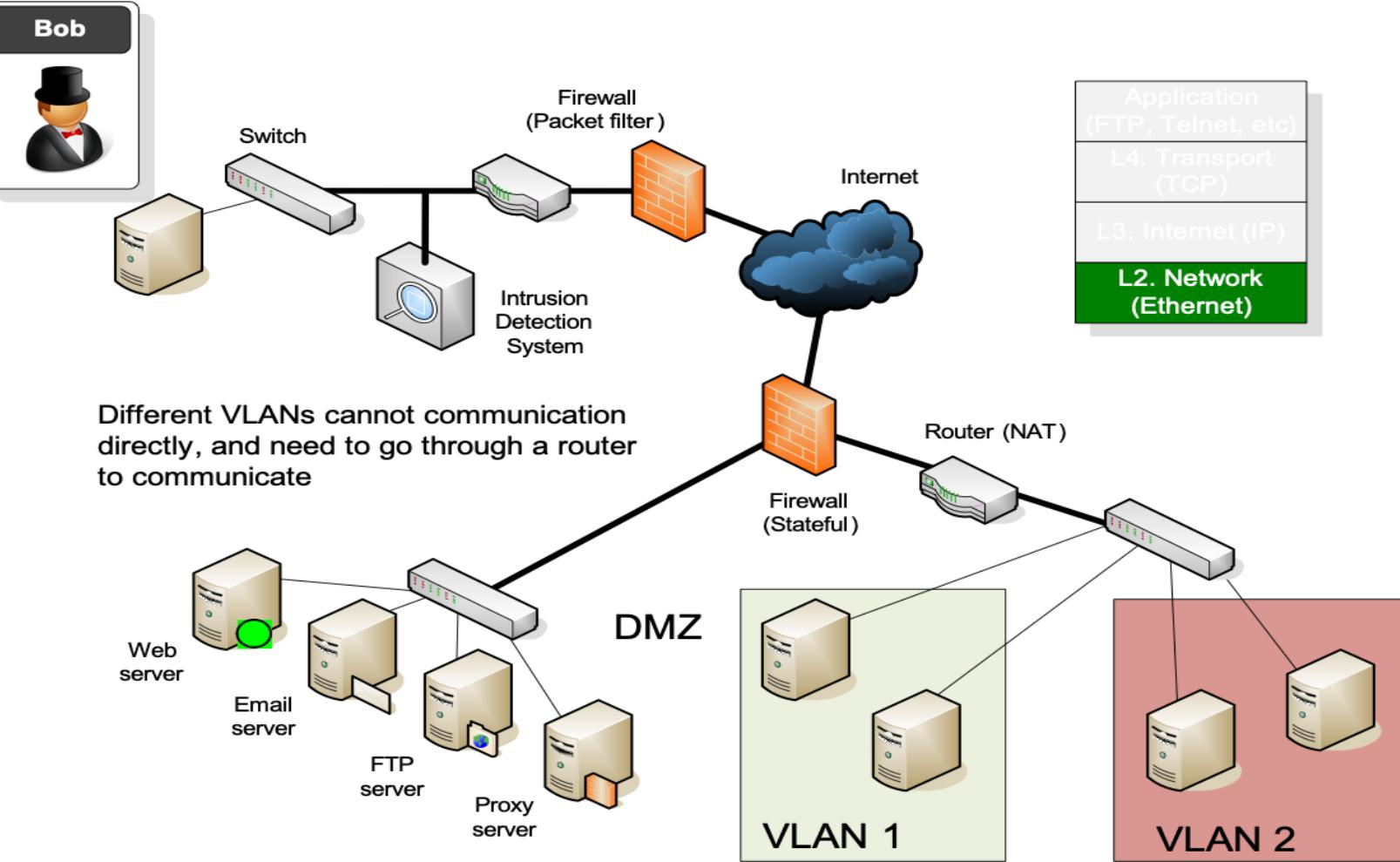


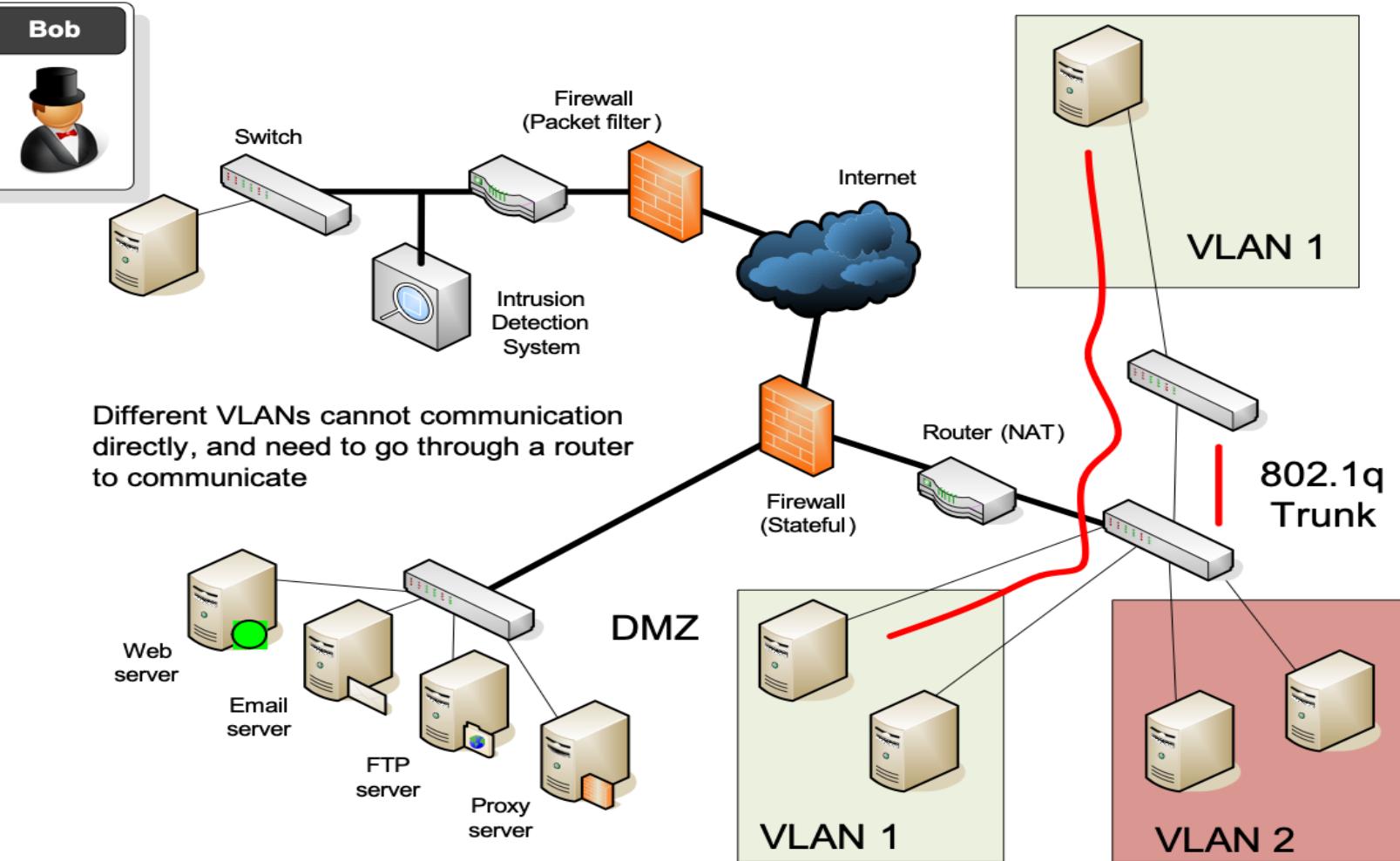


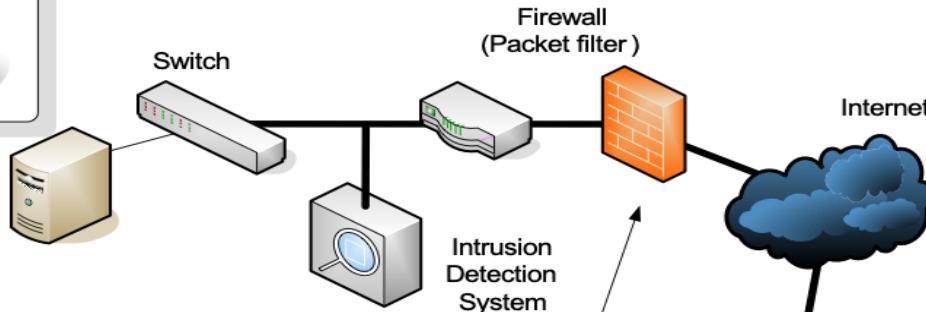


Physical security requires restricted areas and padlocked equipment

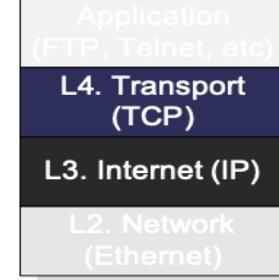




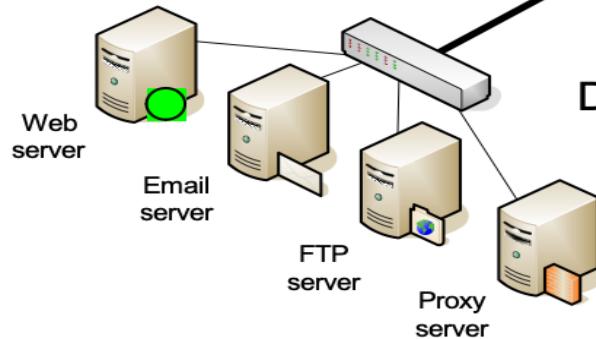


Bob**Screening Firewalls**

filter for IP and TCP packet details, such as addresses and TCP ports, for incoming/outgoing traffic



DMZ



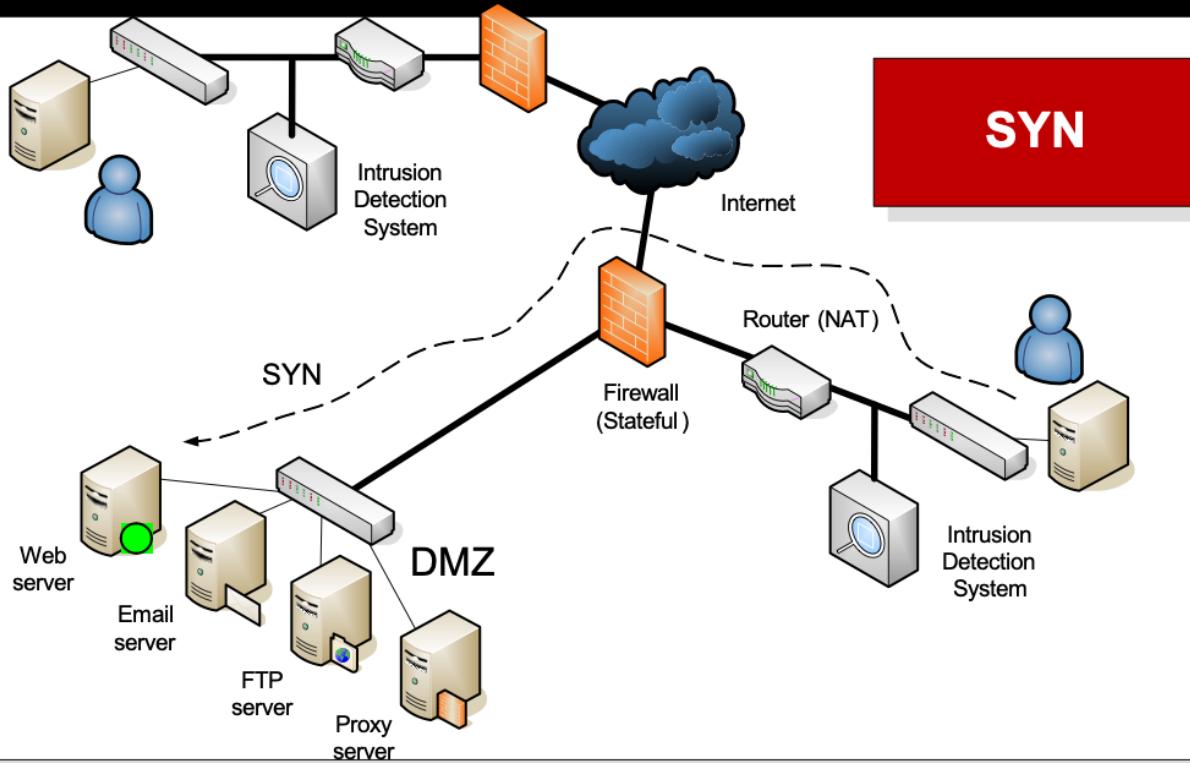
Intrusion
Detection
System

Alice

Network Security

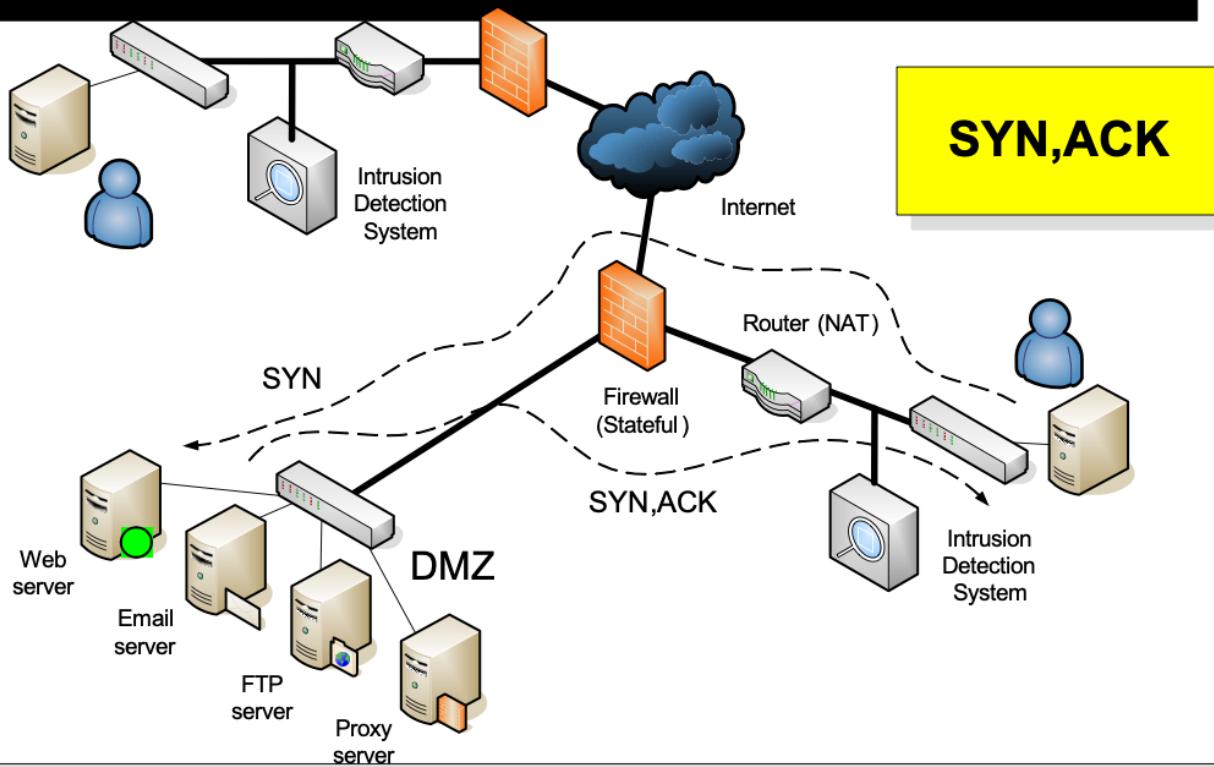
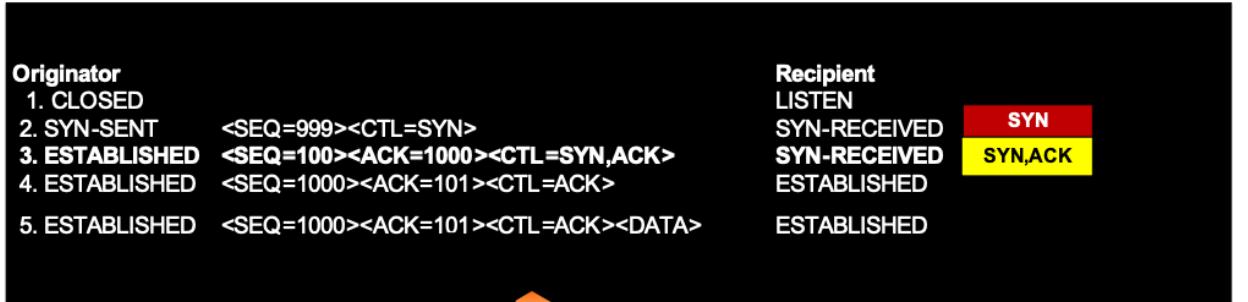
Stateful firewall

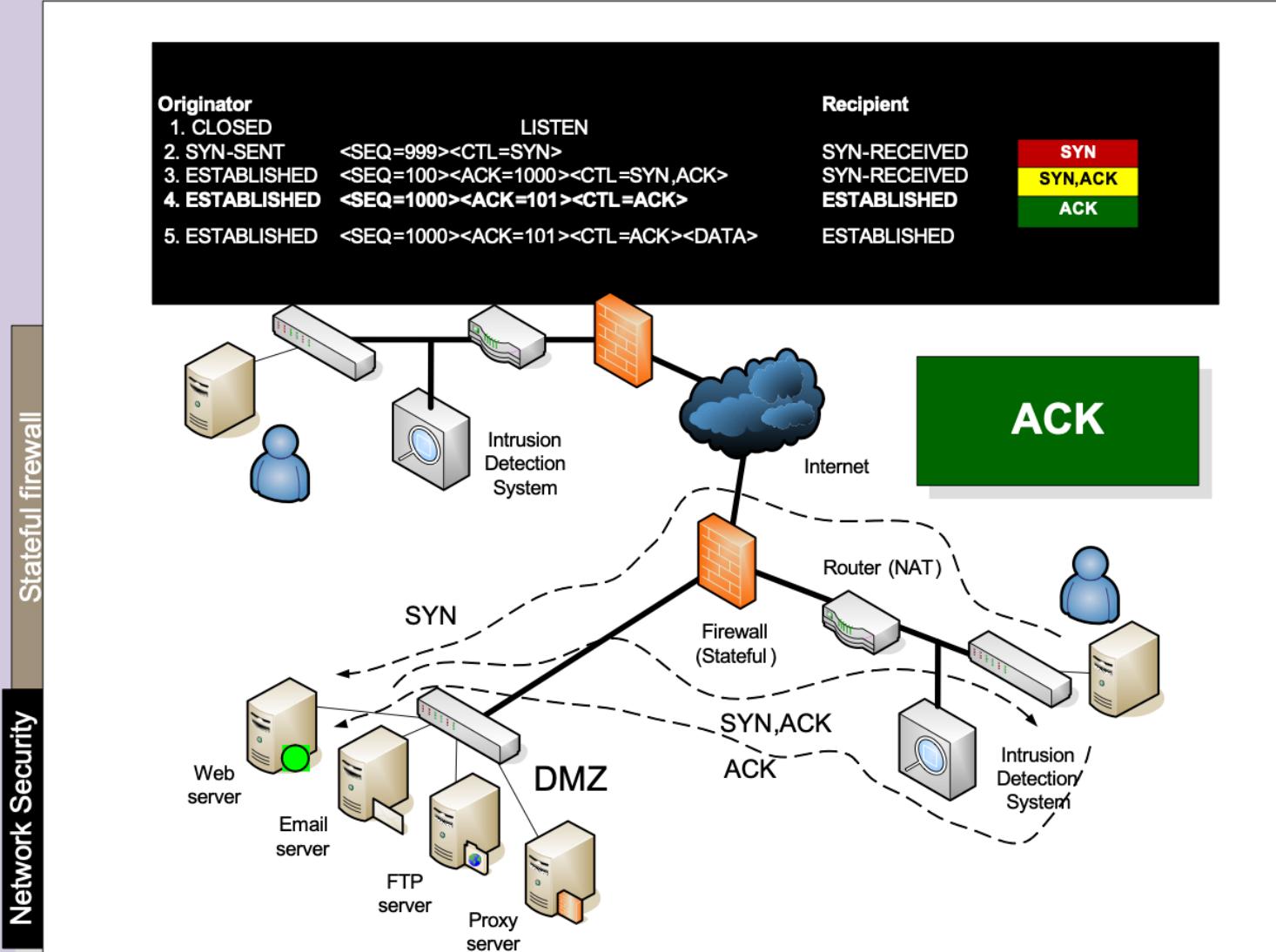
Originator	Recipient
1. CLOSED	LISTEN
2. SYN-SENT <SEQ=999><CTL=SYN>	SYN-RECEIVED
3. ESTABLISHED <SEQ=100><ACK=1000><CTL=SYN,ACK>	SYN-RECEIVED
4. ESTABLISHED <SEQ=1000><ACK=101><CTL=ACK>	ESTABLISHED
5. ESTABLISHED <SEQ=1000><ACK=101><CTL=ACK><DATA>	ESTABLISHED



Network Security

Stateful firewall





68	9.980194	192.168.1.101	resolver2.srv.pol.	DNS	Standard query PTR 255.1.168.192.in-addr.arpa
69	10.005697	resolver2.srv.pol.	192.168.1.101	DNS	Standard query response, No such name
70	14.477532	192.168.1.101	resolver2.srv.pol.	DNS	Standard query A www.napier.ac.uk
71	14.503727	resolver2.srv.pol.	192.168.1.101	DNS	Standard query response A 146.176.1.188
72	14.512705	192.168.1.101	www.napier.ac.uk	TCP	4213 > http [SYN] Seq=0 Ack=0 win=16384 Len=0 MSS=1260
73	14.515118	192.168.1.1	192.168.1.255	SNMP	TRAP-V1 SNMPv2-SMI::enterprises.3955.1.1.0
74	14.553506	www.napier.ac.uk	192.168.1.101	TCP	http > 4213 [SYN, ACK] Seq=0 Ack=1 win=16384 Len=0 MSS=1352
75	14.553533	192.168.1.101	www.napier.ac.uk	TCP	4213 > http [ACK] Seq=1 Ack=1 win=17640 Len=0
76	14.553687	192.168.1.101	www.napier.ac.uk	HTTP	GET / HTTP/1.1

ame 72 (62 bytes on wire, 62 bytes captured)

hernet II, Src: 00:15:00:34:02:f0, Dst: 00:0c:41:f5:23:d5

ternet Protocol, Src Addr: 192.168.1.101 (192.168.1.101), Dst Addr: www.napier.ac.uk (146.176.1.188)

ansmission Control Protocol, Src Port: 4213 (4213), Dst Port: http (80), Seq: 0, Ack: 0, Len: 0

Source port: 4213 (4213)

Destination port: http (80)

Sequence number: 0 (relative sequence number)

Header Length: 28 bytes

Flags: 0x0002 (SYN)

window size: 16384

Checksum: 0x3c0c (correct)

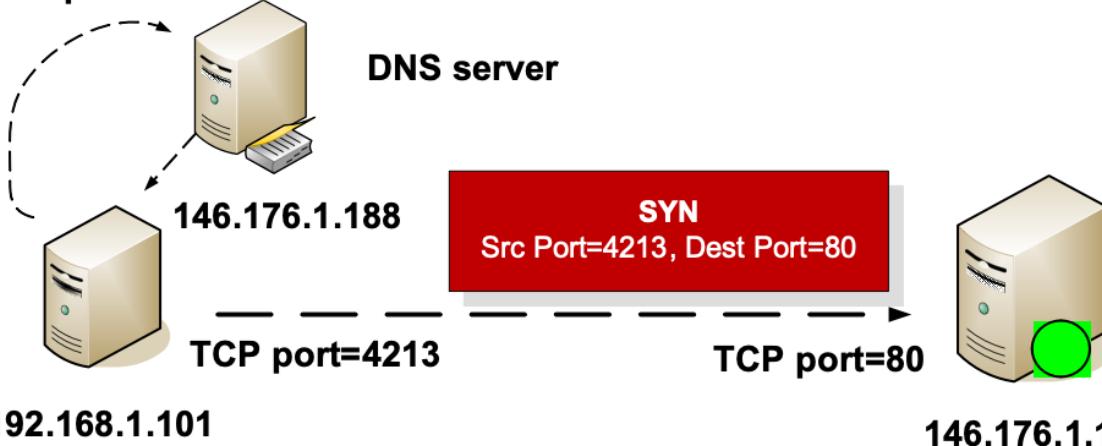
Options: (8 bytes)

SYN

Stateful fire

Network Security

www.napier.ac.uk?



146.176.1.188

192.168.1.101

TCP port=80

TCP port=4213

Client-server (SYN)

Network Security

Stateful firewall

68 9.980194 192.168.1.101 resolver2.srv.pol. DNS Standard query PTR 255.1.168.192.in-addr.arpa
69 10.005697 resolver2.srv.pol. 192.168.1.101 DNS Standard query response, No such name
70 14.477532 192.168.1.101 resolver2.srv.pol. DNS Standard query A www.napier.ac.uk
71 14.503727 resolver2.srv.pol. 192.168.1.101 DNS Standard query response A 146.176.1.188
72 14.512705 192.168.1.101 www.napier.ac.uk TCP 4213 > http [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1260
73 14.515118 192.168.1.1 192.168.1.255 SNMP TRAP-V1 SNMPV2-SMI::enterprises.3955.1.1.0
74 14.553506 www.napier.ac.uk 192.168.1.101 TCP http > 4213 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1352
75 14.553533 192.168.1.101 www.napier.ac.uk TCP 4213 > http [ACK] Seq=1 Ack=1 Win=17640 Len=0
76 14.553687 192.168.1.101 www.napier.ac.uk HTTP GET / HTTP/1.1

Name 74 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: 00:0c:41:f5:23:d5, Dst: 00:15:00:34:02:f0
Internet Protocol, Src Addr: www.napier.ac.uk (146.176.1.188), Dst Addr: 192.168.1.101 (192.168.1.101)
Transmission Control Protocol, Src Port: http (80), Dst Port: 4213 (4213), Seq: 0, Ack: 1, Len: 0
Source port: http (80)
Destination port: 4213 (4213)
Sequence number: 0 (relative sequence number)
Acknowledgement number: 1 (relative ack number)
Header length: 28 bytes
Flags: 0x0012 (SYN, ACK) ← **SYN,ACK**
window size: 16384
checksum: 0xa97c (correct)
options: (8 bytes)
tcpdump -n -v -s 65536 -w -

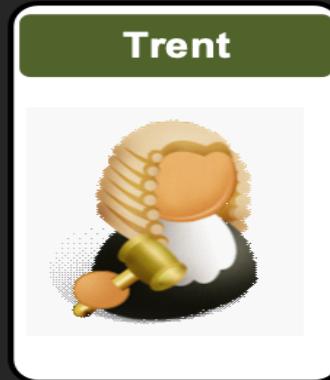
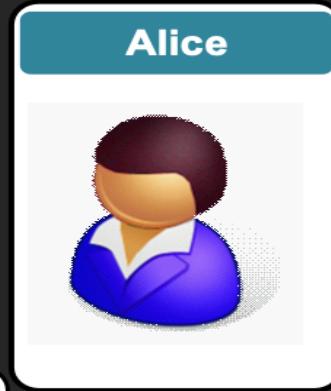
68 9.980194 192.168.1.101 resolver2.srv.pol. DNS Standard query PTR 255.1.168.192.in-addr.arpa
69 10.005697 resolver2.srv.pol. 192.168.1.101 DNS Standard query response, No such name
70 14.477532 192.168.1.101 resolver2.srv.pol. DNS Standard query A www.napier.ac.uk
71 14.503727 resolver2.srv.pol. 192.168.1.101 DNS Standard query response A 146.176.1.188
72 14.512705 192.168.1.101 www.napier.ac.uk TCP 4213 > http [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1260
73 14.515118 192.168.1.1 192.168.1.255 SNMP TRAP-V1 SNMPV2-SMI::enterprises.3955.1.1.0
74 14.553506 www.napier.ac.uk 192.168.1.101 TCP http > 4213 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1352
75 14.553533 192.168.1.101 www.napier.ac.uk TCP 4213 > http [ACK] Seq=1 Ack=1 Win=17640 Len=0
76 14.553687 192.168.1.101 www.napier.ac.uk HTTP GET / HTTP/1.1

Name 75 (54 bytes on wire, 54 bytes captured)
Ethernet II, Src: 00:15:00:34:02:f0, Dst: 00:0c:41:f5:23:d5
Internet Protocol, Src Addr: 192.168.1.101 (192.168.1.101), Dst Addr: www.napier.ac.uk (146.176.1.188)
Transmission Control Protocol, Src Port: 4213 (4213), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0
Source port: 4213 (4213)
Destination port: http (80)
Sequence number: 1 (relative sequence number)
Acknowledgement number: 1 (relative ack number)
Header length: 20 bytes
Flags: 0x0010 (ACK) ← **ACK**
window size: 17640
checksum: 0xd0ec (correct)
[SEQ/ACK analysis]

Advanced Crypto

6. Tunnelling

SSL/TLS



<http://asecuritysite.com/crypto>

Author: Prof Bill Buchanan

HTTP, FTP
Telnet, POP-3
IMAP, SMTP

TCP, UDP, SPX

IP, IPX, ARP,
ICMP

Ethernet,
PPP, HDLC

Cables, Signals

Application

Transport

Network

Data Link

Physical

```
4 0.000602 192.168.75.132      192.168.75.1    TCP      78 http > mgcp-gateway [SYN, ACK] Seq=0 Ack=1 W
5 0.000681 192.168.75.1      192.168.75.132    TCP      66 mgcp-gateway > http [ACK] Seq=1 Ack=1 Win=66
6 0.000835 192.168.75.1      192.168.75.132    HTTP     475 GET / HTTP/1.1
7 0.055477 192.168.75.132    192.168.75.1    TCP      1514 TCP segment of a reassembled PDU

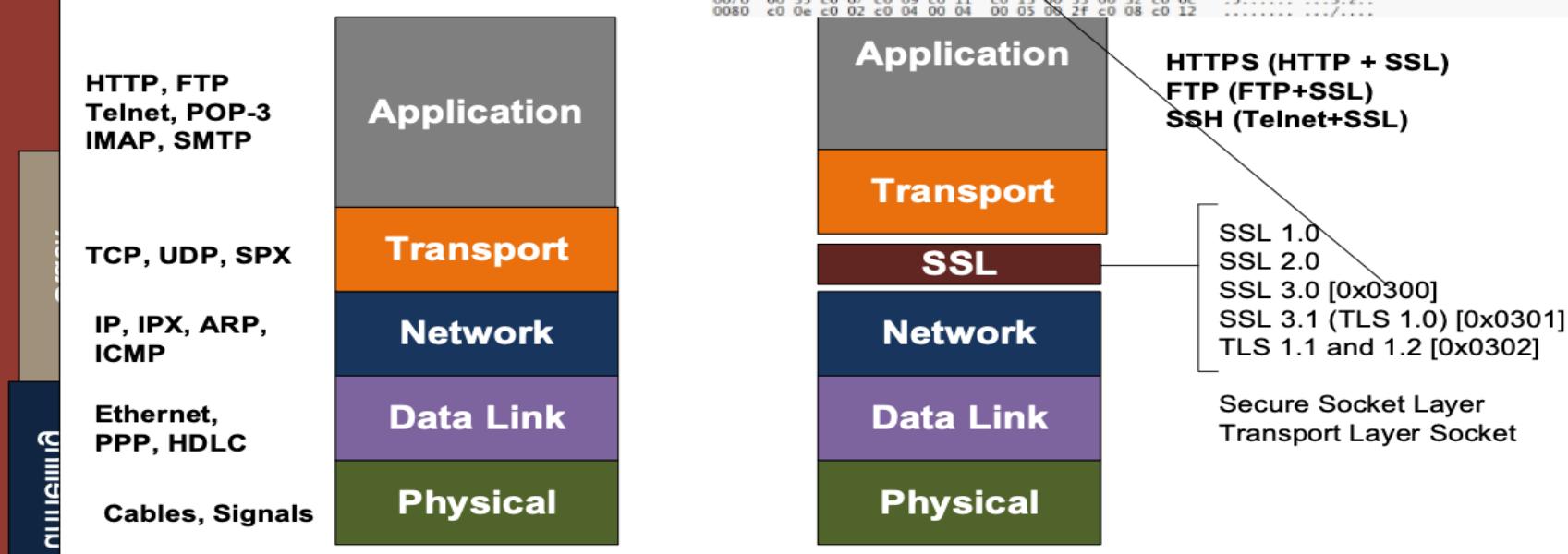
Internet Protocol version 4, src: 192.168.75.1 (192.168.75.1), dst: 192.168.75.132 (192.168.75.132)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: default; ECN: 0x00: Not-ECT (NOT ECN-Capable Transport))
  Total Length: 461
  Identification: 0x011e (286)
  Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 128
  Protocol: TCP (6)
  Header checksum: 0xe036 [validation disabled]
  Source: 192.168.75.1 (192.168.75.1)
  Destination: 192.168.75.132 (192.168.75.132)
  [Source GeoIP: Unknown]
  [Destination GeoIP: unknown]
Transmission Control Protocol, Src Port: mgcp-gateway (2427), Dst Port: http (80), Seq: 1, Ack: 1, Len: 409
  Source port: mgcp-gateway (2427)
  Destination port: http (80)
  [Stream index: 0]
  Sequence number: 1 (relative sequence number)
  [Next sequence number: 410 (relative sequence number)]
  Acknowledgment number: 1 (relative ack number)
  Header length: 32 bytes
  Flags: 0x018 (PSH, ACK)
  window size value: 16652
  [calculated window size: 66608]
  [window size scaling factor: 4]
  Checksum: 0xf834 [validation disabled]
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  [SEQ/ACK analysis]
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
  User-Agent: Opera/9.80 (Windows NT 6.0; U; en) Presto/2.2.15 Version/10.01\r\n
```

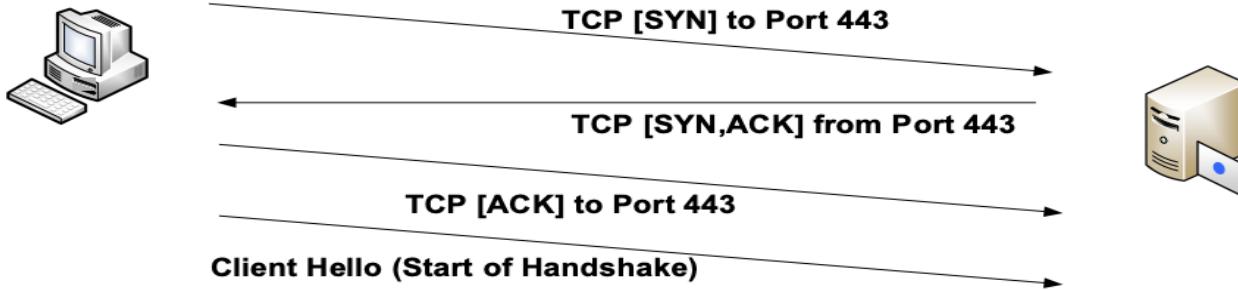
Ports

HTTP	80	HTTPPs	443
TELNET	23	SSH	22
SMTP	25	SMTPs	465
POP-3	110	POP-3s	995

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.20	66.211.169.66	TCP	74	h2250-annex-g > https [SYN] Seq=0 Win=16
2	0.205353	66.211.169.66	192.168.0.20	TCP	58	https > h2250-annex-g [SYN, ACK] Seq=1 Win=16
3	0.205652	192.168.0.20	66.211.169.66	TCP	54	h2250-annex-g > https [ACK] Seq=1 Win=16
4	0.207049	192.168.0.20	66.211.169.66	TLSv1	197	Client Hello
5	0.410585	66.211.169.66	192.168.0.20	TCP	1266	[TCP segment of a reassembled PDU]
6	0.410821	66.211.169.66	192.168.0.20	TCP	1266	[TCP segment of a reassembled PDU]
7	0.411008	192.168.0.20	66.211.169.66	TCP	54	h2250-annex-g > https [ACK] Seq=144 Win=16
8	0.411240	66.211.169.66	192.168.0.20	TLSv1	608	Server Hello, Certificate, Server Hello
9	0.416329	192.168.0.20	66.211.169.66	TLSv1	244	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10	0.615203	66.211.169.66	192.168.0.20	TCP	54	https > h2250-annex-g [ACK] Seq=297 Win=16
11	0.615319	66.211.169.66	192.168.0.20	TLSv1	103	Change Cipher Spec, Encrypted Handshake Message
12	0.616531	192.168.0.20	66.211.169.66	TCP	1266	[TCP segment of a reassembled PDU]
13	0.616544	192.168.0.20	66.211.169.66	TCP	1266	[TCP segment of a reassembled PDU]
14	0.839748	66.211.169.66	192.168.0.20	TCP	54	https > h2250-annex-g [ACK] Seq=303 Win=16
15	0.839934	192.168.0.20	66.211.169.66	TLSv1	483	Application Data
16	1.128526	66.211.169.66	192.168.0.20	TCP	54	https > h2250-annex-g [ACK] Seq=303 Win=16

[window size scaling factor: -2 (no window scaling used)]
 *Checksum: 0x5108 [validation disabled]
 *SEQ/ACK analysis
 *Secure Sockets Layer
 *TLSv1 Record Layer: Handshake Protocol: Client Hello
 Content Type: Handshake (22)
 Version: TLS 1.0 (0x0301)





Wireshark screenshot showing the TLS handshake frames:

Frame 4: 197 bytes on wire (1576 bits), 197 bytes captured (1576 bits)

Ethernet II, Src: IntelCor_4f:30:1d (00:1f:3c:4f:30:1d), Dst: Netgear_b0:d6:8c (00:18:4d:b0:d6:8c)

Internet Protocol version 4, Src: 192.168.0.20 (192.168.0.20), Dst: 66.211.169.66 (66.211.169.66)

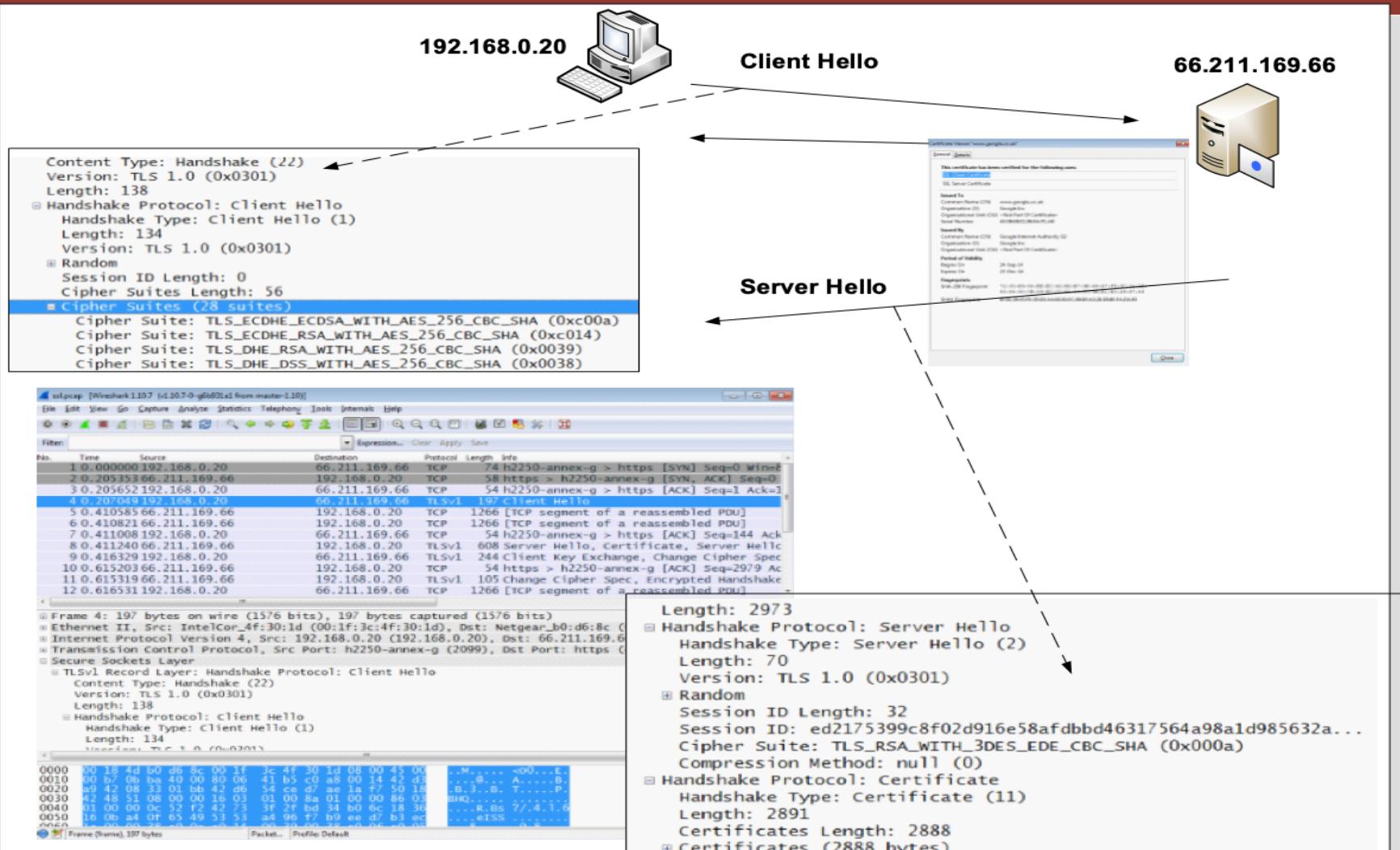
Transmission Control Protocol, Src Port: h2250-annex-g (2099), Dst Port: https (443), Seq: 1, Ack: 1, Len: 1266

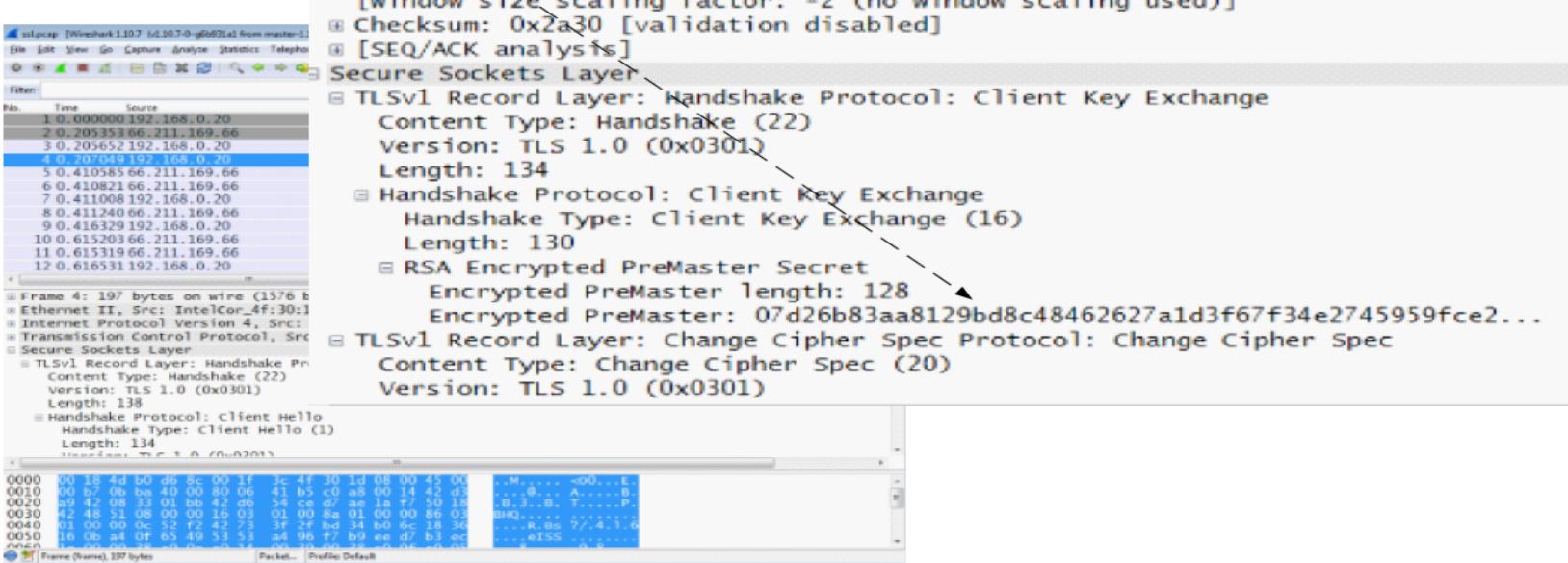
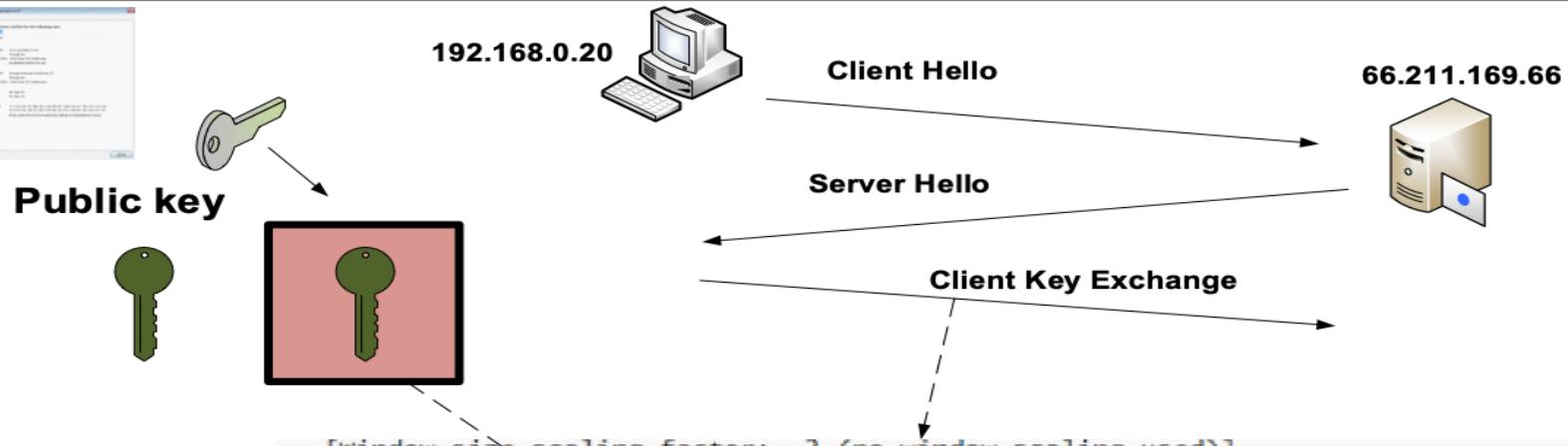
Secure Sockets Layer

- TLSSv1 Record Layer: Handshake Protocol: Client Hello**
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 138
- Handshake Protocol: client Hello**
 - Handshake Type: Client Hello (1)
 - Length: 134

Frame (Frame), 197 bytes

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.20	66.211.169.66	TCP	74	h2250-annex-g > https [SYN] Seq=0 win=8
2	0.205353	66.211.169.66	192.168.0.20	TCP	58	https > h2250-annex-g [SYN, ACK] Seq=0
3	0.205652	192.168.0.20	66.211.169.66	TCP	54	h2250-annex-g > https [ACK] Seq=1 Ack=1
4	0.207049	192.168.0.20	66.211.169.66	TLSSv1	197	client Hello
5	0.410585	66.211.169.66	192.168.0.20	TCP	1266	[TCP segment of a reassembled PDU]
6	0.410821	66.211.169.66	192.168.0.20	TCP	1266	[TCP segment of a reassembled PDU]
7	0.411008	192.168.0.20	66.211.169.66	TCP	54	h2250-annex-g > https [ACK] Seq=144 Ack=144
8	0.411240	66.211.169.66	192.168.0.20	TLSSv1	608	Server Hello, Certificate, Server Hello
9	0.416329	192.168.0.20	66.211.169.66	TLSSv1	244	client Key Exchange, Change Cipher Spec
10	0.615203	66.211.169.66	192.168.0.20	TCP	54	https > h2250-annex-g [ACK] Seq=2979 Ack=2979
11	0.615319	66.211.169.66	192.168.0.20	TLSSv1	105	Change Cipher Spec, Encrypted Handshake
12	0.616531	192.168.0.20	66.211.169.66	TCP	1266	[TCP segment of a reassembled PDU]



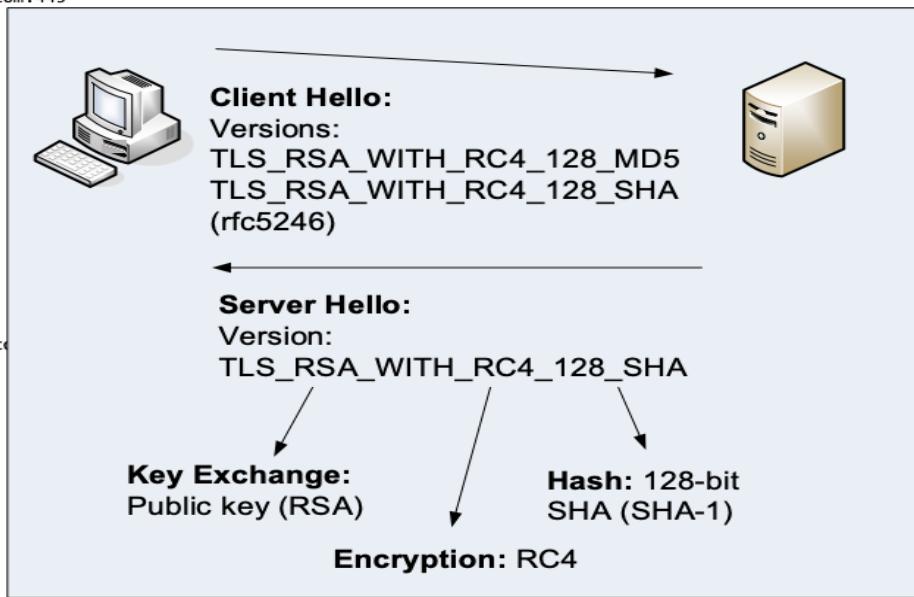


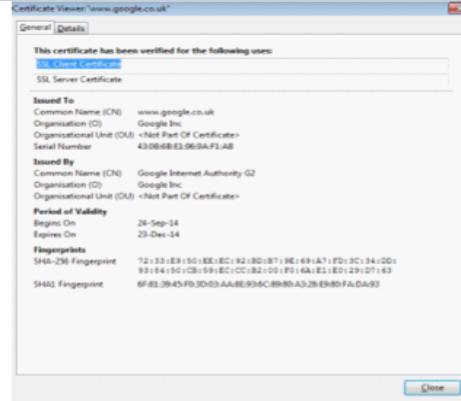
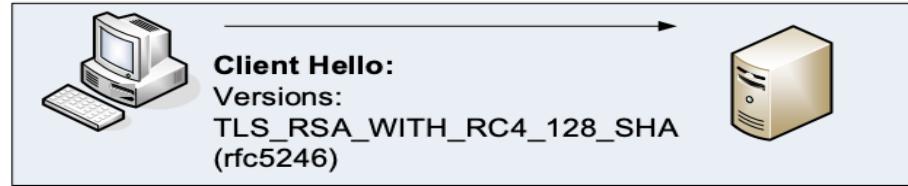
```

billbuchanan@Bill's-MacBook-Pro:~$ openssl s_client -connect www.google.com:443
CONNECTED(00000003)
depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
verify error:num=20:unable to get local issuer certificate
verify return:0
---
Certificate chain
 0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=www.google.com
   i:/C=US/O=Google Inc/CN=Google Internet Authority G2
 1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
   i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
 2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
   i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIEjdCCA16gAwIBAgIISvYJLWn+akUwDQYJKoZIhvcNAQEFBQAwSTELMAkG
-----END CERTIFICATE-----
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=www.google.com
issuer=/C=US/O=Google Inc/CN=Google Internet Authority G2
---
No client certificate CA names sent
---
SSL handshake has read 3719 bytes and written 446 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
  Protocol : TLSv1.2
  Cipher   : ECDHE-RSA-AES128-GCM-SHA256
  Session-ID: 9d92cec32fa9f86c6d902081ee186c4fc68234fff7b903d6621a86c98092bd51
  Session-ID-Ctx:
  Master-Key:
B8A14DB1D3021E80B53F30EA94D2EEA155A995B926879B08E3D971EB16873D16F62929899E2FA368D374716DB14A412
B
  Key-Ag... : None
  PSK ident...: None
  PSK ident... hint: None
  SRP userna...: None
  TLS session ticket lifetime hint: 100800 (seconds)
  TLS session ticket:
  0000 - fa 8d cb 50 53 3d 99 c8-b4 11 20 0c ca 53 e9 bd ...PS=.... .S...
  0010 - f8 8e 15 14 ec 82 c1 56-ab d9 9b 36 c2 56 b0 db .....V....6.V..
  0020 - 2b d4 07 56 a5 02 ac 1f-34 fa 72 21 fd 7c ba 97 +..V....4.r!..|..
  0030 - 2a ae e9 20 04 ef 8a e5-a0 57 28 3a c7 67 04 ac *.. ....W(.:g..
  0040 - 7d 14 bf b0 6d 96 9f cb-eb 0c 0a 40 07 5f a6 84 }....m.....@.|.
  0050 - e2 3b 98 0b e7 f4 b1 e1-04 be 15 6b 36 a5 57 b3 ;.....k6.w.
  0060 - 11 98 f2 f4 20 fe b5 7f-6b 10 4e 7a f9 b5 6d 02 .....k.NZ..m.
  0070 - 30 ec 07 e6 f0 c0 49 81-31 6b 30 f9 b0 d3 c4 25 0.....I.1k0....%
  0080 - 62 f3 92 33 e8 25 cc 22-32 84 54 e6 0e 76 b1 45 b..3%."2.T..v.E
  0090 - 3a 60 83 cf 1b b0 97 7d-05 03 47 20 29 12 d9 8d :.....}.G )...
  00a0 - 6f 5a b4 f2 oZ..

Start Time: 1413136351
Timeout   : 300 (sec)
Verify return code: 20 (unable to get local issuer certificate)

```





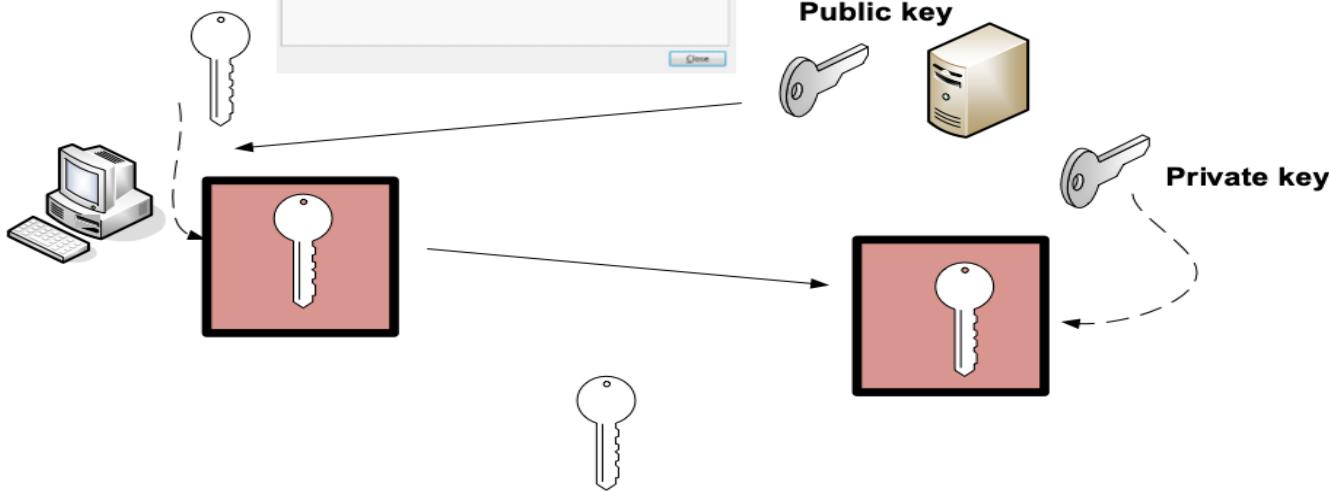
Server Hello:
Version:
TLS_RSA_WITH_RC4_128_SHA

Key Exchange:
Public key (RSA)

Hash: 128-bit SHA (SHA-1)

Encryption: RC4

Session key



Tunnel created (RC4, Hash: SHA-1)

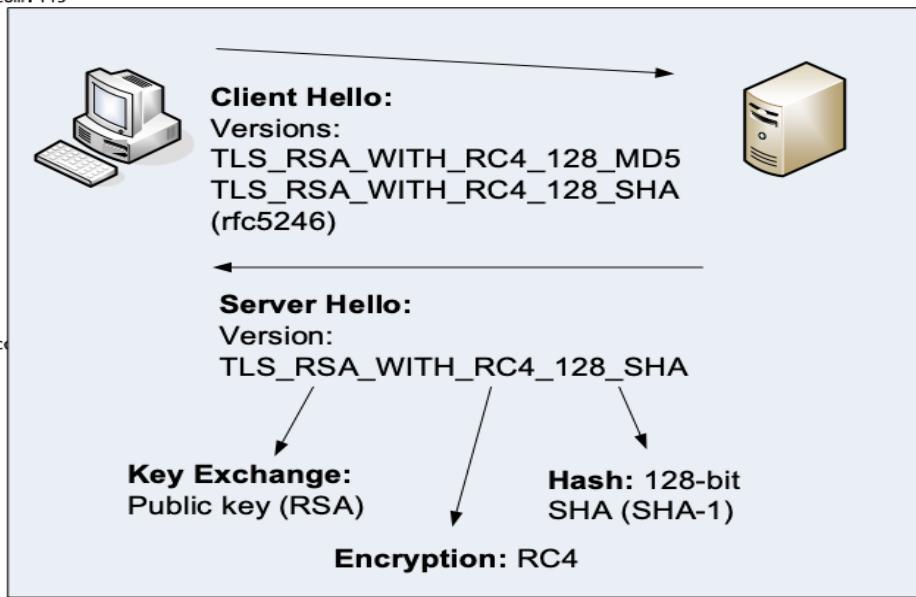
Author: Prof Bill Buchanan

```

billbuchanan@Bill's-MacBook-Pro:~$ openssl s_client -connect www.google.com:443
CONNECTED(00000003)
depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
verify error:num=20:unable to get local issuer certificate
verify return:0
---
Certificate chain
 0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=www.google.com
   i:/C=US/O=Google Inc/CN=Google Internet Authority G2
 1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
   i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
 2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
   i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIEjdCCAl6gAwIBAgIISvYJkOZIhvcNAQEFBQAwSTELMAkGALUE
...
Sox4i5L0D0jZYqKfuUimgCfwdIETq0EpCmkhJfgNHjVdzC/h/T61TmaY
-----END CERTIFICATE-----
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=www.google.com
issuer=/C=US/O=Google Inc/CN=Google Internet Authority G2
...
No client certificate CA names sent
...
SSL handshake has read 3719 bytes and written 446 bytes
...
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
  Protocol : TLSv1.2
  Cipher   : ECDHE-RSA-AES128-GCM-SHA256
  Session-ID: 9D92CEC32FA9F86C6D902081EE186C4FC68234FFF7B903D6621A86C98092BD51
  Session-ID-CTX:
  Master-Key:
B8A14DB1D3021E80B53F30EA94D2EEA155A995B926879B08E3D971EB16873D16F62929899E2FA368D374716DB14A412
B
  Key-Ag... : None
  PSK ident...: None
  PSK ident... hint: None
  SRP userna...: None
  TLS session ticket lifetime hint: 100800 (seconds)
  TLS session ticket:
  0000 - fa 8d cb 50 53 3d 99 c8-b4 11 20 0c ca 53 e9 bd ...PS=.... .S..
  0010 - f8 8e 15 14 ec 82 c1 56-ab d9 9b 36 c2 56 b0 db .....V....6.V..
  0020 - 2b d4 07 56 a5 02 ac 1f-34 fa 72 21 fd 7c ba 97 +..V....4.r!.|..
  0030 - 2a ae e9 20 04 ef 8a e5-a0 57 28 3a c7 67 04 ac *.. ....W(:.g..
  0040 - 7d 14 bf b0 6d 96 9f cb-eb 0c 0a 40 07 5f a6 84 }....m.....@._..
  0050 - e2 3b 98 0b e7 f4 b1 e1-04 be 15 6b 36 a5 57 b3 .;.....k6.w.
  0060 - 11 98 f2 f4 20 fe b5 7f-6b 10 4e 7a f9 b5 6d 02 .....k.Nz..m.
  0070 - 30 ec 07 e6 f0 c0 49 81-31 6b 30 f9 b0 d3 c4 25 0.....I.1k0....%
  0080 - 62 f3 92 33 e8 25 cc 22-32 84 54 e6 0e 76 b1 45 b..3%."2.T..v.E
  0090 - 3a 60 83 cf 1b b0 97 7d-05 03 47 20 29 12 d9 8d : .....}.G )...
  00a0 - 6f 5a b4 f2 oZ..

Start Time: 1413136351
Timeout   : 300 (sec)
Verify return code: 20 (unable to get local issuer certificate)

```

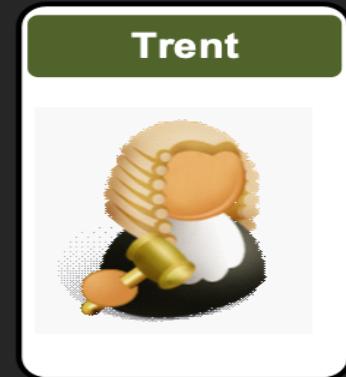
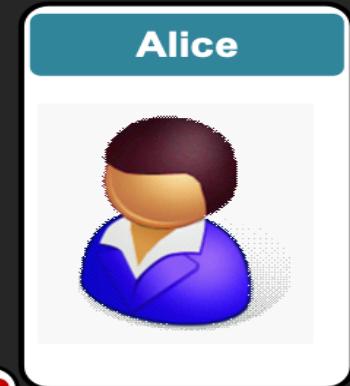


TLS_RSA_WITH_AES_256_CBC_SHA256
Key: RSA Enc: AES_256_CBC Hash: SHA256
TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA
Key ex: DH_DSS Enc: 3DES_EDE_CBC Hash: SHA

Advanced Crypto

6. Tunnelling

Heartbleed



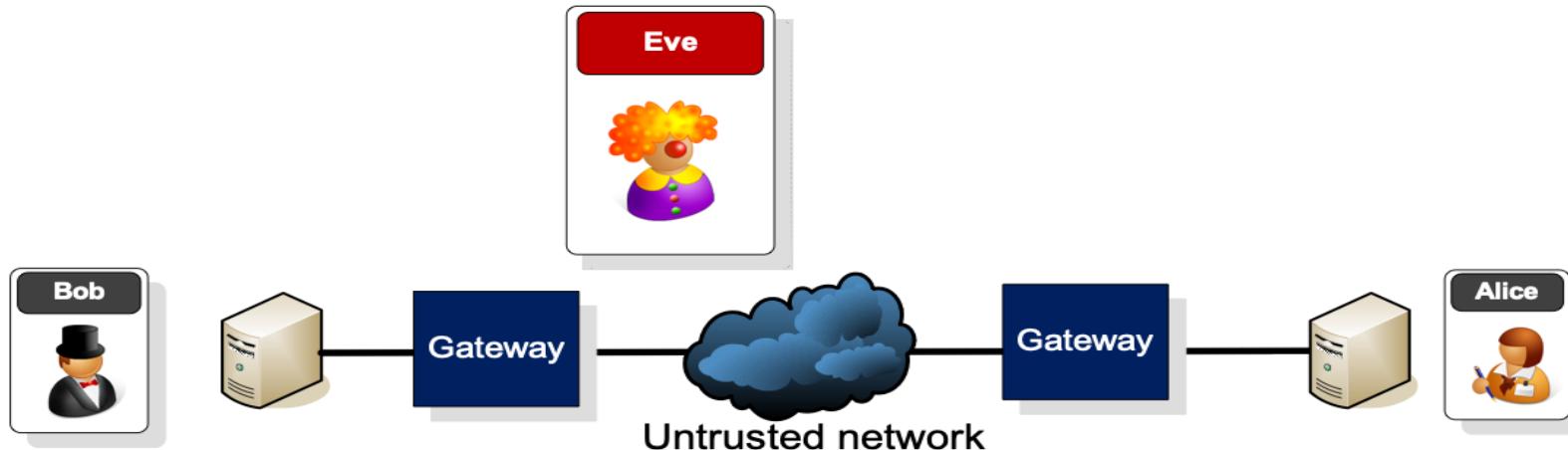
<http://asecuritysite.com/crypto>

Author: Prof Bill Buchanan

Network Security



VPNs



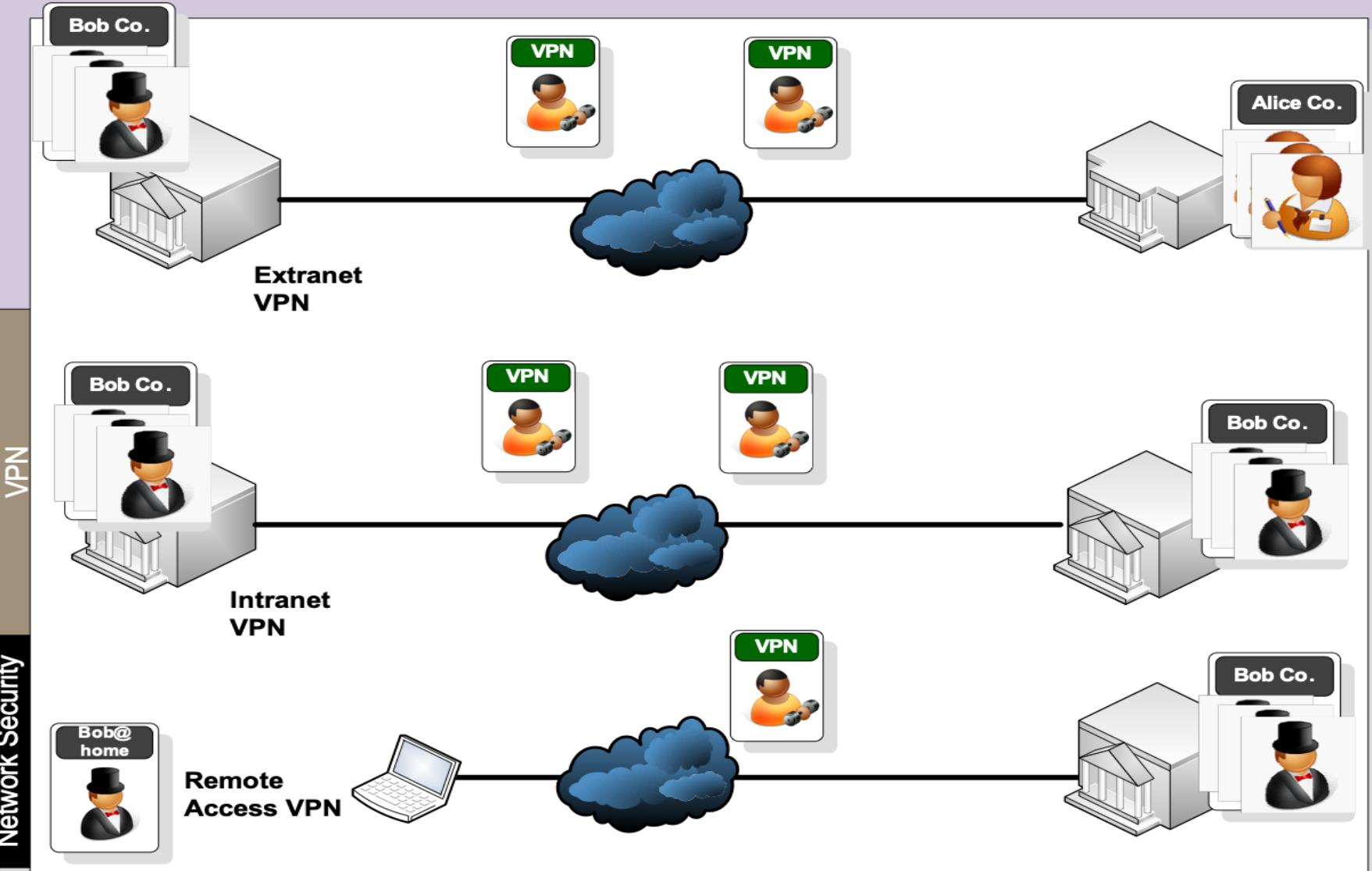
What is required is:

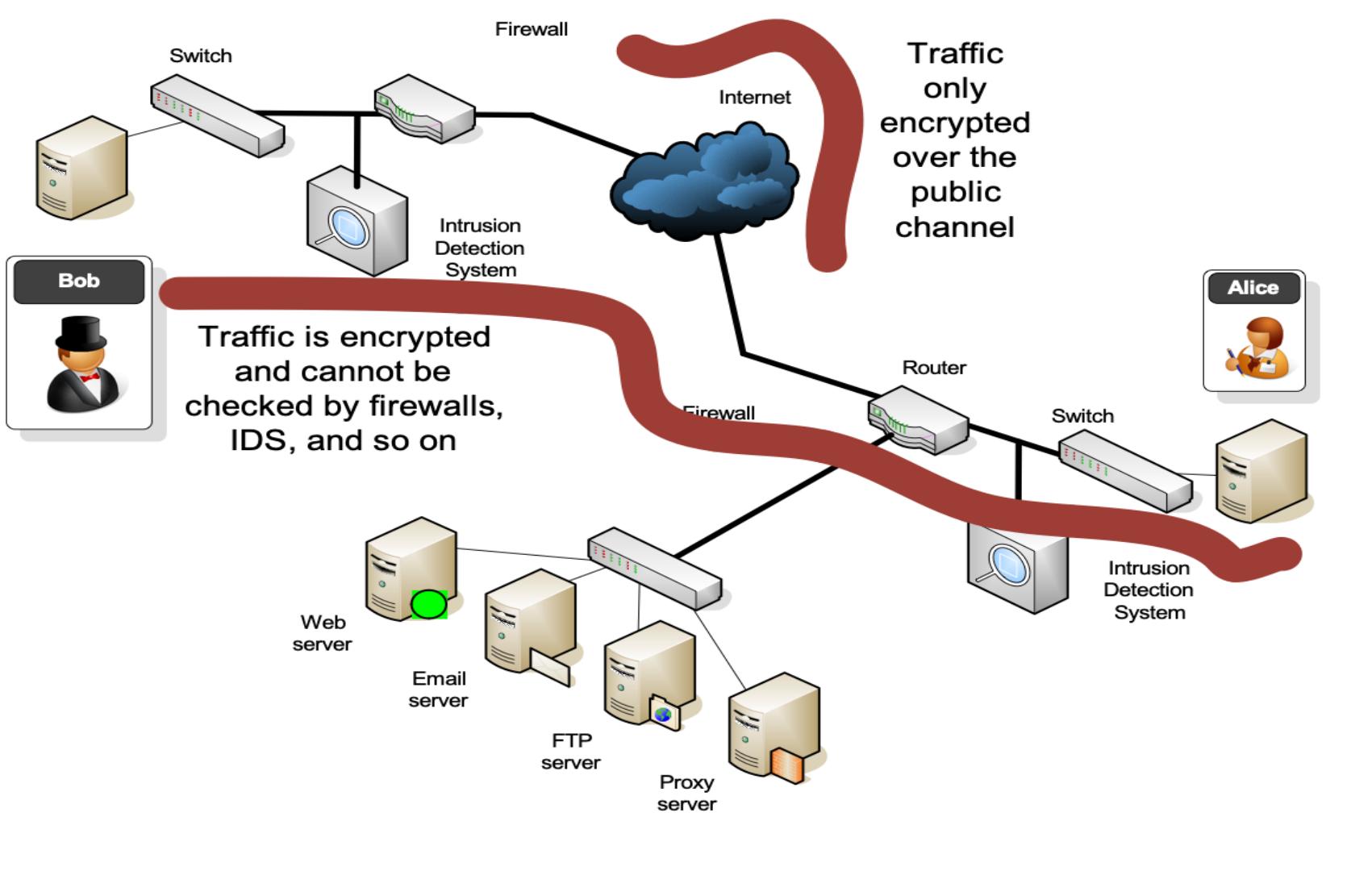
- Encryption.
- Authentication of devices (to overcome spoofing)
- Authentication of packets (for integrity)

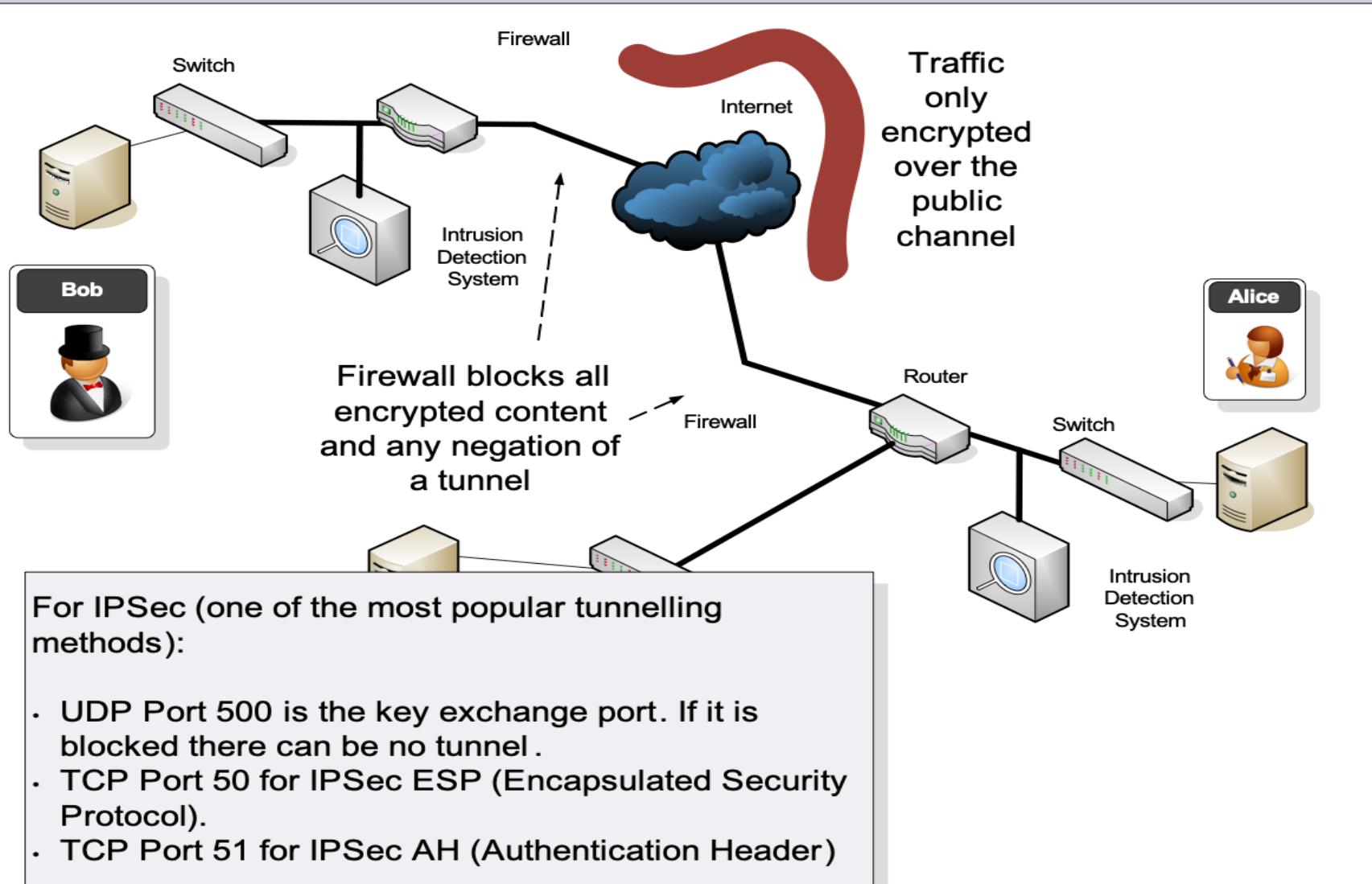
PPTP (Point-to-point Tunneling Protocol). Created by Microsoft and is routable. It uses MPPE (Microsoft Point-to-point Encryption) and user authentication.

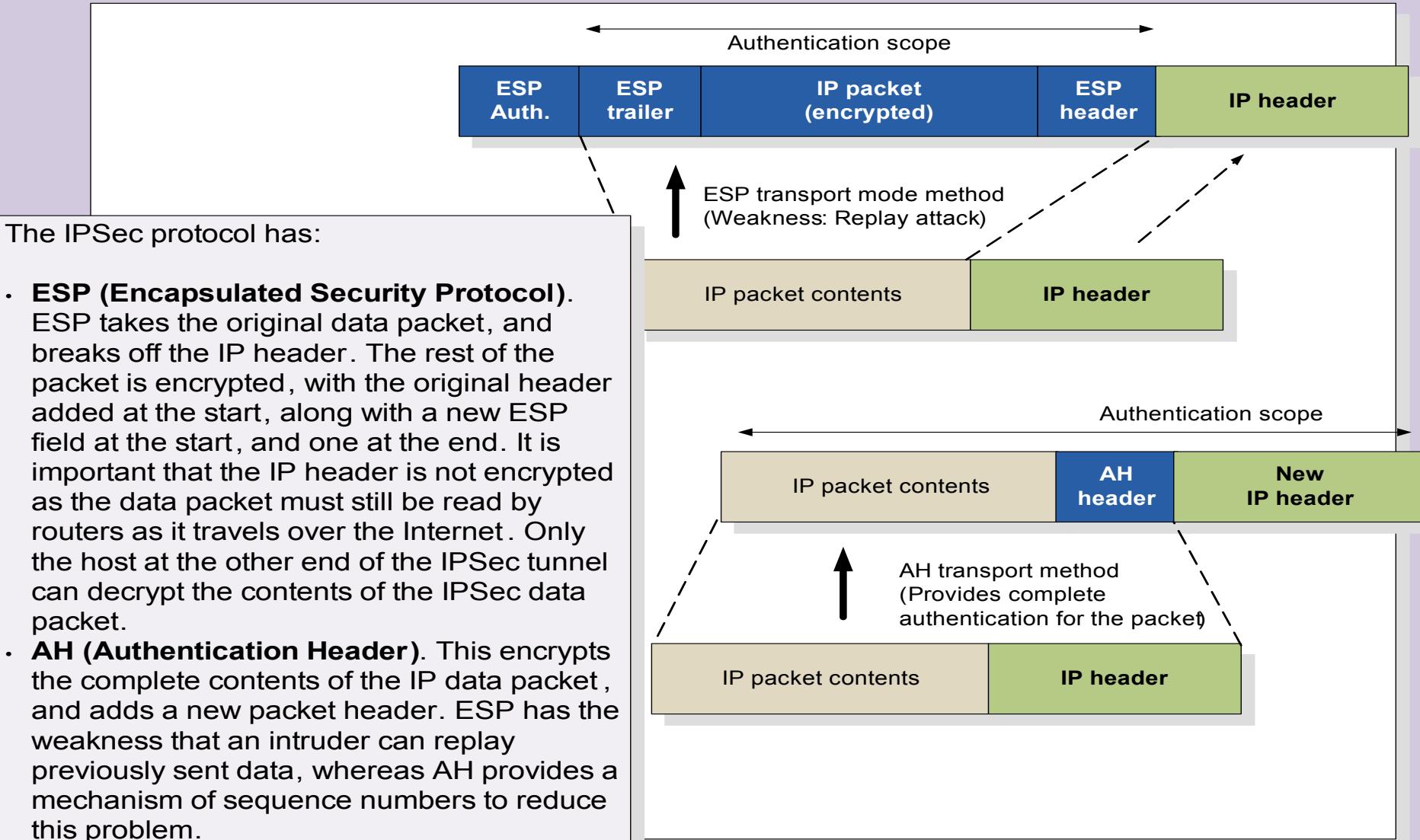
L2TP (Layer 2 Tunneling Protocol). Works at Layer 2 to Forward IP, IPX and AppleTalk (RFC2661). Cisco, Microsoft, Ascent and 3Com developed it. User and machine authentication, but no encryption (but can be used with L2TP over IPSec).

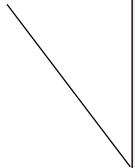
IPSec. An open standard. Includes both encryption and Authentication.

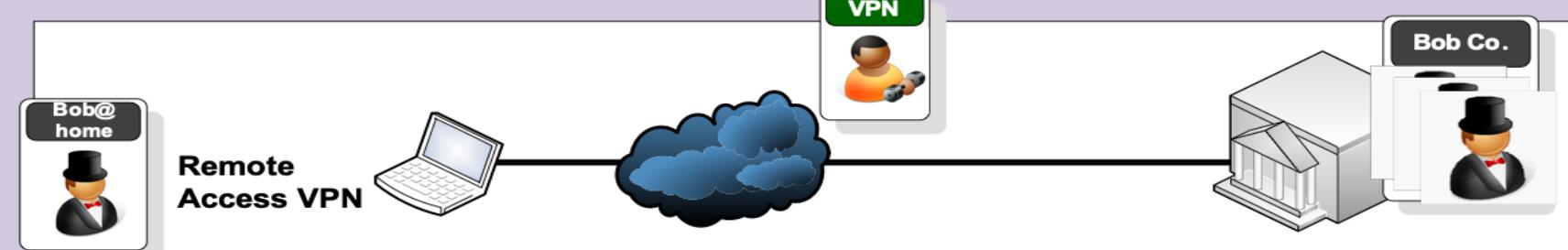








- 
- 1 ICMP Internet Control Message [RFC792]
 - 6 TCP Transmission Control [RFC793]
 - 8 EGP Exterior Gateway Protocol [RFC888]
 - 9 IGP any private interior gateway [IANA]
 - 47 GRE General Routing Encapsulation (PPTP)**
 - 50 ESP Encap Security Payload [RFC2406]**
 - 51 AH Authentication Header [RFC2402]**
 - 55 MOBILE IP Mobility
 - 88 EIGRP EIGRP [CISCO]
 - 89 OSPFIGP OSPFIGP [RFC1583]
 - 115 L2TP Layer Two Tunneling Protocol**



Phase 1 (IKE – Internet Key Exchange)

UDP port 500 is used for IKE

Define the policies between the peers

IKE Policies

- Hashing algorithm (SHA/MD5)
- Encryption (DES/3DES)
- Diffie-Hellman agreements
- Authentication (pre-share, RSA nonces, RSA sig).

```
isakmp enable outside
isakmp key ABC&FDD address 176.16.0.2 netmask
255.255.255.255
isakmp identity address
isakmp policy 5 authen pre-share
isakmp policy 5 encrypt des
isakmp policy 5 hash sha
isakmp policy 5 group 1
isakmp policy 5 lifetime 86400
sysopt connection permitipsec
```

Phase 2

Defines the policies for transform sets, peer IP addresses/hostnames and lifetime settings.

Crypto maps are exchanged

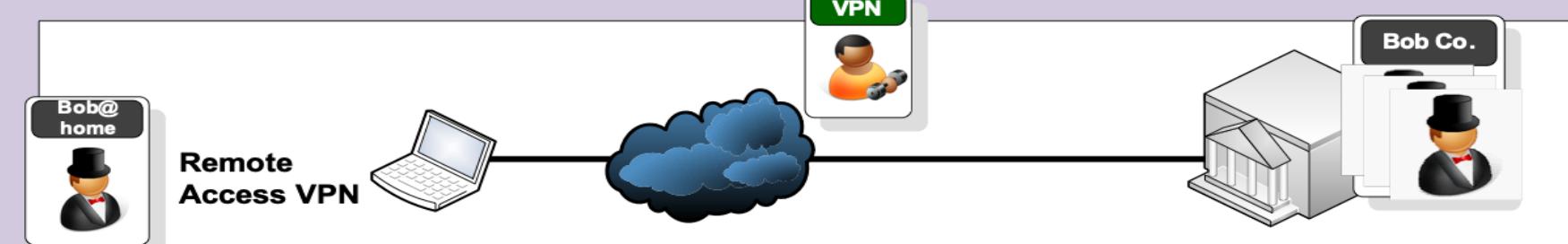
- AH, ESP (or both)
- Encryption (DES, 3DES)
- ESP (tunnel or transport)
- Authentication (SHA/MD5)
- SA lifetimes defined
- Define the traffic of interest

```
crypto ipsec transformset MYIPSECFORMAT espdes esp-sha-hmac
crypto map MYIPSEC10 ipsec-isakmp
access-list 111 permit ip 10.0.0.0 255.255.255.0 176.16.0.0
255.255.255.0
crypto map MYIPSEC10 match address 111
crypto map MYIPSEC10 set peer 176.16.0.2
crypto map MYIPSEC10 set transform-set MYIPSECFORMAT
crypto map MYIPSEC interface outside
```

10.0.0.1

No.	Time	Source	Destination	Protocol Info
81	5.237402	192.168.0.3	146.176.210.2	ISAKMP Aggressive

Frame 81 (918 bytes on wire, 918 bytes captured)
Ethernet II, Src: IntelCor_34:02:f0 (00:15:20:34:62:f0), Dst: Netgear_b0:d6:8c (00:18:4d:b0:d6:8c)
Internet Protocol, Src: 192.168.0.3 (192.168.0.3), Dst: 146.176.210.2 (146.176.210.2)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Source port: isakmp (500)
Destination port isakmp (500)
Length: 884
Checksum: 0xd89d [correct]
Internet Security Association and Key Management Protocol
Initiator cookie 5ABABE2D49A2D42A
Responder cookie 0000000000000000
Next payload: Security Association(1)
Version: 1.0
Exchange type: Aggressive (4)
Flags: 0x00
Message ID: 0x00000000
Length: 860
Security Association payload
Next payload: Key Exchange (4)
Payload length: 556
Domain of interpretation IPSEC (1)
Situation: IDENTITY (1)
Proposal payload# 1
Next payload: NONE (0)
Payload length: 544
Proposal number: 1
Protocol ID: ISAKMP (1)
SPI Size: 0
Proposal transforms 14
Transform payload# 1
Next payload: Transform (3)
Payload length: 40
Transform number: 1
Transform ID: KEY_IKE (1)
Encryption-Algorithm (1): AES-CBC (7)
Hash-Algorithm (2): SHA (2)
Group-Description (4): Alternate 1024-bit MODP group (2)
Authentication-Method (3): XAUTHInitPreshared (65001)
Life-Type (11): Seconds (1)
Life-Duration (12): Duration-value (2147483)
Key-Length (14): Key-Length (256)



VPN

```
C:\>route print
=====
Interface List
 10 ...00 1d 09 3f 49 8d ..... Broadcom NetLink (TM) Fast Ethernet
  7 ...00 1f 3c 4f 30 1d ..... Intel(R) PRO/Wireless 3945ABG Network Connection

 1 ..... Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination      Netmask        Gateway        Interface Metric
          0.0.0.0      0.0.0.0    192.168.0.1  192.168.0.3    25
          127.0.0.0    255.0.0.0   On-link        127.0.0.1    306
          127.0.0.1    255.255.255.255  On-link        127.0.0.1    306
 127.255.255.255  255.255.255.255  On-link        127.0.0.1    306
          192.168.0.0  255.255.255.0   On-link        192.168.0.3    281
          192.168.0.3  255.255.255.255  On-link        192.168.0.3    281
          192.168.0.255 255.255.255.255  On-link        192.168.0.3    281
          224.0.0.0      240.0.0.0   On-link        127.0.0.1    306
          224.0.0.0      240.0.0.0   On-link        192.168.0.3    281
 255.255.255.255  255.255.255.255  On-link        127.0.0.1    306
 255.255.255.255  255.255.255.255  On-link        192.168.0.3    281
=====

Persistent Routes:
 None
```

Network Security

Network Security

Bob@home

VPN Client - Version 5.0.0.1.0560

Connection Entries Status Certificates Log Options Help

Connect New Import Modify Delete

Connection Entries Certificates Log

Connection Entry	Host	Transport
Napier VPN Windows 2000 and XP	146.176.210.2	IPSec/UDP
Napier VPN Windows Vista with Zone Alarm PRO	146.176.210.2	IPSec/UDP
Napier VPN Windows Vista with Zone Alarm PRO	146.176.210.2	IPSec/UDP

Not connected.

C:\>route print

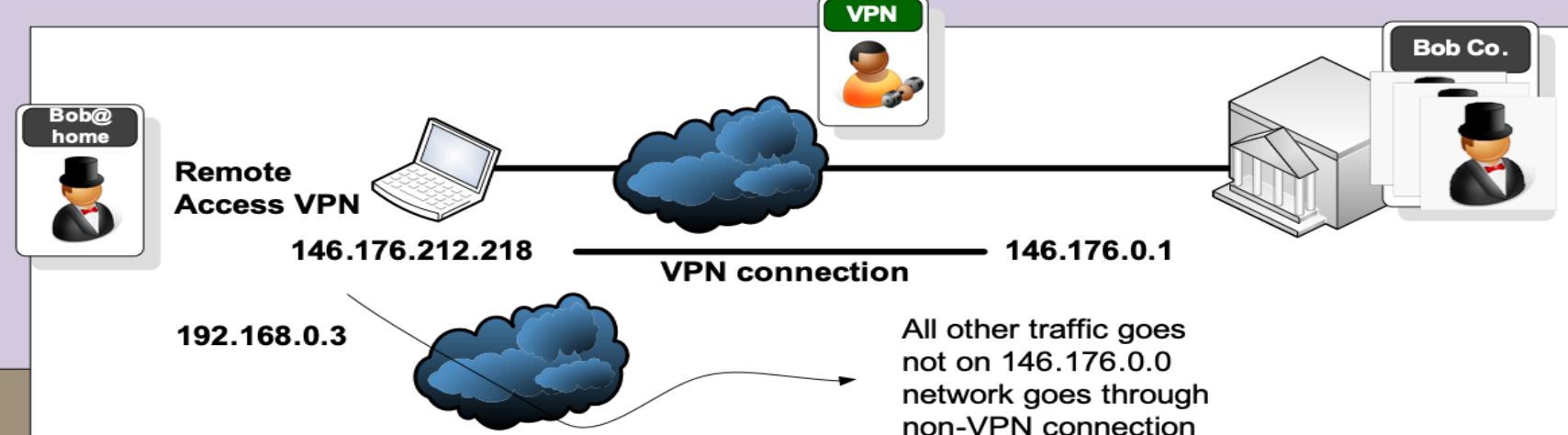
```
=====
Interface List
21 ...00 05 9a 3c 78 00 .... Cisco Systems VPN Adapter
10 ...00 1d 09 3f 49 8d .... Broadcom NetLink (TM) Fast Ethernet
 7 ...00 1f 3c 4f 30 1d .... Intel(R) PRO/Wireless 3945ABG Network Connectio
 1 ..... Software Loopback Interface 1
=====
```

IPv4 Route Table

```
=====
Active Routes:
Network Destination      Netmask          Gateway        Interface Metric
          0.0.0.0        0.0.0.0    192.168.0.1    192.168.0.3    25
         127.0.0.0    255.0.0.0    On-link        127.0.0.1    306
         127.0.0.1  255.255.255.255    On-link        127.0.0.1    306
127.255.255.255  255.255.255.255    On-link        127.0.0.1    306
         146.176.0.0    255.255.0.0    On-link    146.176.212.218    281
         146.176.1.0    255.255.255.0  146.176.0.1    146.176.212.218    100
         146.176.2.0    255.255.255.0  146.176.0.1    146.176.212.218    100
...
         146.176.210.2  255.255.255.255  192.168.0.1    192.168.0.3    100
         146.176.211.0  255.255.255.0  146.176.0.1    146.176.212.218    100
146.176.212.218  255.255.255.255    On-link    146.176.212.218    281
...
         255.255.255.255  255.255.255.255    On-link        127.0.0.1    306
         255.255.255.255  255.255.255.255    On-link    192.168.0.3    281
         255.255.255.255  255.255.255.255    On-link    146.176.212.218    281
=====
```

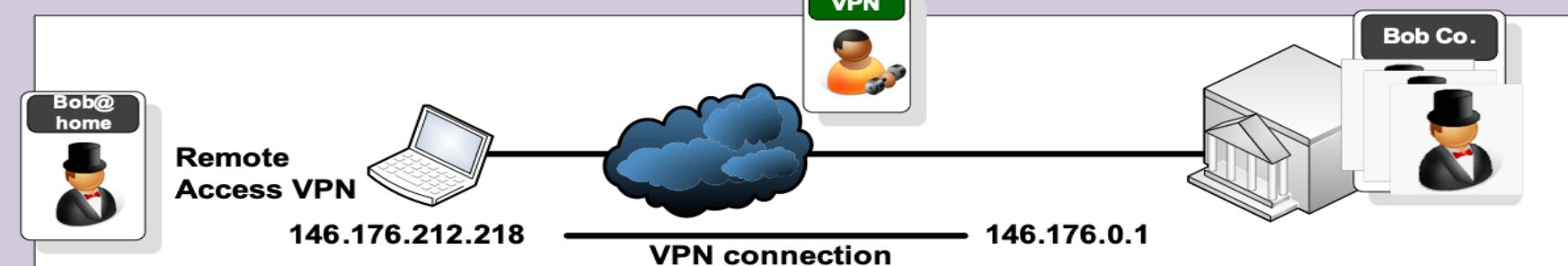
Persist

After connecting to the VPN



```
=====
Interface List
21 ...00 05 9a 3c 78 00 ..... Cisco Systems VPN Adapter
10 ...00 1d 09 3f 49 8d ..... Broadcom NetLink (TM) Fast Ethernet
 7 ...00 1f 3c 4f 30 1d ..... Intel(R) PRO/Wireless 3945ABG Network Connectio
 1 ..... Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination      Netmask          Gateway        Interface Metric
          0.0.0.0        0.0.0.0    192.168.0.1    192.168.0.3    25
          127.0.0.0     255.0.0.0   on-link        127.0.0.1    306
          127.0.0.1     255.255.255.255  on-link        127.0.0.1    306
        127.255.255.255  255.255.255.255  on-link        127.0.0.1    306
          146.176.0.0     255.255.0.0   on-link    146.176.212.218    281
          146.176.1.0     255.255.255.0  146.176.0.1    146.176.212.218    100
          146.176.2.0     255.255.255.0  146.176.0.1    146.176.212.218    100
...
=====
```



```
C:\>tracert www.napier.ac.uk
```

Tracing route to www.napier.ac.uk [146.176.222.174]
over a maximum of 30 hops:

```
1      2 ms      2 ms      6 ms  192.168.0.1  
2      36 ms     38 ms     38 ms  cr0.escra.uk.easynet.net [87.87.249.224]  
3      31 ms     31 ms     30 ms  ip-87-87-146-129.easynet.co.uk [87.87.146.129]  
4      43 ms     43 ms     43 ms  be2.er10.thlon.ov.easynet.net [195.66.224.43]  
5      48 ms     45 ms     45 ms  linx-gw1.ja.net [195.66.224.15]  
6      45 ms     44 ms     45 ms  so-0-1-0.lond-sbr4.ja.net [146.97.35.129]  
7      49 ms     79 ms     49 ms  so-2-1-0.leed-sbr1.ja.net [146.97.33.29]  
8      58 ms     56 ms     56 ms  EastMAN-E1.site.ja.net [146.97.42.46]  
9      59 ms     57 ms     57 ms  vlan16.s-pop2.eastman.net.uk [194.81.56.66]  
10     57 ms     59 ms     58 ms  gi0-1.napier-pop.eastman.net.uk [194.81.56.46]  
11
```

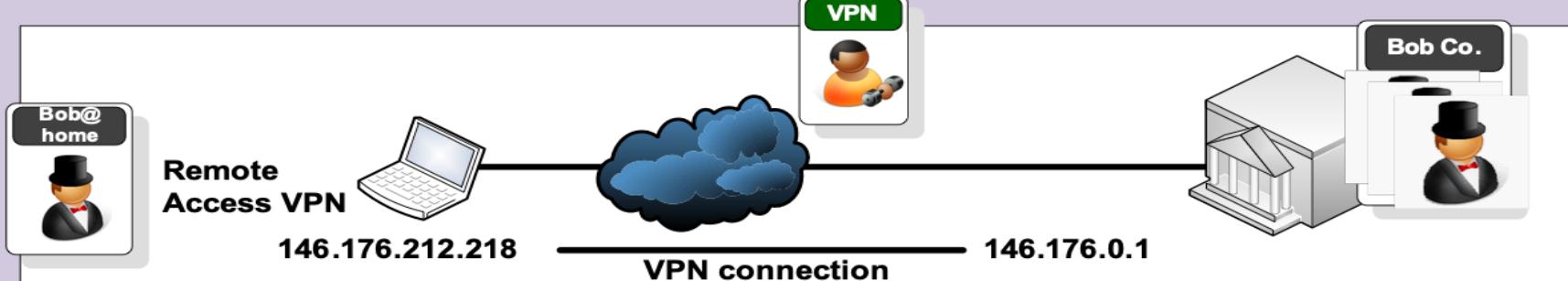
Before VPN connection

```
C:\>tracert www.napier.ac.uk
```

Tracing route to www.napier.ac.uk [146.176.222.174]
over a maximum of 30 hops:

```
1      57 ms     58 ms     57 ms  146.176.210.2  
2      58 ms     56 ms     57 ms  www.napier.ac.uk [146.176.222.174]  
3      58 ms     59 ms     56 ms  www.napier.ac.uk [146.176.222.174]
```

After VPN connection



```
C:\>tracert www.intel.com
```

Tracing route to a961.g.akamai.net [90.223.246.33]
over a maximum of 30 hops:

1	3 ms	1 ms	1 ms	192.168.0.1
2	35 ms	43 ms	36 ms	cr0.escra.uk.easynet.net [87.87.249.224]
3	32 ms	31 ms	32 ms	ip-87-87-146-129.easynet.co.uk [87.87.146.129]
4	46 ms	45 ms	45 ms	te7-0-0.sr0.enlcs.ov.easynet.net [89.200.132.109]
5	46 ms	47 ms	47 ms	5adff621.bb.sky.com [90.223.246.33]

Before VPN connection

```
C:\>tracert www.intel.com
```

Tracing route to a961.g.akamai.net [90.223.246.33]
over a maximum of 30 hops:

1	3 ms	1 ms	1 ms	192.168.0.1
2	35 ms	43 ms	36 ms	cr0.escra.uk.easynet.net [87.87.249.224]
3	32 ms	31 ms	32 ms	ip-87-87-146-129.easynet.co.uk [87.87.146.129]
4	46 ms	45 ms	45 ms	te7-0-0.sr0.enlcs.ov.easynet.net [89.200.132.109]
5	46 ms	47 ms	47 ms	5adff621.bb.sky.com [90.223.246.33]

After VPN connection

Advanced Crypto

6. Tunnelling

Introduction

<http://asecuritysite.com/crypto>

Author: Prof Bill Buchanan

