

Tunnelling

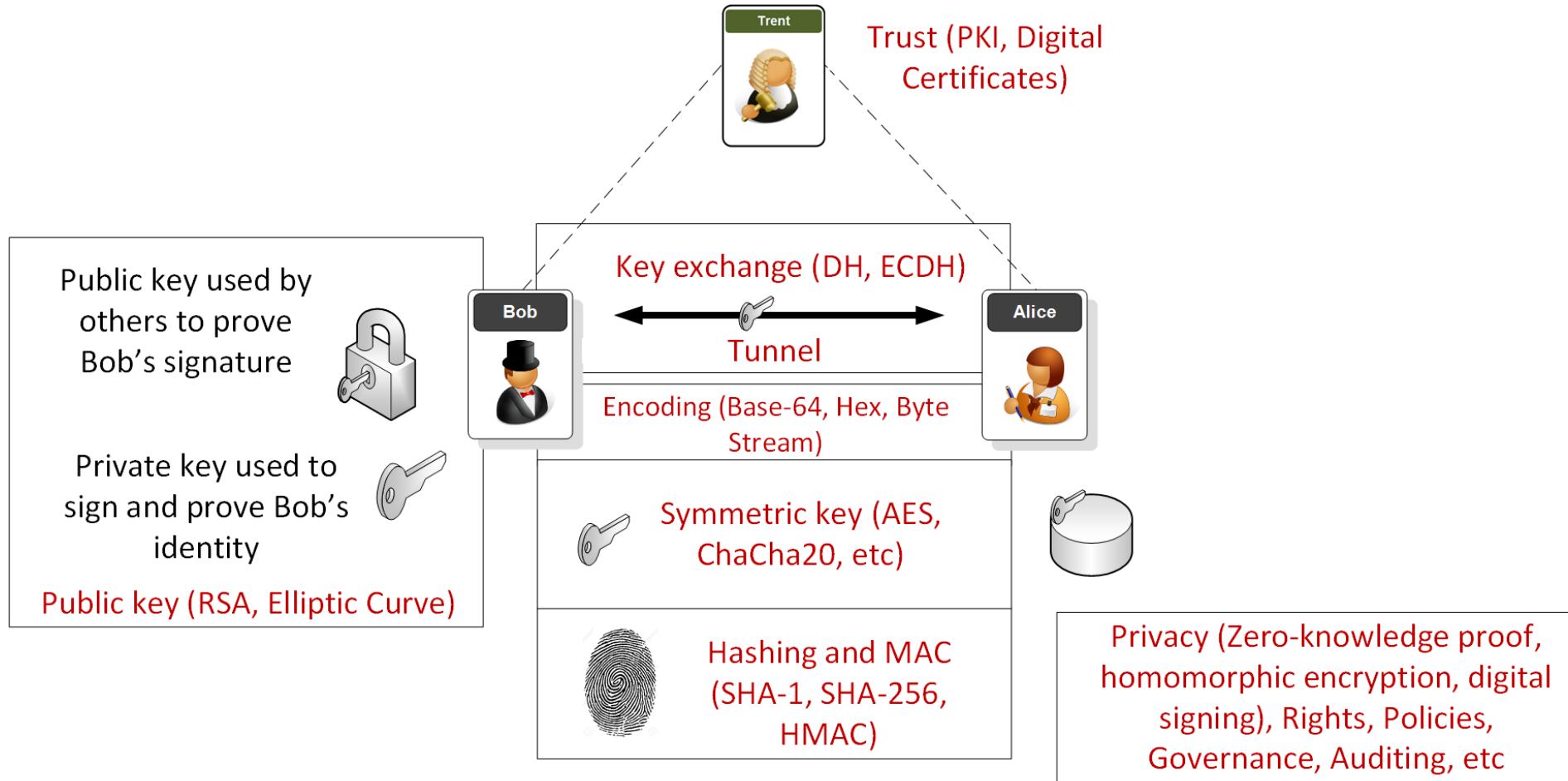
Scanners
SSL/TLS
VPN/IPSec

Prof Bill Buchanan OBE

<http://asecuritysite.com/tunnelling>



Overview



You are here: [Home](#) > [Projects](#) > SSL Server Test

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

Hostname:

Do not show the results on the boards

Recently Seen

[www.yaklink.com](#)
[billiardunderground.org](#)
[ha.homenetwork.biz](#)
[srv-web02.imageware.ch](#)
[evisa.gov.ge](#)
[www.thelevelupleague.com](#)
[sportclinic.it](#)
[edpnet.net](#)
[bungholio.ch](#)
[trade.eurocarparts.com](#)

Err

Recent Best

[forachange.co.il](#) A+
[auth.touchesurgery.com](#) A+
[www.cheqaga.de](#) A+
[ps-metro-fsd-mm-10-0-fsd-mm-...](#) A
[callback.datinglab.net](#) A
[www.rivanov.nl](#) A
[www.ioffice.kz](#) B
[afficheo.com](#) B
[populabor-bw.de](#) B
[mobile.imageware.ch](#) B

Recent Worst

[chepai.alltobid.com](#) F
[mail.frende.no](#) F
[mitpfa.dk](#) F
[ow-analytics.com](#) F
[mft.imageware.ch](#) T
[selfservice.kvk.nl](#) F
[www.migrosmagazin.ch](#) F
[www.vkekkl.it](#) F
[www.preiswerte-werbeartikel....](#) F
[bbapp.toddmorton.net](#) T

Scan your site now

enter address here

Scan

Hide results Follow redirects

Grand Totals

A+	657,797
A	4,792,956
B	1,573,217
C	789,919
D	2,710,689
E	1,788,375
F	11,569,900
R	2,313,267
Total	26,196,120

Recent Scans

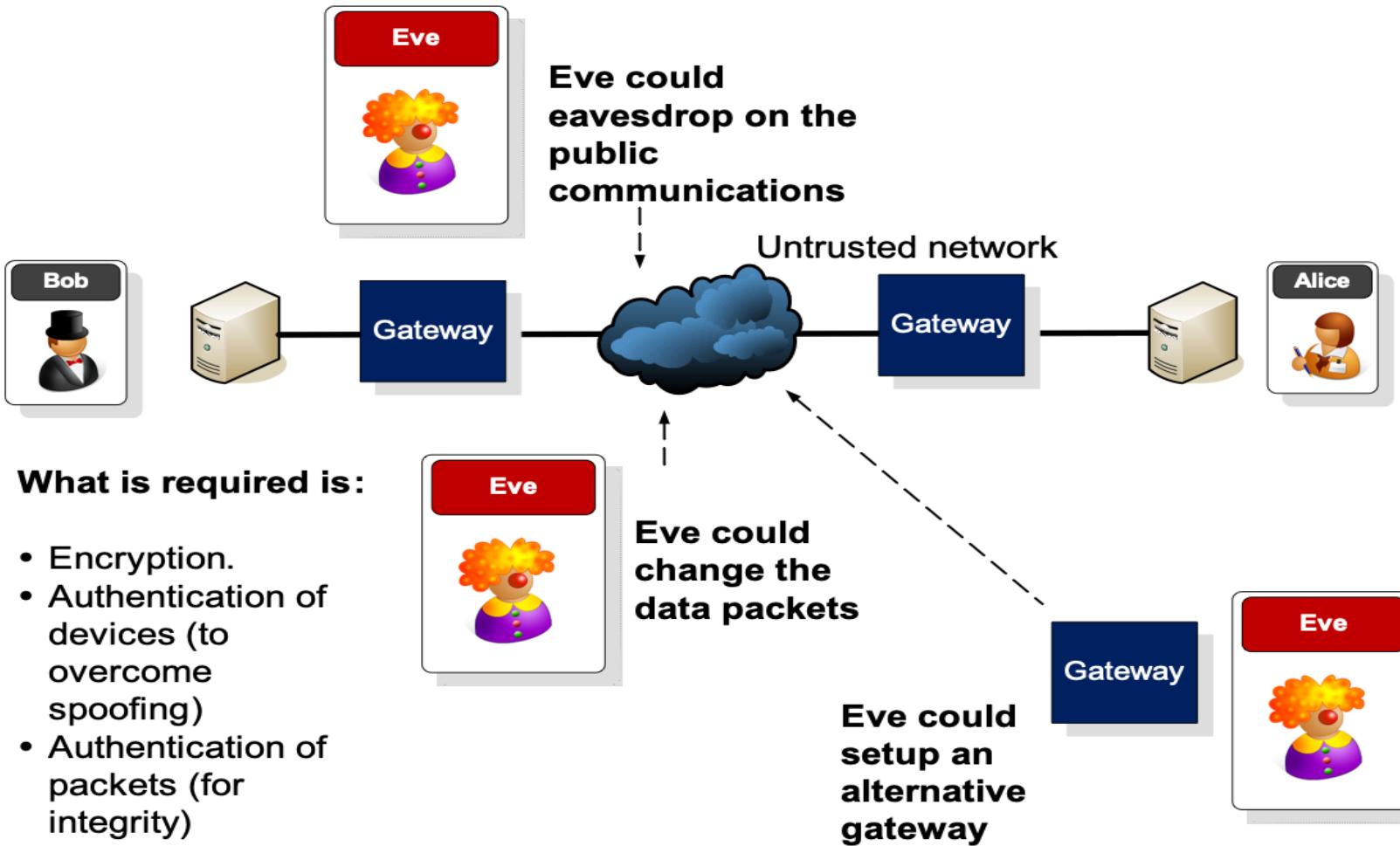
twitter.com	A
lifar.ciotor.se	F
www.infodaymedia.c...	E
content-marketing-...	F
foxpd.bestwomepri...	F
deonath.com	F
www.ijamat.com	F
www.google.co.jp	D
activatemomentum.c...	F

Hall of Fame

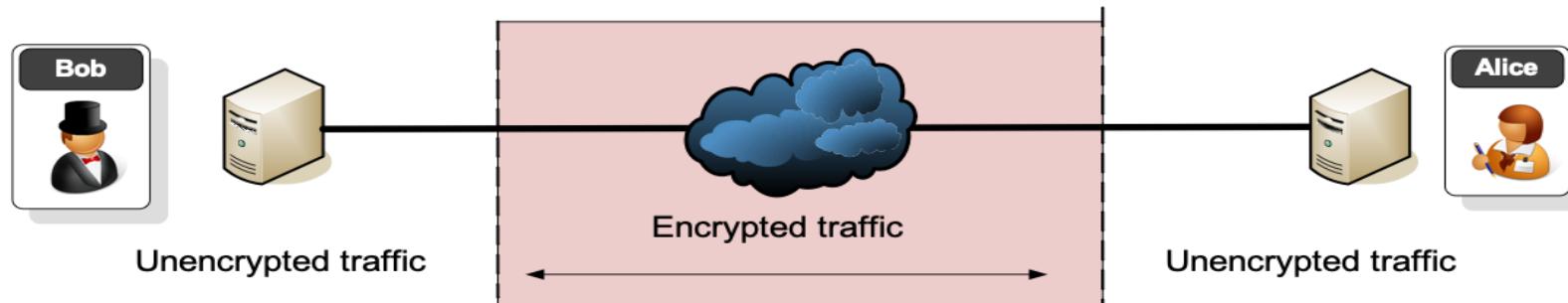
www.le-systems.com	A
gltorsystem.com	A+
msdapps-dev.hamilt...	A+
twitter.com	A
fated.org	A+
www.fbhackpass.com	A+
dwpocrusapi-test.a...	A
dwpocranthemapi-te...	A
dev.hamiltonapps.r...	A+

Hall of Shame

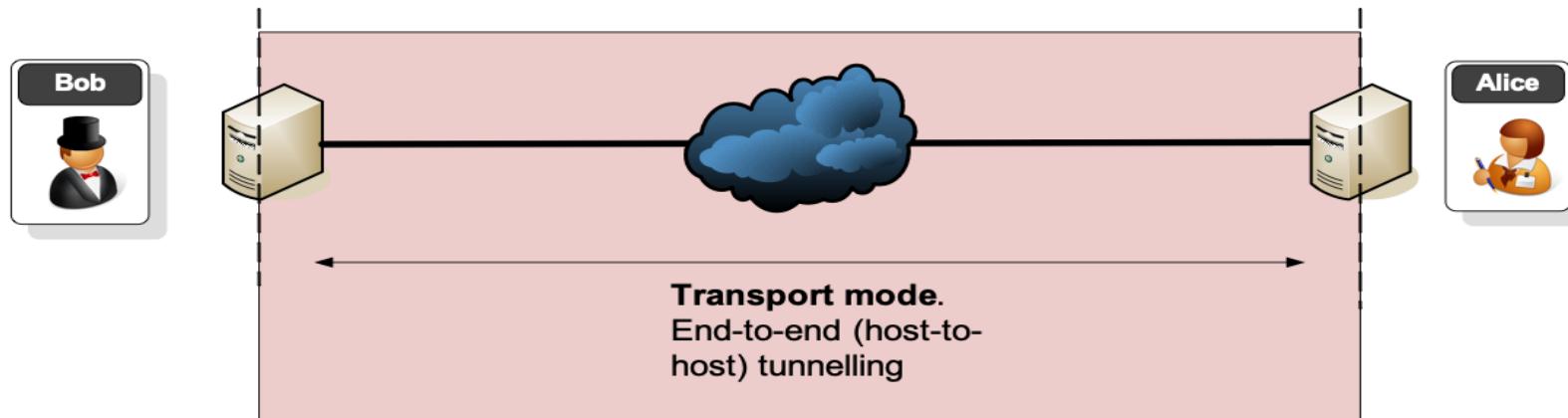
lifar.ciotor.se	F
content-marketing-...	F
foxpd.bestwomepri...	F
deonath.com	F
www.ijamat.com	F
activatemomentum.c...	F
www.janter.co.nz	F
guardiansafetybarr...	F
www.finderguru.com	F



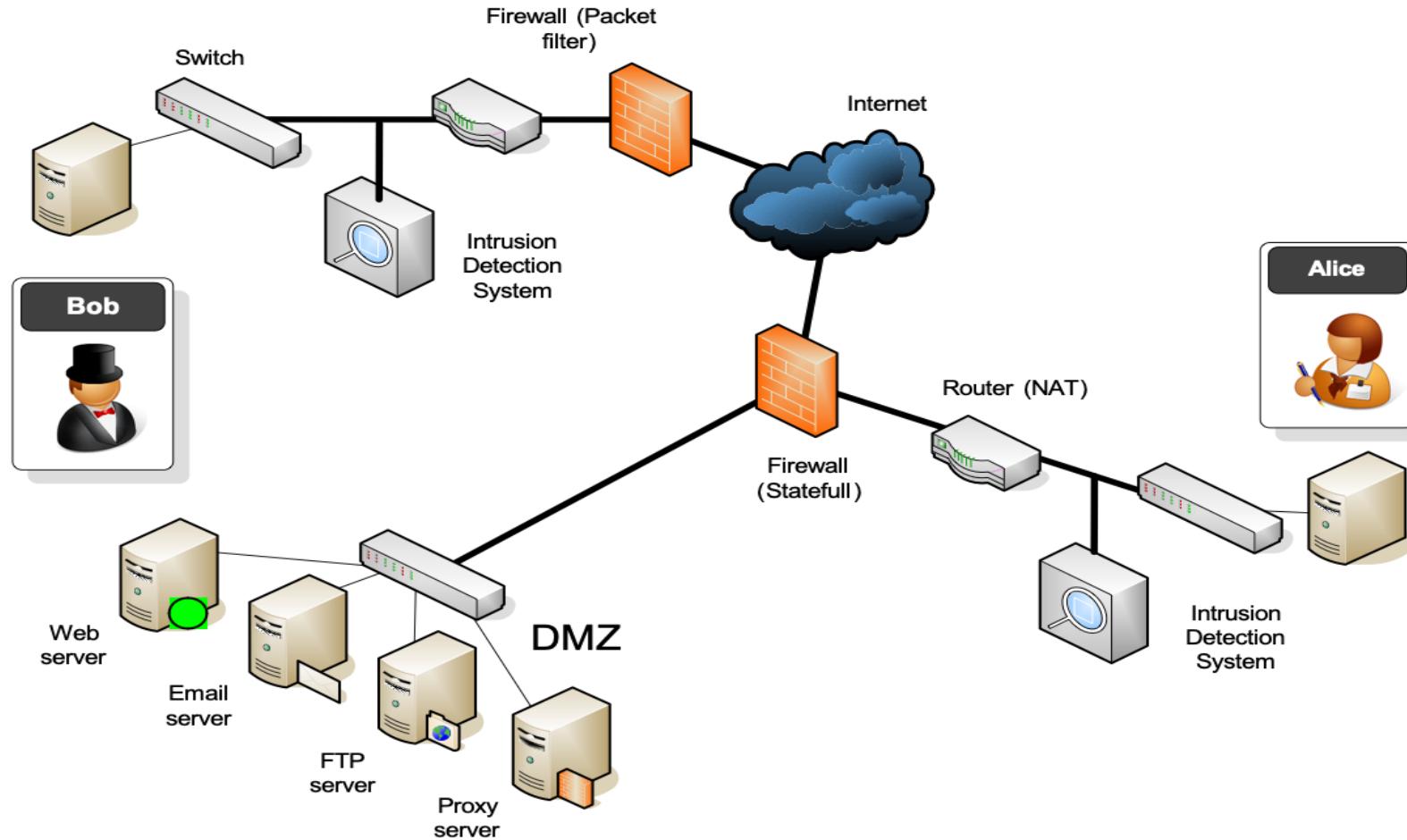
Traffic is encrypted over the untrusted network.

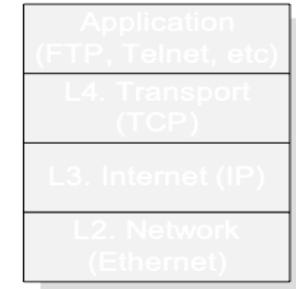
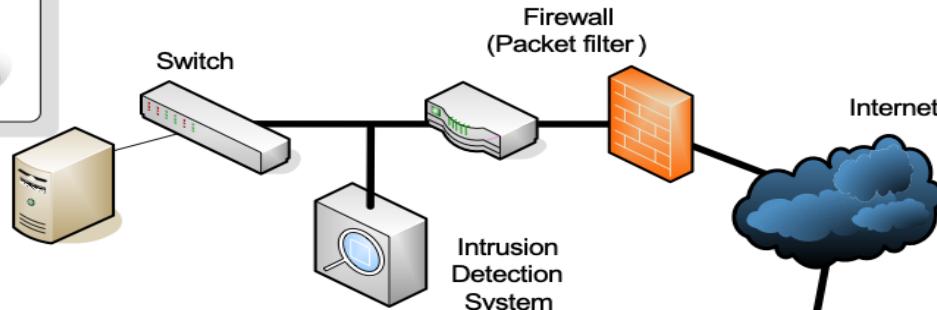


Tunelling mode (over untrusted connections)

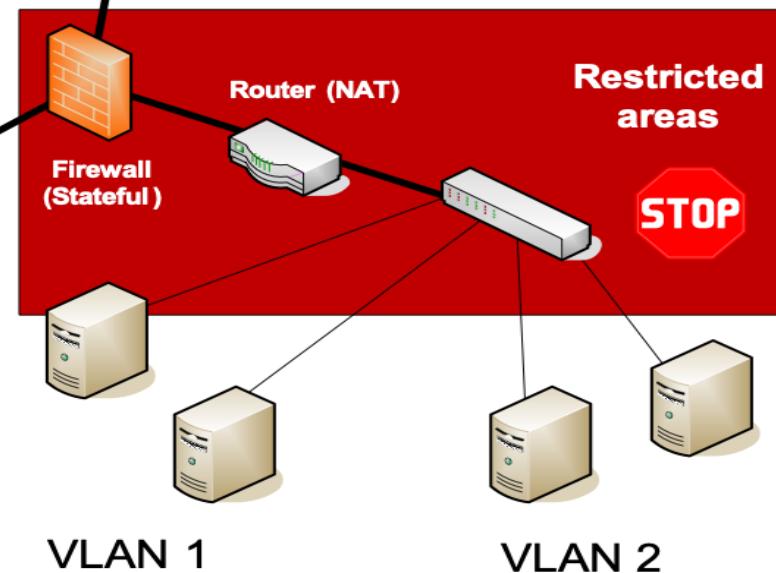
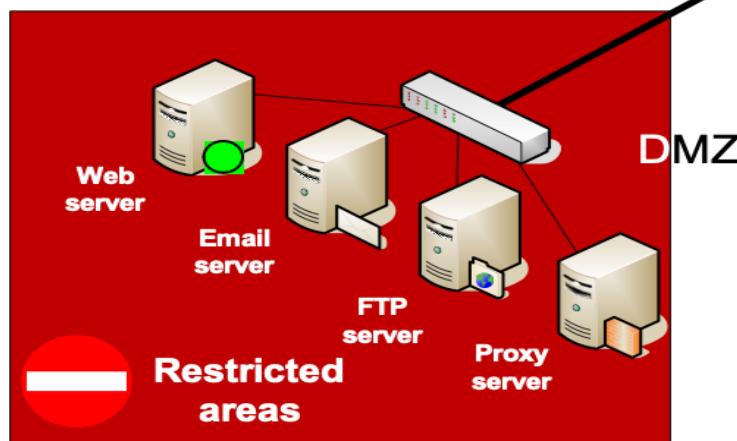


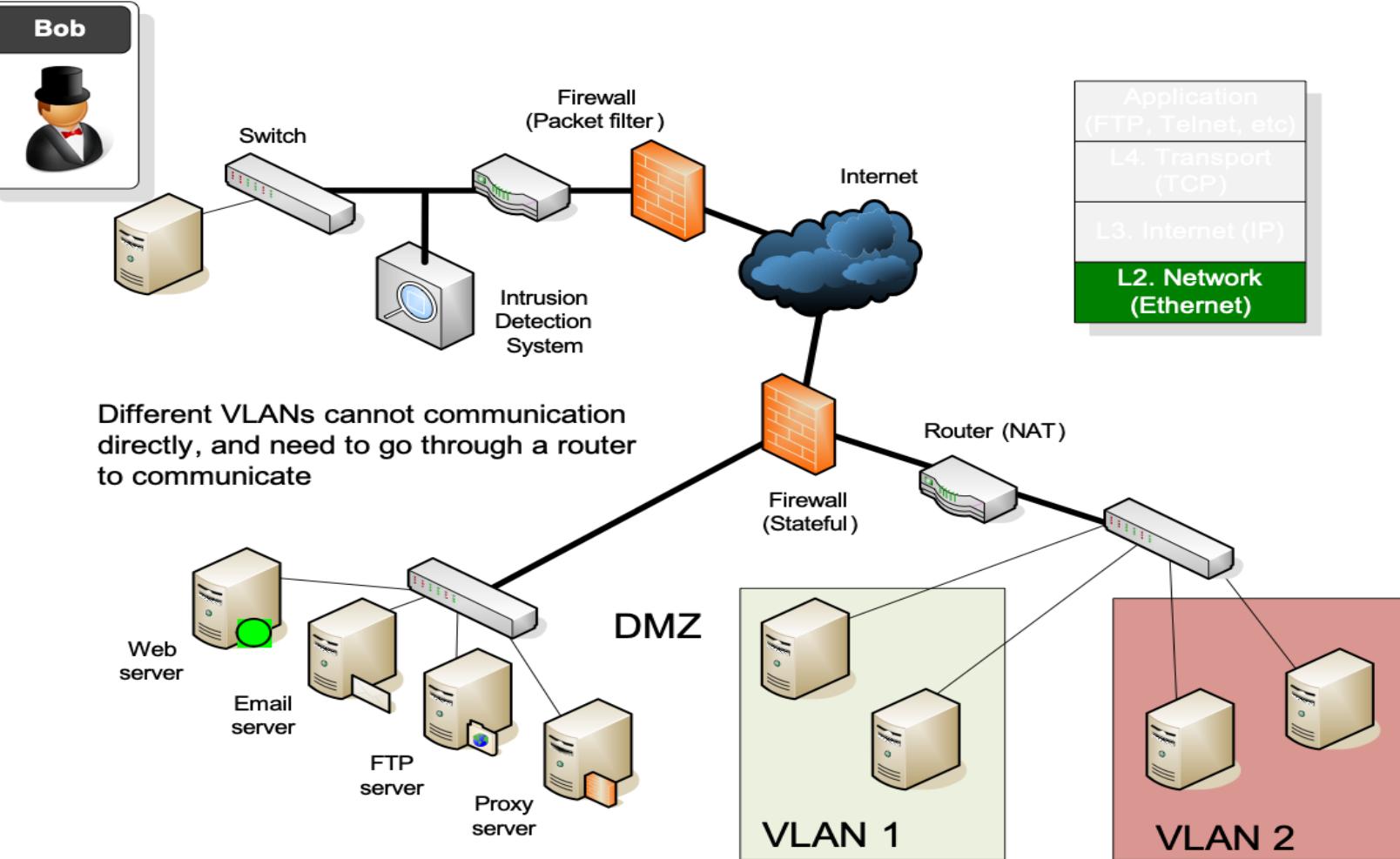
**Transport mode.
End-to-end (host-to-host) tunnelling**

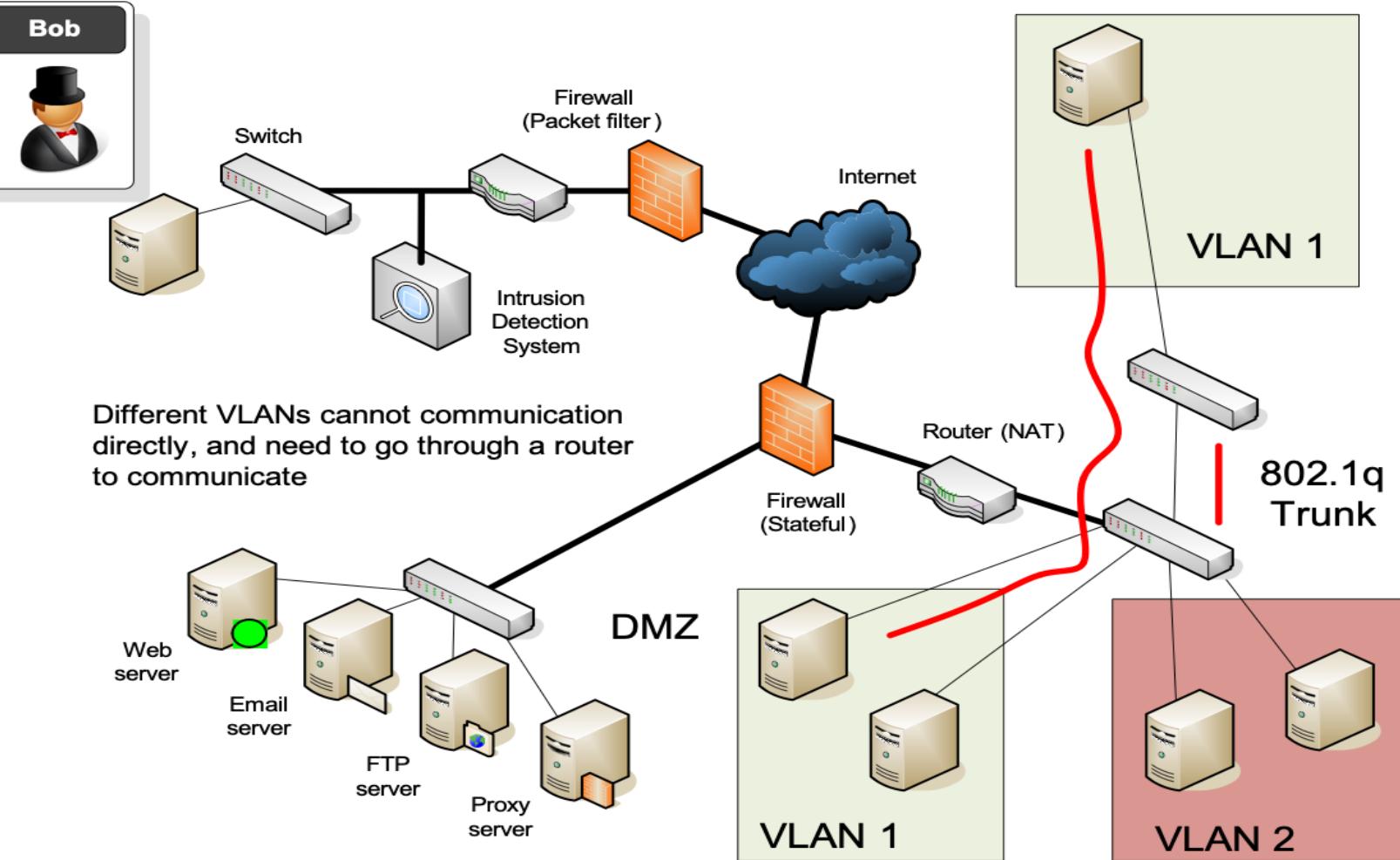


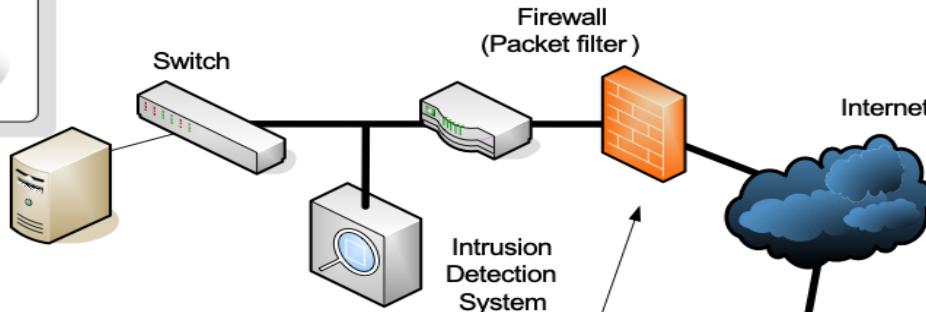


Physical security requires restricted areas and padlocked equipment

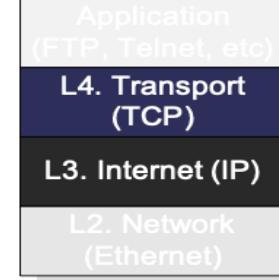




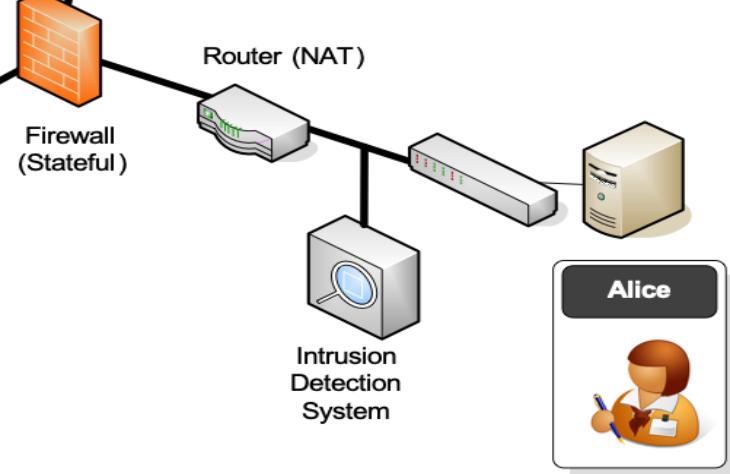
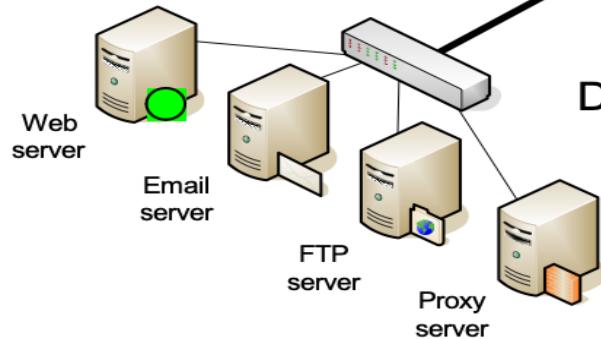


Bob**Screening Firewalls**

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



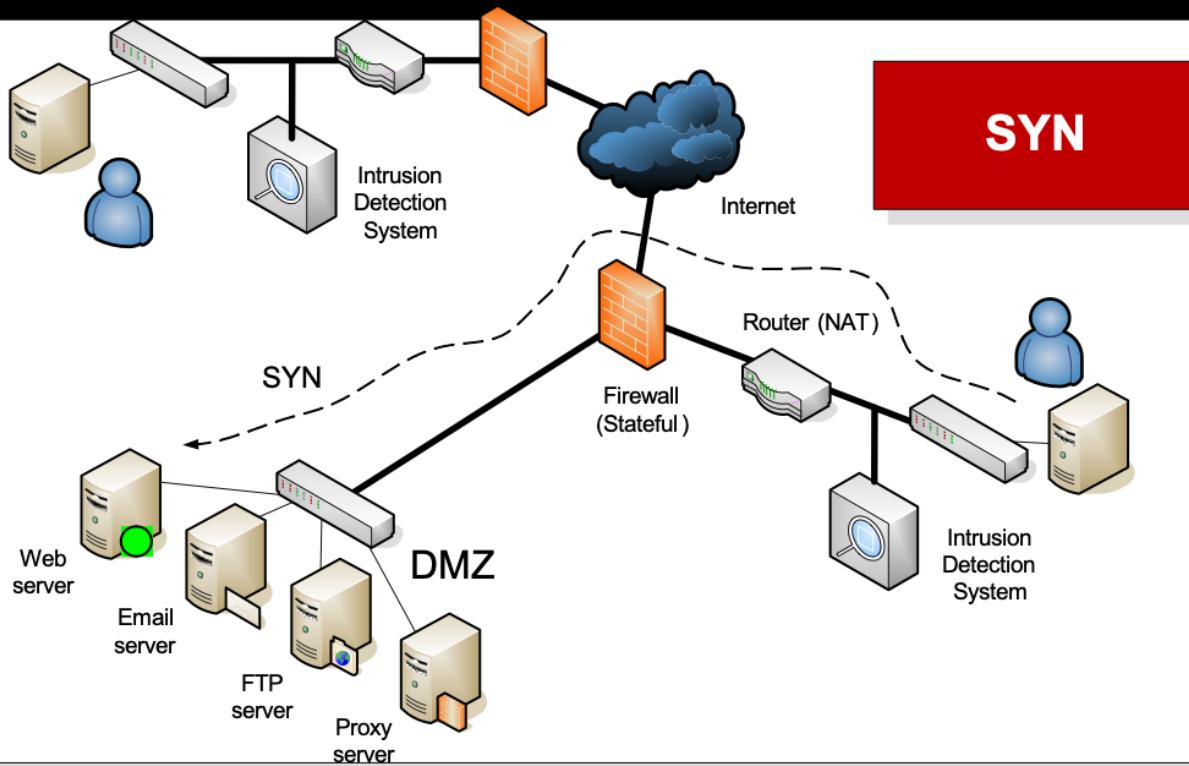
DMZ



Network Security

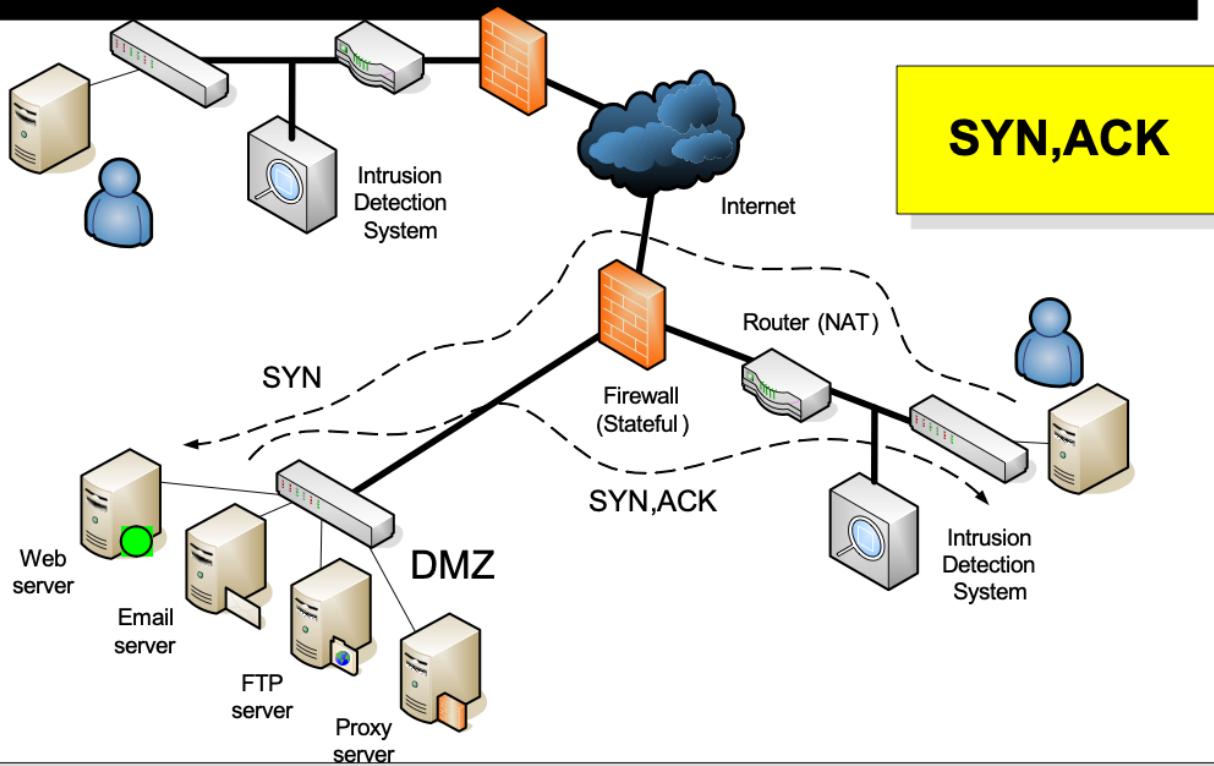
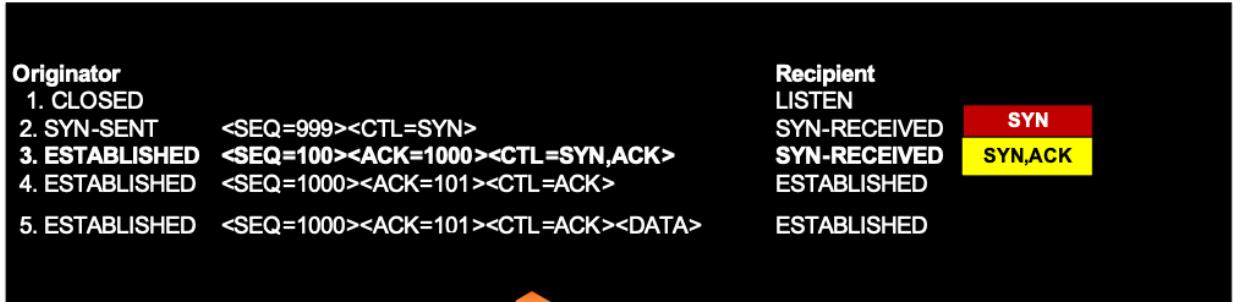
Stateful firewall

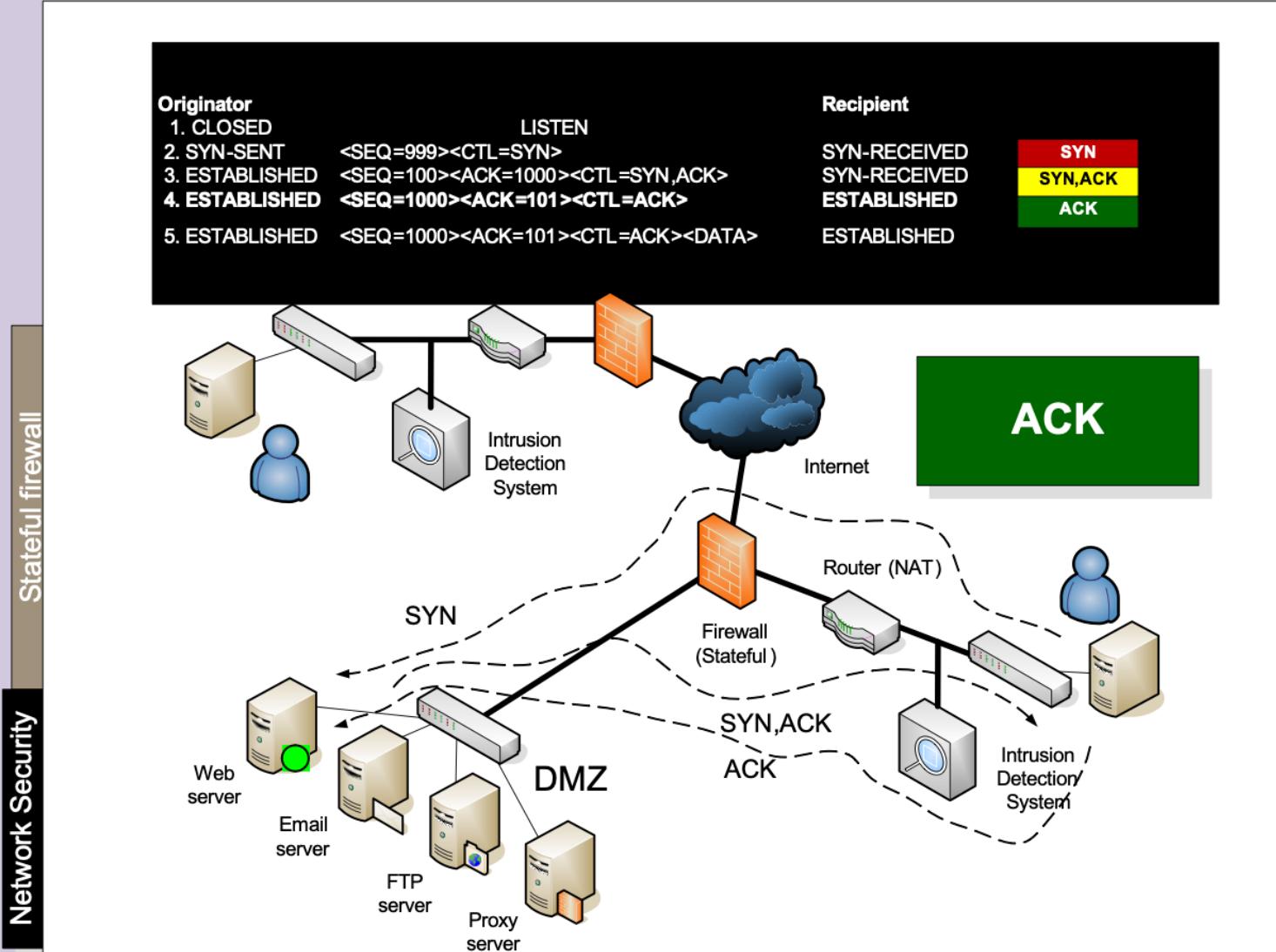
Originator	Recipient
1. CLOSED	LISTEN
2. SYN-SENT <SEQ=999><CTL=SYN>	SYN-RECEIVED
3. ESTABLISHED <SEQ=100><ACK=1000><CTL=SYN,ACK>	SYN-RECEIVED
4. ESTABLISHED <SEQ=1000><ACK=101><CTL=ACK>	ESTABLISHED
5. ESTABLISHED <SEQ=1000><ACK=101><CTL=ACK><DATA>	ESTABLISHED



Network Security

Stateful firewall





Tunnelling

Scanners
SSL/TLS
VPN/IPSec

Prof Bill Buchanan OBE

<http://asecuritysite.com/tunnelling>



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)

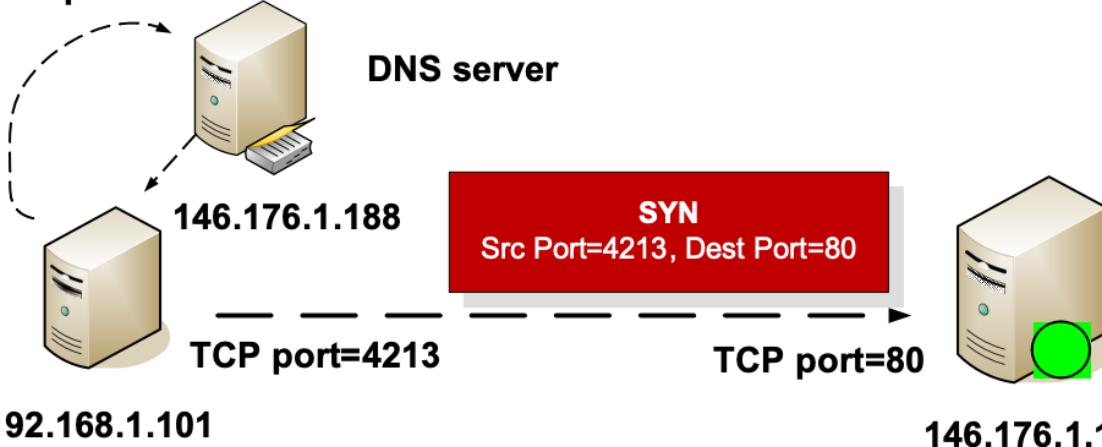
Options: (8 bytes)

SYN

Stateful fire

Network Security

www.napier.ac.uk?



146.176.1.188

192.168.1.101

Client-server (SYN)

Network Security

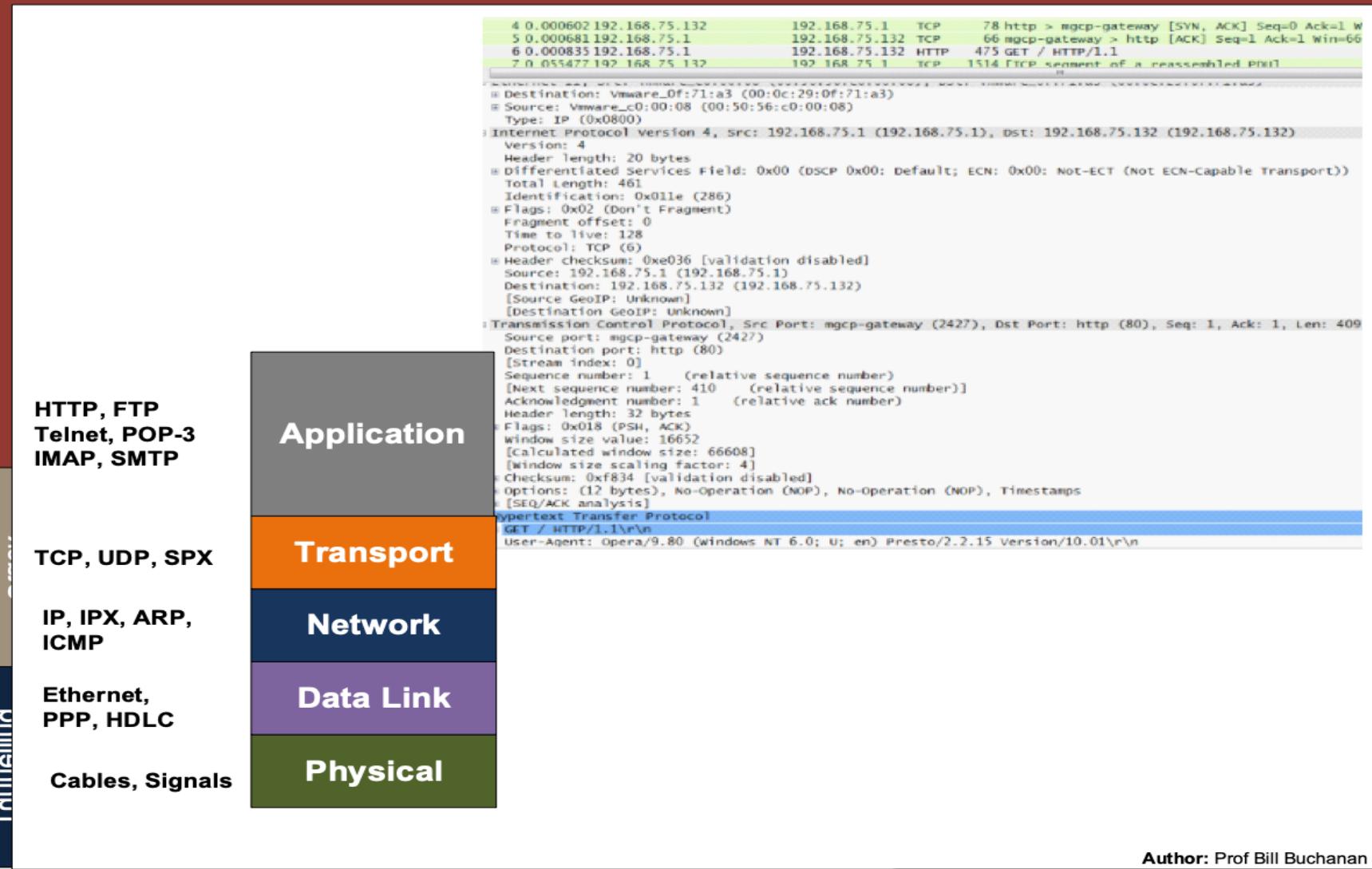
Stateful firewall

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 -

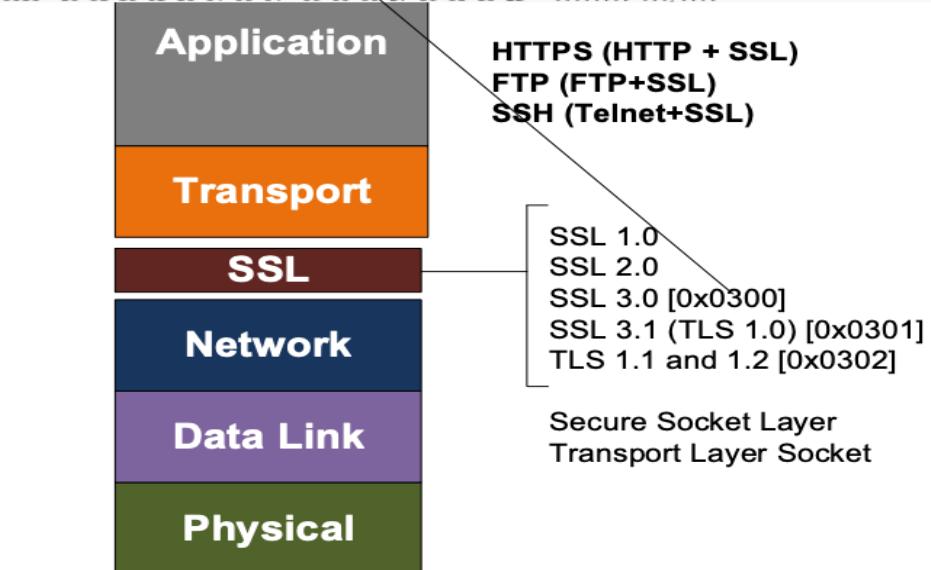
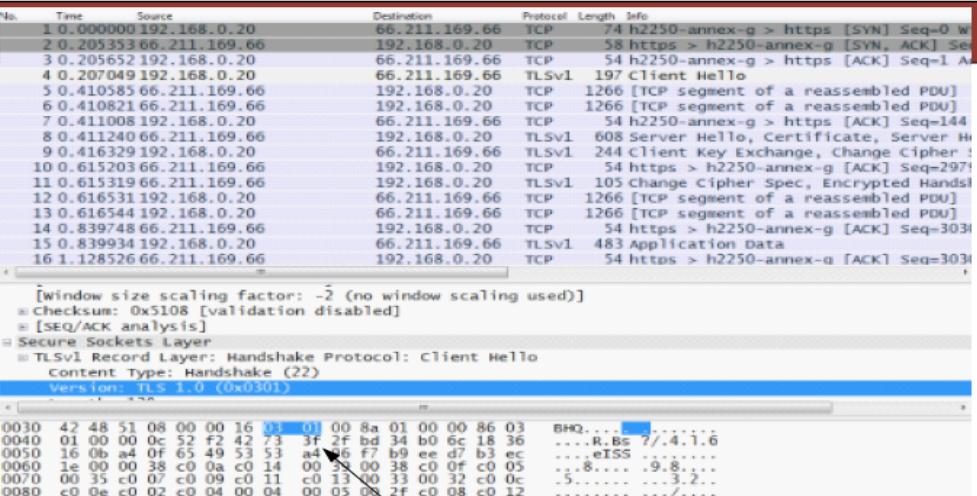
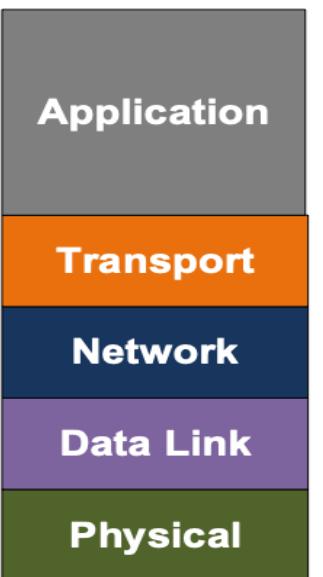
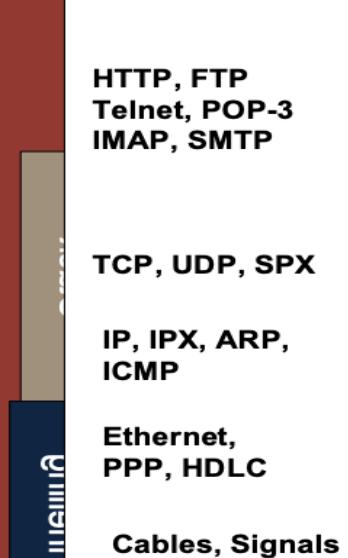
68 9.980194 192.168.1.101 resolver2.srv.pol. DNS Standard query PTR 255.1.168.192.in-addr.arpa
69 10.005697 resolver2.srv.pol. 192.168.1.101 DNS Standard query response, No such name
70 14.477532 192.168.1.101 resolver2.srv.pol. DNS Standard query A www.napier.ac.uk
71 14.503727 resolver2.srv.pol. 192.168.1.101 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

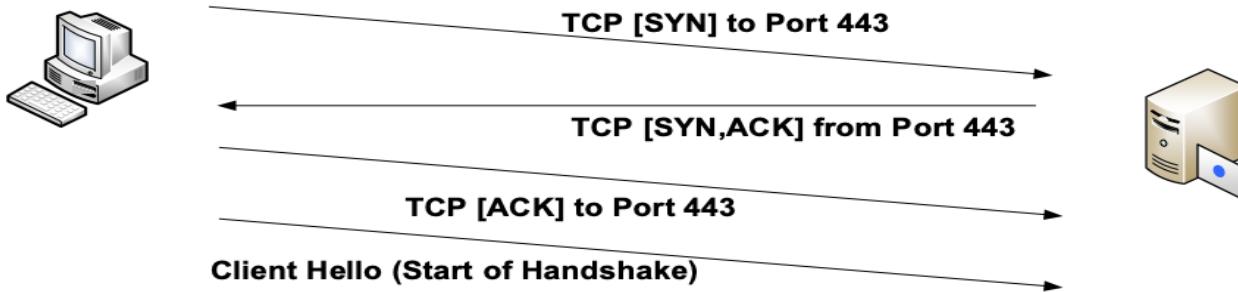
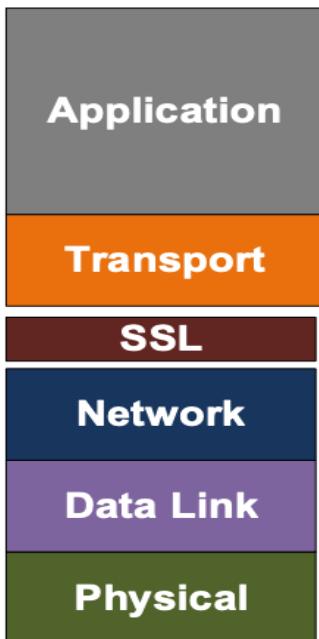
Name 75 (54 bytes on wire, 54 bytes captured)
Ethernet II, Src: 00:15:00:34:02:f0, Dst: 00:0c:41:f5:23:d5
Internet Protocol, Src Addr: 192.168.1.101 (192.168.1.101), Dst Addr: www.napier.ac.uk (146.176.1.188)
Transmission Control Protocol, Src Port: 4213 (4213), Dst Port: http (80), Seq: 1, Ack: 1, Len: 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]



Ports

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





Wireshark screenshot showing the TLS handshake frames:

Selected Frame: Frame 4: 197 bytes on wire (1576 bits), 197 bytes captured (1576 bits)
Protocol: TLSv1

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	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 Ack=144
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
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	TLSv1	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]

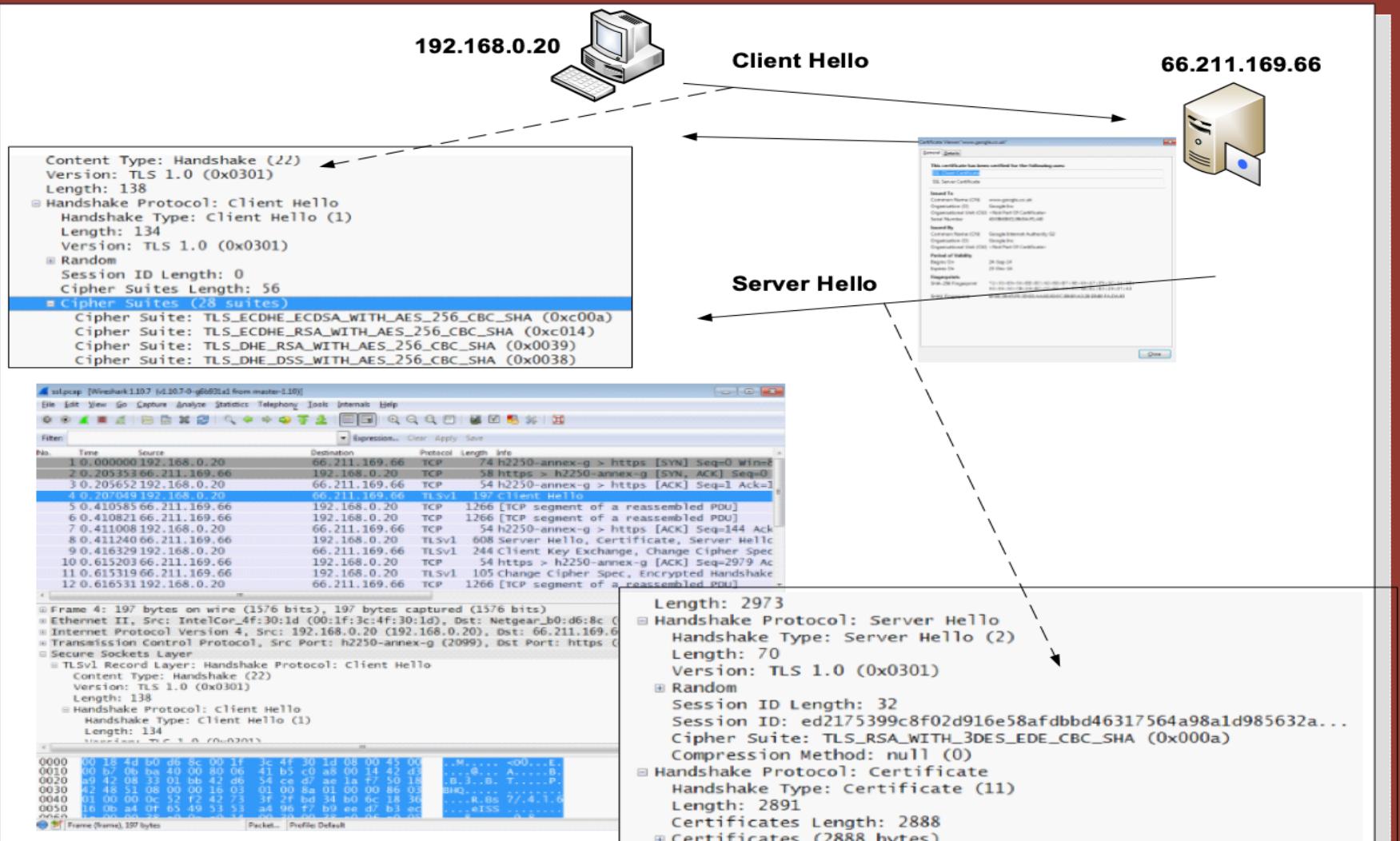
Details View:

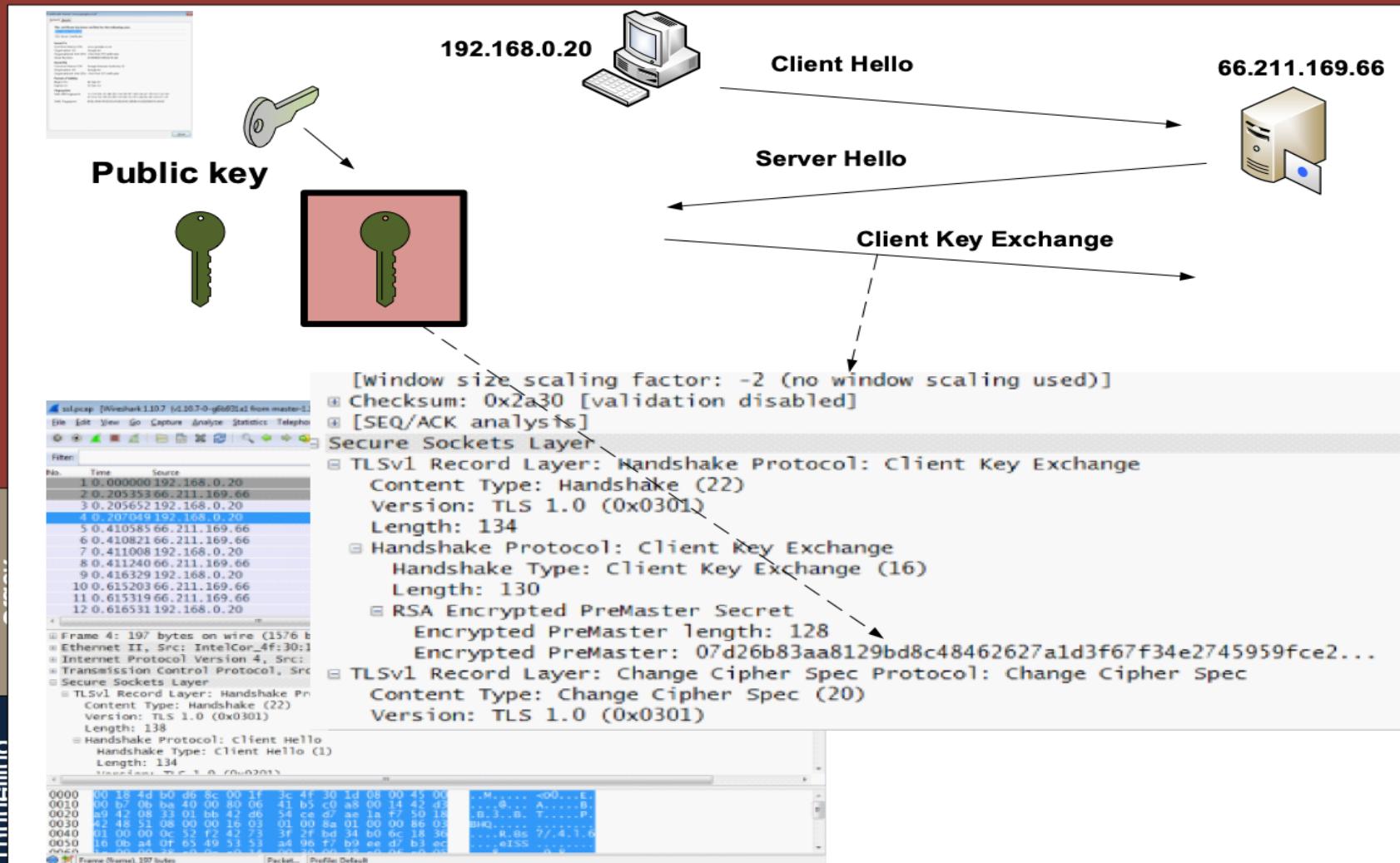
- Frame 4: 197 bytes on wire (1576 bits), 197 bytes captured (1576 bits)
- Ethernet II, Src: IntelCor_4f:30:1d (00:1f:3c:4f:30:1d), Dst: Netgear_b0:d6:8c (00:18:4d:b0:d6:8c)
- Internet Protocol version 4, Src: 192.168.0.20 (192.168.0.20), Dst: 66.211.169.66 (66.211.169.66)
- Transmission Control Protocol, Src Port: h2250-annex-g (2099), Dst Port: https (443), Seq: 1, Ack: 1, Len: 197
- Secure Sockets Layer
 - TLSv1 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

Hex View:

```

0000  00 18 4d b0 d6 8c 00 1f 3c 4f 30 1d 08 00 45 00 .M...<00...E
0010  00 b7 08 ba 40 00 80 06 41 b5 c0 a8 00 14 42 d3 ..0...A.B
0020  a9 42 08 33 01 bb 42 d6 54 ce d7 ae 1a f7 30 18 .B.3..T.P
0030  42 48 51 08 00 00 16 03 01 00 8a 01 00 00 86 03 BHQ
0040  01 00 00 0c 52 f2 42 73 3f 2f 34 b0 6c 18 36 .R.Rs?/.4.1.6
0050  16 0b a4 0f 65 49 53 53 a4 96 f7 b9 ee d7 b3 ec .eISS
0060  1c 00 00 28 00 00 00 00 00 00 00 00 00 00 00 00
    
```



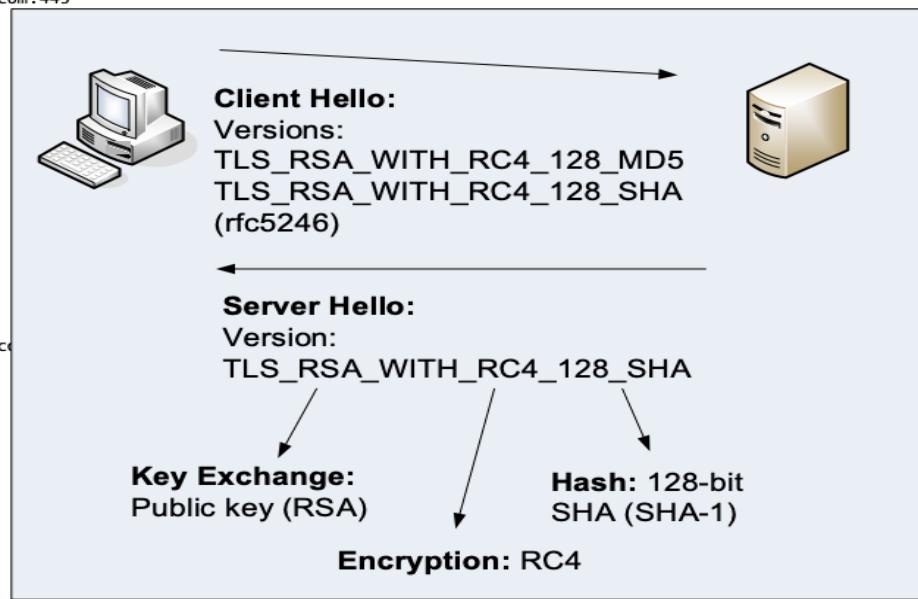


```

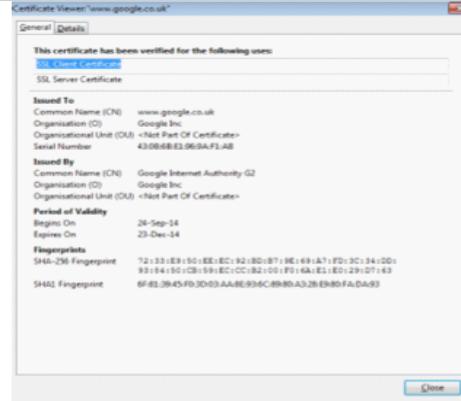
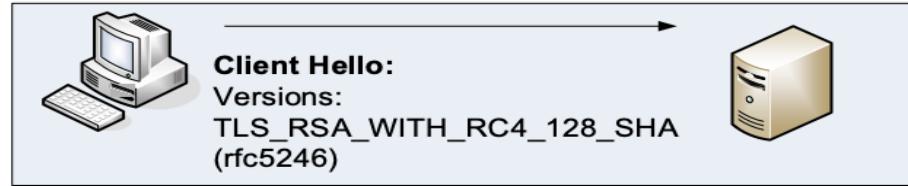
billbuchanan@Bill's-MacBook-Pro:~$ openssl s_client -connect www.google.com:443
CONNECTED(00000003)
depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
verify error:num=20:unable to get local issuer certificate
verify return:0
---
Certificate chain
 0 s:/C=US/ST=California/L=Mountain View/O=Google 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-----
MIIEjdCCA16gAwIBAgIISVyALW...+akUwDQYJKoZIhvcNAQEFBQAwSTELMAkG
-----END CERTIFICATE-----
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=www.google.co
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 ee 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



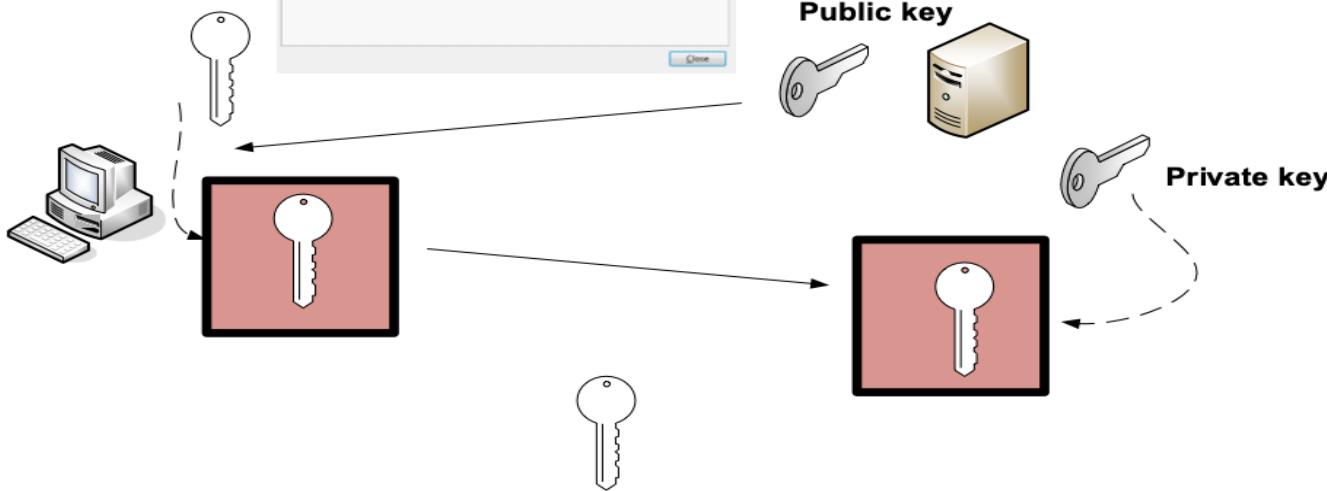
Server Hello:
Version:
TLS_RSA_WITH_RC4_128_SHA

Key Exchange:
Public key (RSA)

Hash: 128-bit SHA (SHA-1)

Encryption: RC4

Session key



Tunnel created (RC4, Hash: SHA-1)

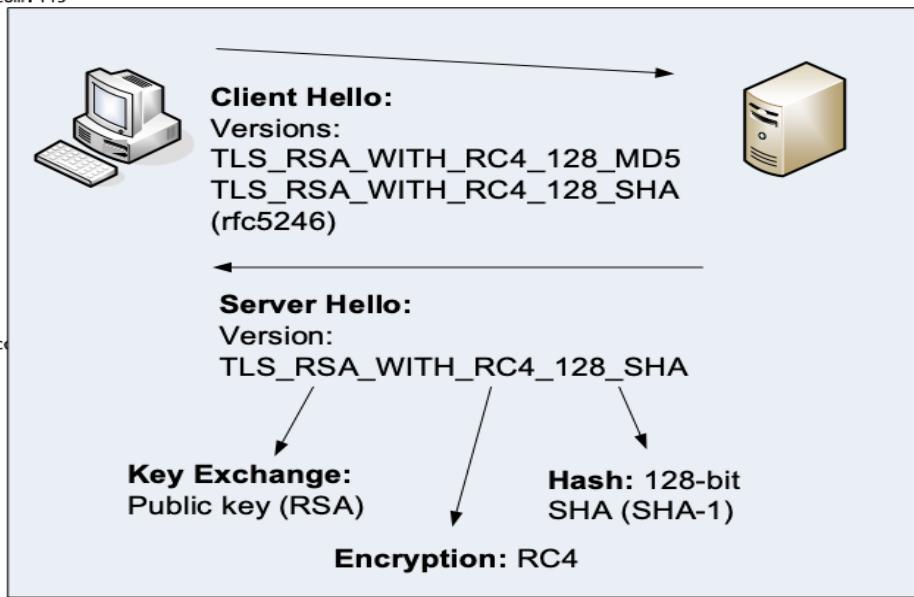
Author: Prof Bill Buchanan

```

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
...
Sox4i5L0D0jZYqKfuUmGfwdIETq0EpCmkhJfgNHjVdzC/h/T61TmaY
-----END CERTIFICATE-----
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=www.google.co
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-Arg   : None
PSK identity: None
PSK identity hint: None
SRP username: 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

```
import socket, ssl

context = ssl.SSLContext(ssl.PROTOCOL_TLSv1)
context.load_cert_chain(certfile="mycert.pem")

def handle(conn):
    conn.write(b'GET / HTTP/1.1\n')
    print(conn.recv().decode())

while True:
    sock = socket.socket()
    sock.bind(('', 444))
    sock.listen(5)
    context = ssl.create_default_context(ssl.Purpose.CLIENT_AUTH)
    context.load_cert_chain(certfile="mycert.pem")
    context.options |= ssl.OP_NO_TLSv1 | ssl.OP_NO_TLSv1_1 # optional
    context.set_ciphers('AES256+ECDH:AES256+EDH')
    while True:
        conn = None
        ssock, addr = sock.accept()
        try:
            conn = context.wrap_socket(ssock, server_side=True)
            handle(conn)
        except ssl.SSLError as e:
            print(e)
        finally:
            if conn:
                conn.close()
```

```
import socket, ssl

context = ssl.SSLContext(ssl.PROTOCOL_TLSv1)
context.load_cert_chain(certfile="mycert.pem")

def handle(conn):
    conn.write(b'GET / HTTP/1.1\n')
    print(conn.recv().decode())

while True:
    sock = socket.socket()
    sock.bind(('', 444))
    sock.listen(5)
    context = ssl.create_default_context(ssl.Purpose.CLIENT_AUTH)
    context.load_cert_chain(certfile="mycert.pem")
    context.options |= ssl.OP_NO_TLSv1 | ssl.OP_NO_TLSv1_1
    context.set_ciphers('AES256+ECDH:AES256+EDH')
    while True:
        conn = None
        ssock, addr = sock.accept()
        try:
            conn = context.wrap_socket(ssock, server_side=True)
            handle(conn)
        except ssl.SSLError as e:
            print(e)
        finally:
            if conn:
                conn.close()
```

```
import socket, ssl

HOST, PORT = '10.214.0.96', 443

def handle(conn):
    conn.write(b'GET / HTTP/1.1\n')
    print(conn.recv().decode())

def main():
    sock = socket.socket(socket.AF_INET)

    context = ssl.create_default_context(ssl.Purpose.SERVER_AUTH)
    context.check_hostname = False
    context.verify_mode=ssl.CERT_NONE

    context.options |= ssl.OP_NO_TLSv1 | ssl.OP_NO_TLSv1_1

    conn = context.wrap_socket(sock, server_hostname=HOST)

    try:
        conn.connect((HOST, PORT))
        handle(conn)
    finally:
        conn.close()

if __name__ == '__main__':
    main()
```

```
import socket, ssl

context = ssl.SSLContext(ssl.PROTOCOL_TLSv1)
context.load_cert_chain(certfile="mycert.pem")

def handle(conn):
    conn.write(b'HTTP/1.1\n')
    print(conn.recv().decode())

while True:
    sock = socket.socket()
    sock.bind(('', 444))
    sock.listen(5)
    context = ssl.create_default_context()
    context.load_cert_chain(certfile="mycert.pem")
    context.options |= ssl.OP_NO_TLSv1
    context.set_ciphers('AES256+ECDSA')
    while True:
        conn = None
        ssock, addr = sock.accept()
        try:
            conn = context.wrap_socket(ssock)
            handle(conn)
        except ssl.SSLError as e:
            print(e)
        finally:
            if conn:
                conn.close()
```

```
import socket, ssl

Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
8 0.002270000 10.221.0.7 10.221.0.7 TLSv1.2 1364 Server Hello, Certificate, Se...
9 0.002277000 10.221.0.7 10.221.0.7 TCP 66 60770 > https [ACK] Seq=279 A...
10 0.003070000 10.221.0.7 10.221.0.7 TLSv1.2 192 Client Key Exchange, Change C...
11 0.003530000 10.221.0.7 10.221.0.7 TLSv1.2 308 New Session Ticket, Change Ci...
12 0.003693000 10.221.0.7 10.221.0.7 TLSv1.2 110 Application Data
13 0.003714000 10.221.0.7 10.221.0.7 TLSv1.2 110 Application Data
14 0.004240000 10.221.0.7 10.221.0.7 TCP 66 60770 > https [FIN, ACK] Seq=...
15 0.041712000 10.221.0.7 10.221.0.7 TCP 66 https > 60770 [ACK] Seq=1585 ...

[+] Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 62
    Version: TLS 1.2 (0x0303)
[+] Random
    Session ID Length: 0
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
    Compression Method: null (0)
    Extensions Length: 22
[+] Extension: renegotiation_info

0060 d3 e6 2a 6c fd cf 62 3f 47 fc 8d d3 8e 00 c0 90 ...l..b? 0.....
0070 00 00 16 ff 01 00 01 00 00 0b 00 04 03 00 01 02 ..... .
0080 00 23 00 00 00 0f 00 01 01 16 03 03 03 6b 0b 00 .#..... ....k...
0090 03 67 00 03 64 00 03 61 30 82 03 5d 30 82 02 45 .g..d..a 0..]0..E
00a0 a0 03 02 02 01 02 02 09 00 83 74 d7 0e 41 d4 0e .....,t..A...
```

Internet Engineering Task Force (IETF)
Request for Comments: 8446
Obsoletes: 5077, 5246, 6961
Updates: 5705, 6066
Category: Standards Track
ISSN: 2070-1721

E. Rescorla
Mozilla
August 2018

The Transport Layer Security (TLS) Protocol Version 1.3

Abstract

This document specifies version 1.3 of the Transport Layer Security (TLS) protocol. TLS allows client/server applications to communicate over the Internet in a way that is designed to prevent eavesdropping, tampering, and message forgery.

This document updates RFCs 5705 and 6066, and obsoletes RFCs 5077, 5246, and 6961. This document also specifies new requirements for TLS 1.2 implementations.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at
<https://www.rfc-editor.org/info/rfc8446>.

Internet Engineering Task Force (IETF)
Request for Comments: 8446
Obsoletes: 5077, 5246, 6961
Updates: 5705, 6066
Category: Standards Track
ISSN: 2070-1721

The Transport Layer Security (TLS)

Abstract

This document specifies version 1.3 of the Transport Layer Security (TLS) protocol. TLS allows client/server communication over the Internet in a way that is designed to prevent tampering, and message forgery.

This document updates RFCs 5705 and 6066, 5246, and 6961. This document also specifies TLS 1.2 implementations.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the community. It has received public review and has been approved by the Internet Engineering Steering Group (IESG). The latest version of this document is available in the IESG Approved area.

Information about the current status of this document and how to provide feedback on it may be found at <https://www.rfc-editor.org/info/rfc8446>.

Rescorla
RFC 8446

Standards Track
TLS

E. Rescorla
Mozilla
August 2018

Replay Attacks on Zero Round-Trip Time: The Case of the TLS 1.3 Handshake Candidates

Marc Fischlin

Felix Günther

Cryptoplexy, Technische Universität Darmstadt, Germany
marc.fischlin@cryptoplexy.de, guenther@cs.tu-darmstadt.de

February 2, 2017

Abstract. We investigate security of key exchange protocols supporting so-called zero round-trip time (0-RTT), enabling a client to establish a fresh provisional key without interaction, based only on cryptographic material obtained in previous connections. This key can then be already used to protect early application data, transmitted to the server before both parties interact further to switch to fully secure keys. Two recent prominent examples supporting such 0-RTT modes are Google's QUIC protocol and the latest drafts for the upcoming TLS version 1.3.

We are especially interested in the question how replay attacks, enabled through the lack of contribution from the server, affect security in the 0-RTT case. Whereas the first proposal of QUIC uses state on the server side to thwart such attacks, the latest version of QUIC and TLS 1.3 rather accept them as inevitable. We analyze what this means for the key secrecy of both the pre-shared-key-based 0-RTT handshake in draft-14 of TLS 1.3 as well as the Diffie-Hellman-based 0-RTT handshake in TLS 1.3 draft-12. As part of this we extend previous security models to capture such cases, also shedding light on the limitations and options for 0-RTT security under replay attacks.

August 2018

Replayable 0-RTT data presents a number of security threats to TLS-using applications, unless those applications are specifically engineered to be safe under replay (minimally, this means idempotent, but in many cases may also require other stronger conditions, such as constant-time response). Potential attacks include:

- Duplication of actions which cause side effects (e.g., purchasing an item or transferring money) to be duplicated, thus harming the site or the user.
- Attackers can store and replay 0-RTT messages in order to re-order them with respect to other messages (e.g., moving a delete to after a create).
- Exploiting cache timing behavior to discover the content of 0-RTT messages by replaying a 0-RTT message to a different cache node and then using a separate connection to measure request latency, to see if the two requests address the same resource.

and how to provide feedback on it may be
<https://www.rfc-editor.org/info/rfc8446>.

Rescorla
RFC 8446

Standards Trac
TLS

inevitable. We analyze what this means for the key secrecy of both the preshared-key-based 0-RTT handshake in draft-14 of TLS 1.3 as well as the Diffie-Hellman-based 0-RTT handshake in TLS 1.3 draft-12. As part of this we extend previous security models to capture such cases, also shedding light on the limitations and options for 0-RTT security under replay attacks.

August 2010

Tunnelling

Scanners

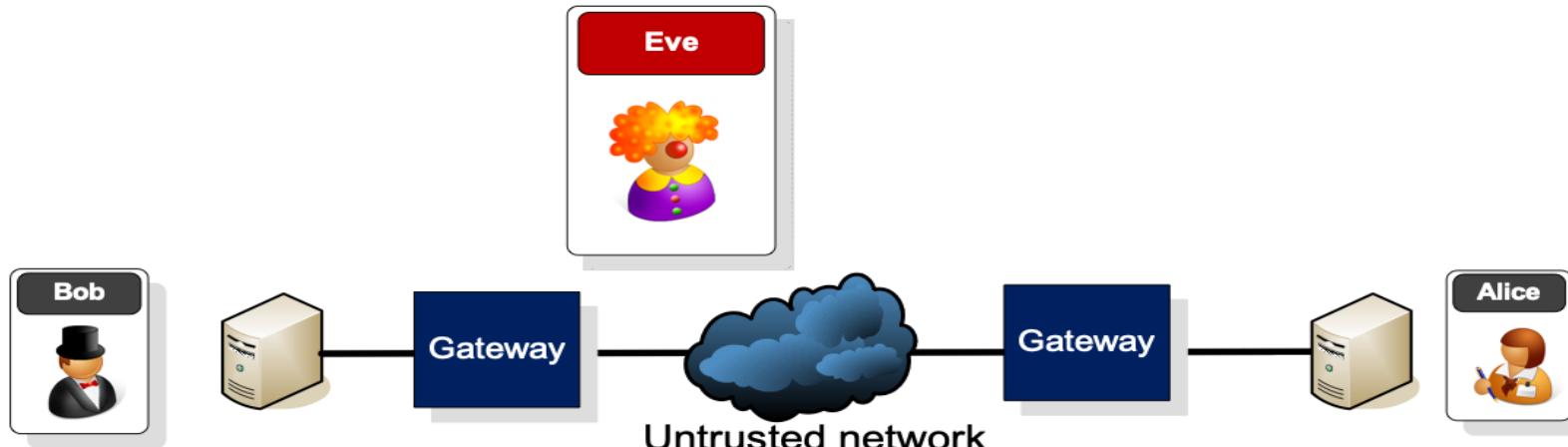
SSL/TLS

VPN/IPSec

Prof Bill Buchanan OBE

<http://asecuritysite.com/tunnelling>





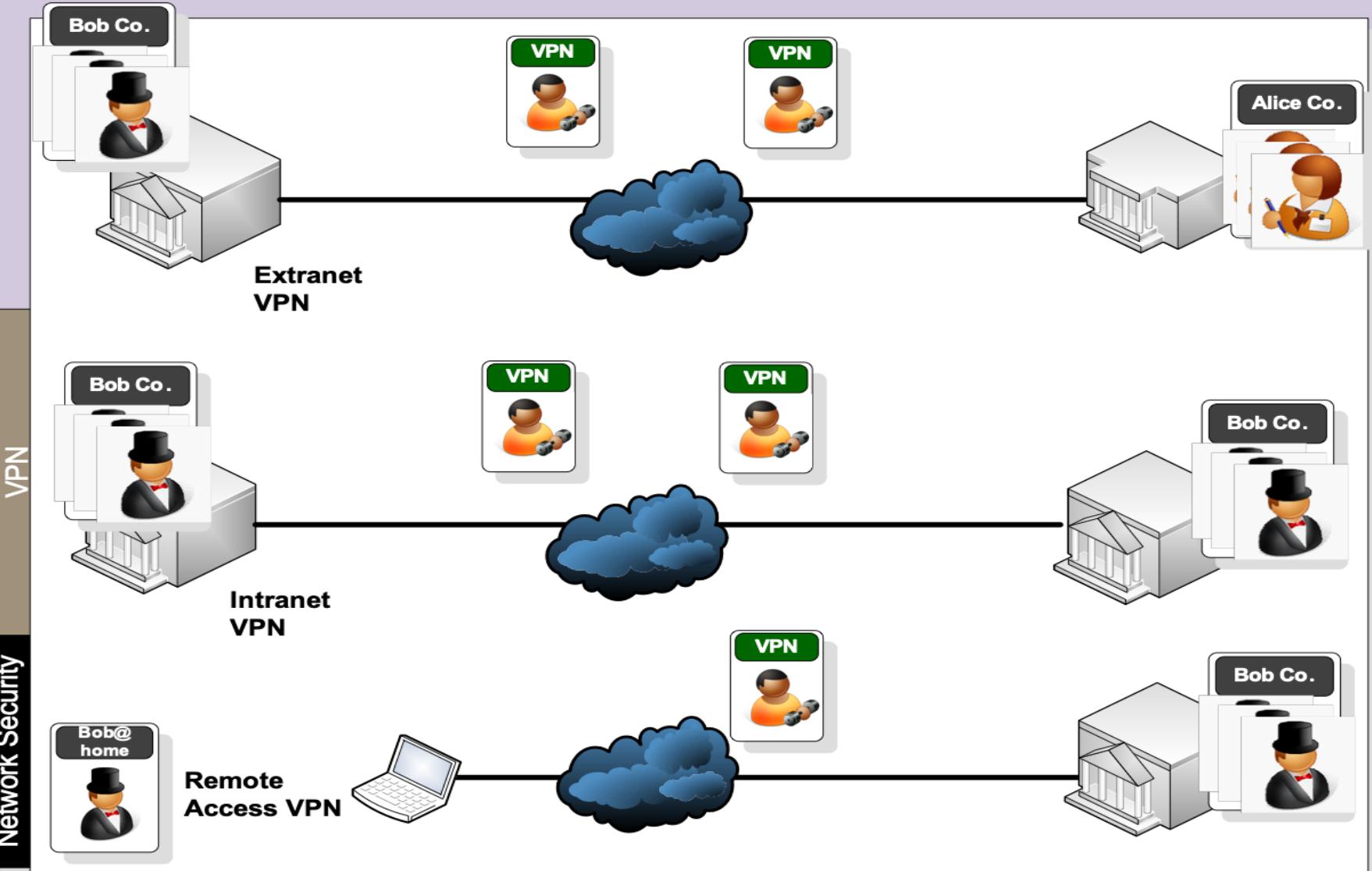
What is required is:

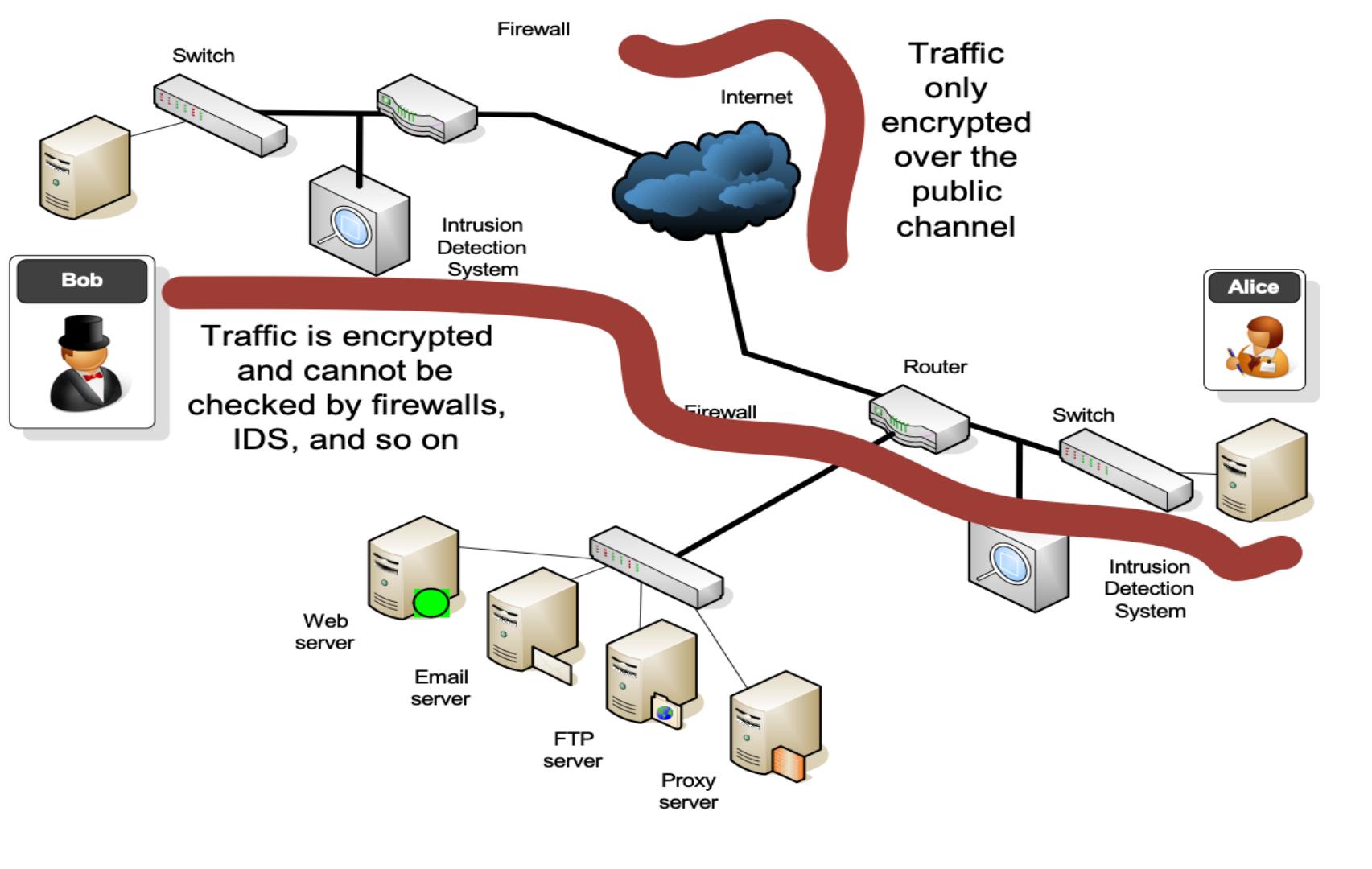
- Encryption.
- Authentication of devices (to overcome spoofing)
- Authentication of packets (for integrity)

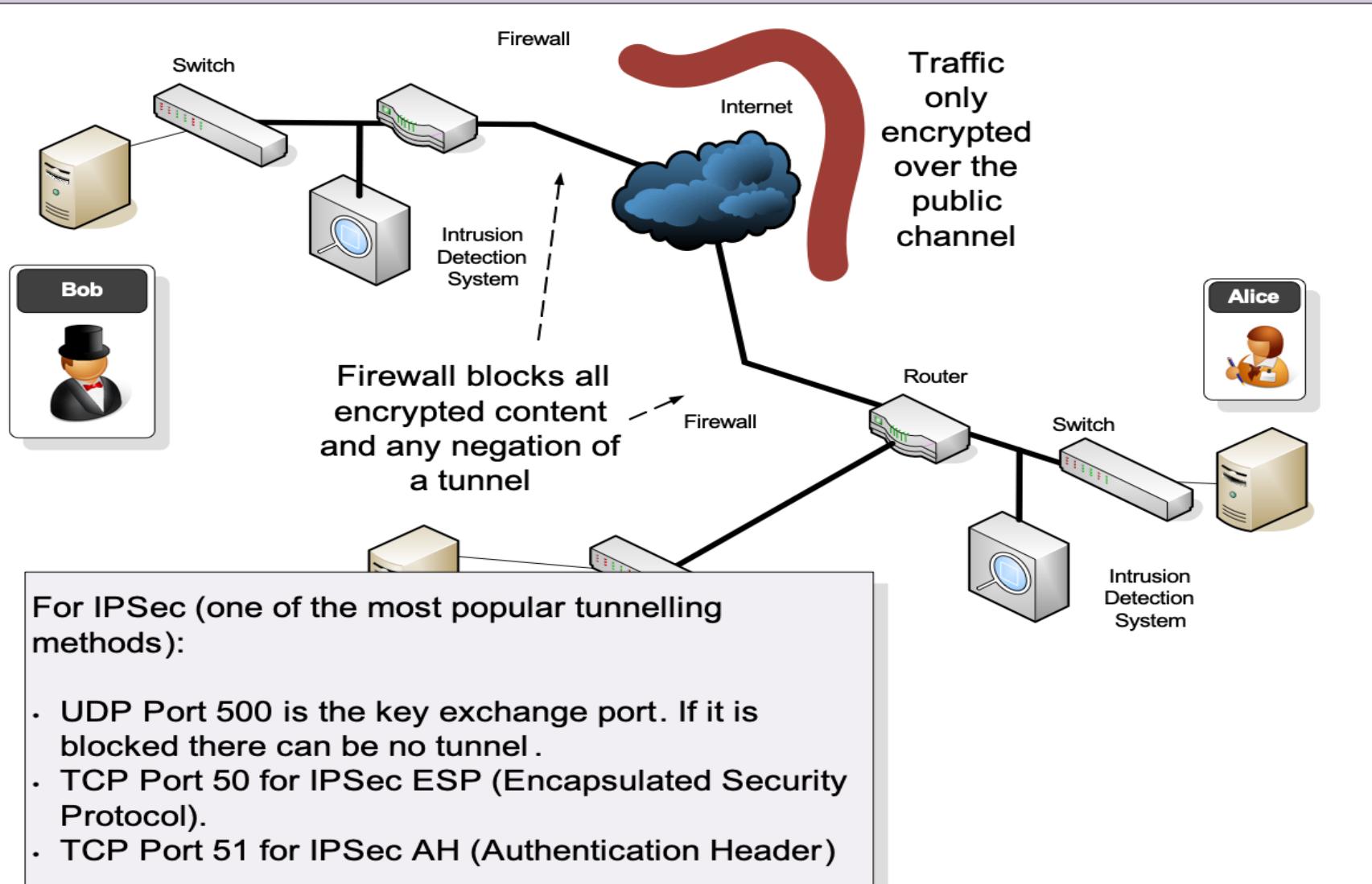
PPTP (Point-to-point Tunneling Protocol). Created by Microsoft and is routable. It uses MPPE (Microsoft Point-to-point Encryption) and user authentication.

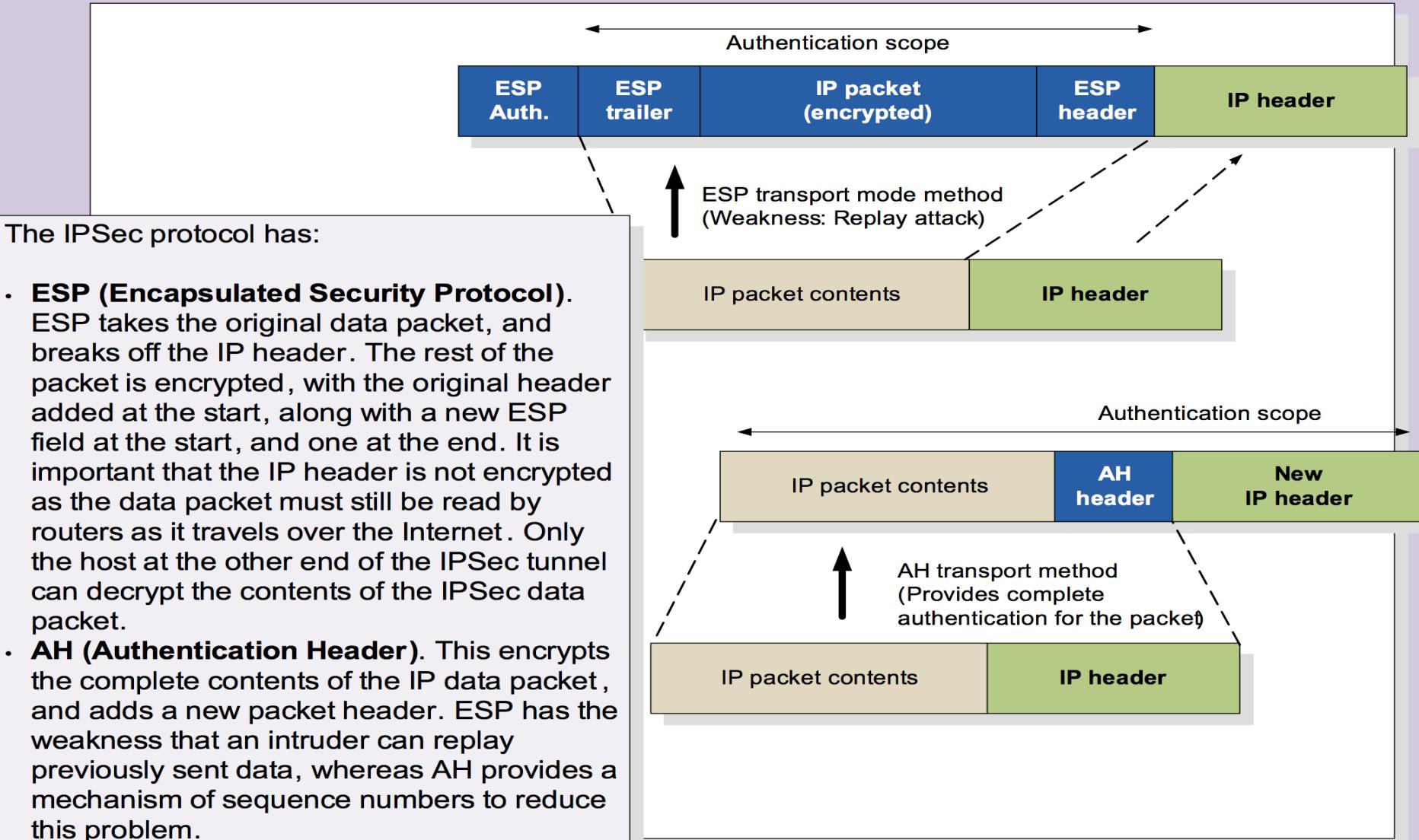
L2TP (Layer 2 Tunneling Protocol). Works at Layer 2 to Forward IP, IPX and AppleTalk (RFC2661). Cisco, Microsoft, Ascent and 3Com developed it. User and machine authentication, but no encryption (but can be used with L2TP over IPSec).

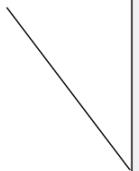
IPSec. An open standard. Includes both encryption and Authentication.

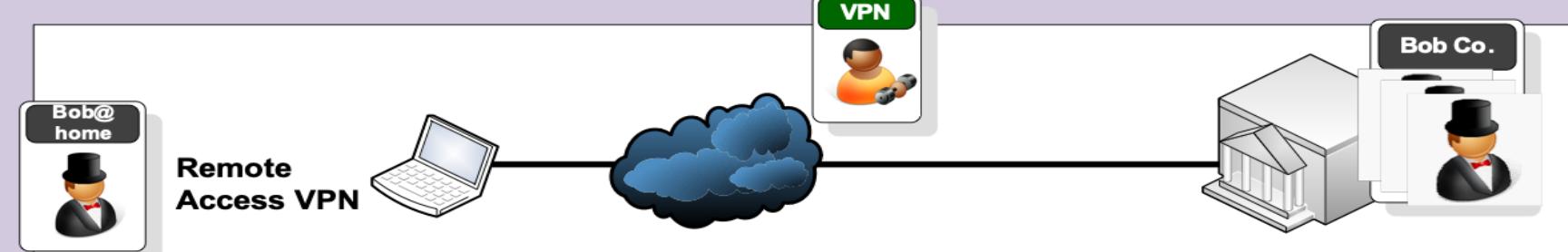








- 
- 1 ICMP Internet Control Message [RFC792]
 - 6 TCP Transmission Control [RFC793]
 - 8 EGP Exterior Gateway Protocol [RFC888]
 - 9 IGP any private interior gateway [IANA]
 - 47 GRE General Routing Encapsulation (PPTP)**
 - 50 ESP Encap Security Payload [RFC2406]**
 - 51 AH Authentication Header [RFC2402]**
 - 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 ABCDEFDD 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

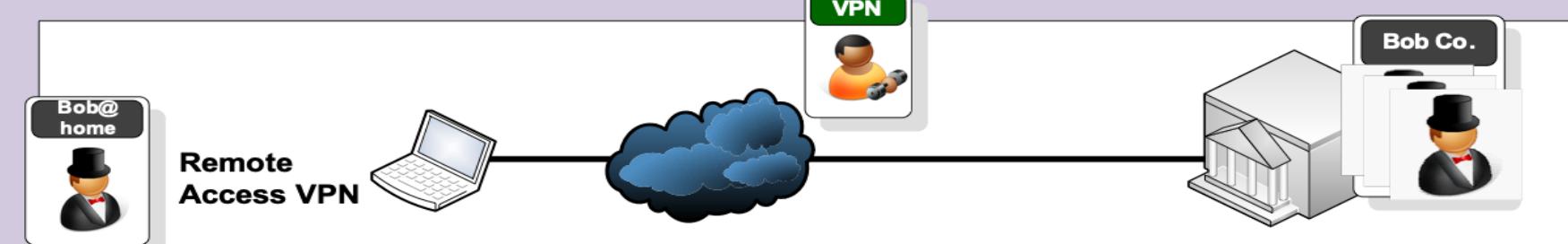
- AH, ESP (or both)
- Encryption (DES, 3DES)
- ESP (tunnel or transport)
- Authentication (SHA/MD5)
- SA lifetimes defined
- Define the traffic of interest

```
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

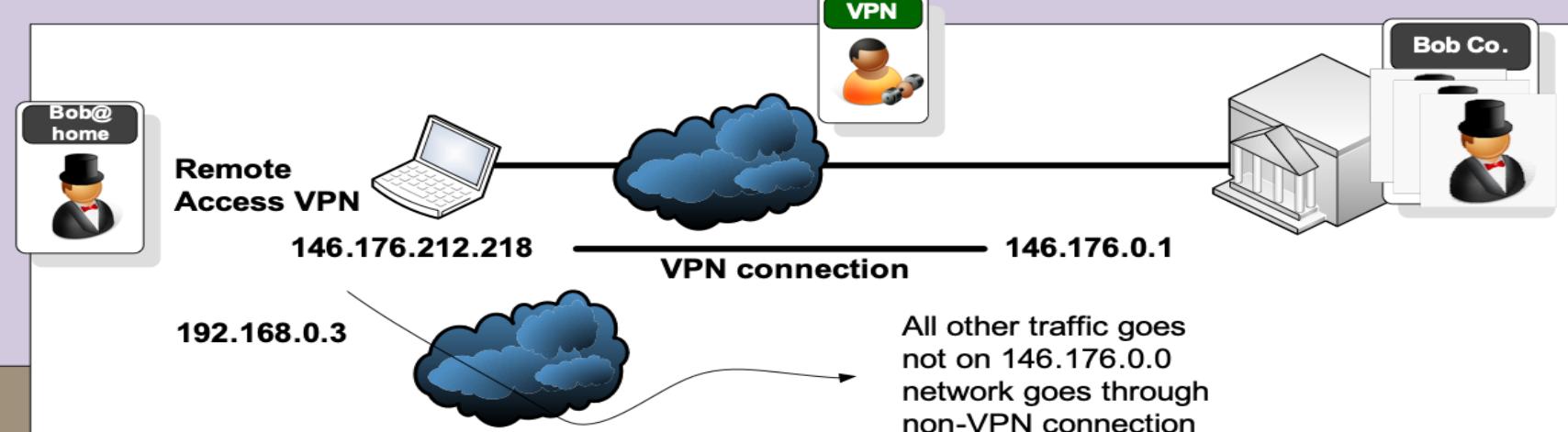
```
=====
Interface List
21 ...00 05 9a 3c 78 00 .... Cisco Systems VPN Adapter
10 ...00 1d 09 3f 49 8d .... Broadcom NetLink (TM) Fast Ethernet
 7 ...00 1f 3c 4f 30 1d .... Intel(R) PRO/Wireless 3945ABG Network Connectio
 1 ..... Software Loopback Interface 1
=====
```

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
=====
```

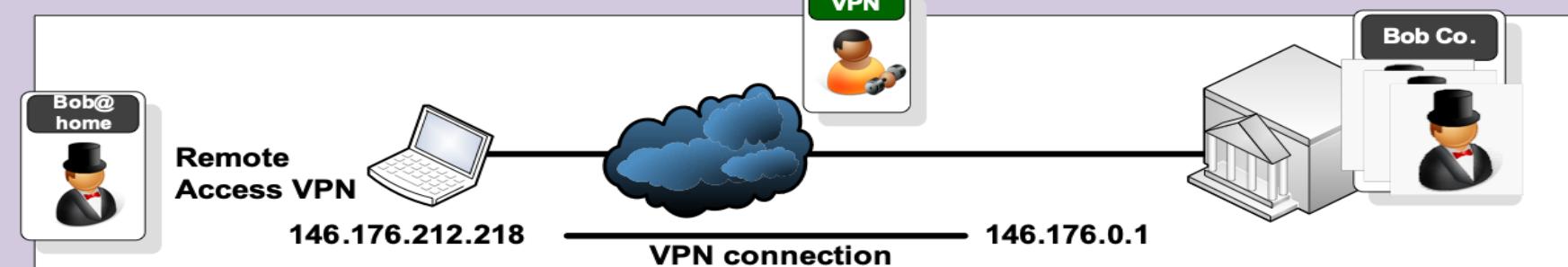
Persist

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
```

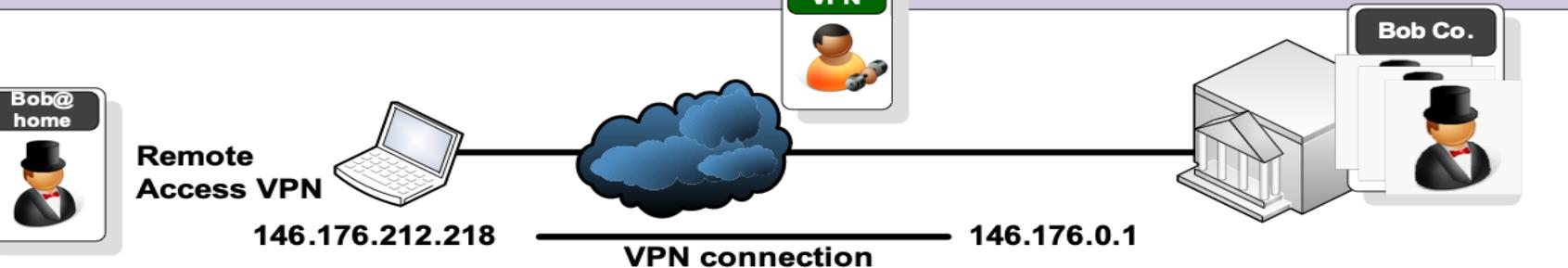
Before VPN connection

```
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

Tunnelling

Scanners
SSL/TLS
VPN/IPSec

Prof Bill Buchanan OBE

<http://asecuritysite.com/tunnelling>

