

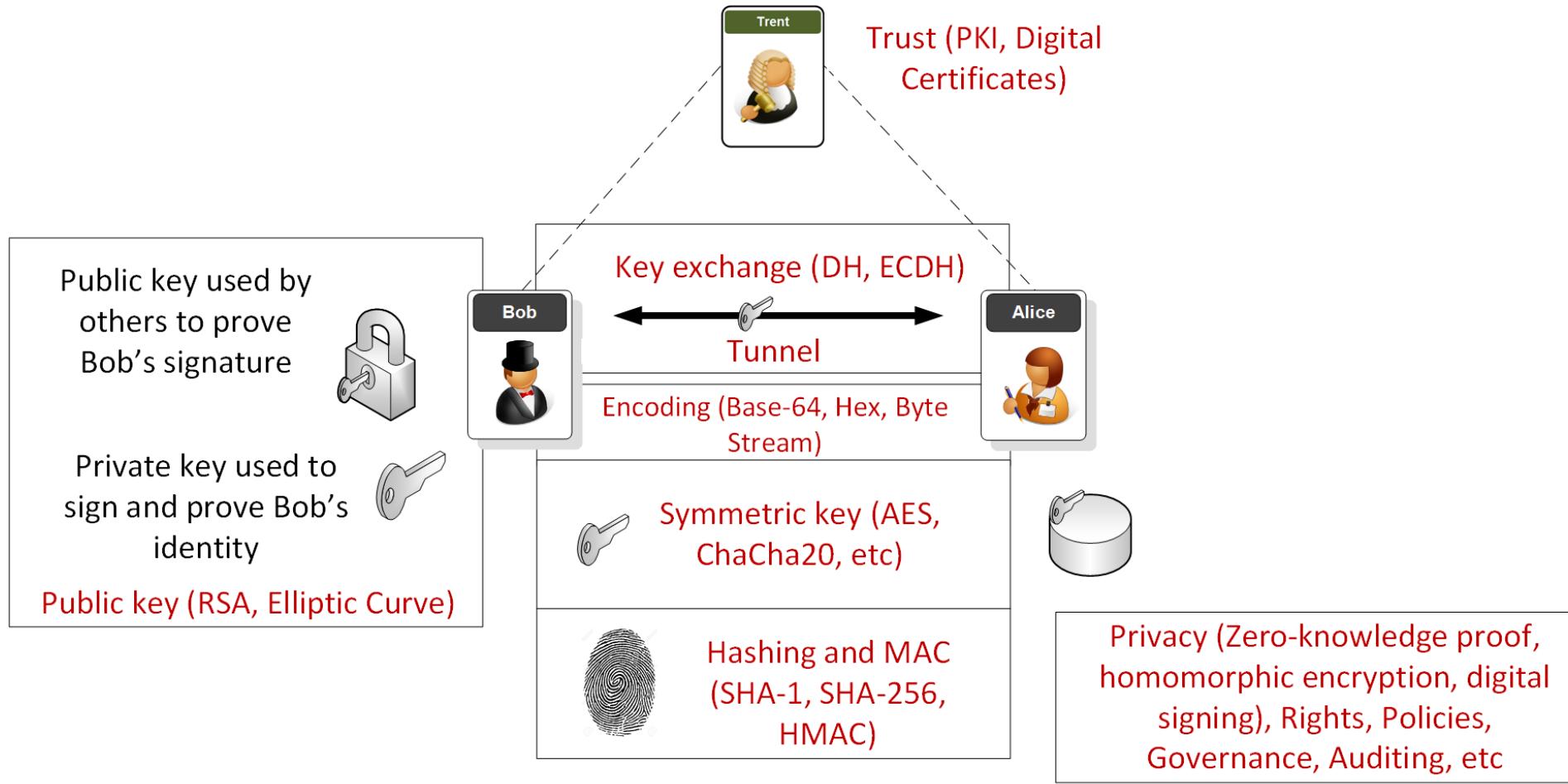
Tunnelling

Basics.
TLS.
VPNs.

Prof Bill Buchanan OBE
<https://asecuritysite.com/tunnelling>



Overview



Scan your site now

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.citor.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
dwpocrantherapi-te...	A
dev.hamiltonapps.r...	A+

Hall of Shame

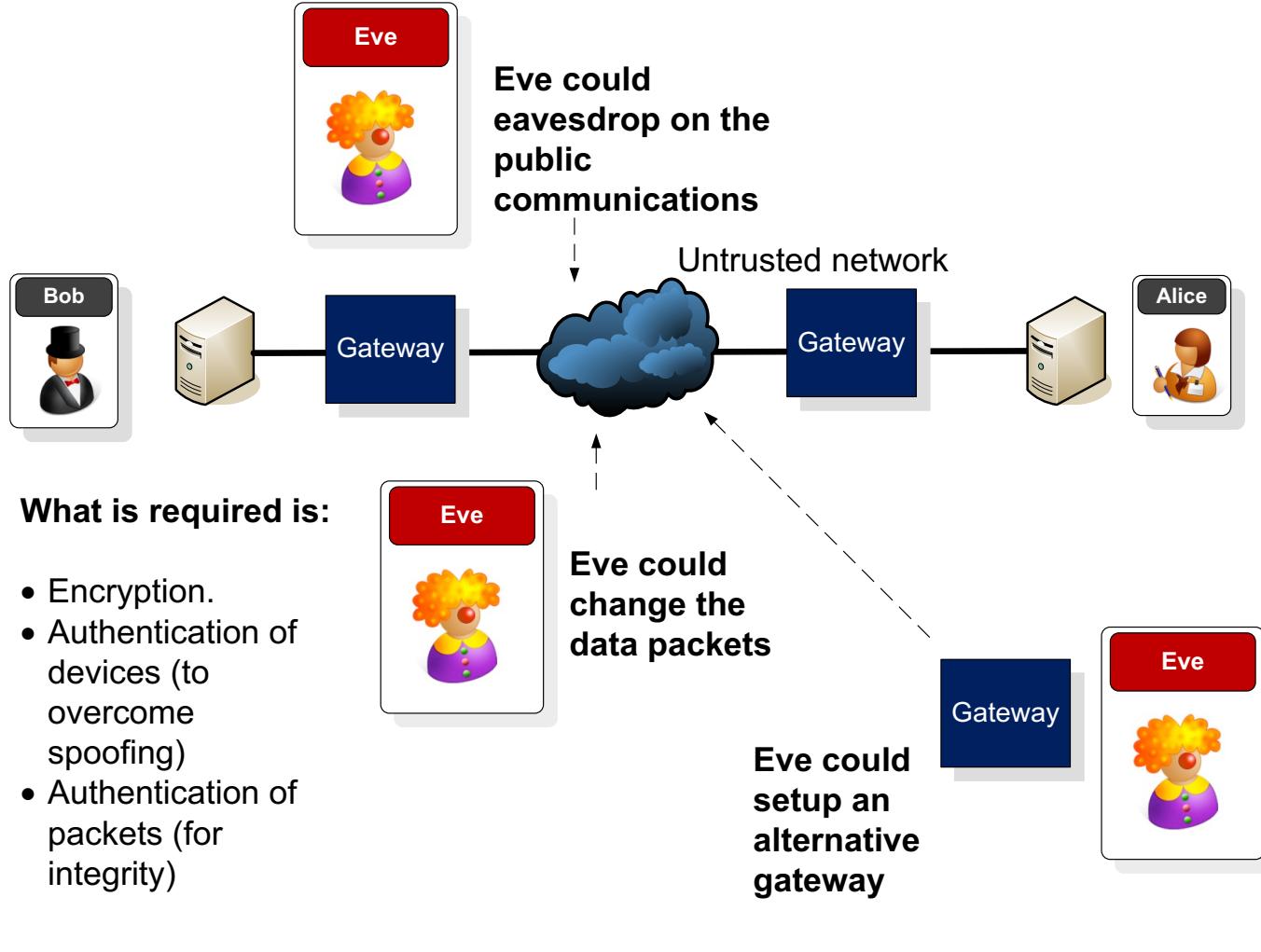
lifar.citor.se	F
content-marketing-...	F
foxpd.bestwomepri....	F
deonath.com	F
www.ijamat.com	F
activatemomentum.c...	F
www.janter.co.nz	F
guardiansafetybarr...	F
www.finderguru.com	F

Tunnelling

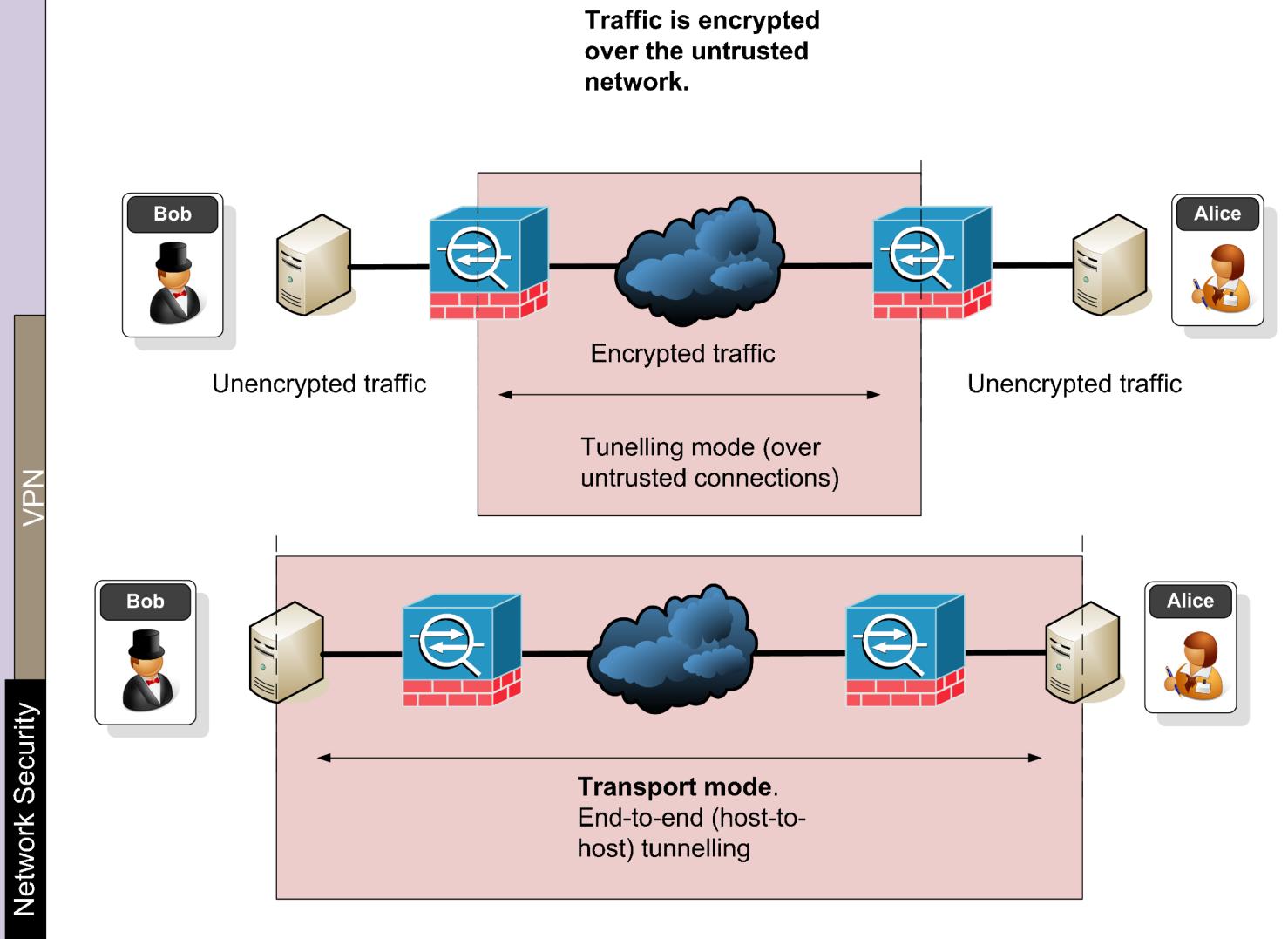
Basics.
TLS.
VPNs.

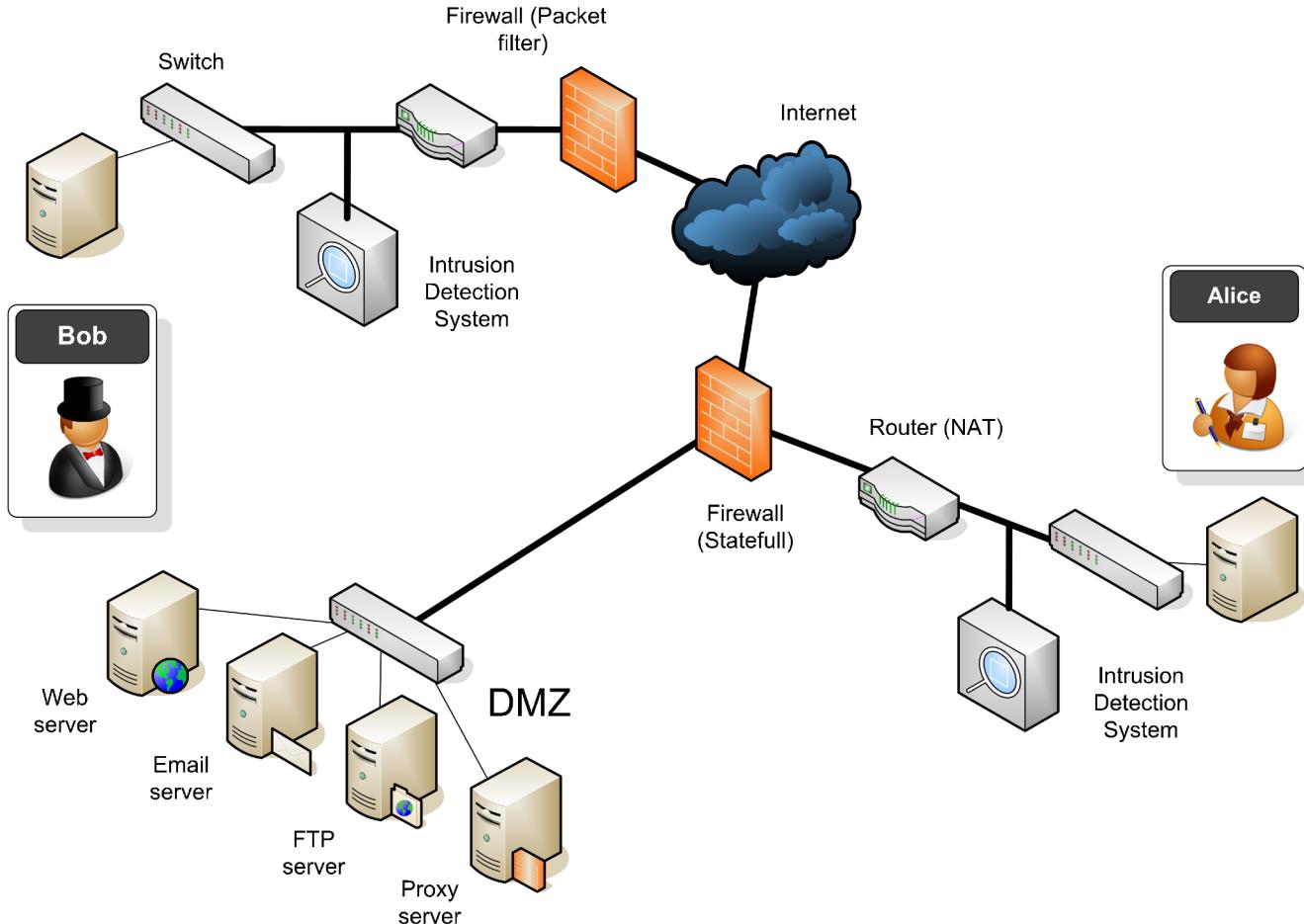
Prof Bill Buchanan OBE
<https://asecuritysite.com/tunnelling>

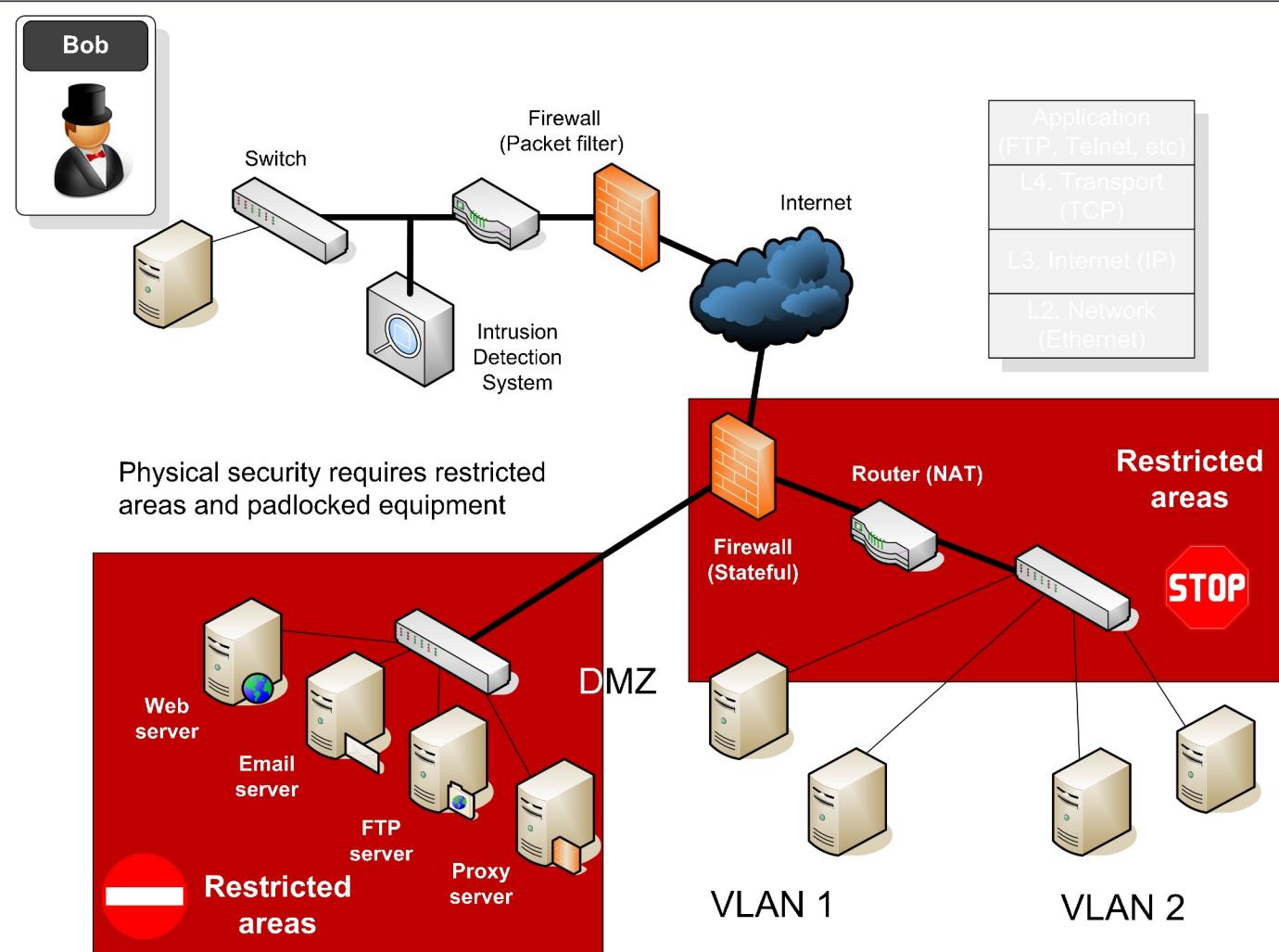


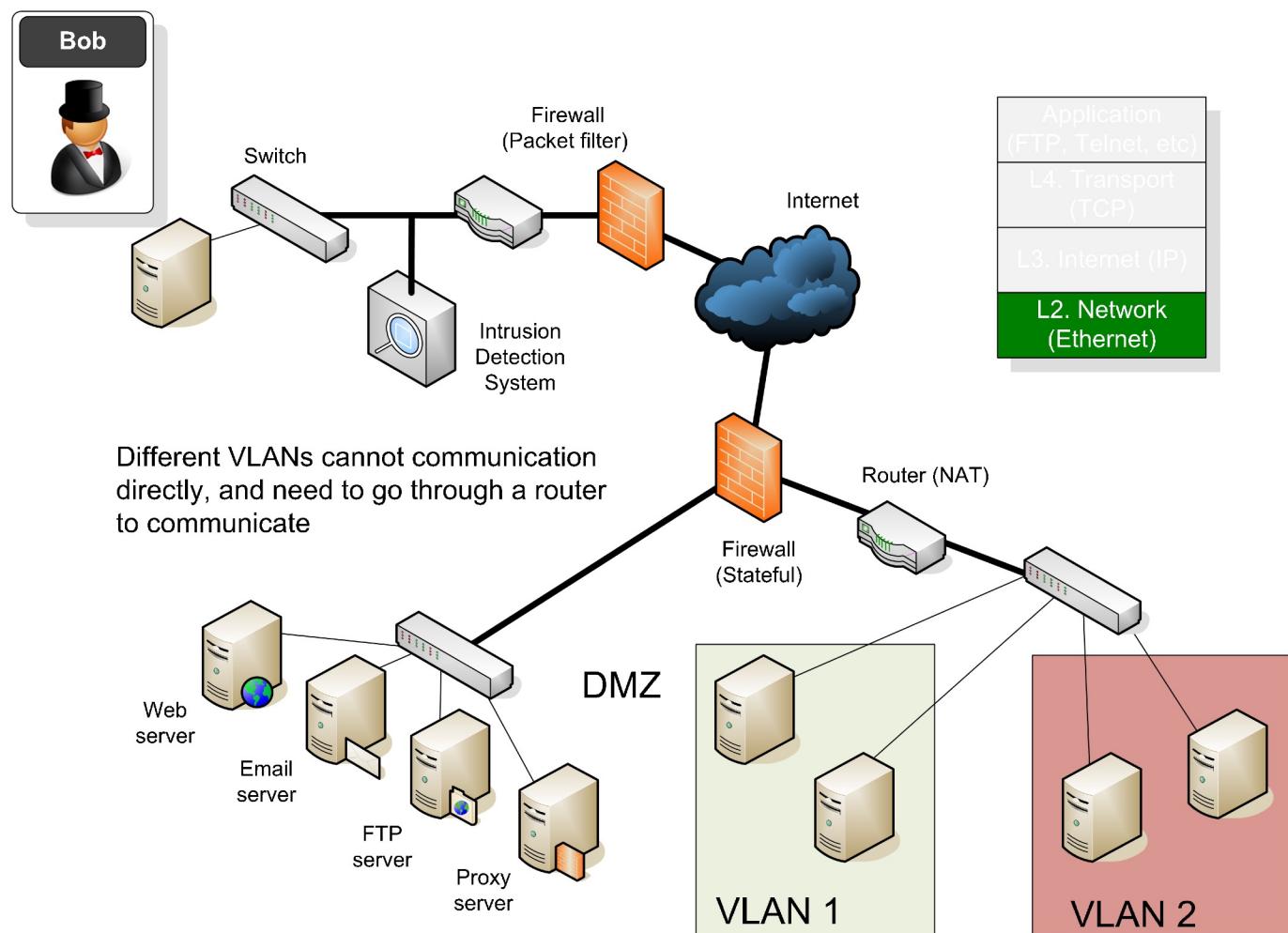


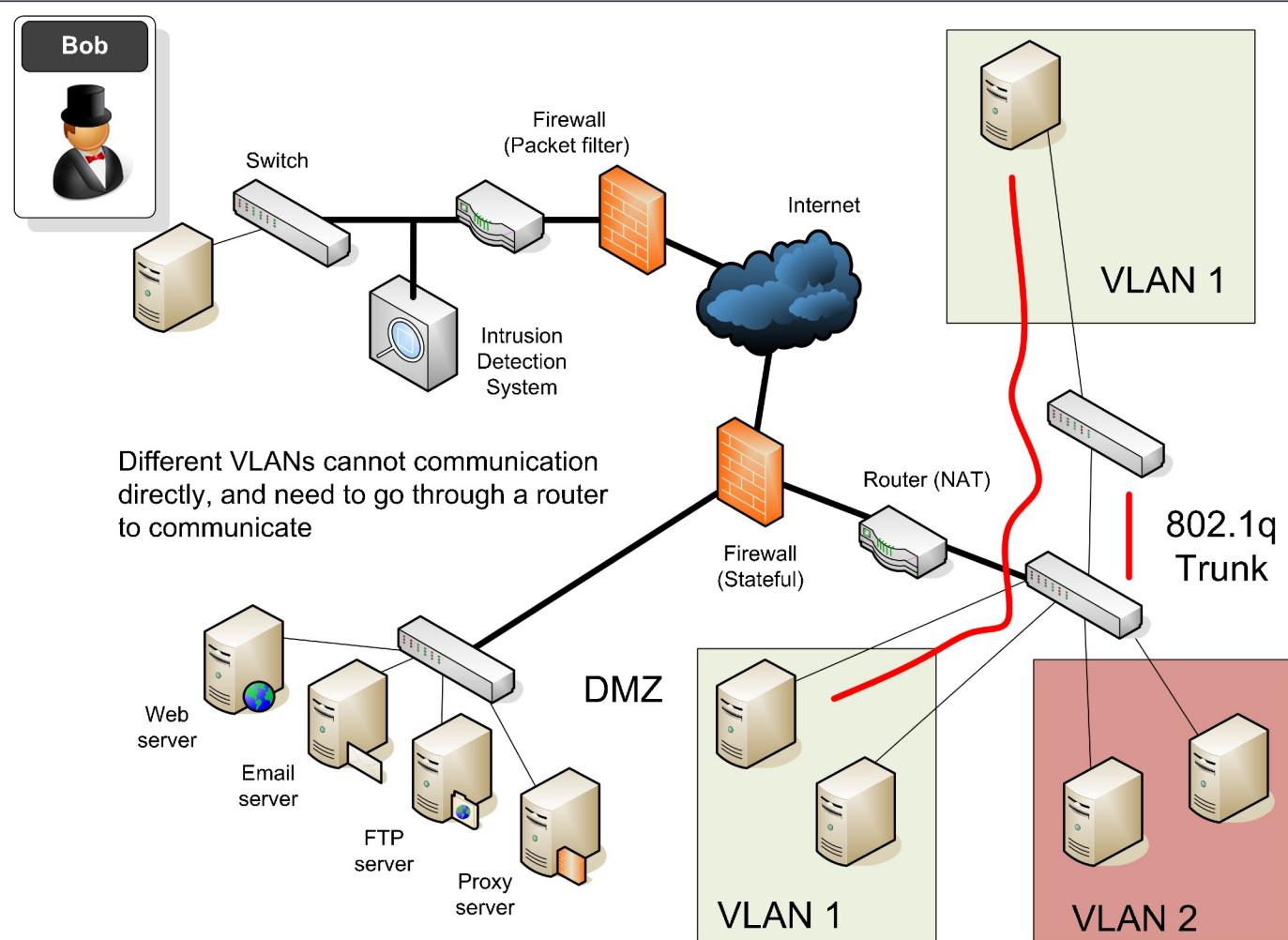
Network Security

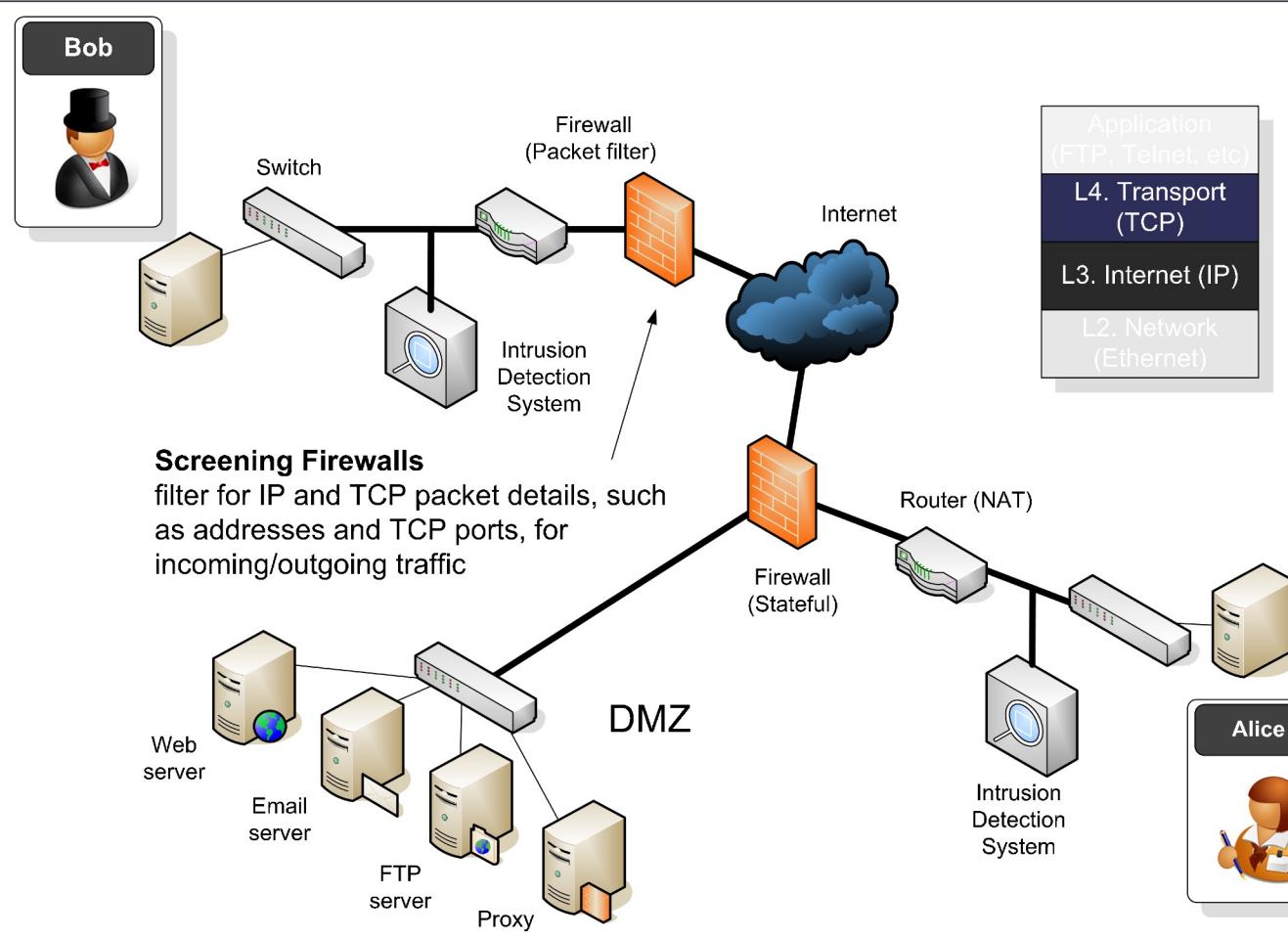


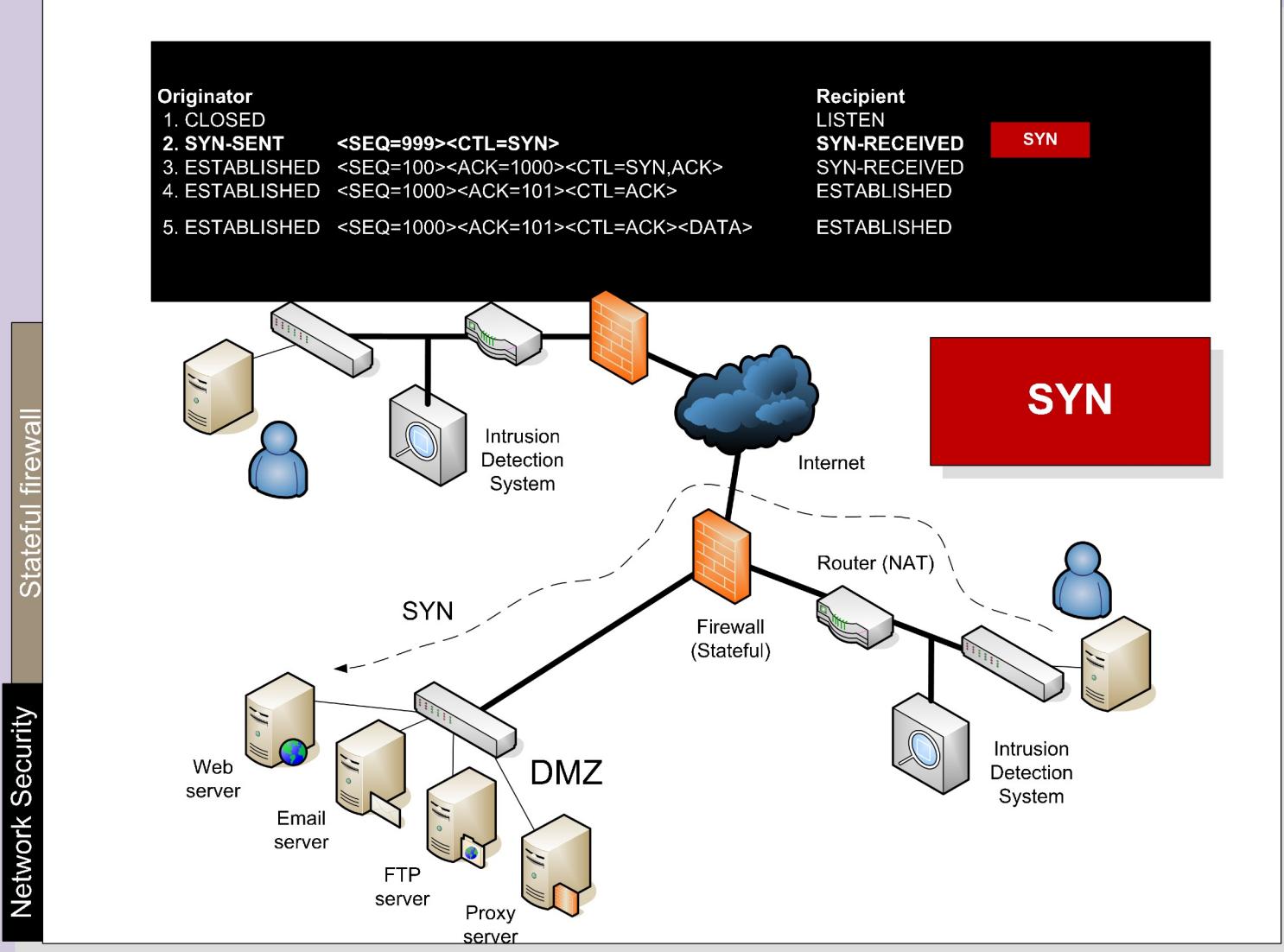


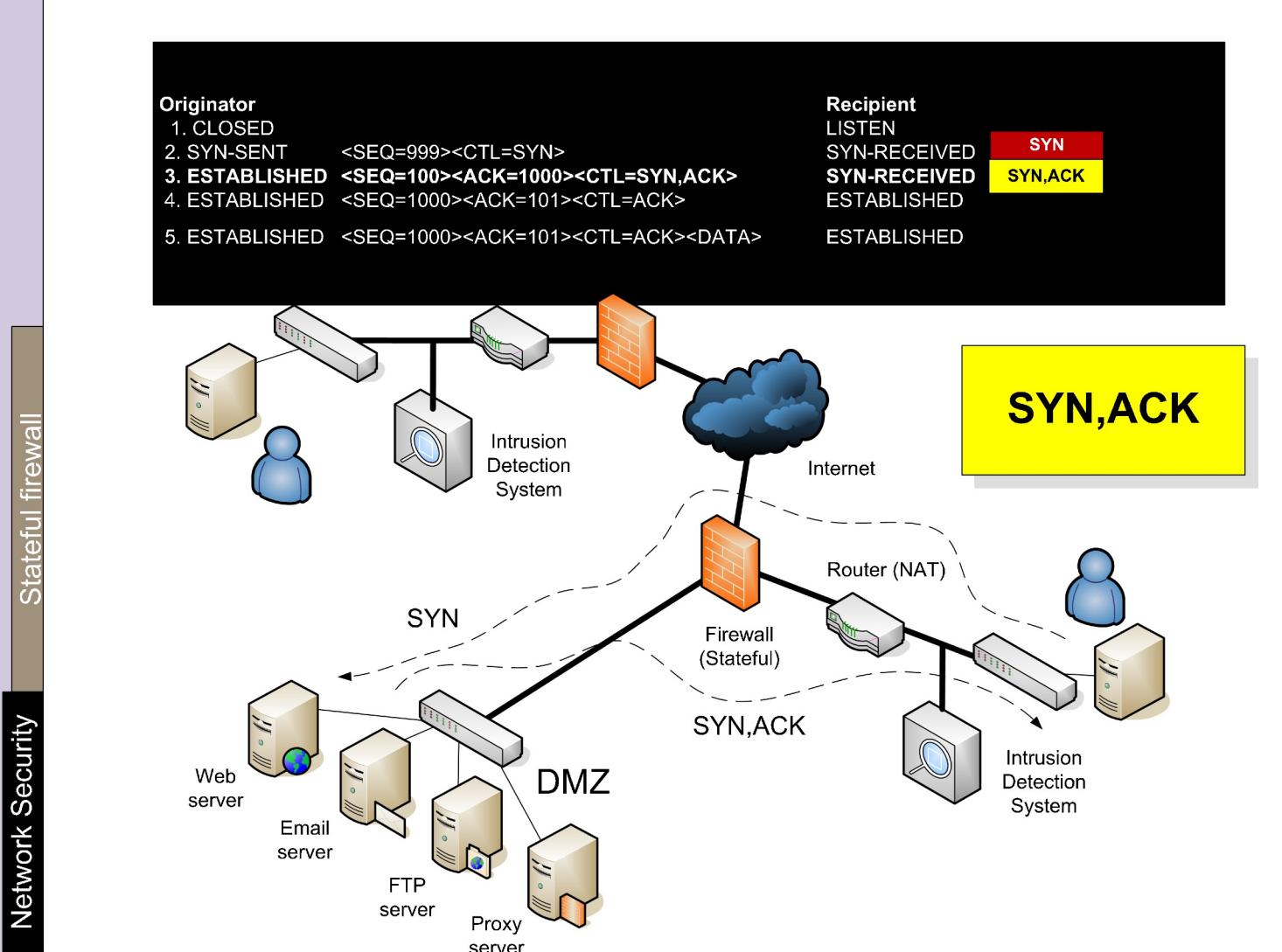


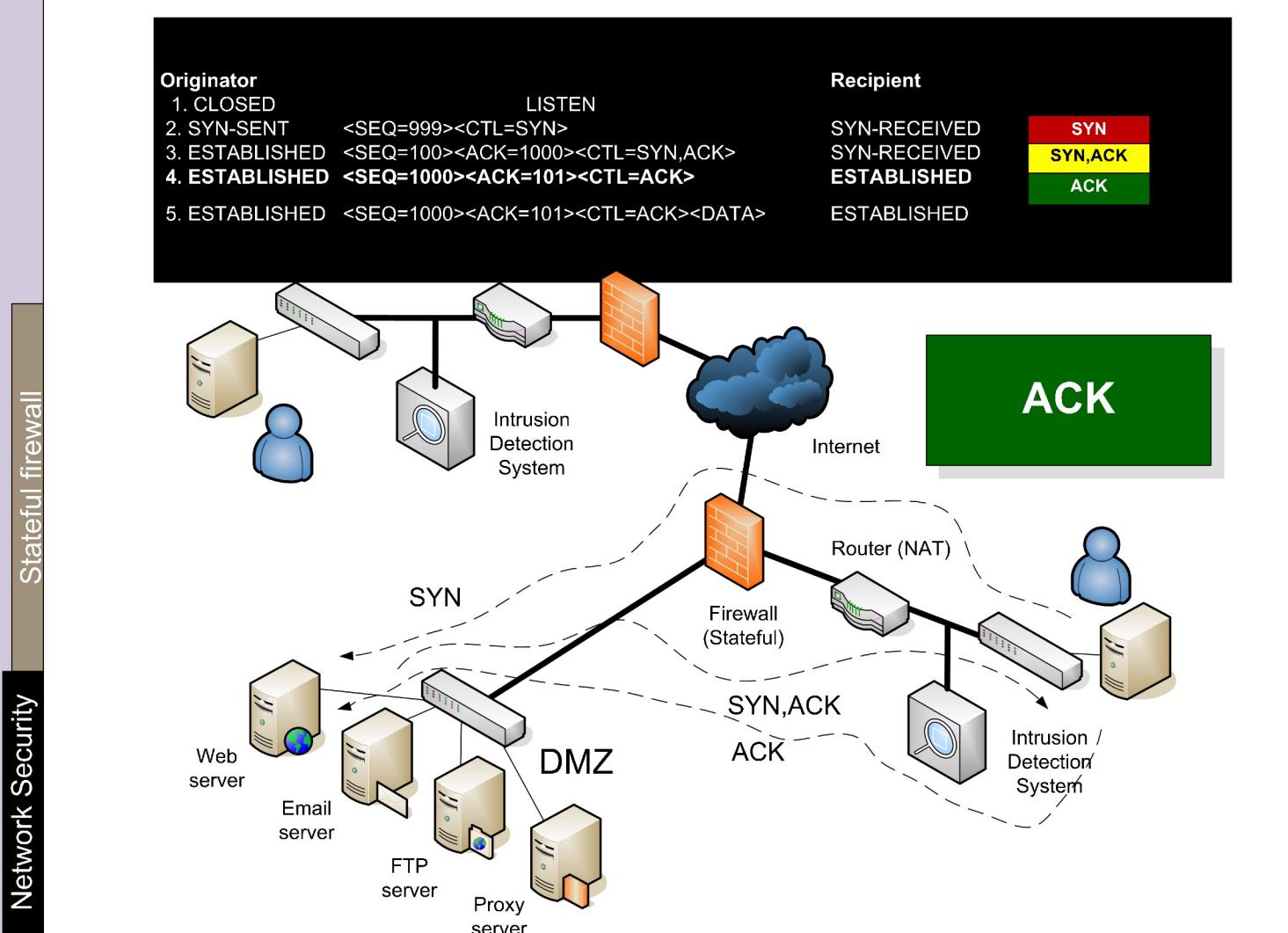












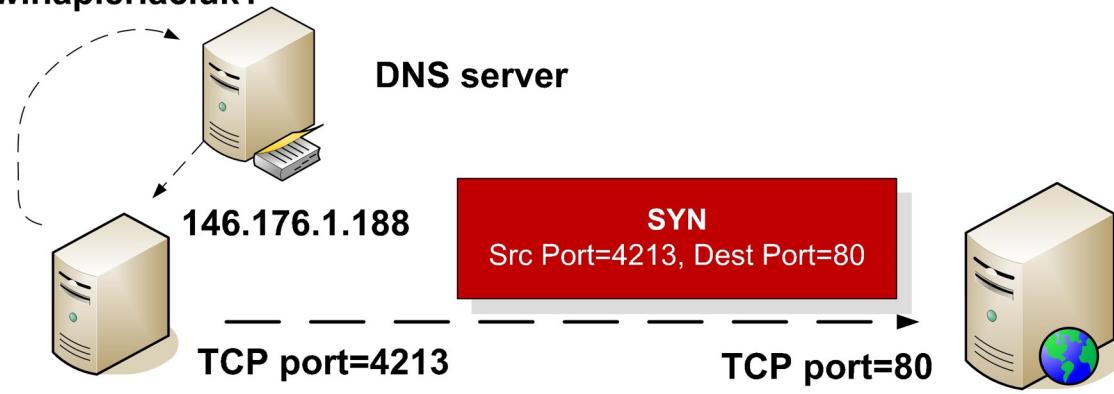
68	9.980194	192.168.1.101	resolver2.srv.pol.	DNS	Standard query PTR 255.1.168.192.in-addr.arpa
69	10.005697	resolver2.srv.pol.	192.168.1.101	DNS	Standard query response, No such name
70	14.477532	192.168.1.101	resolver2.srv.pol.	DNS	Standard query A www.napier.ac.uk
71	14.503727	resolver2.srv.pol.	192.168.1.101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

www.napier.ac.uk?

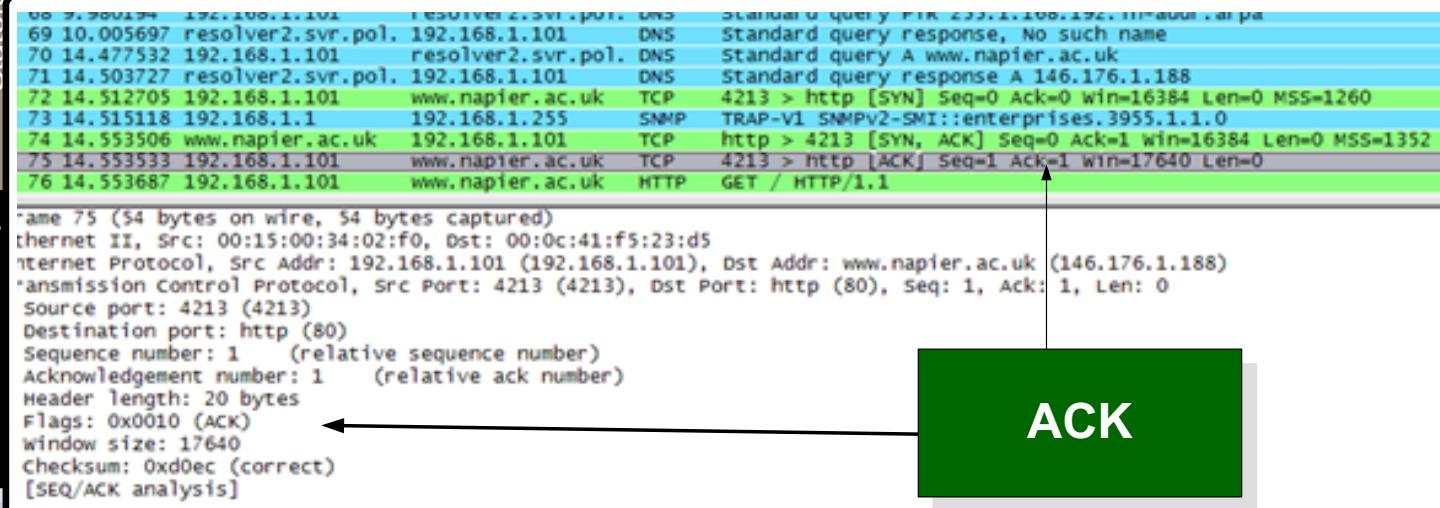
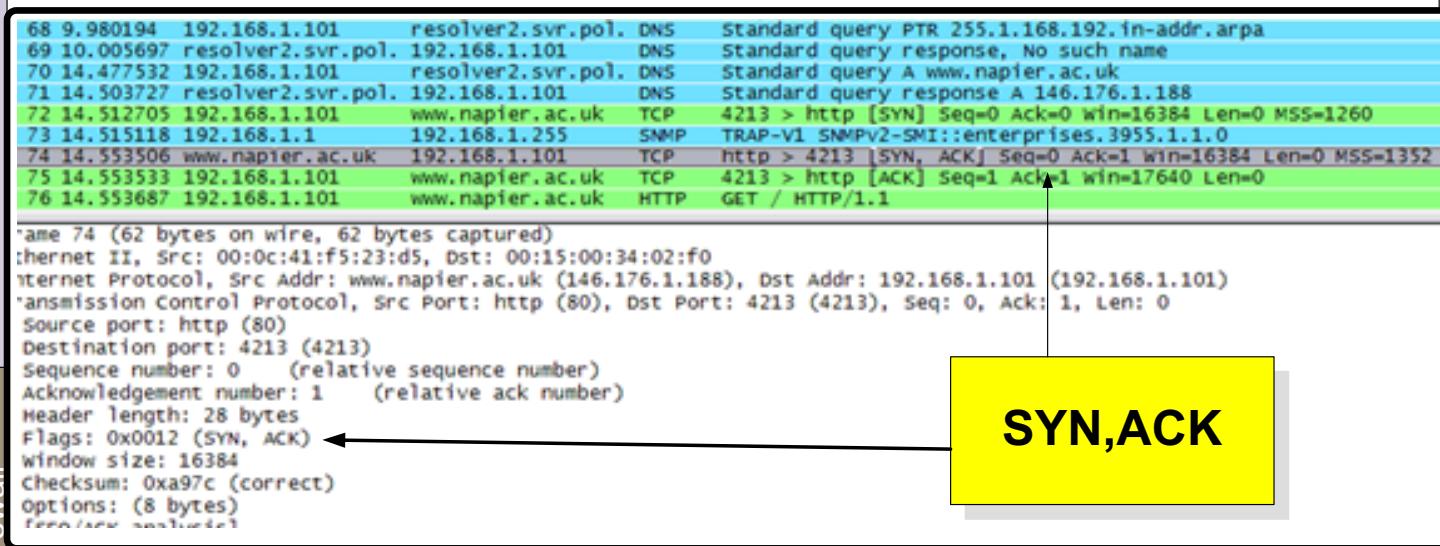


146.176.1.188

Client-server (SYN)

Network Security

Stateful firewall

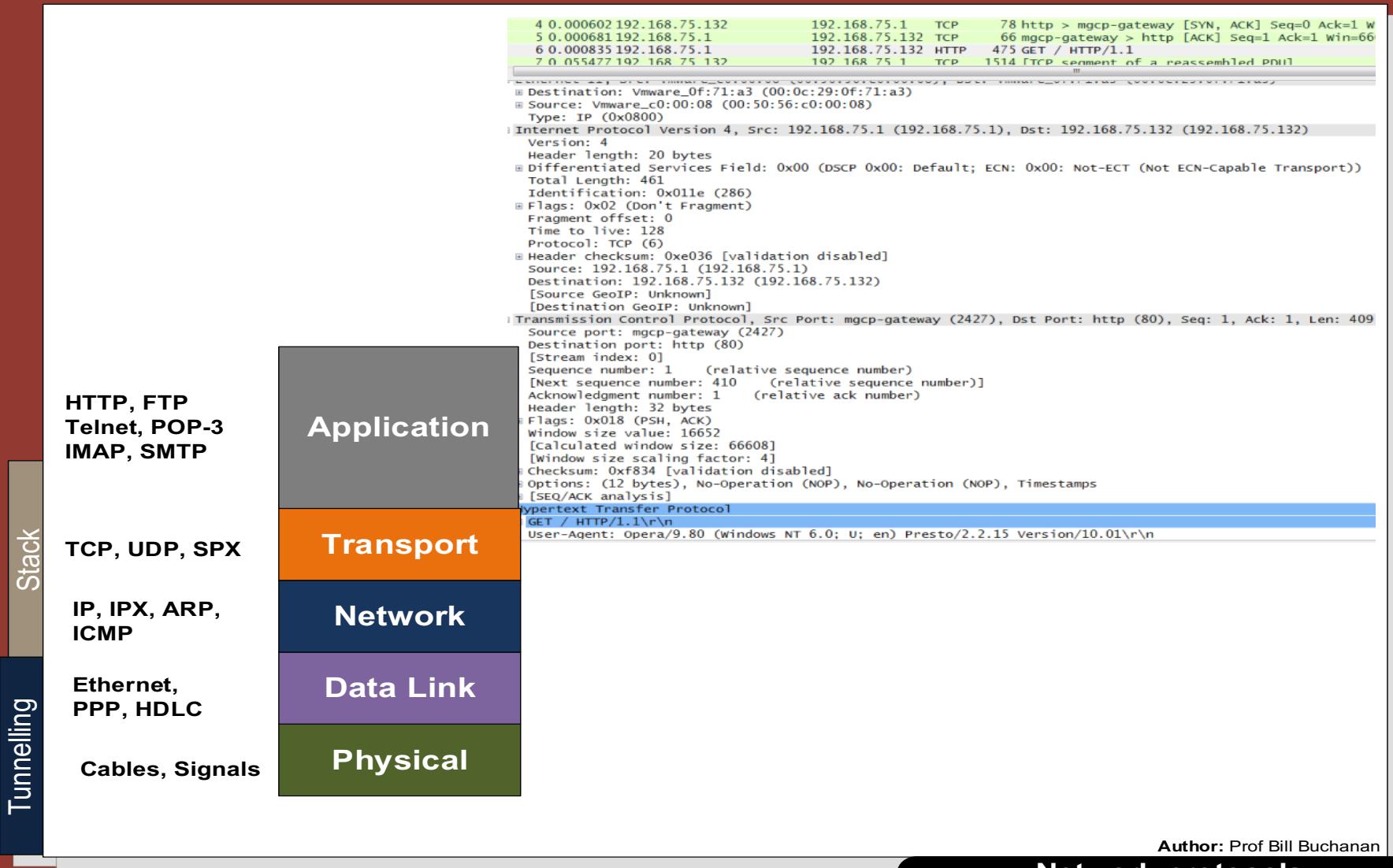


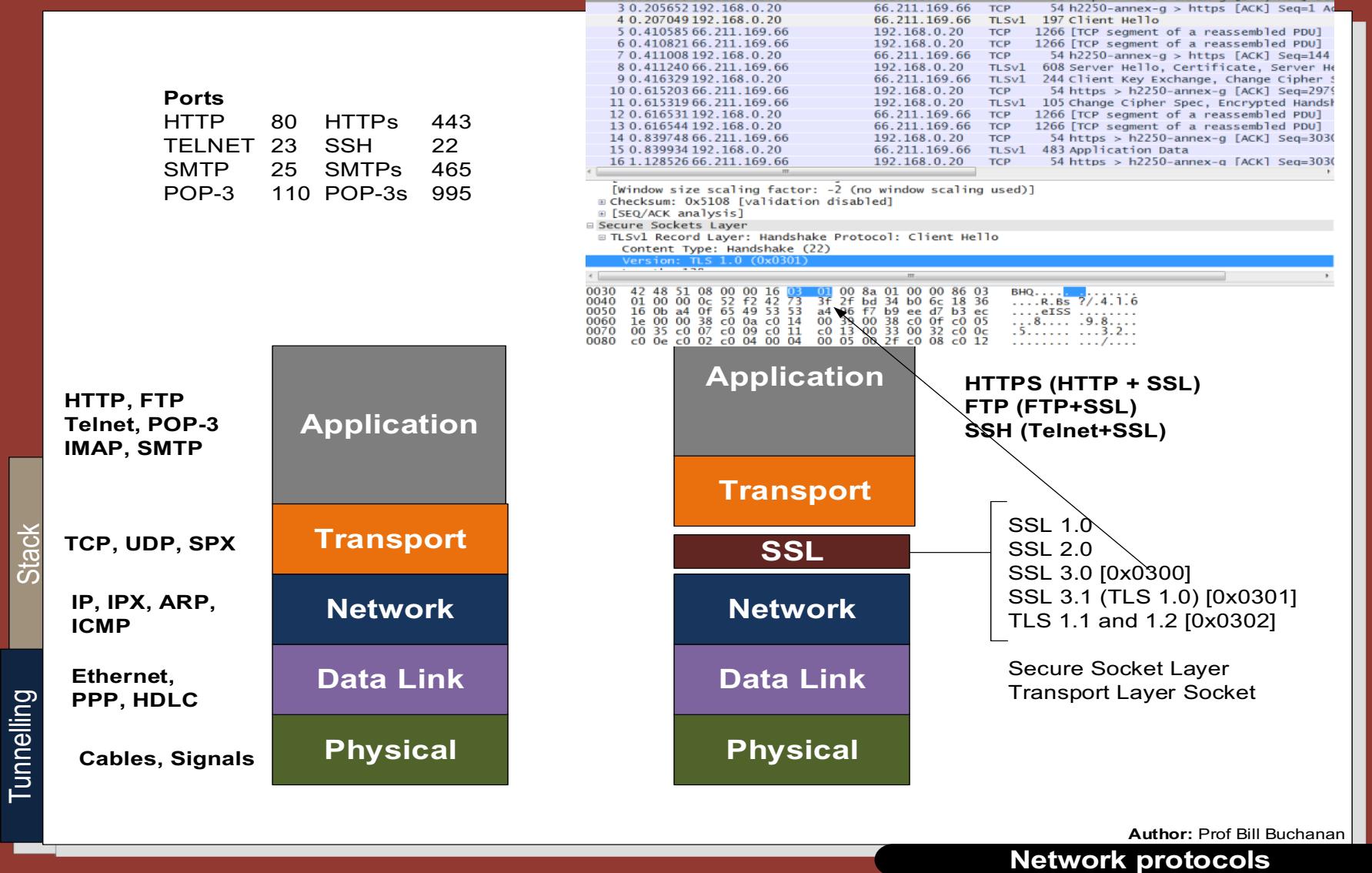
Tunnelling

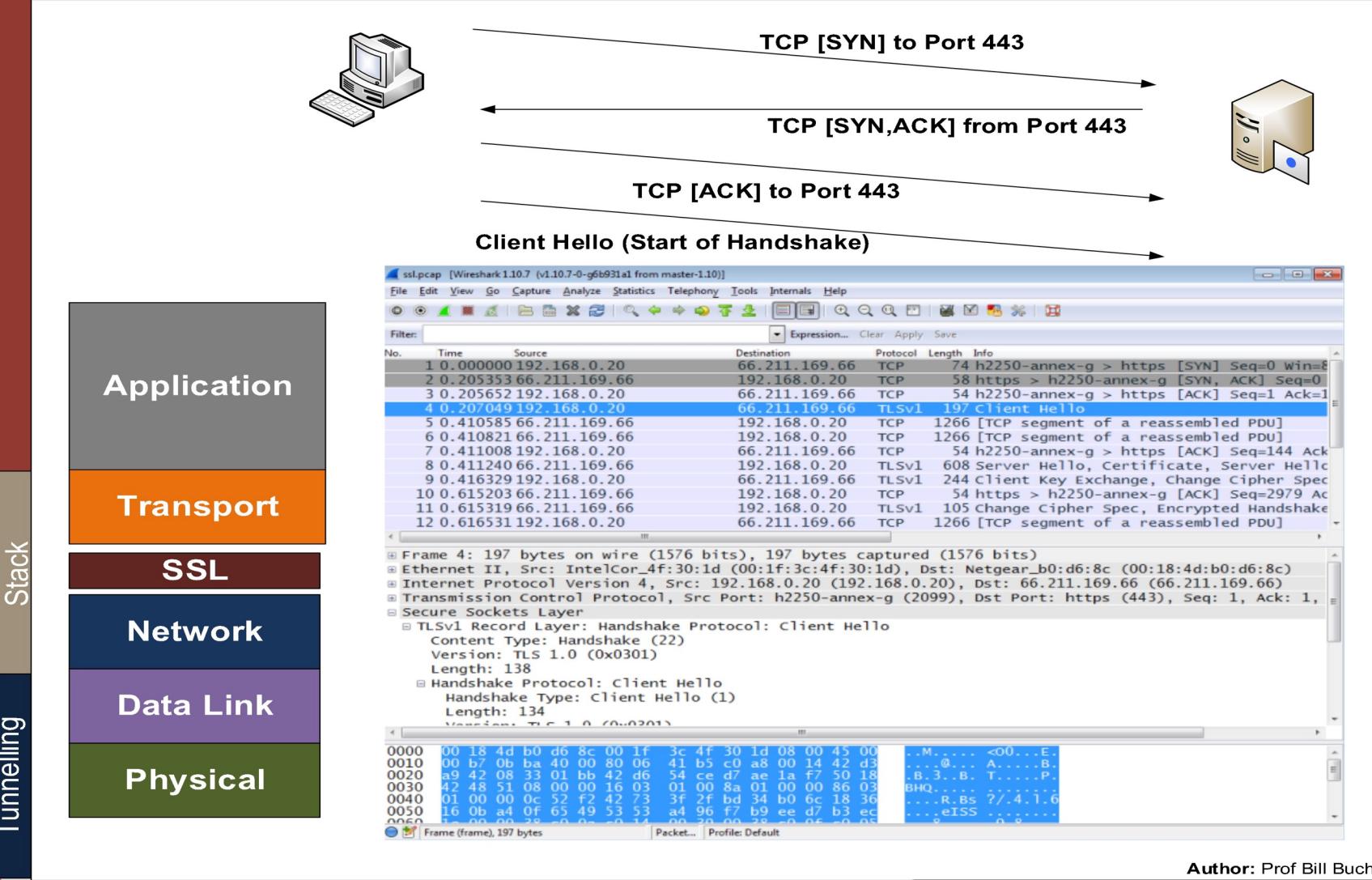
Basics.
TLS.
VPNs.

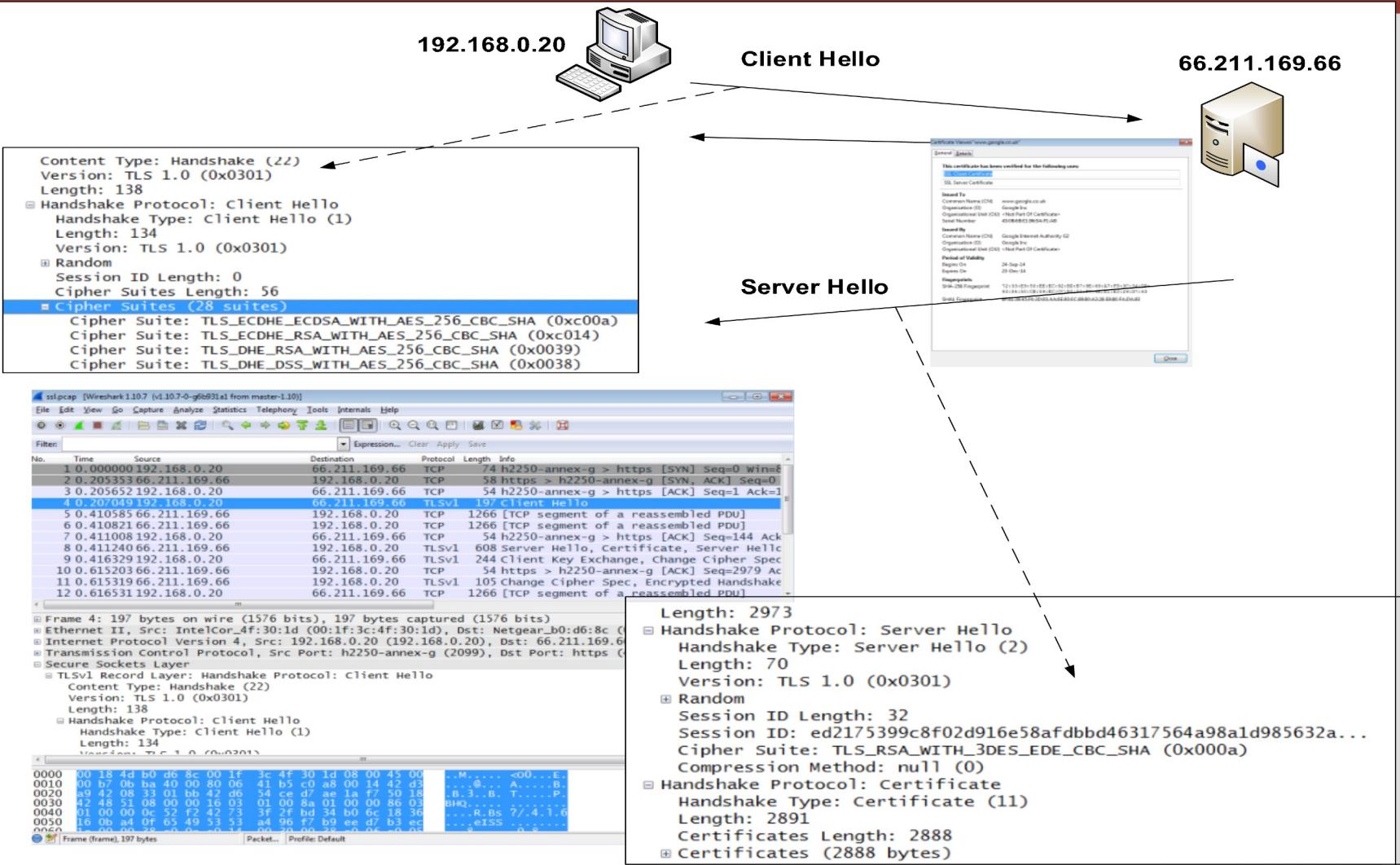
Prof Bill Buchanan OBE
<https://asecuritysite.com/tunnelling>



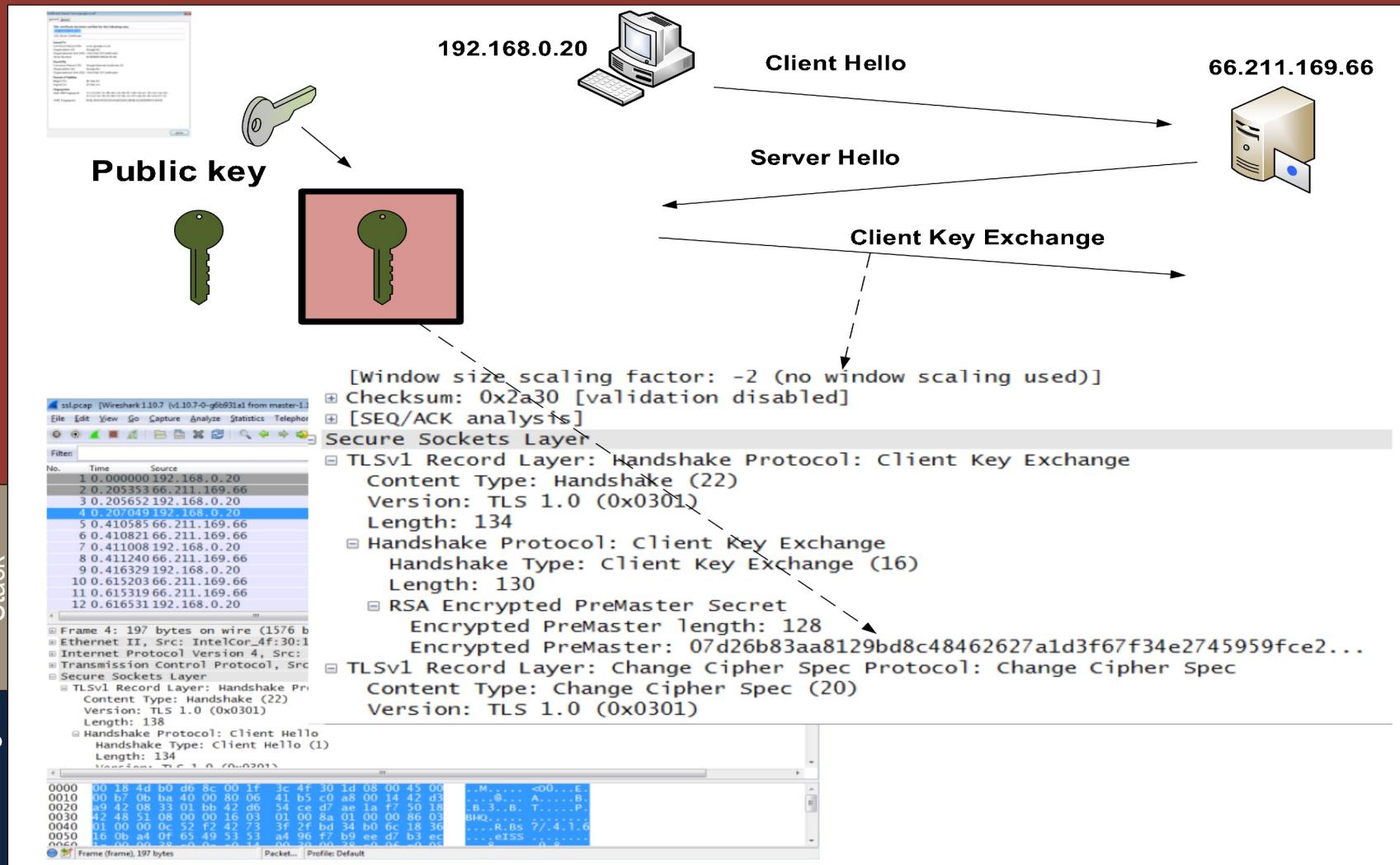








Tunnelling

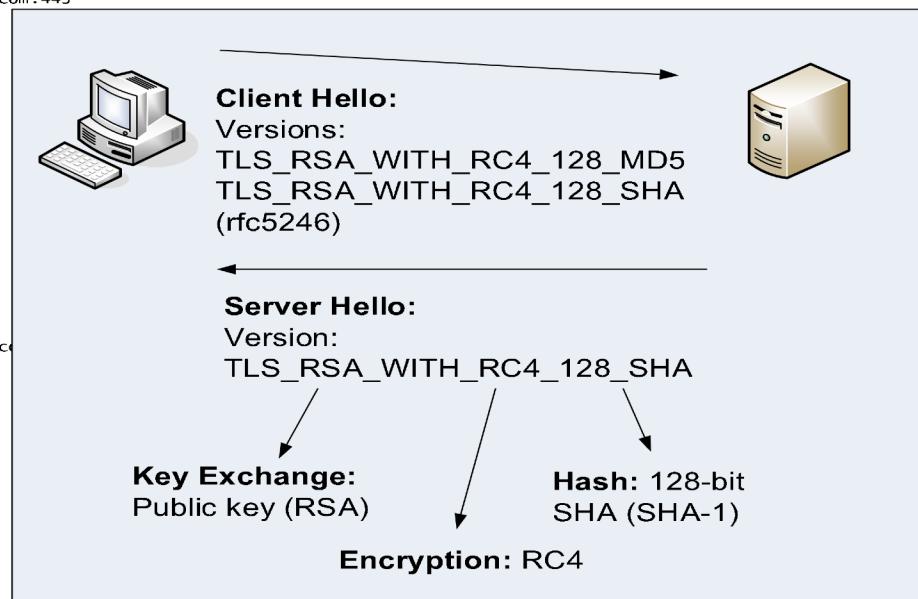


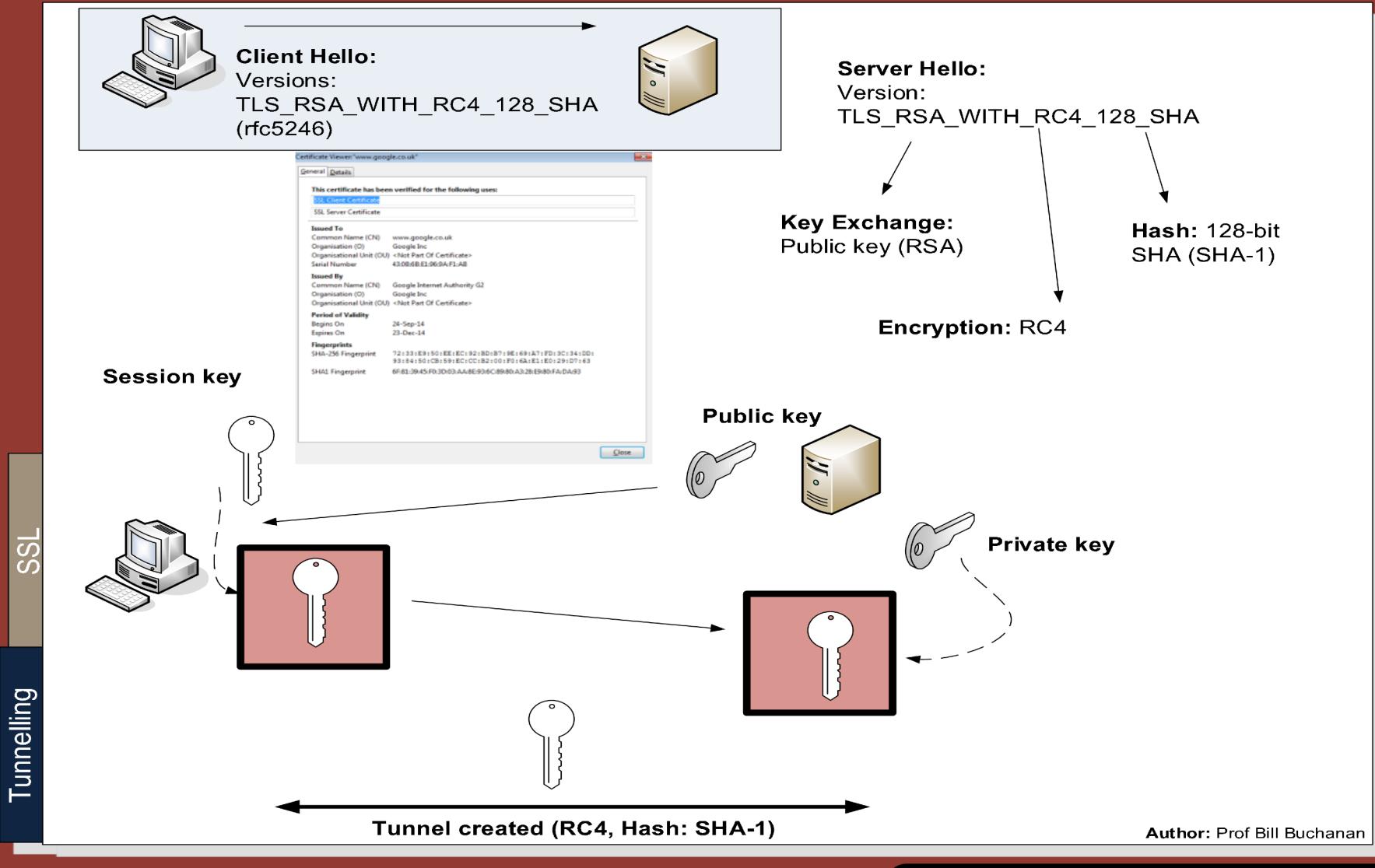
```

billbuchanan@bill$-MacBook-Pro:~$ 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-----
MIIEjdCCAc16gAwIBAgITTSvYALWn+akUwDQYJKoZIhvcNAQEFBQAwSTELMAkGA1UE
...
soX4i5L0D0jzyqKfjuIMGcFwdIETq0EpCmkhJfGNHjvdzc/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-Ag... : None
  PSK ident...: None
  PSK ident... 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.!..|..
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 20 fe b5 7f-6b 10 4e 7a f9 b5 b6 02 .....k.Nz..m.
0070 - 30 ec 07 e6 f0 c0 49 81-31 6b 30 f9 b0 d3 c4 25 0.....T.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)

```



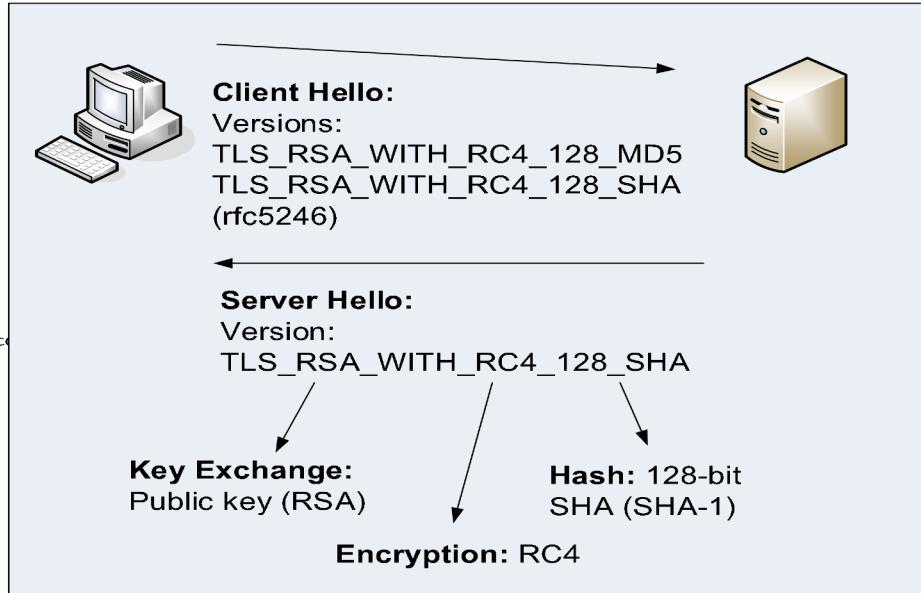


```

billbuchanan@bill$-MacBook-Pro:~$ 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-----
MIIEjdCCAc16gAwIBAgITTSvYALWN+akUwDQYJKoZIhvcNAQEFBQAwSTELMAkGA1UE
...
soX4i5L0D0jZYqKf/uImGcFwdIETq0EpCmkhJfgNHjVdzC/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-Ag... : None
PSK ident...: None
PSK ident... 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.....T.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)

```

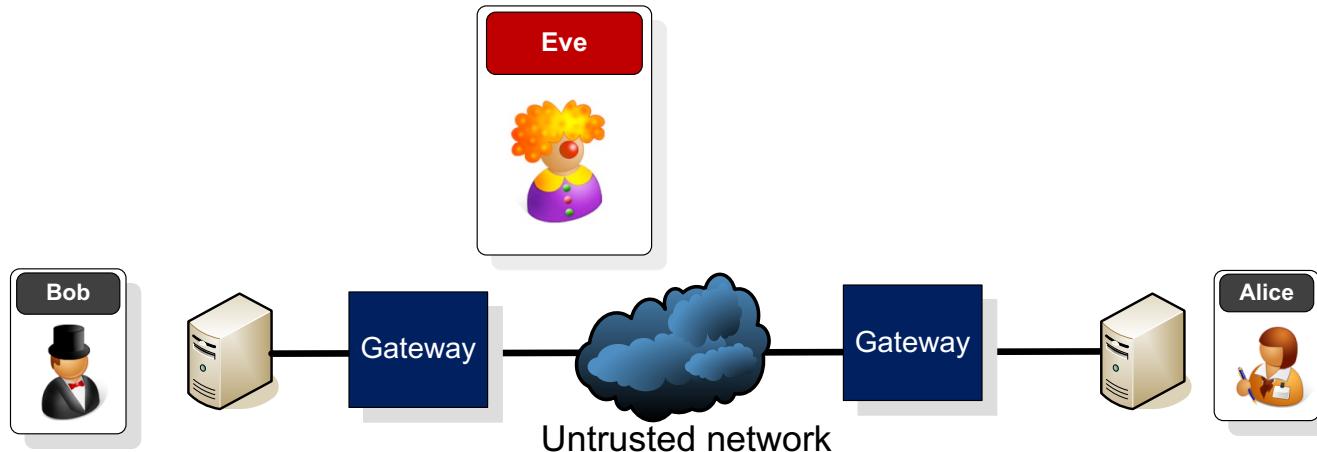


Tunnelling

Basics.
TLS.
VPNs.

Prof Bill Buchanan OBE
<https://asecuritysite.com/tunnelling>





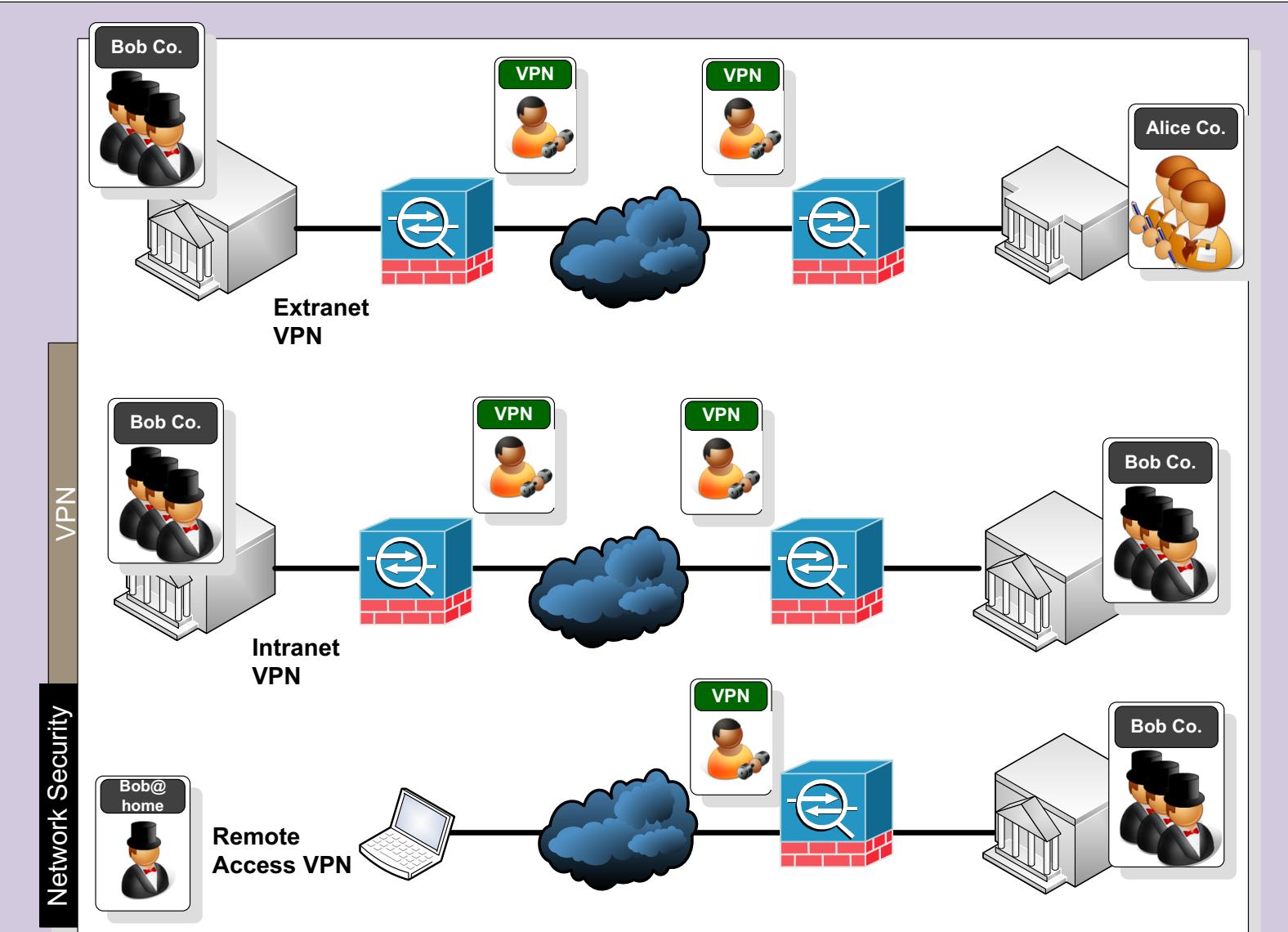
What is required is:

- 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.

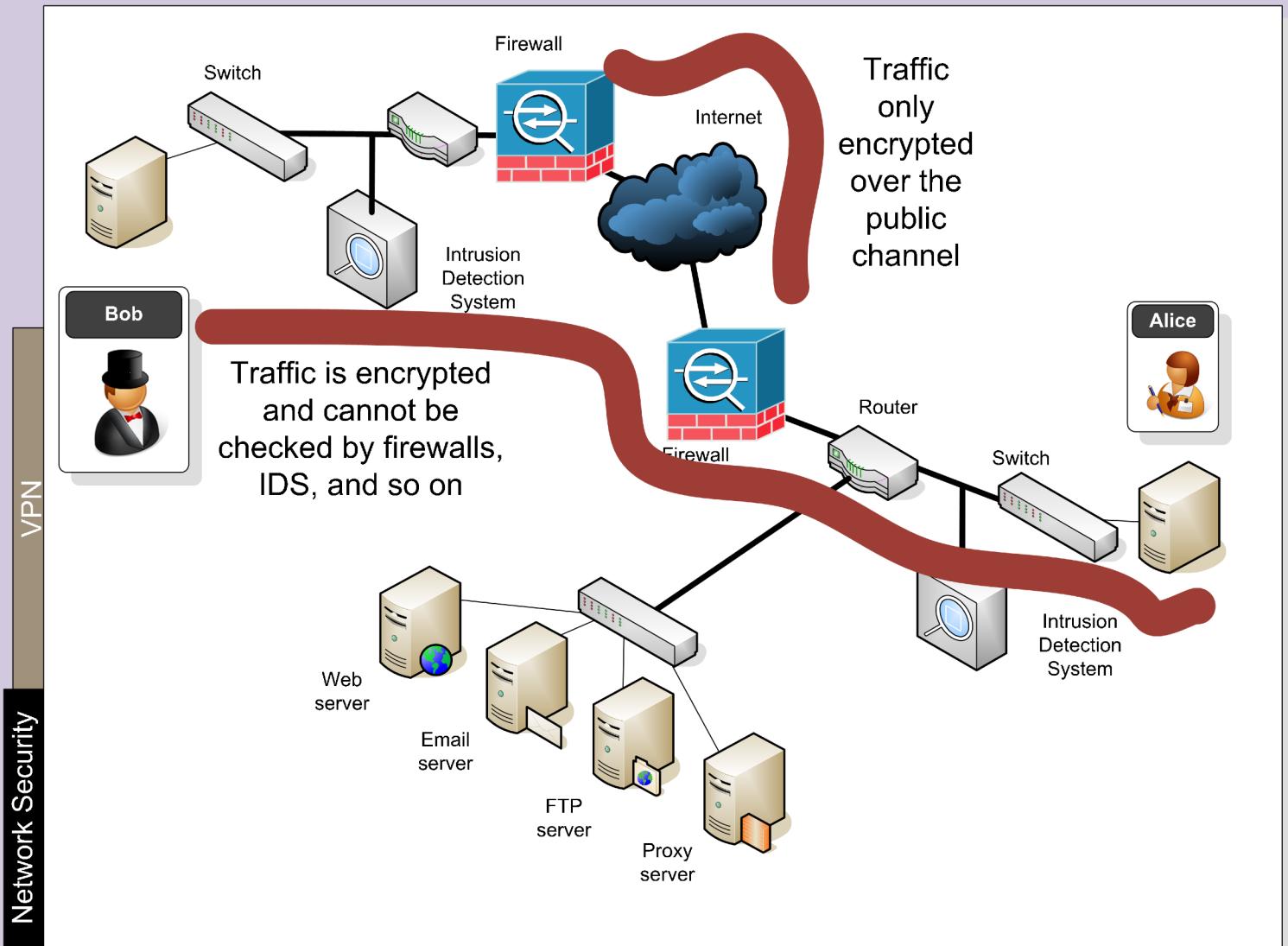
L2TP (Layer 2 Tunneling Protocol). Works at Layer 2 to Forward IP, IPX and AppleTalk (RFC2661). Cisco, Microsoft, Ascent and 3Com developed it. User and machine authentication, but no encryption (but can be used with L2TP over IPSec).

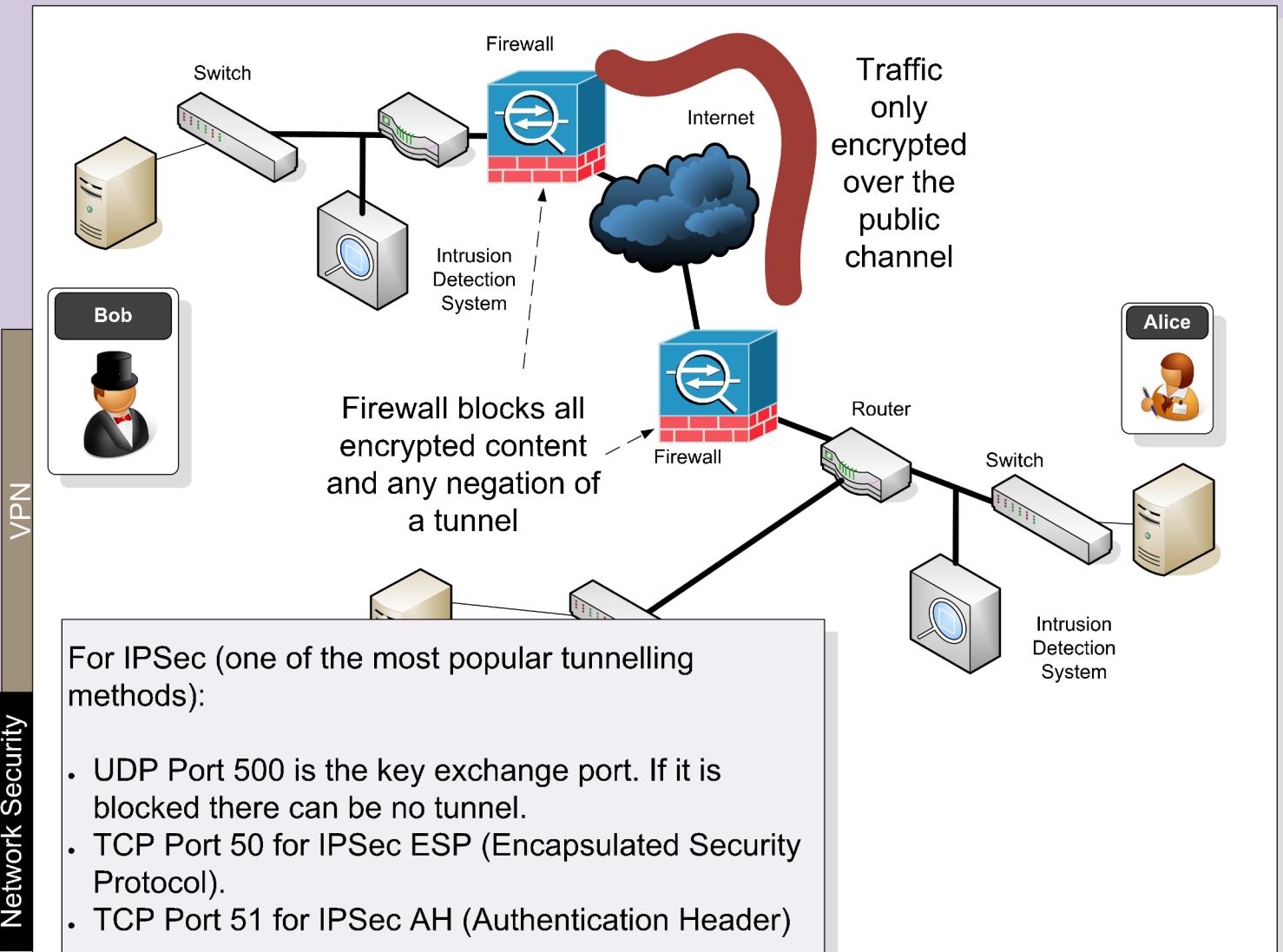
IPSec. An open standard. Includes both encryption and Authentication.

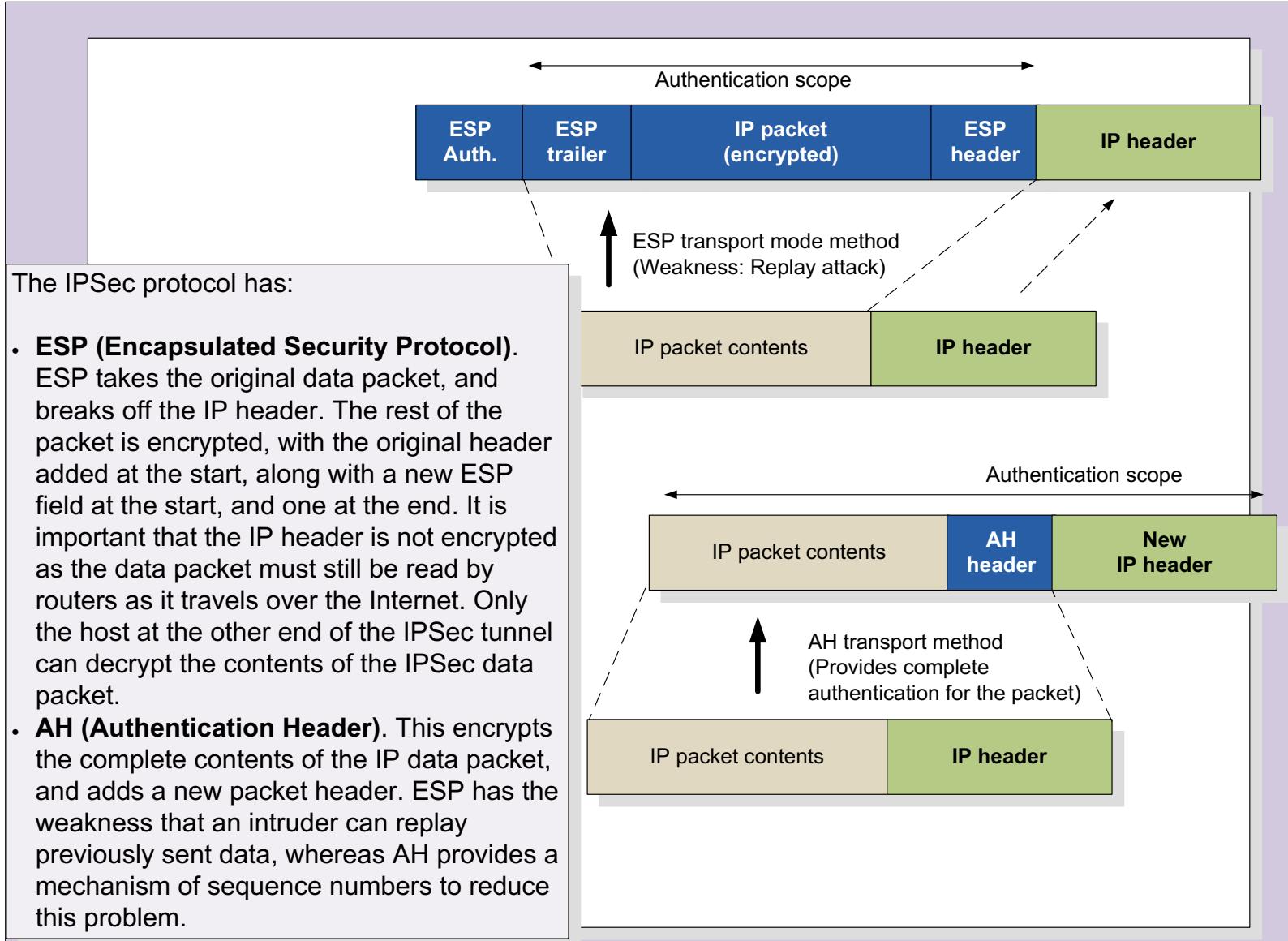


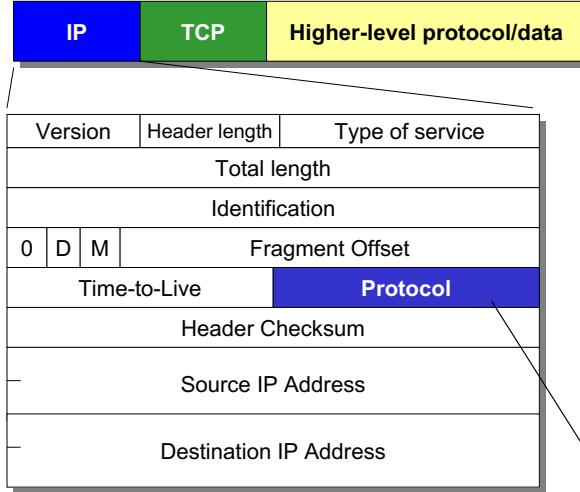
VPN types

Network Security





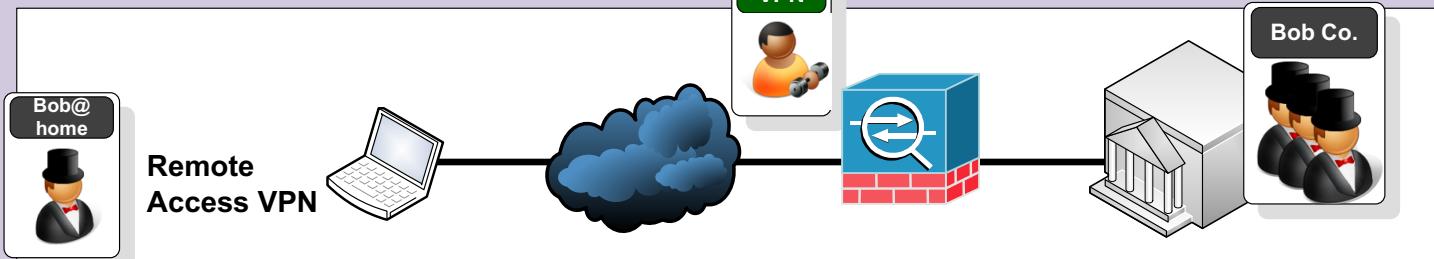




VPN

Network Security

- 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 permit-ipsec
```

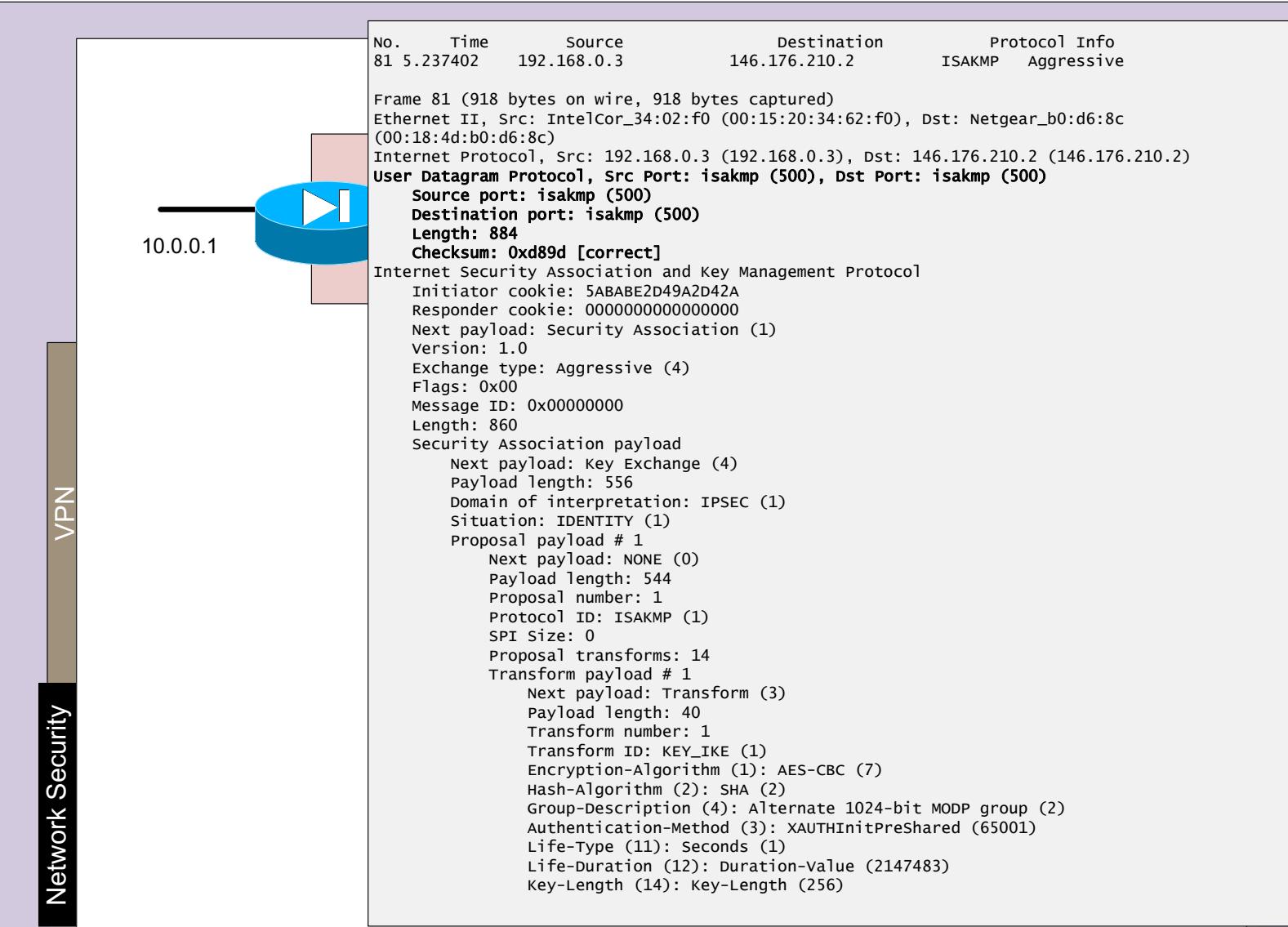
Phase 2

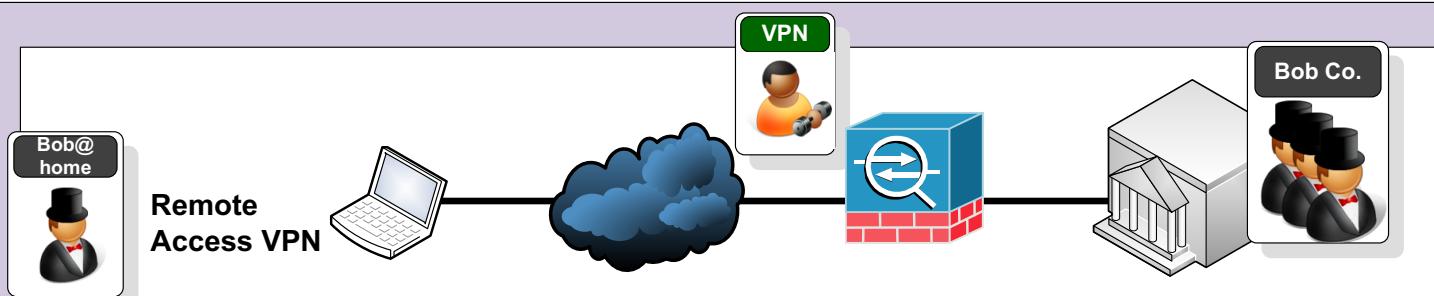
Defines the policies for transform sets, peer IP addresses/hostnames and lifetime settings.

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 transform-set MYIPSECFORMAT esp-des esp-sha-hmac
crypto map MYIPSEC 10 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 MYIPSEC 10 match address 111
crypto map MYIPSEC 10 set peer 176.16.0.2
crypto map MYIPSEC 10 set transform-set MYIPSECFORMAT
crypto map MYIPSEC interface outside
```





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

=====

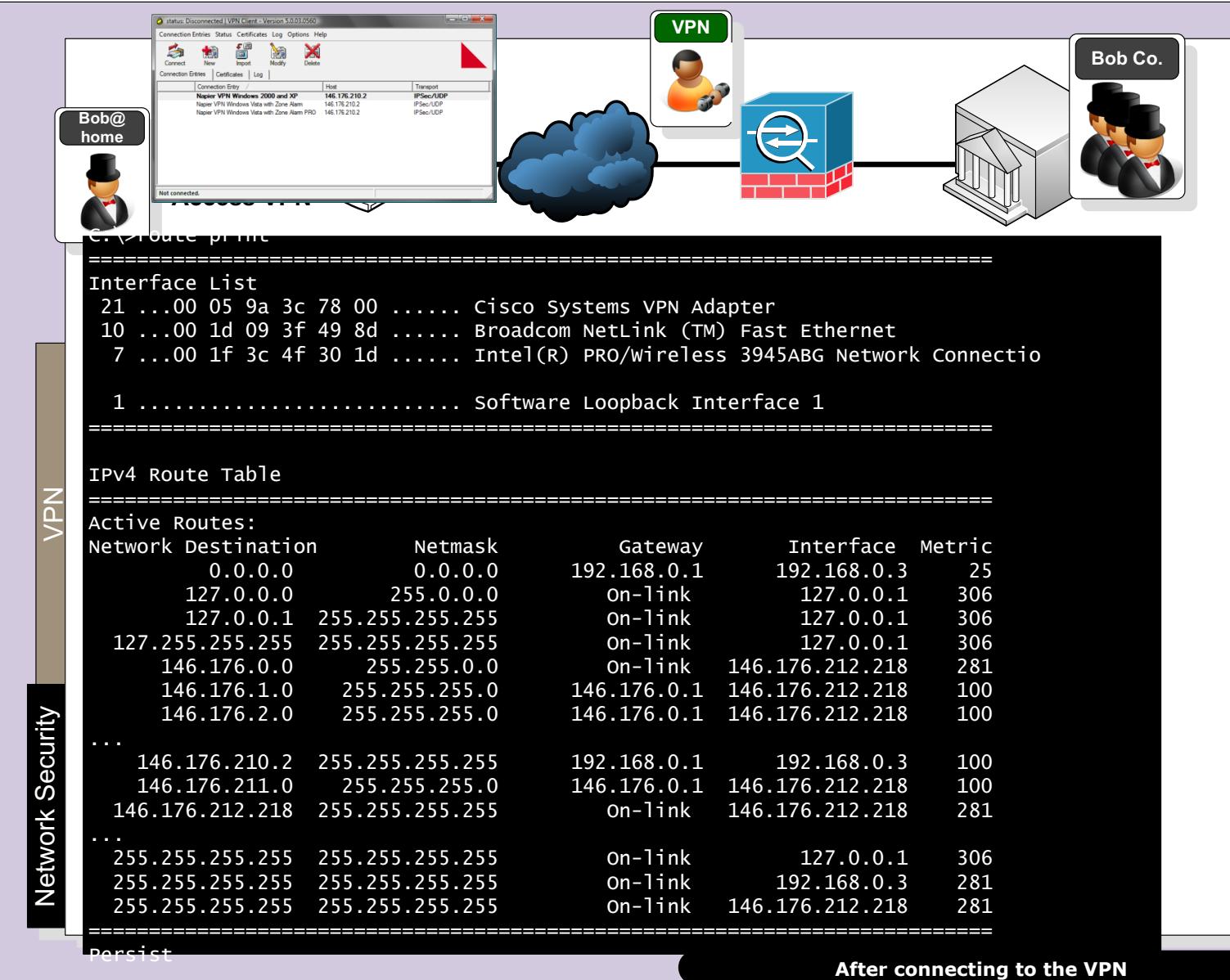
Persistent Routes:

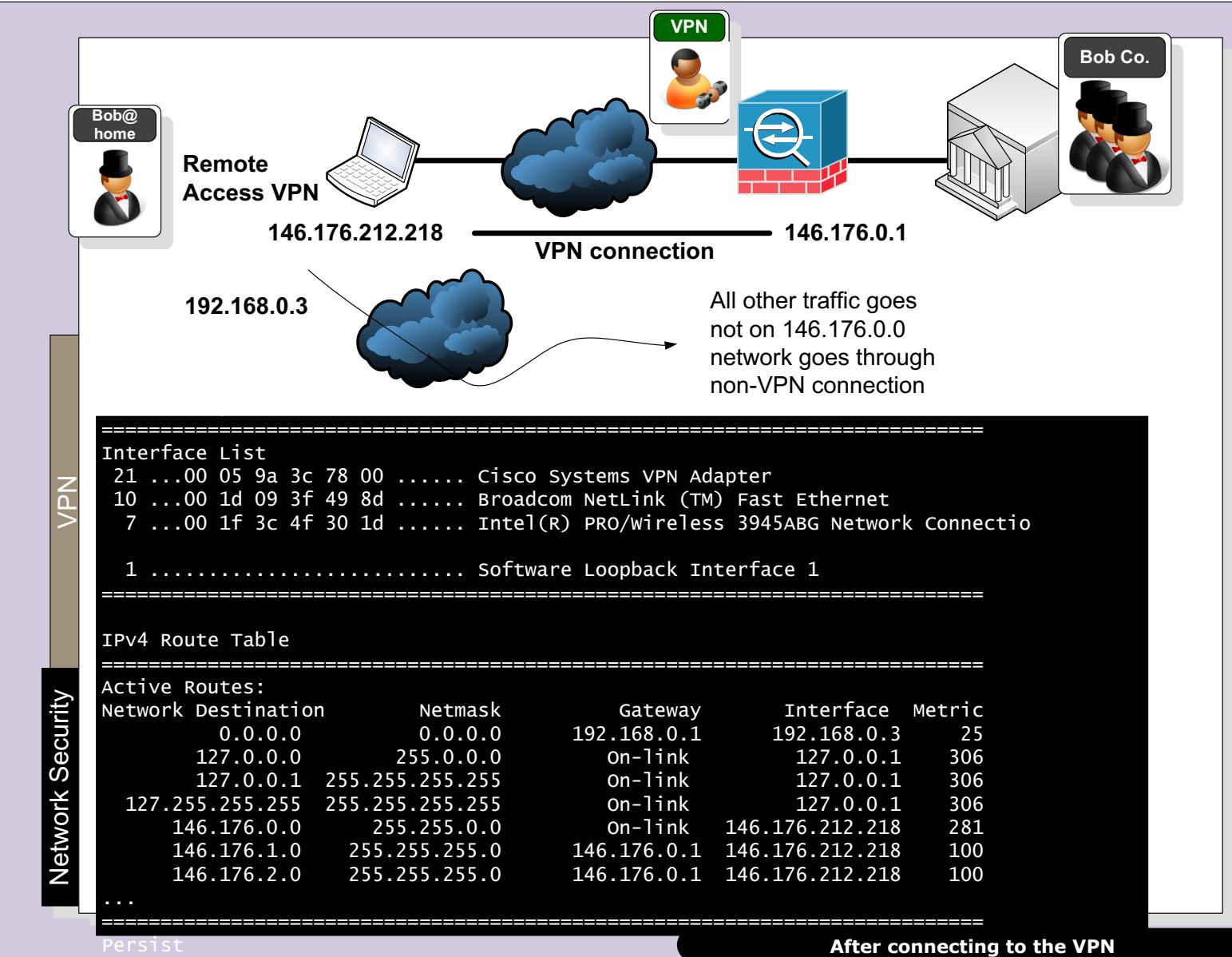
None

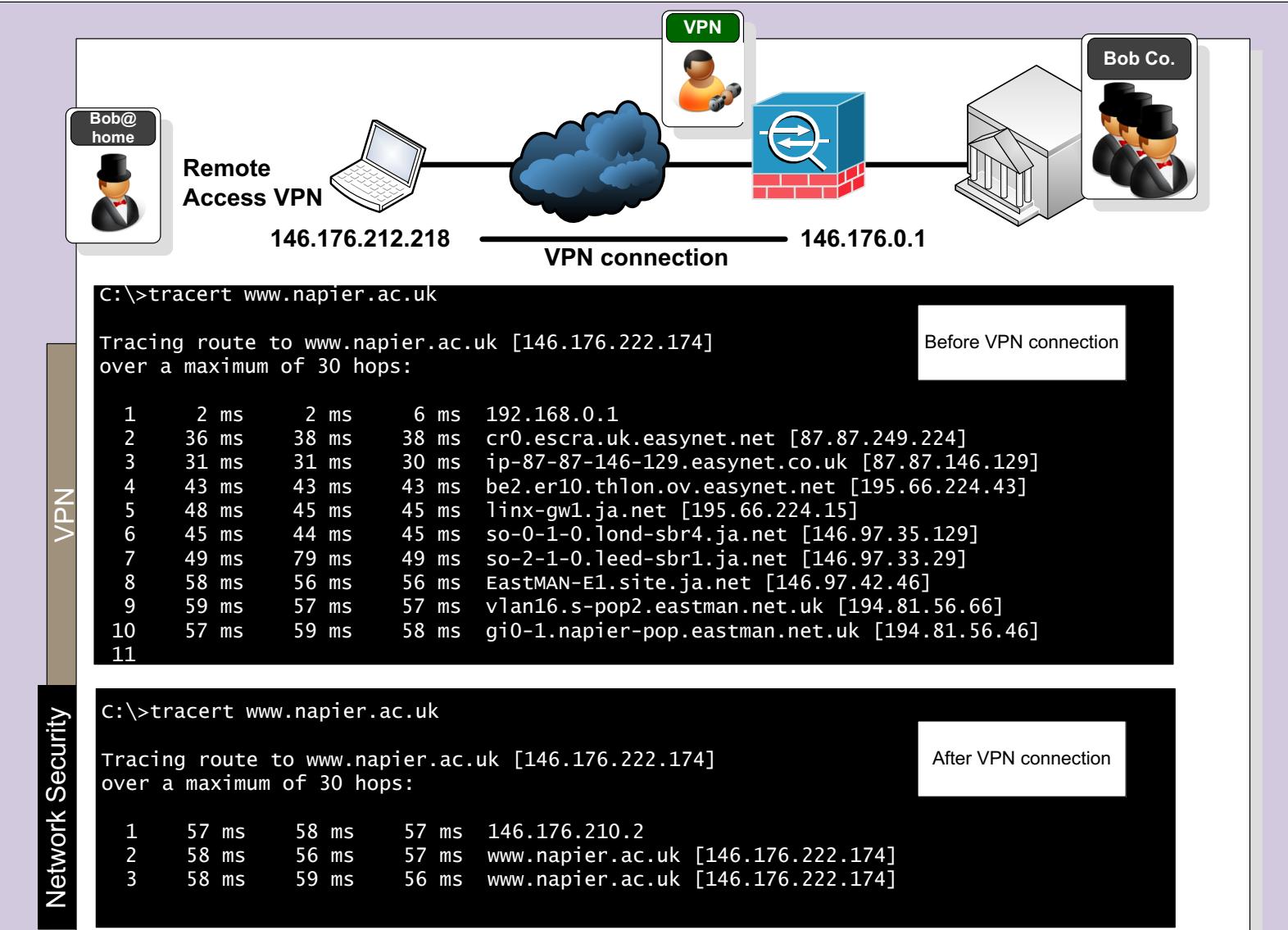
VPN

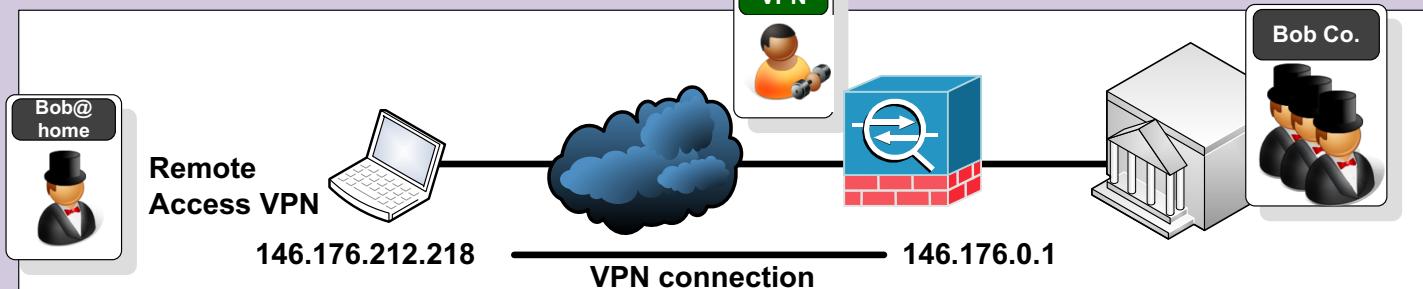
Network Security

Before connecting to the VPN









```
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

VPN

```
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

Network Security

Tunnelling

Basics.
TLS.
VPNs.

Prof Bill Buchanan OBE
<https://asecuritysite.com/tunnelling>

