

Tunneling

Introduction

Bob



Alice

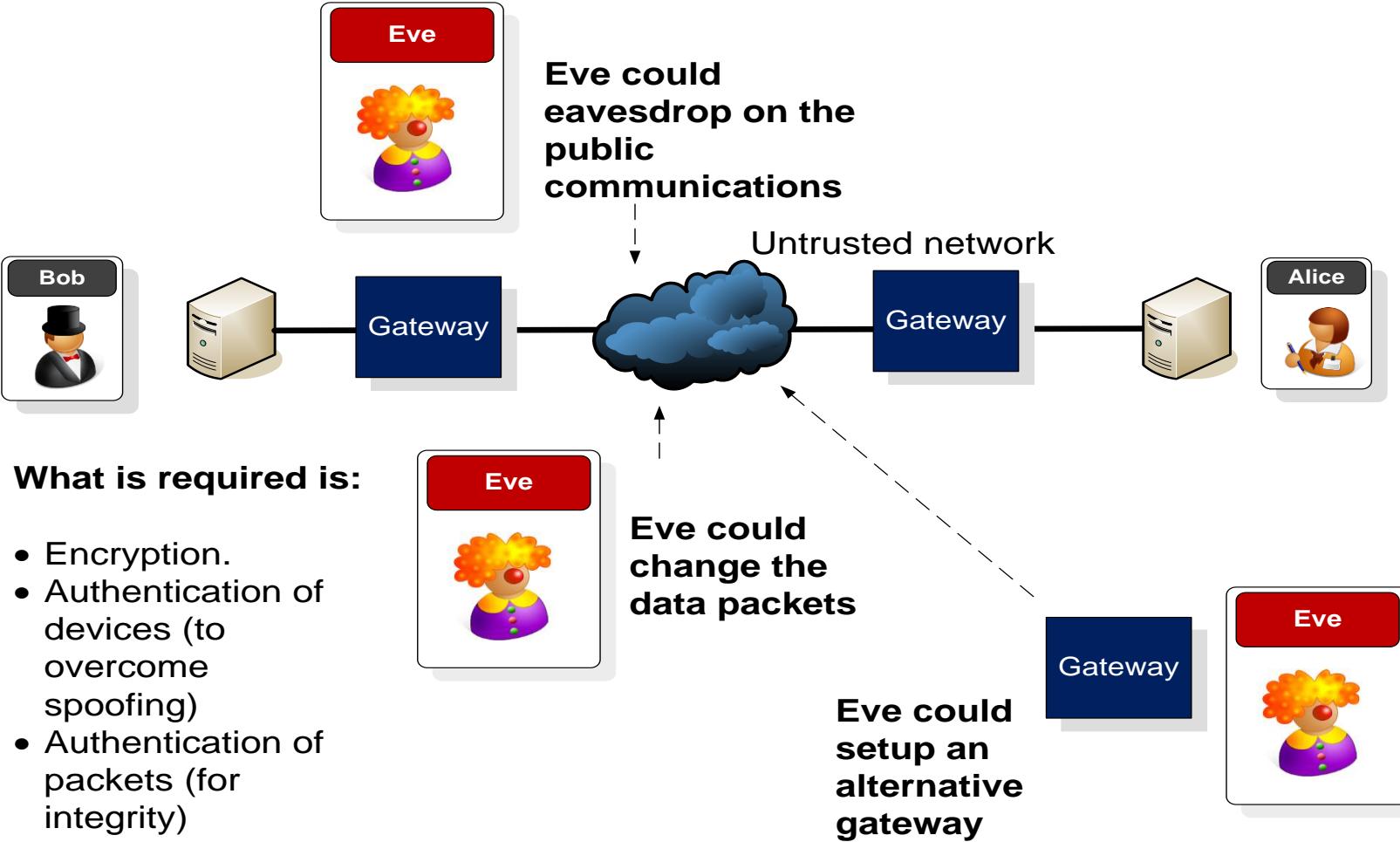


Eve

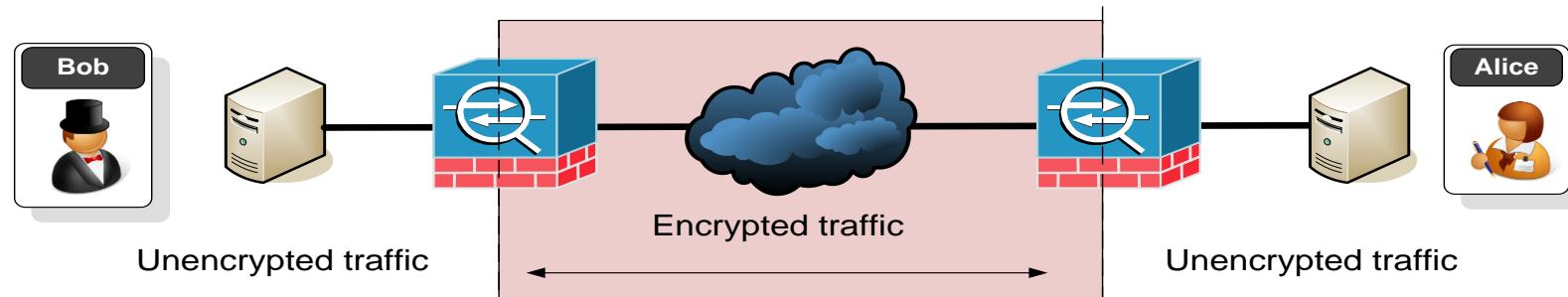


Trent



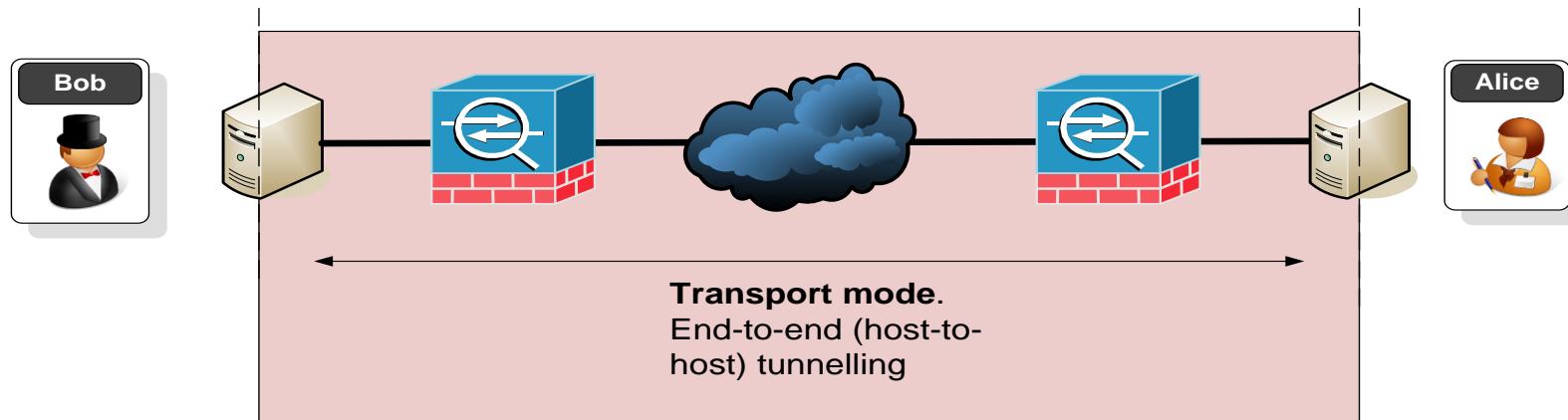


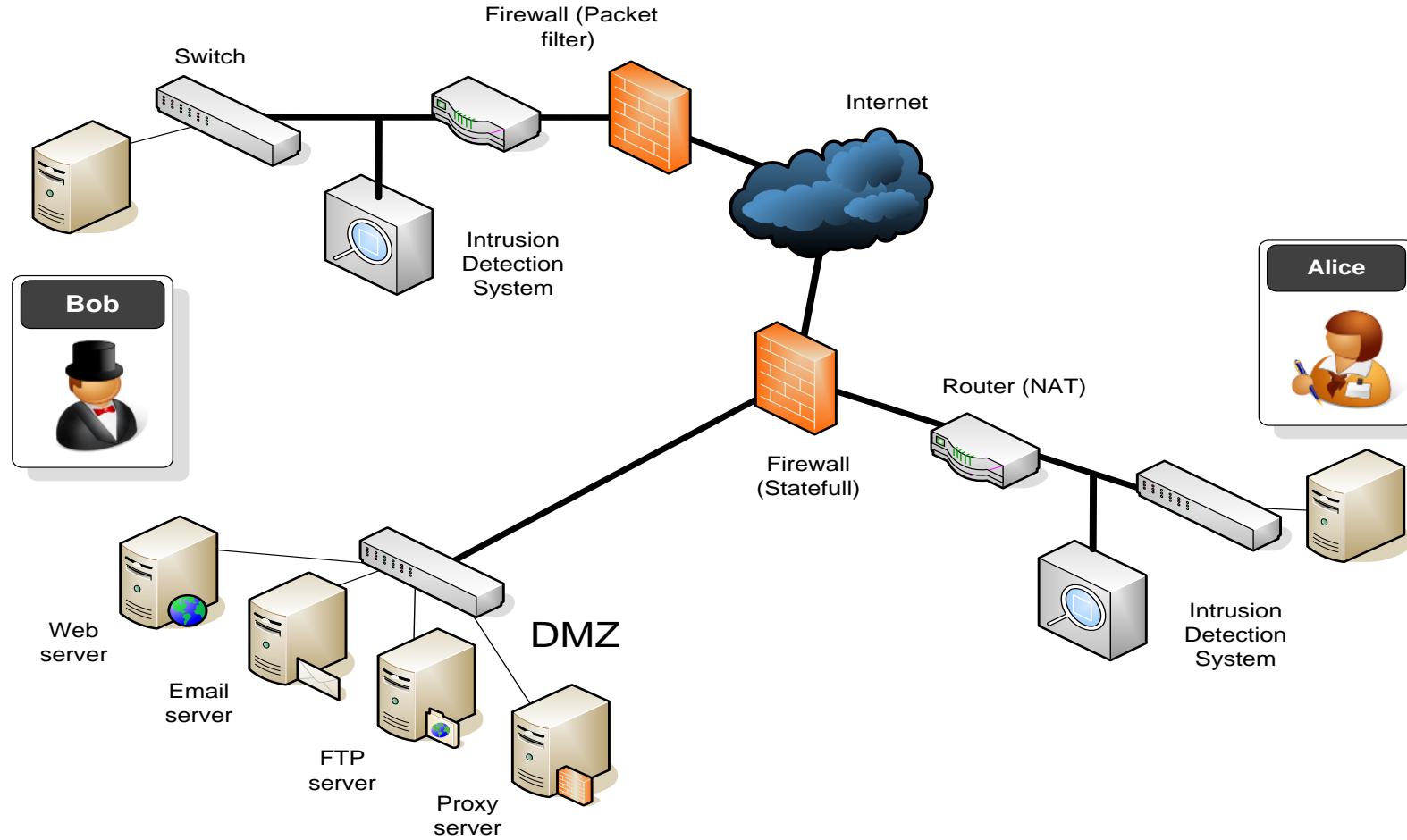
Traffic is encrypted over the untrusted network.

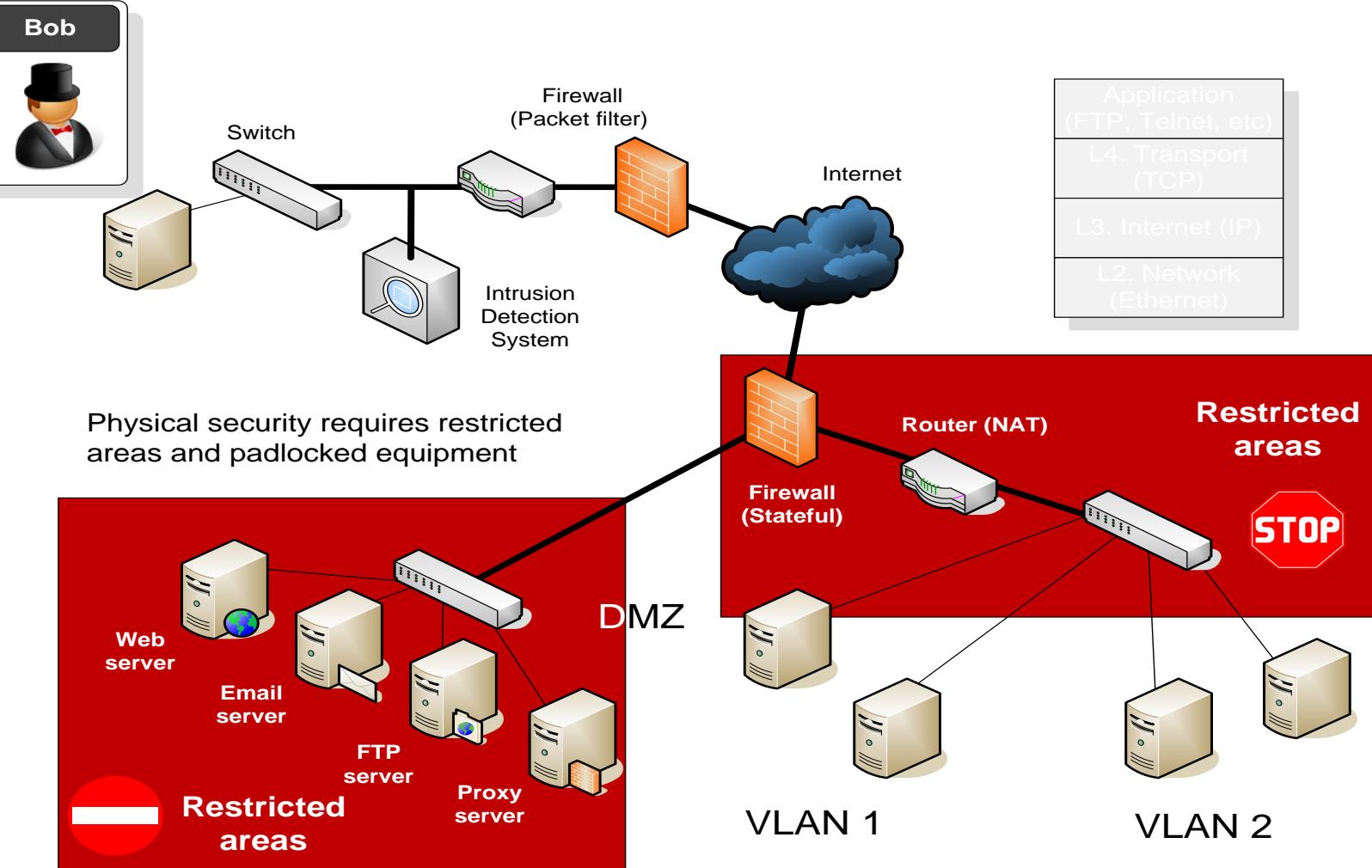


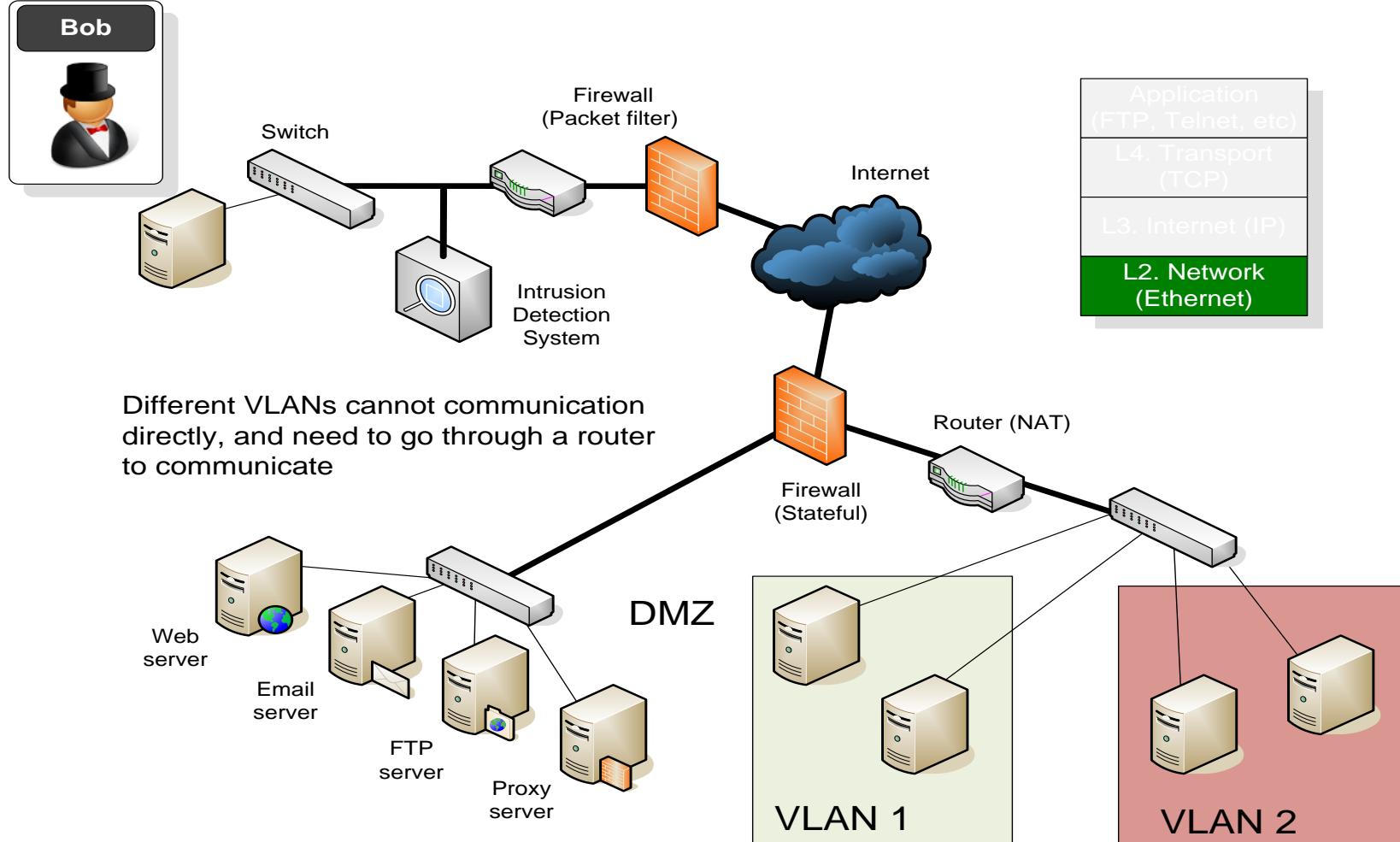
Tunelling mode (over untrusted connections)

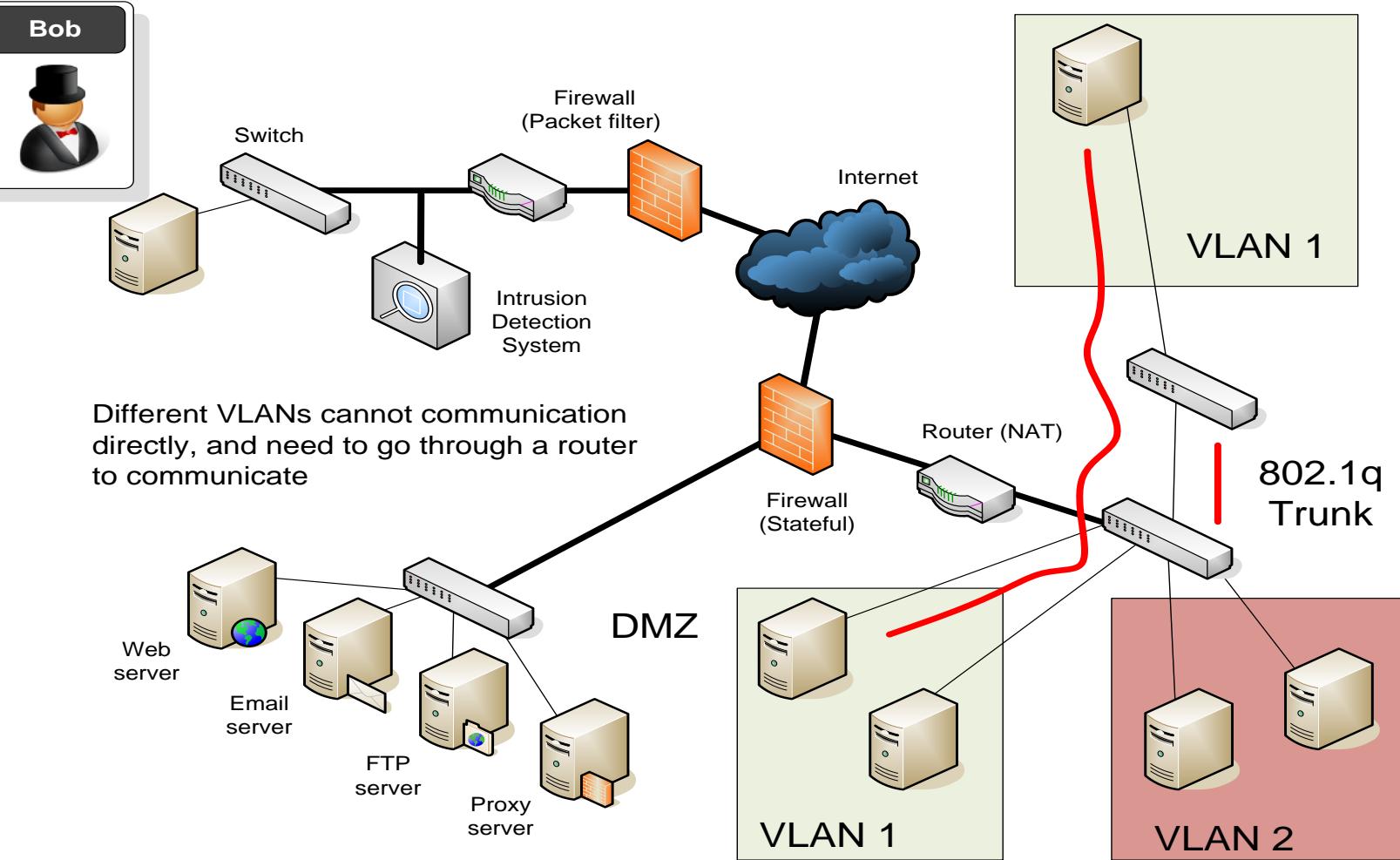
Transport mode.
End-to-end (host-to-host) tunnelling

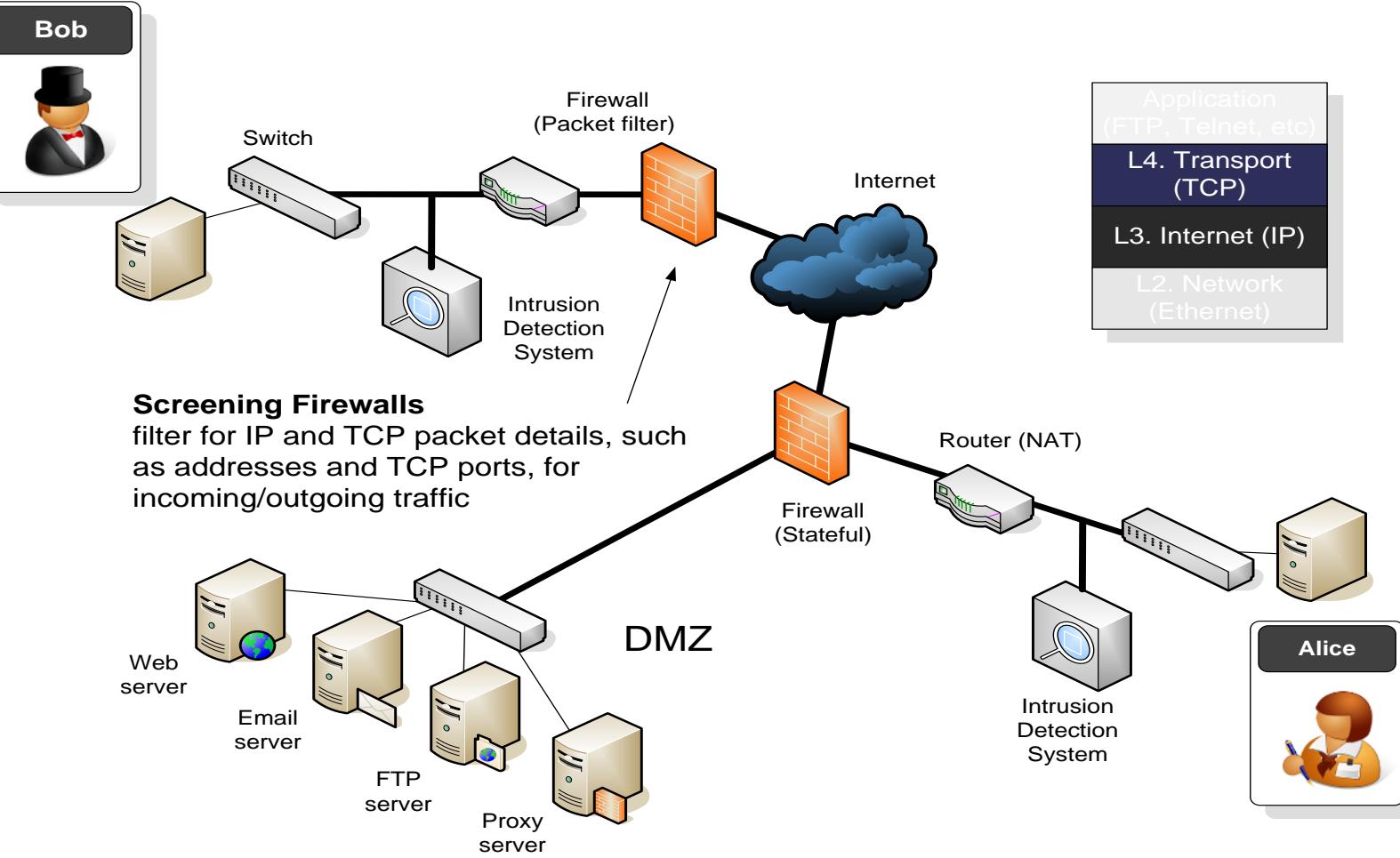












Network Security

Stateful firewall

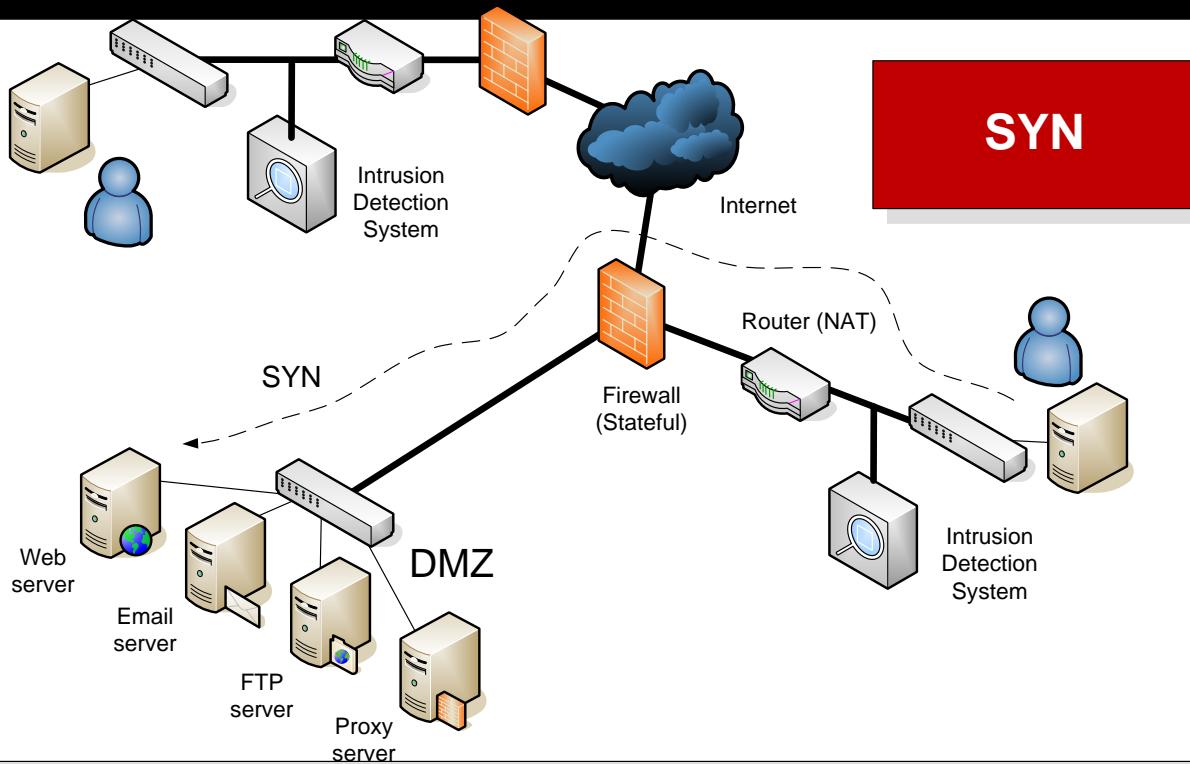
Originator

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

Recipient

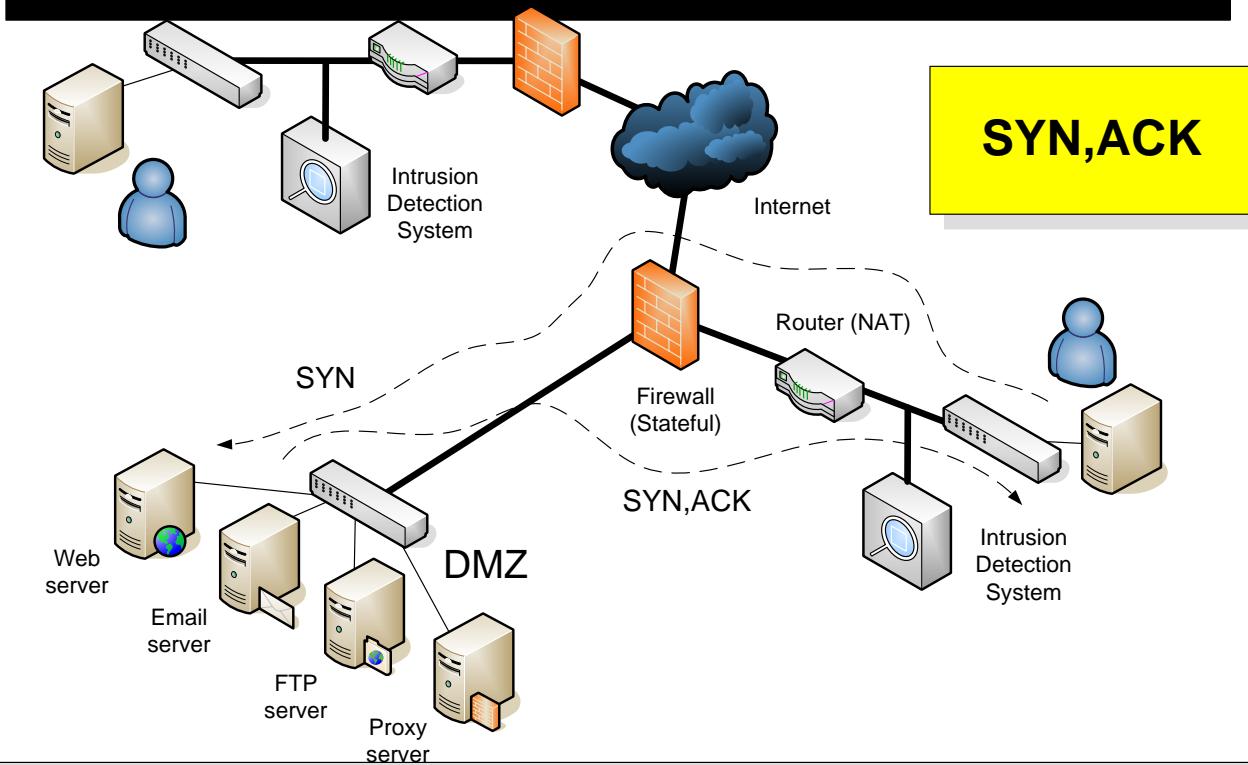
LISTEN
SYN-RECEIVED
SYN-RECEIVED
ESTABLISHED
ESTABLISHED

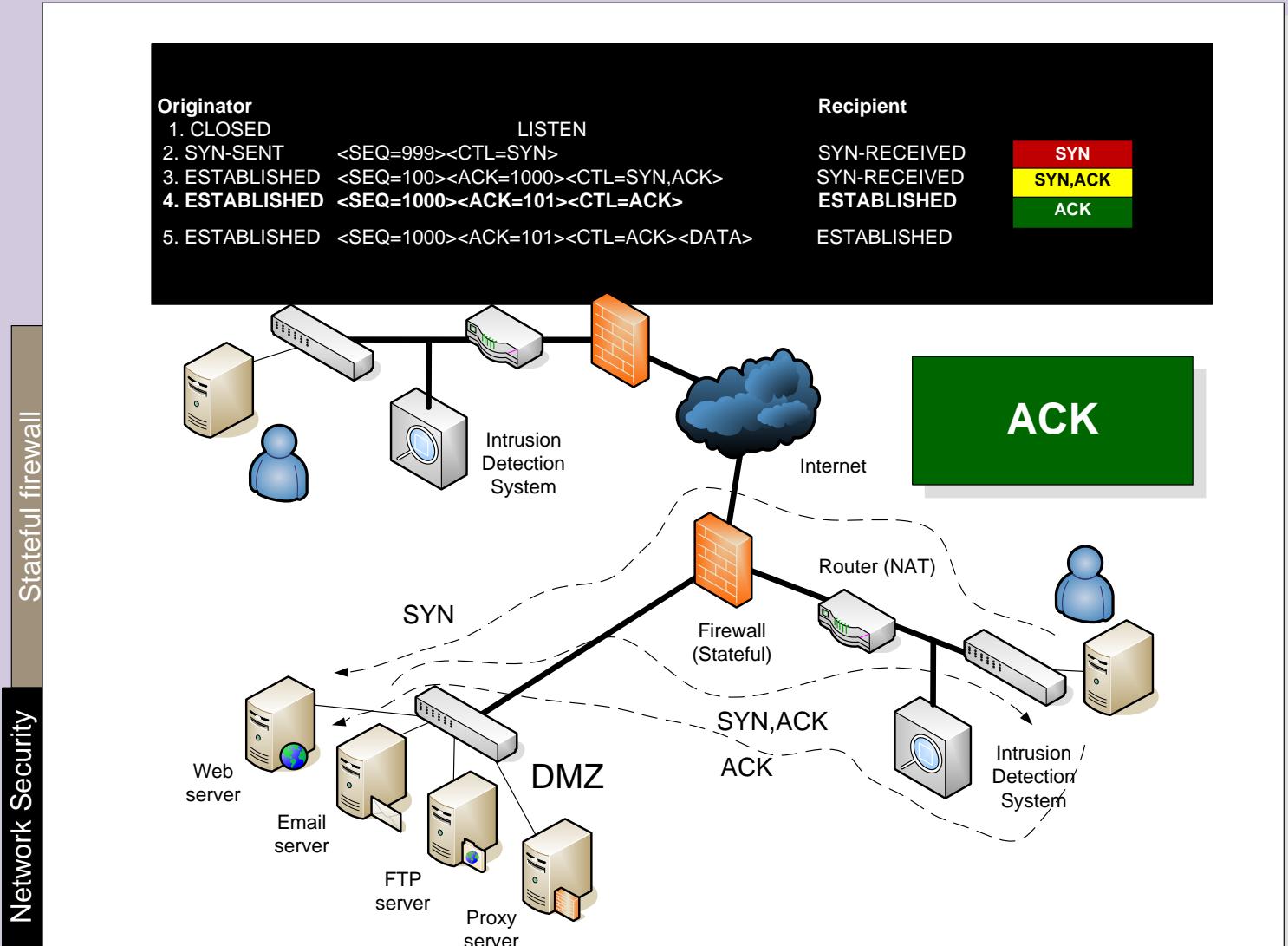
SYN



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

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

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

Internet Protocol Version 4, 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)

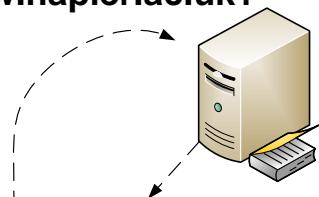
SYN

Stateful fire

Network Security

www.napier.ac.uk?

DNS server



146.176.1.188

TCP port=4213

192.168.1.101

SYN

Src Port=4213, Dest Port=80

TCP port=80



146.176.1.188

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)
[SEQ/ACK analysis]

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]

SSL/TLS

Bob



Alice

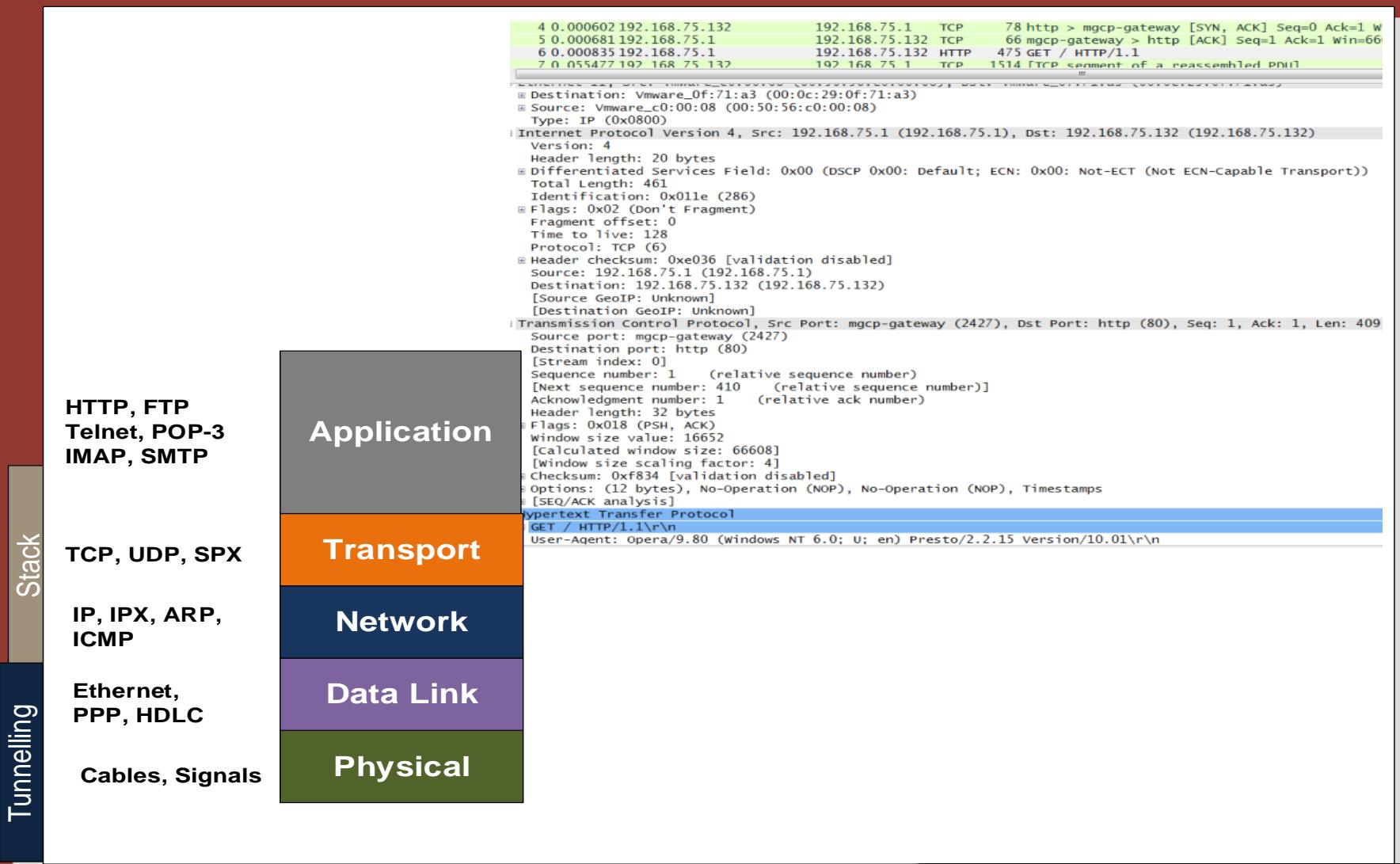


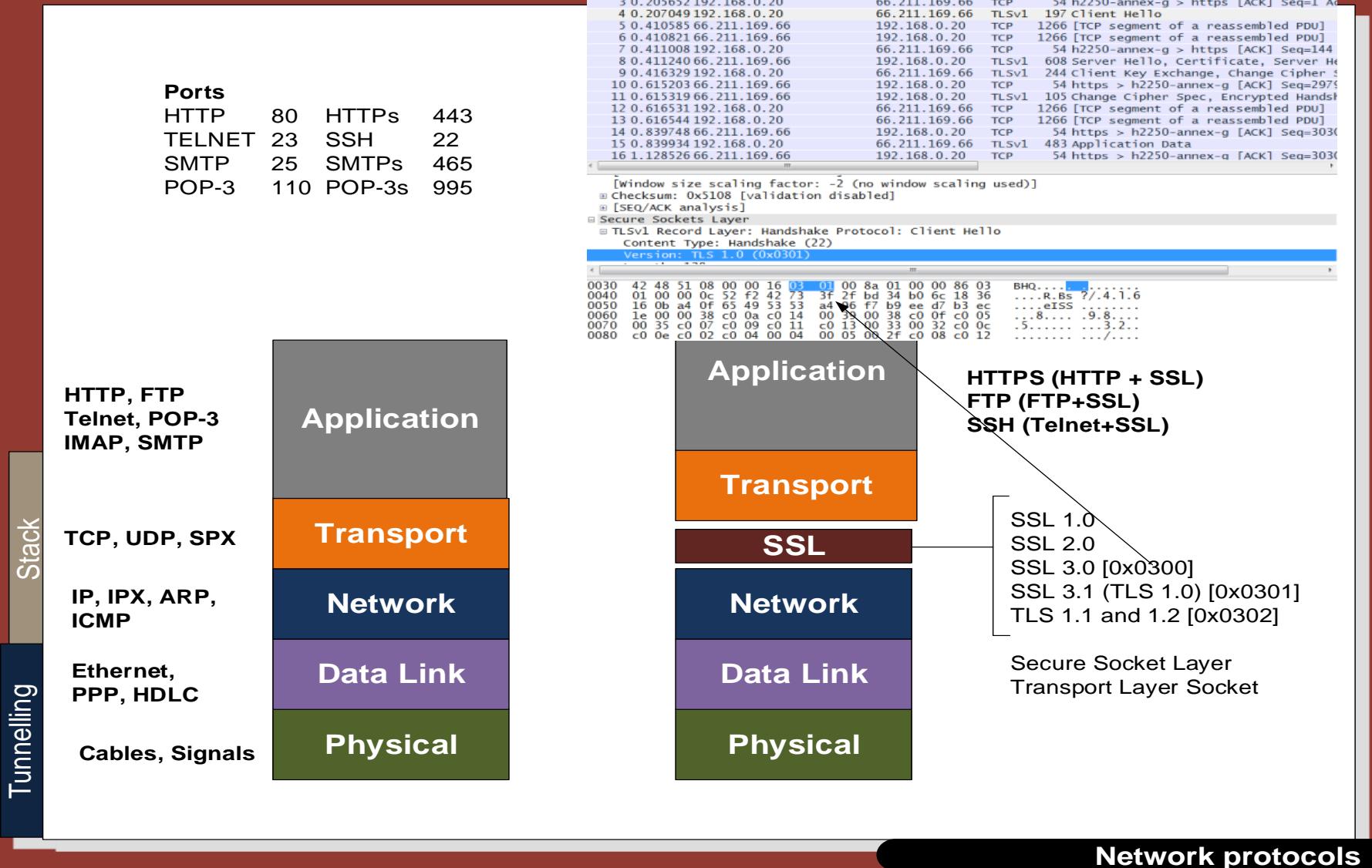
Eve



Trent

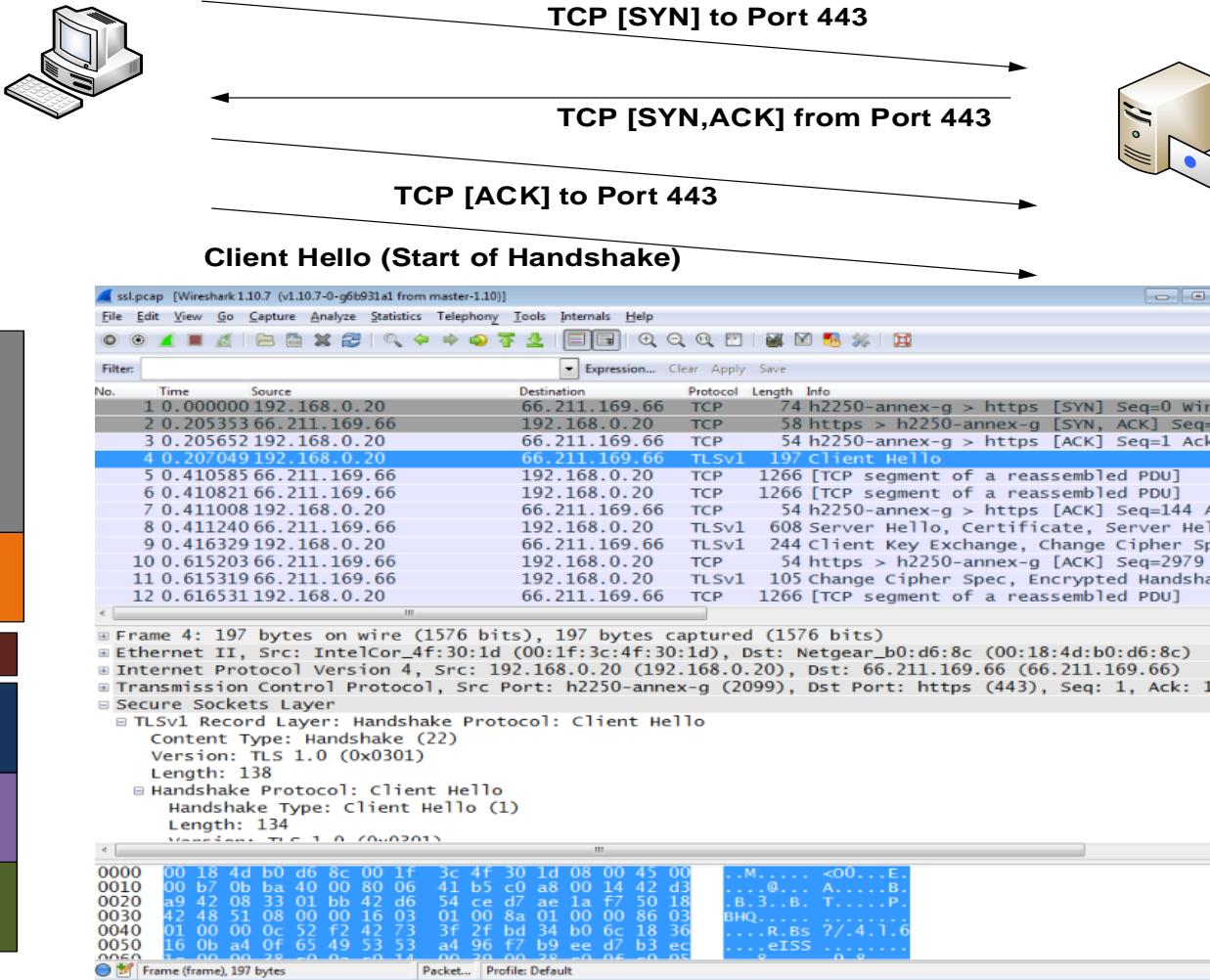
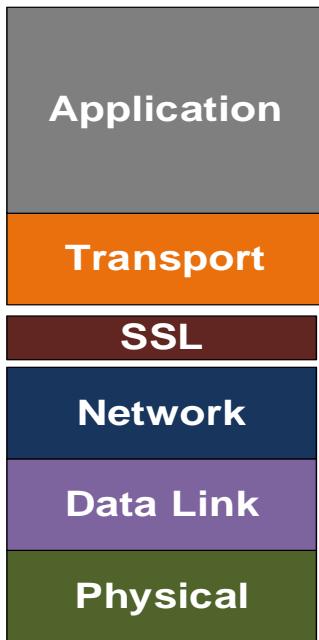






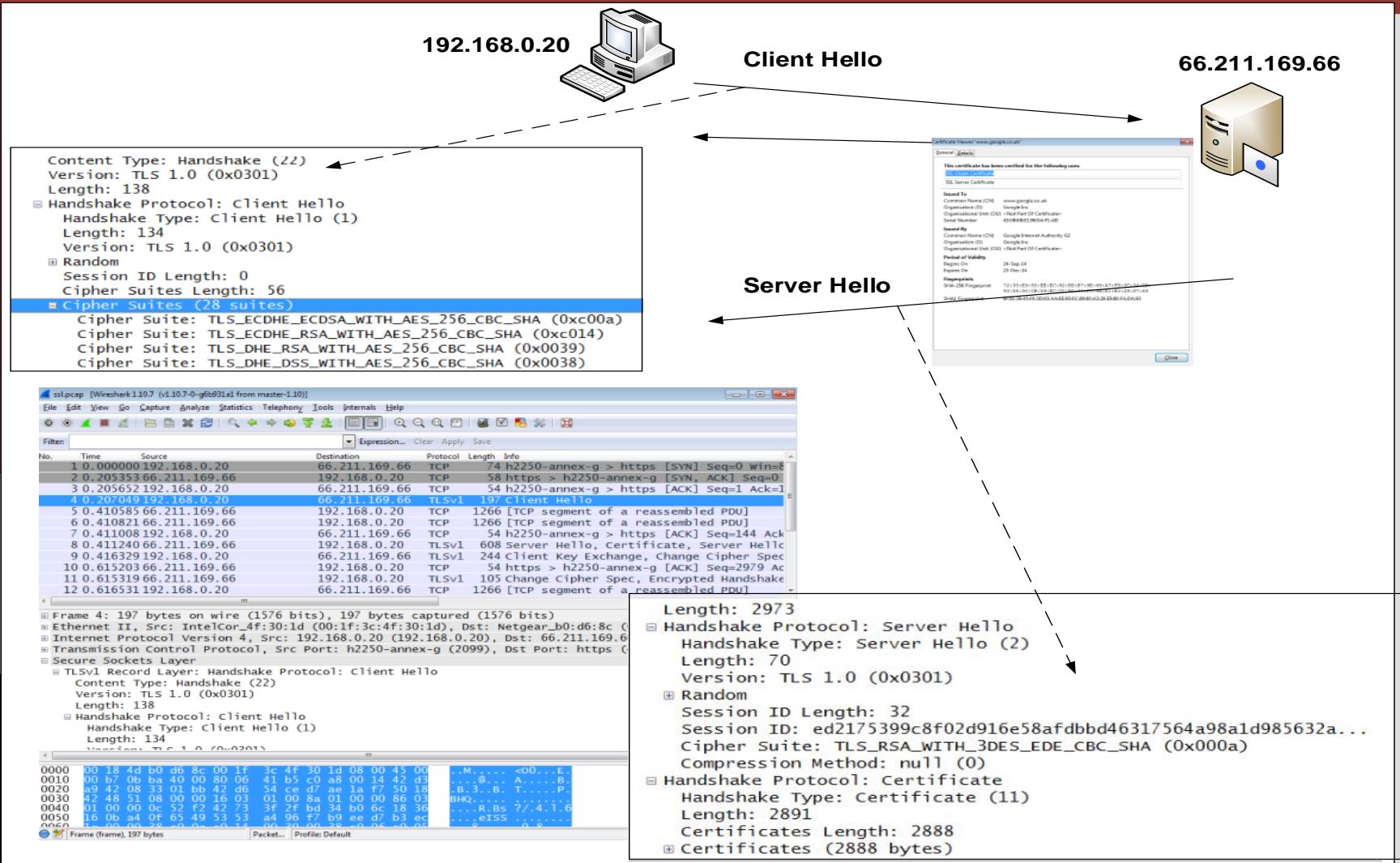
Tunnelling

Stack

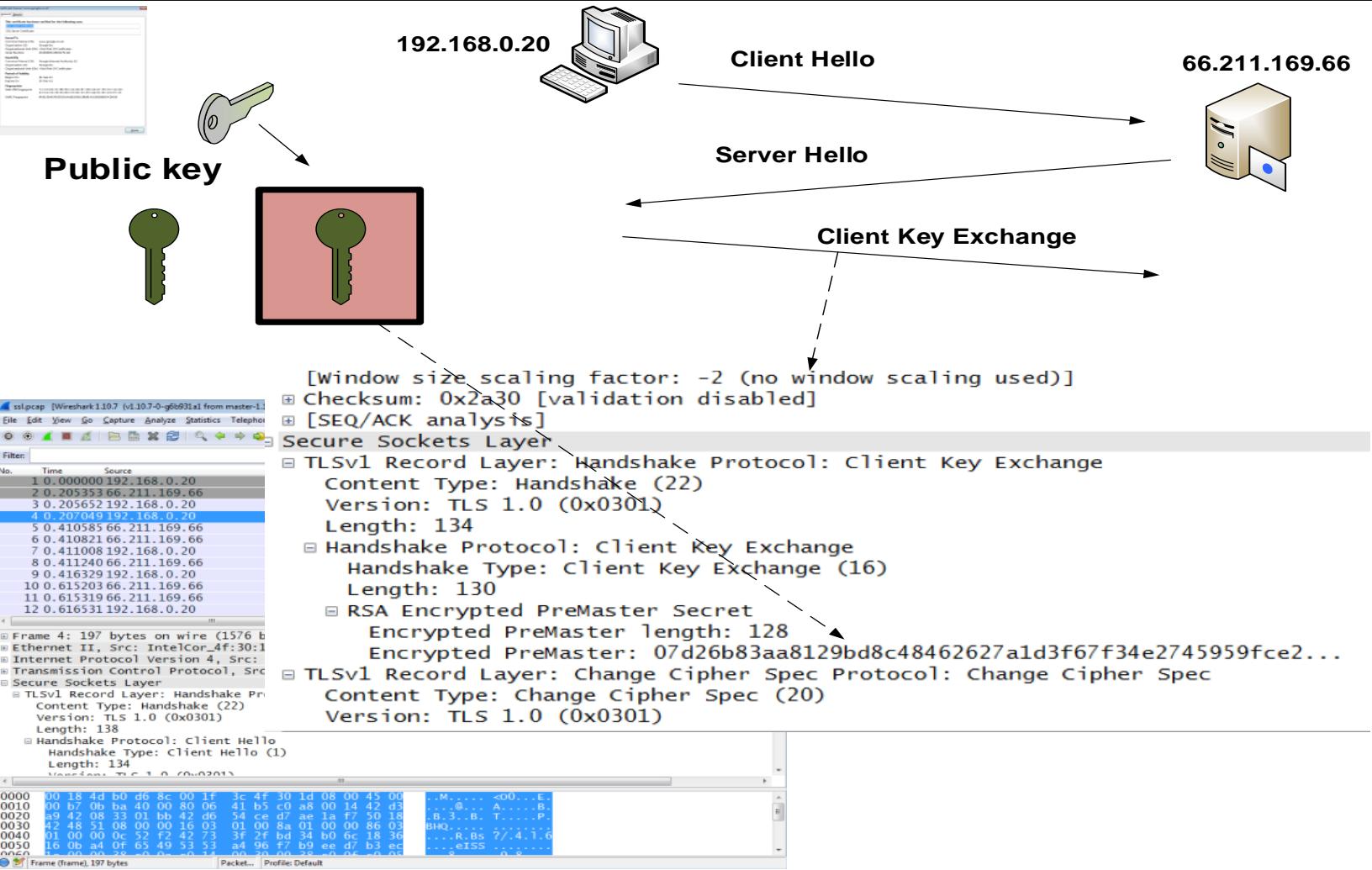


TLS

Tunnelling Stack



Tunnelling Stack



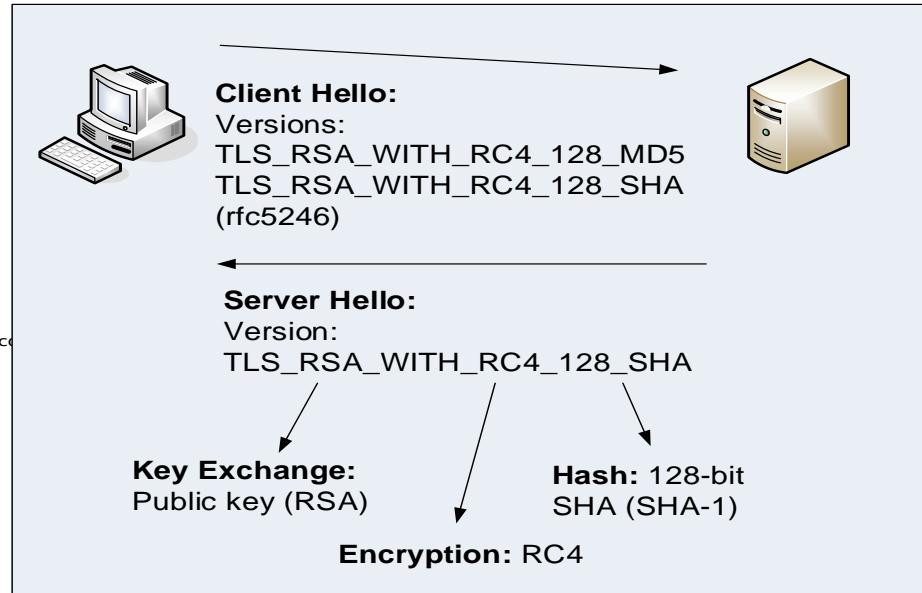
TLS

```

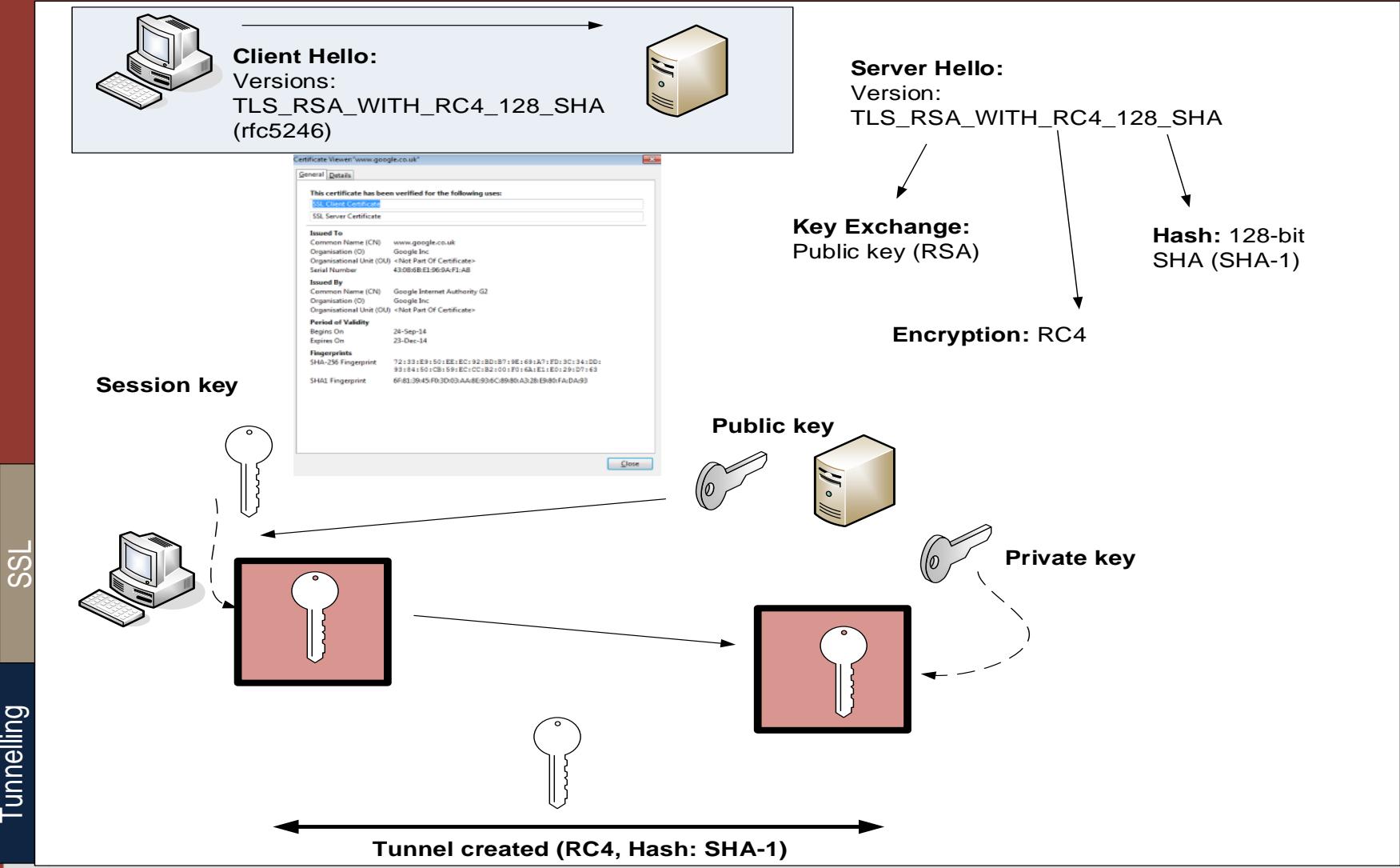
billbuchanan@Bill's-MacBook-Pro:~$ openssl s_client -connect www.google.com:443
CONNECTED(00000003)
depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
verify error:num=20:unable to get local issuer certificate
verify return:0
---
Certificate chain
 0 s:/C=US/ST=California/L=Mountain View/O=Google 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-----
MIIEjdCCA16gAwIBAgIISVyALWn+akUwDQYJKoZIhvcNAQEFBQAwSTELMAkGA1UE
...
SoX4i5L0D0jzyqKfuiMgFwdETq0EpCmkhJfGNHjvdzc/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:
B8A14DB1B3021E80B53F30EA94D2EEA155A995B926879B08E3D971EB16873D16F62929899E2FA368D374716DB14A412
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 *.. ....wC: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

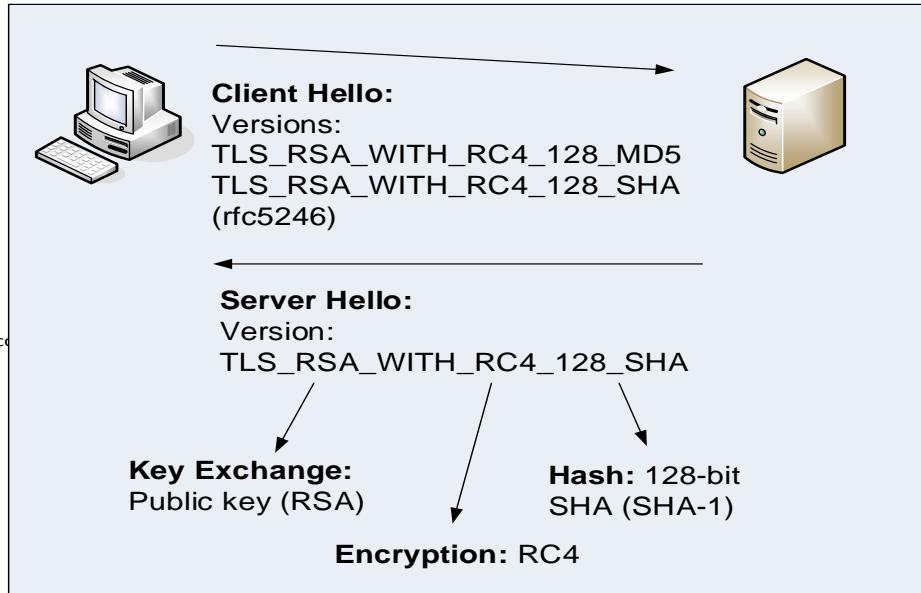


```

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-----
MIIEjdCCAc16gAwIBAgIISvYJALWn+akUwDQYJKoZIhvcNAQEFBQAwSTELMAkGA1UE
...
-----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 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)

```



Heartbleed ... A Short History

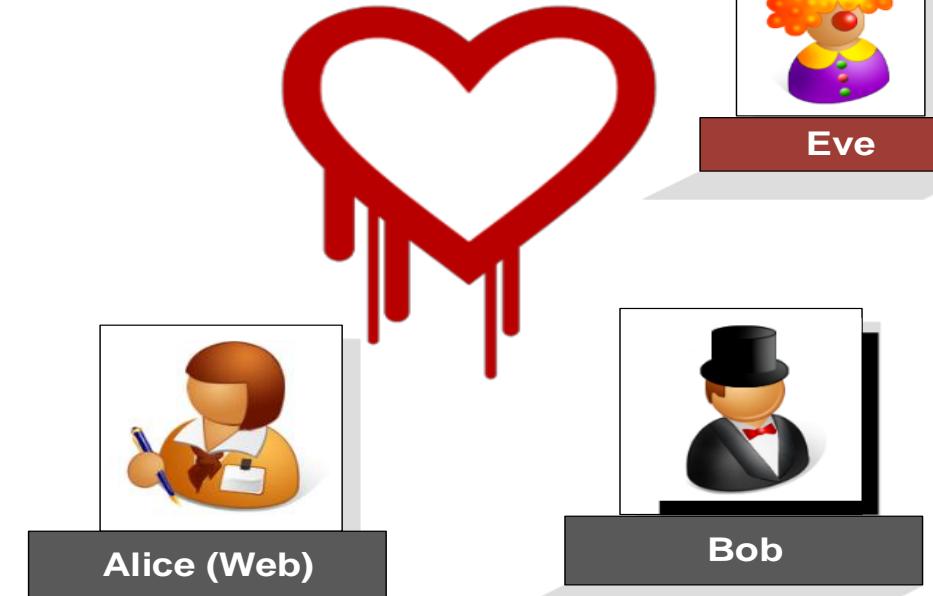
Outline

OpenSSL

Heartbeat

Heartbleed

Timeline



Heartbleed

Bob



Alice



Eve

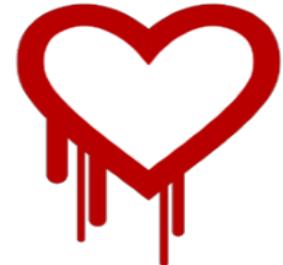
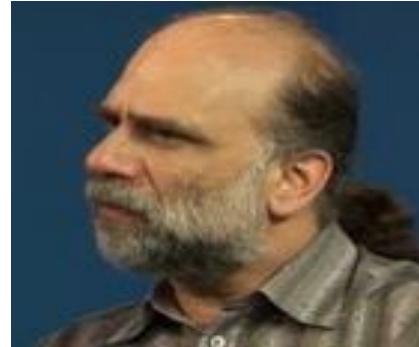
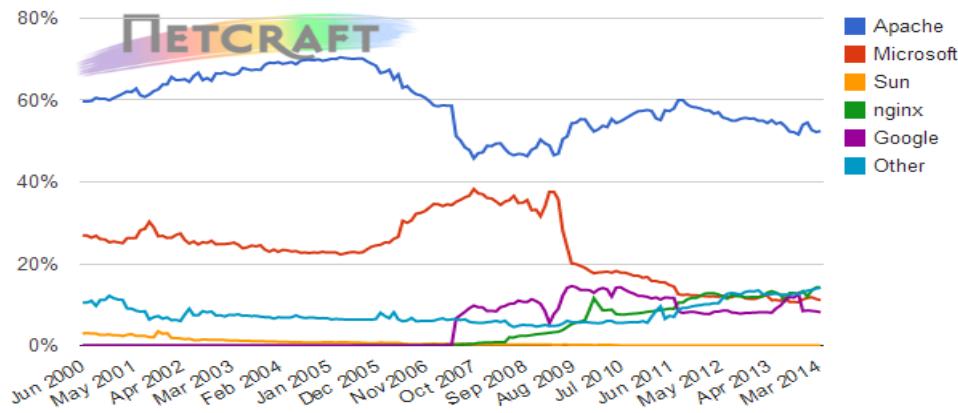


Trent



"On the scale of 1 to 10, this is an 11. Half a million sites are vulnerable, including my own."

Has anyone looked at all the low-margin non-upgradable embedded systems that use OpenSSL? An upgrade path that involves the trash, a visit to Best Buy, and a credit card isn't going to be fun for anyone.



... a 'catastrophic' revelation and suggested it could have been created deliberately to help snoop through firms' data.

I'm hearing that the CAs are completely clogged, trying to reissue so many new certificates. And I'm not sure we have anything close to the infrastructure necessary to revoke half a million certificates.



```
# cat /etc/shadow  
root:$1$Etg2ExUZ$F9NTP7omafhK1lqaBMqng1:15651:0:99999:7:::  
# openssl passwd -1 -salt Etg2ExUZ redhat  
$1$Etg2ExUZ$F9NTP7omafhK1lqaBMqng1
```



Bob

SSL/TLS

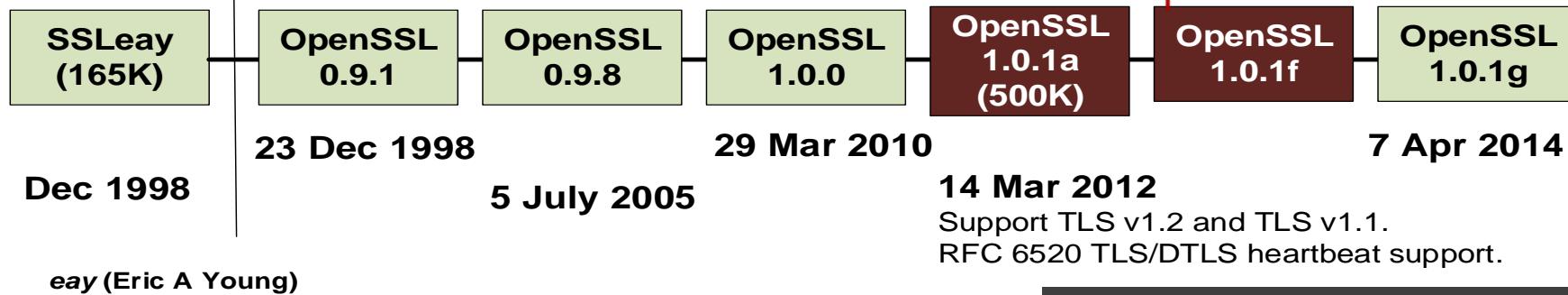


Alice (Web)

OpenSSL Software Foundation (OSF):

- Steve Marquess (US) and Stephen Henson (UK) + 8 volunteer devs.
- <\$1million per year.
- Funded by donations eg United States Department of Homeland Security and the United States Department of Defense.

Eric Young and Tim Hudson



Timeline



```
# cat /etc/shadow  
root:$1$Etg2ExUZ$F9NTP7omafhK1lqaBMqng1:15651:0:99999:7:::  
# openssl passwd -1 -salt Etg2ExUZ redhat  
$1$Etg2ExUZ$F9NTP7omafhK1lqaBMqng1
```

SSL/TLS



Bob



OpenSSL Software Foundation (OSF):

- Steve Marquess (US) and Stephen Henson (UK) + 8 volunteer devs.
- <\$1million per year.
- Funded by donations eg United States Department of Homeland Security and the United States Department of Defense.

Stephen Henson

- Only full-time developer.
- UK-based Mathematical.
- 60% of all code.
- 31 Dec 2011, Bug introduced by German developer Robin Seggelmann and okayed.



Alice (Web)



Steve Marquess

- “no money going toward reviewing the code or performing audits.”
- \$9K since Heartbleed. Where are all the Fortune 1000 companies who use it for free?



OSF

OpenSSL

Cryptography and SSL/TLS Toolkit

```
# cat /etc/shadow
root:$1$Etg2ExUZ$F9NTP7omafhK1lqaBMqng1:15651:0:99999:7:::
# openssl passwd -1 -salt Etg2ExUZ redhat
$1$Etg2ExUZ$F9NTP7omafhK1lqaBMqng1
```

```
#else
/*
 * XXXX just disable all digests for now, because it sucks.
 * we need a better way to decide this - i.e. I may not
 * want digests on slow cards like hifn on fast machines,
 * but might want them on slow or loaded machines, etc.
 * will also want them when using crypto cards that don't
 * suck moose gonads - would be nice to be able to decide something
 * as reasonable default without having hackery that's card dependent.
 * of course, the default should probably be just do everything,
 * with perhaps a sysctl to turn algorithms off (or have them off
 * by default) on cards that generally suck like the hifn.
 */
*nids = NULL;
return (0);
#endif
}
```

```
static long ssl_callback_ctrl(BIO *b, int cmd, bio_info_cb *fp)
{
    SSL *ssl;
    BIO_SSL *bs;
    long ret=1;

    bs=(BIO_SSL *)b->ptr;
    ssl=bs->ssl;
    switch (cmd)
    {
        case BIO_CTRL_SET_CALLBACK:
            {
/* FIXME: setting this via a completely different prototype
           seems like a crap idea */
                SSL_set_info_callback(ssl,(void (*)(const SSL *,int,int))fp);
            }
            break;
        default:
            ret=BIO_callback_ctrl(ssl->rbio,cmd,fp);
            break;
    }
    return(ret);
}
```

```
#else
/* EEK! Experimental code starts */
if(iterator) return iterator;
/* Prevent infinite recursion if we're looking for the dynamic engine. */
if (strcmp(id, "dynamic"))
{
#ifndef OPENSSL_SYS_VMS
    if((load_dir = getenv("OPENSSL_ENGINES")) == 0) load_dir = "SSLROOT:[ENGINES]";
#else
    if((load_dir = getenv("OPENSSL_ENGINES")) == 0) load_dir = ENGINESDIR;
#endif
    iterator = ENGINE_by_id("dynamic");
    if(!iterator || !ENGINE_ctrl_cmd_string(iterator, "ID", id, 0) ||
       !ENGINE_ctrl_cmd_string(iterator, "DIR_LOAD", "2", 0) ||
       !ENGINE_ctrl_cmd_string(iterator, "DIR_ADD",
                               load_dir, 0) ||
       !ENGINE_ctrl_cmd_string(iterator, "LOAD", NULL, 0))
        goto notfound;
    return iterator;
}
notfound:
    ENGINE_free(iterator);
    ENGINEerr(ENGINE_F_ENGINE_BY_ID,ENGINE_R_NO_SUCH_ENGINE);
    ERR_add_error_data(2, "id=", id);
    return NULL;
/* EEK! Experimental code ends */
#endif
}
```



```
# cat /etc/shadow
root:$1$Etg2ExUZ$F9NTP7omafhK1lqaBMqng1:15651:0:99999:7:::
# openssl passwd -1 -salt Etg2ExUZ redhat
$1$Etg2ExUZ$F9NTP7omafhK1lqaBMqng1
```

```
$ openssl version
```

```
openSSL 1.0.1f 6 Jan 2014
```

```
$ openssl dgst -md5 file
```

```
MD5(file)= b1946ac92492d2347c6235b4d2611184
```

```
$ openssl genrsa -out mykey.pem 1024
```

```
Generating RSA private key, 1024 bit long modulus
```

```
.....+++++
```

```
...+++++
```

```
e is 65537 (0x10001)
```

```
$ openssl rsa -in mykey.pem -pubout > mykey.pub
```

```
writing RSA key
```

```
$ cat mykey.pub
```

```
-----BEGIN PUBLIC KEY-----
```

```
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDXv9HSFkpM+ZoOQcpdHBZiuwX8
```

```
EzIKmOnsgjc5ZTYVaF9CMLtmKoTzep7aQX9o9nKepFt1kQ73Ta9vOPd6CX61/cgY
```

```
Xy2tShw0imrtFaVDFjx+7kLmc0uwbFFCoZMtJxIaxaa9sv2kARxOCTJ2uojRTCCe
```

```
XU09IJGHnIhSNJeIJQIDAQAB
```

```
-----END PUBLIC KEY-----
```

```
$ cat /etc/shadow
```

```
root:$1$Etg2ExUZ$F9NTP7omafhK1lqaBMqng1:15651:0:99999:7:::
```

```
$ openssl passwd -1 -salt Etg2ExUZ redhat
```

```
$1$Etg2ExUZ$F9NTP7omafhK1lqaBMqng1
```

Heartbleed ... A Short History

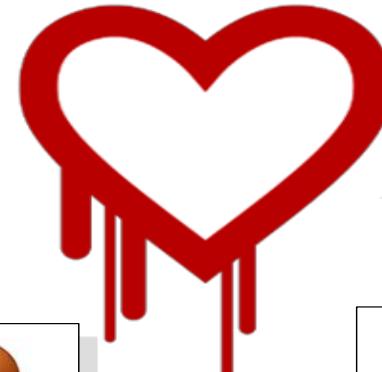
Heartbeat

Heartbleed

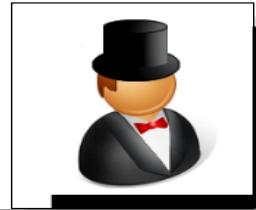
Timeline



Alice (Web)



Eve



Bob

```
# cat /etc/shadow  
root:$1$Etg2ExUZ$F9NTP7omafhK1lqaBMqng1:15651:0:99999:7:::  
# openssl passwd -1 -salt Etg2ExUZ redhat  
$1$Etg2ExUZ$F9NTP7omafhK1lqaBMqng1
```

Internet Engineering Task Force (IETF)
Request for Comments: 6520
Category: Standards Track
ISSN: 2070-1721

R. Seggelmann
M. Tuexen
Muenster Univ. of Appl. Sciences
M. Williams
GWhiz Arts & Sciences
February 2012



Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) Heartbeat Extension

Abstract

This document describes the Heartbeat Extension for the Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) protocols.

The Heartbeat Extension provides a new protocol for TLS/DTLS allowing the usage of keep-alive functionality without performing a renegotiation and a basis for path MTU (PMTU) discovery for DTLS.

```
struct {  
    HeartbeatMessageType type;           64KB max  
    uint16 payload_length;  
    opaque payload[HeartbeatMessage.payload_length];  
    opaque padding[padding_length];  
} HeartbeatMessage;  
  
payload: The payload consists of  
arbitrary content.
```



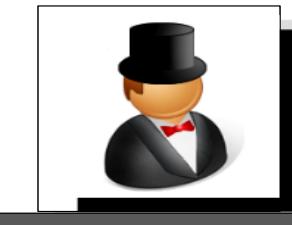
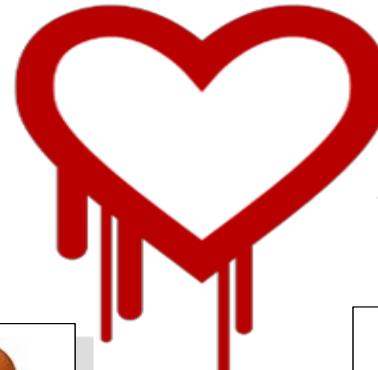
Heartbleed ... A Short History

Heartbleed

Timeline



Alice (Web)



Bob



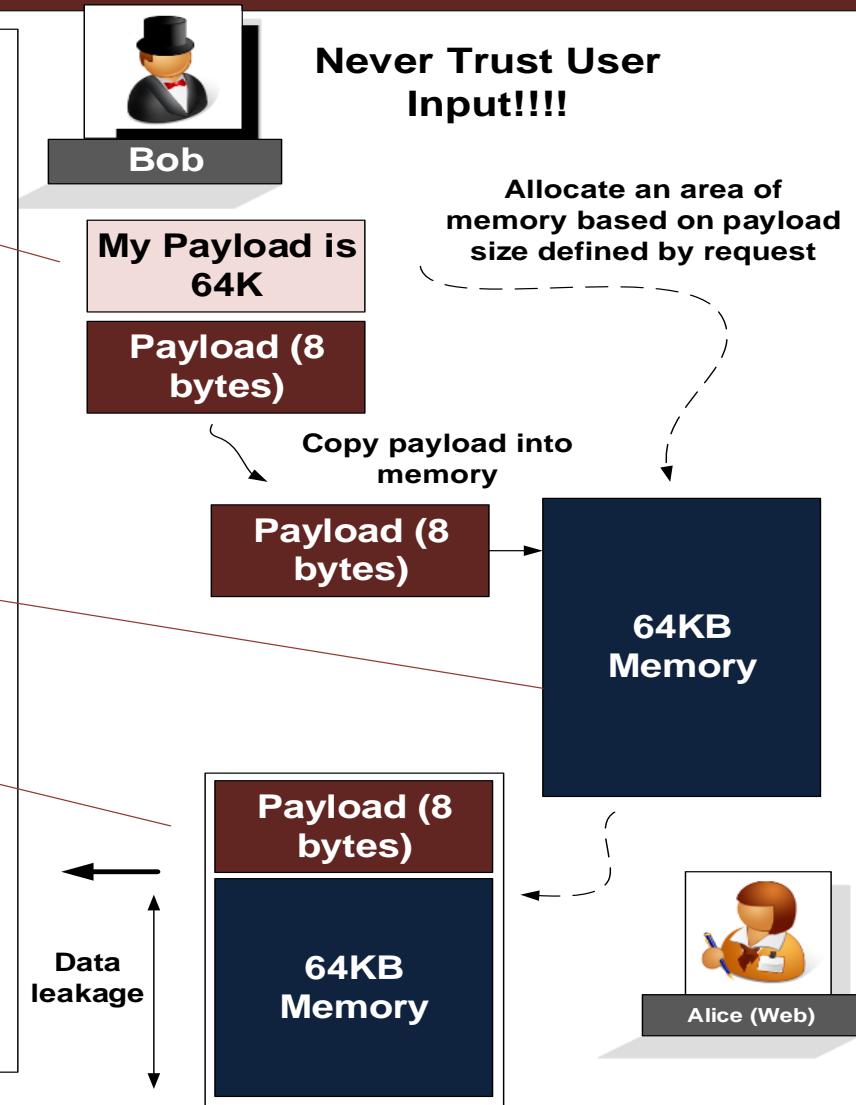
Eve

```

2412 /* Read type and payload length first */
2413 hbtpe = *p++;
2414 n2s(p, payload);
2415 pl = p;
2416
2417 if (s->msg_callback)
2418     s->msg_callback(0, s->version, TLS1_RT_HEARTBEAT,
2419                     &s->s3->rrec.data[0], s->s3->rrec.length,
2420                     s, s->msg_callback_arg);
2421
2422 if (hbtpe == TLS1_HB_REQUEST)
2423 {
2424     unsigned char *buffer, *bp;
2425     int r;
2426
2427     /* Allocate memory for the response, size is 1 bytes
2428      * message type, plus 2 bytes payload length, plus
2429      * payload, plus padding
2430     */
2431     buffer = OPENSSL_malloc(1 + 2 + payload + padding);
2432     bp = buffer;
2433
2434     /* Enter response type, length and copy payload */
2435     *bp++ = TLS1_HB_RESPONSE;
2436     s2n(payload, bp);
2437     memcpy(bp, pl, payload);
2438
2439     r = ssl3_write_bytes(s, TLS1_RT_HEARTBEAT, buffer, 3
+ payload + padding);
2440
2441     /* Read type and payload length first */
2442     if (1 + 2 + 16 > s->s3->rrec.length)
2443         return 0; /* silently discard */
2444     hbtpe = *p++;
2445     n2s(p, payload);
2446     if (1 + 2 + payload + 16 > s->s3->rrec.length)
2447         return 0; /* silently discard per RFC 6520 sec. 4 */
2448     pl = p;

```

Never Trust User Input!!!!



Heartbleed Request

heart.pcap [Wireshark 1.10.7 (v1.10.7-0-g6b931a1 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `tcp matches "\x18\x03"` Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
38	24.35351	172.16.121.1	172.16.121.150	TLSv1.	74	Heartbeat Request
39	24.35400	172.16.121.150	172.16.121.1	TCP	1514	[TCP segment of a reassembled PDU]

Frame 38: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: Vmware_c0:00:08 (00:50:56:c0:00:08), Dst: Vmware_15:f3:e9 (00:0c:29:15:f3:e9)
Internet Protocol Version 4, Src: 172.16.121.1 (172.16.121.1), Dst: 172.16.121.150 (172.16.121.150)
Transmission Control Protocol, Src Port: 64667 (64667), Dst Port: https (443), Seq: 226, Ack: 1126, Len: 8
Secure Sockets Layer
 TLSv1.1 Record Layer: Heartbeat Request
 Content Type: Heartbeat (24)
 Version: TLS 1.1 (0x0302)
 Length: 3
 Heartbeat Message
 Type: Request (1)
 Payload Length: 16384
[Malformed Packet: SSL]

No payload

0000 00 0c 29 15 f3 e9 00 50 56 c0 00 08 08 00 45 00 ..)....P V.....E.
0010 00 3c 58 eb 40 00 40 06 97 18 ac 10 79 01 ac 10 .:<X.@@.y...
0020 79 96 fc 9b 01 bb ee e0 a5 10 d2 3b 4b d2 80 18 y..... .;K..
0030 20 00 3c fa 00 00 01 01 08 0a 2a 72 9e b8 00 24 .<.... ...*r....\$
0040 f8 50 18 03 02 00 03 01 40 00 .P..... @.

Payload Length (ssl.heartbeat_message.payload.length): 16384 Packets: 60 · Displayed: 2 (3.3%) · Load time: 0.000s Profile: Default

18 03 02 00 03 1 40 00

My Payload is 64K

Heartbeat TLS 1.1 Length Request Payload length Little Endian: 0x4000 -> 16,384

Heartbleed Reply

heart.pcap [Wireshark 1.10.7 (v1.10.7-0-g6b931a1 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp matches "\x18\x03"

No. Time Source Destination Protocol Length Info

38	24.35351	172.16.121.1	172.16.121.150	TLSv1.	74	Heartbeat Request
39	24.35400	172.16.121.150	172.16.121.1	TCP	1514	[TCP segment of a reassembled PDU]

Frame 39: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)

Ethernet II, Src: Vmware_15:f3:e9 (00:0c:29:15:f3:e9), Dst: Vmware_c0:00:08 (00:50:56:c0:00:08)

Internet Protocol Version 4, Src: 172.16.121.150 (172.16.121.150), Dst: 172.16.121.1 (172.16.121.1)

Transmission Control Protocol, Src Port: https (443), Dst Port: 64667 (64667), Seq: 1126, Ack: 234, Len: 1448

Source port: https (443)
Destination port: 64667 (64667)
[Stream index: 2]
Sequence number: 1126 (relative sequence number)
[Next sequence number: 2574 (relative sequence number)]
Acknowledgment number: 234 (relative ack number)
Header length: 32 bytes
Flags: 0x010 (ACK)
Window size value: 235
[Calculated window size: 30080]
[Window size scaling factor: 1281]

0120 00 01 01 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e ...Lang usage: en
0130 2d 55 53 2c 65 6e 3b 71 3d 30 2e 35 0d 0a 41 63 -US,en;q =0.5..Ac
0140 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 cept-Enc oding: g
0150 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 43 6f zip, def late..Co
0160 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 nnection : keep-a
0170 6c 69 76 65 0d 0a 49 66 2d 4d 6f 64 69 66 69 65 live..If -Modifie
0180 64 2d 53 69 6e 63 65 3a 20 54 75 65 2c 20 31 35 d-Since: Tue, 15
0190 20 41 70 72 20 32 30 31 34 20 31 39 3a 32 34 3a Apr 2014 19:24:
01a0 34 38 20 47 4d 54 0d 0a 49 66 2d 4e 6f 6e 65 2d 48 GMT.. If-None-
01b0 4d 61 74 63 68 3a 20 22 62 31 2d 34 66 37 31 39 Match: " b1-4f719

File: "C:\Users\BILLBU~1\AppData\Local\Te... Packets: 60 · Displayed: 2 (3.3%) · Load ti... Profile: Default

443 – Should be encrypted

Memory copy from server – Non-encrypted!



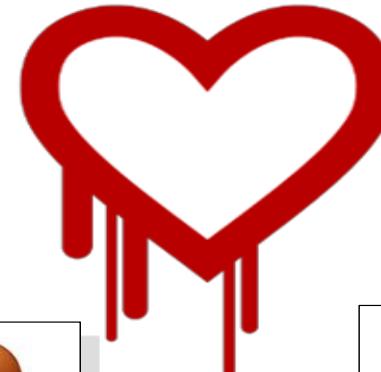
Live Demo ...
perhaps?

Heartbleed ... A Short History

Timeline



Alice (Web)



Bob



Eve

Day Zero Minus 7 (1 April)

New Year's Eve 2011. Robin Seggelmann commits Heartbeat code.



Robin Seggelmann Stephen Henson

1 April 2014. Google inform OpenSSL about vulnerability found by Neel Mehta.



Finnish security company Codenomicon dub it “Heartbleed.”



Day Zero (7 April)

April 8, half of which had no SSL encryption at all. Of those that did, 15% were exposed to the vulnerability.

Trevor Timm @trevortimm 09 Apr Huge thanks to @neelmehta, who just donated his \$15k OpenSSL bounty to support our open-source encryption tools campaign at [@FreedomofPress!](#)

Trevor Timm @trevortimm Thanks to @neelmehta's donation, we've now raised over \$100,000 for a group of great open-source encryption tools: [pressfreedomfoundation.org](#) 2:17 AM - 9 Apr 2014 69 RETWEETS 51 FAVORITES

Re: heartbleed OpenSSL bug CVE-2014-0160

From: Andrew Case <atcuno () gmail com>
Date: Mon, 07 Apr 2014 19:35:47 -0500
its 64KB per request so you can read much more than that through multiple requests
Thanks,
Andrew (@attrc)
On 4/7/2014 7:10 PM, Kirils Solovjovs wrote:
we are doomed.
Description: <http://www.openssl.org/news/vulnerabilities.html>
Article dedicated to the bug: <http://heartbleed.com/>
Tool to check if TLS heartbeat extension is supported:
<http://possible.lv/tools/hb/>

A missing bounds check in the handling of the TLS heartbeat extension can be used to reveal up to 64kB of memory to a connected client or server.
1.0.1[abcdef] affected.
P.S. Happy Monday!

21 March. Neel Mehta discovers



IP Addresses are: [54.230.19.147]
[54.240.160.39] [54.240.160.40] [54.230.17.45]
[54.230.17.192] [54.230.17.201] [54.230.18.79]
[54.230.19.102]

Domain Name: HEARTBLEED.COM

Registrar: GODADDY.COM, LLC

whois Server: whois.godaddy.com

Referral URL: http://registrar.godaddy.com

Name Server: NS-1338.AWSDNS-39.ORG

Name Server: NS-1621.AWSDNS-10.CO.UK

Name Server: NS-473.AWSDNS-59 The Heartbleed Bug

Name Server: NS-697.AWSDNS-23

Status: clientDeleteProhibited

Status: clientRenewProhibited

Status: clientTransferProhibited

Status: clientUpdateProhibited

Updated Date: 07-apr-2014

Creation Date: 05-apr-2014

Expiration Date: 05-apr-2015



21 March (10:23). Google patches



31 March. CloudFare Patch. “Friend says it’s messy!”

1 April. Google inform OpenSSL team



1 April (4pm). OpenSSL distributed to rest of the team.

2 April (9:30) Codenomicon discover bug

3 April Codenomicon tell National Cyber Security Centre Finland (NCSC-FI)

6 April. National Cyber Security Centre Finland asks CERT for CVE number: “on a critical OpenSSL issue”

5 April. Codenomicon register Heartbleed.com

4 April. Rumours abound in Open Source Community

4 April. Akami.com patch servers.



Finnish Communications
Regulatory Authority
National Cyber Security Centre

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected by SSL/TLS for communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and private virtual private networks (VPNs). The Heartbleed bug is being actively exploited on the Internet to steal the memory of the servers enabled to use the vulnerable version of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and impersonate services and users.

What leads in practice?

We review the list of our own services from

attackers perspective. The attacked sources from outside, without leaving a trace. Without using any privileged information or credentials we were able to steal from ourselves the secret keys used for our SSL/TLS services, user names and passwords, instant messages, emails and business critical documents and communication.

How to stop the leak?

As long as the vulnerable version of OpenSSL is in use, it can be exploited. From OpenSSL 1.0.2, has been released, and now it has to be deployed. Operating system vendors and distribution, appliance vendors, independent software vendors have to adopt the fix and update their systems. Software developers have to install the fix as it becomes available for the operating systems, networked appliances and software themselves.



5 April. Codenomicon register Heartbleed.com

be_emo_ava1.jpg be_emo_ava2.jpg be_emo_ava3.jpg

All brushes used were downloaded from www.bittbox.com

Filed under: [Avatars, wallpapers](#) | [21 Comments](#)

The red bubble

11Mar07

This update brings you the wallpaper just right for you. I also made 2 avatars to You can download your version in the wallpaper section.



ava20.jpg ava18.jpg

Filed under: [Avatars, wallpapers](#) | [28 Comments](#)

Heartbleed.com (2005)



The Heartbleed Bug

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop communications, steal data directly from the services and users and to impersonate services and users.

Present

The Heartbleed Bug

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.



Stop the leak?

The vulnerable version of OpenSSL is in use and is to be deployed. Operating system distribution, appliance vendors, software vendors have to adopt the fix for their users. Service providers and users all the fix as it becomes available for the systems, networked appliances and software



8pm, 7 April 2014

6 April. Mark Cox (OpenSSL and Red Hat) notifies Red Hat and private bug fix added.

7 April (before this date). Facebook “Informed through a friend.” and patch systems.

7 April. The National Cyber Security Centre Finland reports bug to OpenSSL core team members Ben Laurie (who works for Google) and Mark Cox (Red Hat) via encrypted email.

7 April (10:30) OpenSSL fix bug and posts bug.



11am: CloudFlare publish details



12:35: Neel tweets details



CODENOMICON

13:13: Codenomicon tweet details



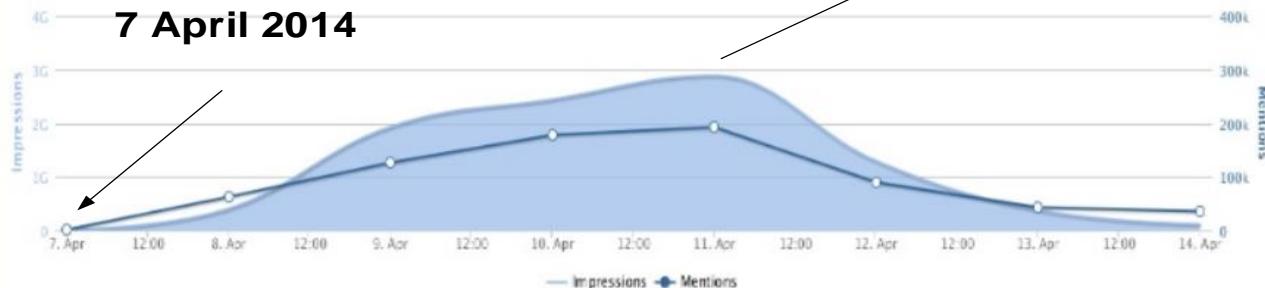
MENTIONS AND REACH

11 April 2014



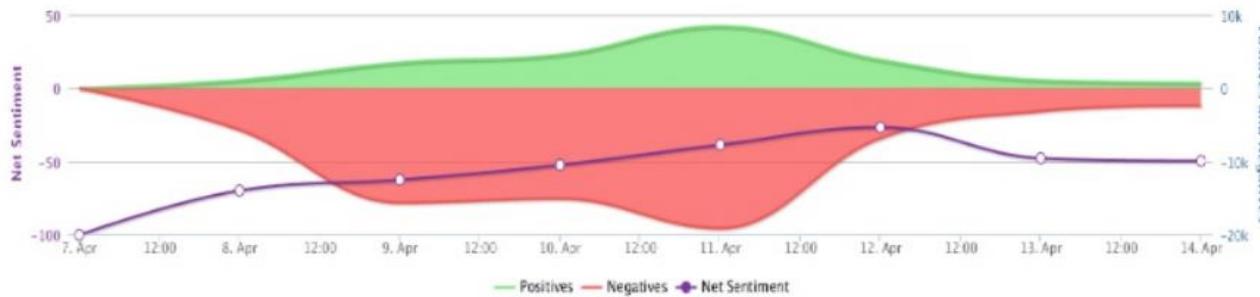
Mentions, which refers to the number of times "Heartbleed" appeared on a website or social media post, peaked on April 11, four days after the news broke.

7 April 2014



SENTIMENT

Despite the ebb and flow of conversation volume, sentiments of relevant dialogue continued to be extremely negative.



Source: NetBase Aggregated Social Listening Data, April 7 to April 14, 2014 (Global)

Apr 03, 2014 - Apr 11, 2014

● NASDAQ:AMZN -8.75% ● NYSE:HP -1.51% ● NASDAQ:DELL -0.00% ● GOOGL -4.41% ● AOL -2.77% ● MSFT -4.67% ● YHOO -9.41%



Untitled - Notepad

```
File Edit Format View Help

0700: BC 9C 2D 61 5F 32 36 30 35 26 2E 73 61 76 65 3D ...-a_2605&.save=
0710: 26 70 61 73 73 77 64 5F 72 61 77 3D 06 14 CE 6F &passwd_raw=...o
0720: A9 13 96 CA A1 35 1F 11 79 2B 20 BC 2E 75 3D 63 .....5..y+ ..u=c
0730: 6A 66 6A 6D 31 68 39 6B 37 6D 36 30 26 2E 76 3D jfjm1h9k7m60&.v=
0740: 30 26 2E 63 68 61 6C 6C 65 6E 67 65 3D 67 7A 37 0&.challenge=gz7
0750: 6E 38 31 52 6C 52 4D 43 6A 49 47 4A 6F 71 62 33 n81R1RMcJIGJoqb3
0760: 75 69 72 61 2E 6D 6D 36 61 26 2E 79 70 6C 75 73 uira.mm6a&.yplus
0770: 3D 26 2E 65 6D 61 69 6C 43 6F 64 65 3D 26 70 6B =&.emailCode=&pk
0780: 67 3D 26 73 74 65 70 69 64 3D 26 2E 65 76 3D 26 g=&stepid=&.ev=&
0790: 68 61 73 4D 73 67 72 3D 30 26 2E 63 68 6B 50 3D hasMsgr=&.chkP=
07a0: 59 26 2E 64 6F 6E 65 3D 68 74 74 70 25 33 41 25 Y&.done=http%3A%
07b0: 32 46 25 32 46 6D 61 69 6C 2E 79 61 68 6F 6F 2E 2F%2Fmail.yahoo.

07c0: 63 6F 6D 26 2E 78 64 3D 79 6D 5F 76 65 72 25 33 com&.pd-y_m_ver%3
07d0: 44 30 25 32 36 63 25 33 44 25 32 36 69 76 74 25 D0%26c%3D%261vt%3
07e0: 33 44 25 32 36 73 67 25 33 44 26 2E 77 73 3D 31 3D%26sg%3D&.ws=1
07f0: 26 2E 63 70 3D 30 26 6E 72 3D 30 26 70 61 64 3D &.cp=0&nr=0&pad=
0800: 36 26 61 61 64 3D 36 26 6C 6F 67 69 6E 3D 61 67 6&aad=6&login=ag
0810: 6E 65 73 61 64 75 62 6F 61 74 65 6E 67 25 34 38 nesaduboateng%40
0820: 79 61 68 6F 6F 2E 63 6F 6D 26 70 61 73 73 77 64 yahoo.com&passwd
0830: 3D 30 32 34 =024 &pe
```

Major
companies
informed

Users are being encouraged to change their passwords on sites that have tackled the bug.

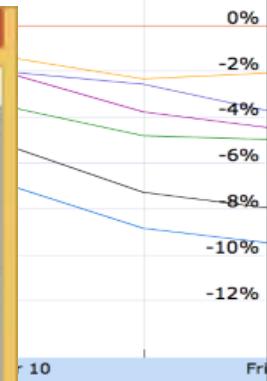
Several tech firms are urging people to change all their passwords after the discovery of a major security flaw.

Related Stories



Bazooka that Brazuca
Secrets of the new ball for the World Cup

Stallholder's son



Turkey mine blast
death toll rises

victims found
new peace bid
for young and old
business appeal

James diary
parts from the Croisette on this
film festival

campus
self-contained community for
young people

ban

seeks to clamp down on
subsidy misuse

Agnes Adu Boateng



bible@gospelhall.org

0244718210	027-6661888	alanadua@yahoo.co.uk albertadjei7@yahoo.com
0244652780	0262652780	c_amusahadjie@yahoo.com
0277-442491		hayford.king@gmail.com
0244-624848		adoboemensah@yahoo.co.uk
0302-256224/5		aak@ghana.com
0248418422		agnesaduboateng@yahoo.com
277495932		safarihost@yahoo.com
020812525		kbadusei@hotmail.com / kbadusei@gmail.com
0244174956	0208120068	ralak58@yahoo.com

agnesaduboateng@yahoo.com

Untitled - Notepad

```
File Edit Format View Help
0700: BC 9C 2D 61 5F 32 36 30 35 26 2E 73 61 76 65 3D ...-a_2605&.save=
0710: 26 70 61 73 73 77 64 5F 72 61 77 3D 06 14 CE 6F &passwd_raw=...o
0720: A9 13 96 CA A1 35 1F 11 79 2B 20 BC 2E 75 3D 63 ....5..y+ ..u=c
0730: 6A 66 6A 6D 31 68 39 6B 37 6D 36 30 26 2E 76 3D jfjm1h9k7m60&.v=
0740: 30 26 2E 63 68 61 6C 6C 65 6E 67 65 3D 67 7A 37 0&.challenge=gz7
0750: 6E 38 31 52 6C 52 4D 43 6A 49 47 4A 6F 71 62 33 n81R1RMcJIGJoqb3
0760: 75 69 72 61 2E 6D 6D 36 61 26 2E 79 70 6C 75 73 uira.mm6a&.yplus
0770: 3D 26 2E 65 6D 61 69 6C 43 6F 64 65 3D 26 70 6B =&.emailCode=&pk
0780: 67 3D 26 73 74 65 70 69 64 3D 26 2E 65 76 3D 26 g=&stepid=&.ev=&
0790: 68 61 73 4D 73 67 72 3D 30 26 2E 63 68 6B 50 3D hasMsgr=0&.chkP=
07a0: 59 26 2E 64 6F 6E 65 3D 68 74 74 70 25 33 41 25 Y.&.done=http%3A%
07b0: 32 46 25 32 46 6D 61 69 6C 2E 79 61 68 6F 6F 2E 2F%2Fmail.yahoo.
07c0: 63 6F 6D 26 2E 70 64 3D 79 6D 5F 76 65 72 25 33 com&.pd=y_m_ver%3
07d0: 44 30 25 32 36 63 25 33 44 25 32 36 69 76 74 25 D0%26c%3D%26ivt%
07e0: 33 44 25 32 36 73 67 25 33 44 26 2E 77 73 3D 31 3D%26sg%3D&.ws=1
07f0: 26 2E 63 70 3D 30 26 6E 72 3D 30 26 70 61 64 3D &.cp=0&nr=0&pad=
0800: 36 26 61 61 64 3D 36 26 6C 6F 67 69 6E 3D 61 67 6&aad=6&login=ag
0810: 6E 65 73 61 64 75 62 6F 61 74 65 6E 67 25 34 30 nesaduboateng%40
0820: 79 61 68 6F 2E 63 6F 6D 26 70 61 73 73 77 64 yahoo.com&passwd
0830: 3D 30 32 34 =024 &.pe
```



Chartered Institute of Taxation (Ghana)
(ESTABLISHED IN 1980)
THE PROFESSIONAL BODY FOR TAX PROFESSIONALS

<http://www.taxghana.org>
List of Members in Good Standing at 2013



How much do you need for open source?



**Apache Software
Foundation
(\$905,732- 2013)**

**Linux Foundation
(\$6.25 million -
2014)**

**Mozilla Foundation
(\$311 million - 2012)**

OpenSSL? Marquess ... “A few million a year would do grandly. There should be half a dozen guys working full-time, plus support.”

24 April 2104

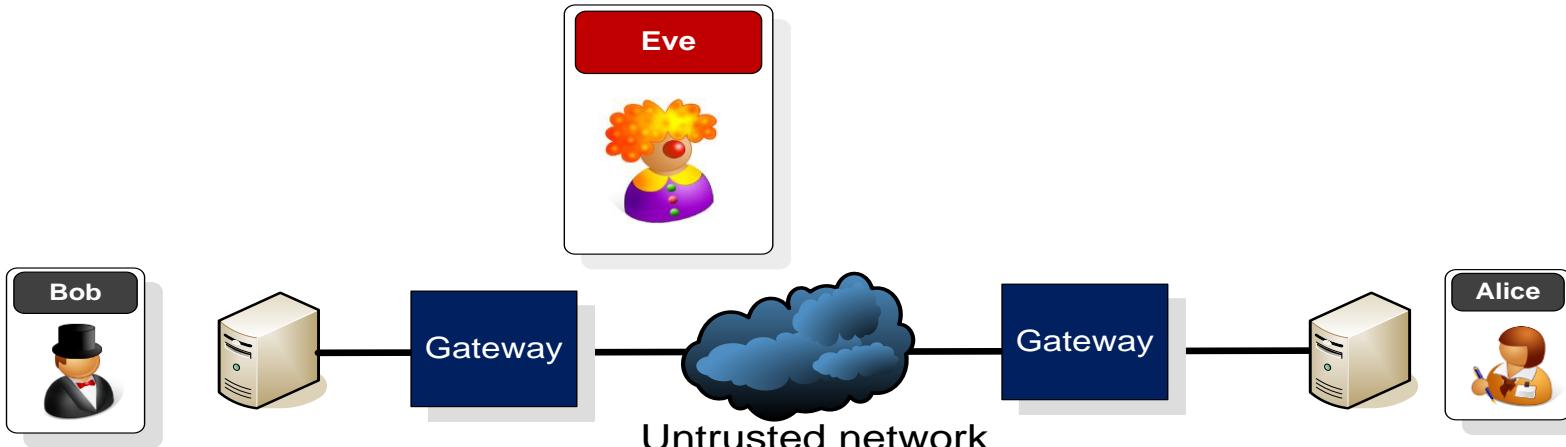
Linux Foundation defines Core Infrastructure Initiative, - multimillion-dollar project funding critical path - \$3.9 million for three years, ... Top of List ... OpenSSL.



Network Security



VPNs



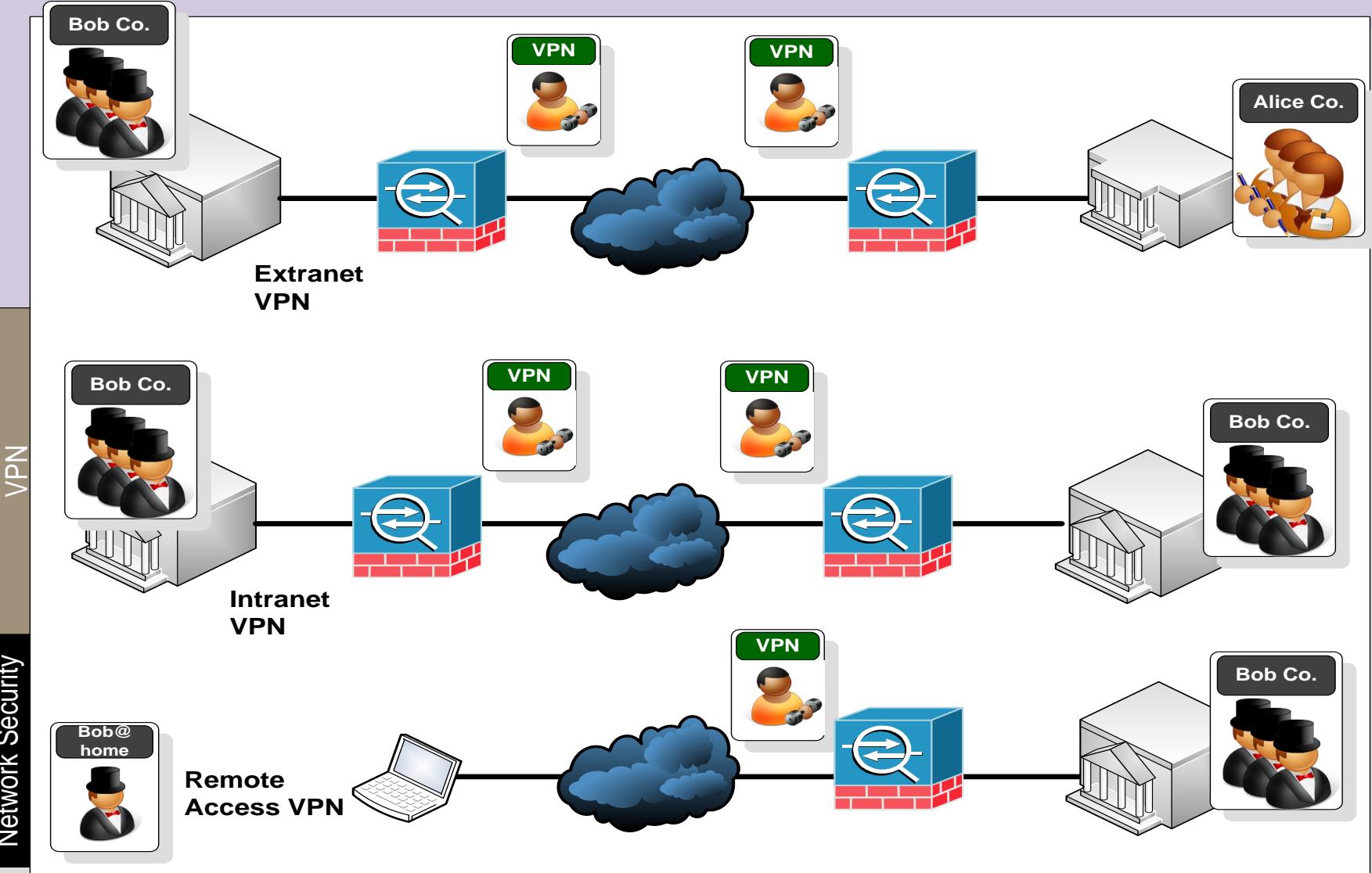
What is required is:

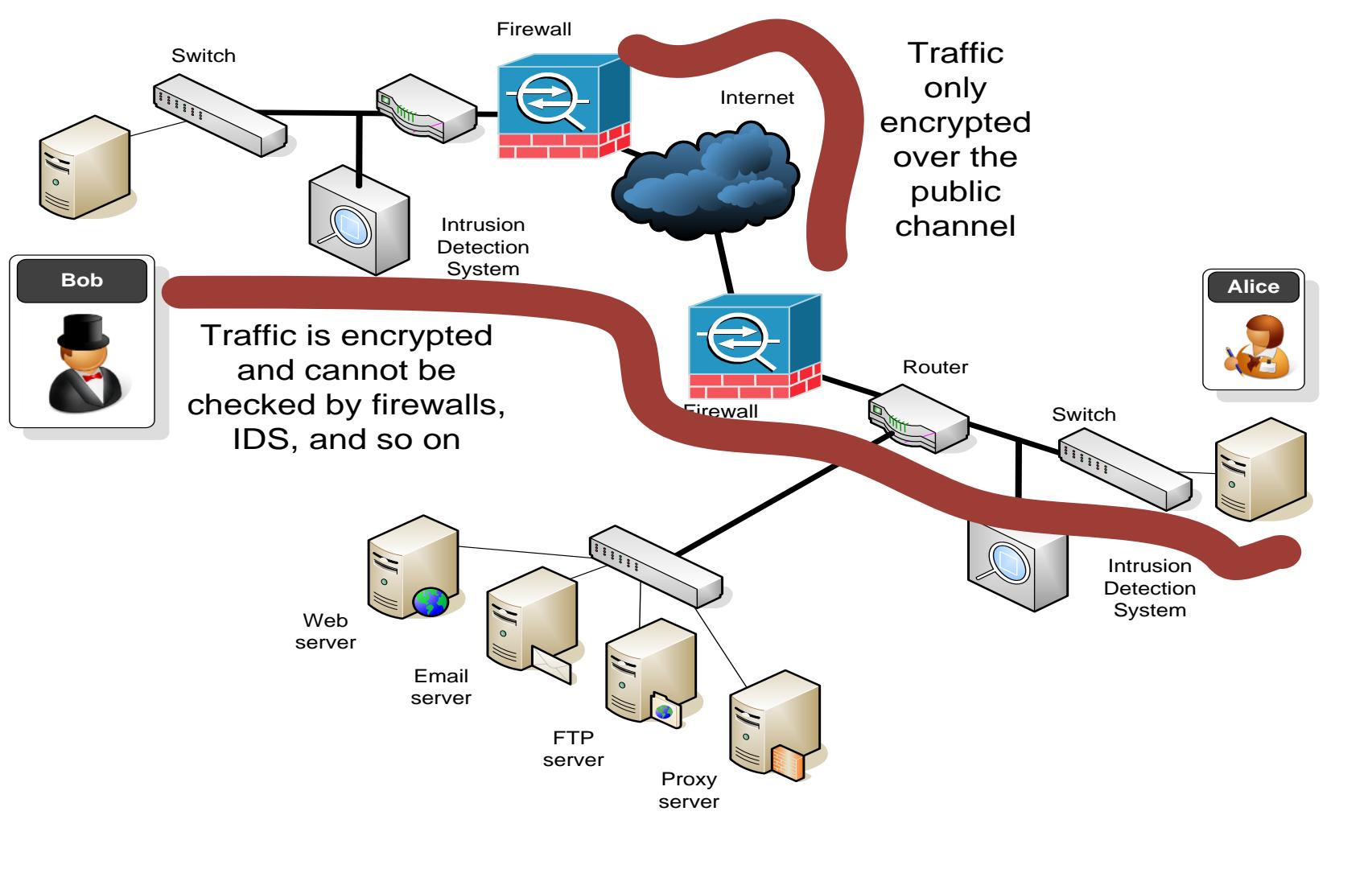
- Encryption.
- Authentication of devices (to overcome spoofing)
- Authentication of packets (for integrity)

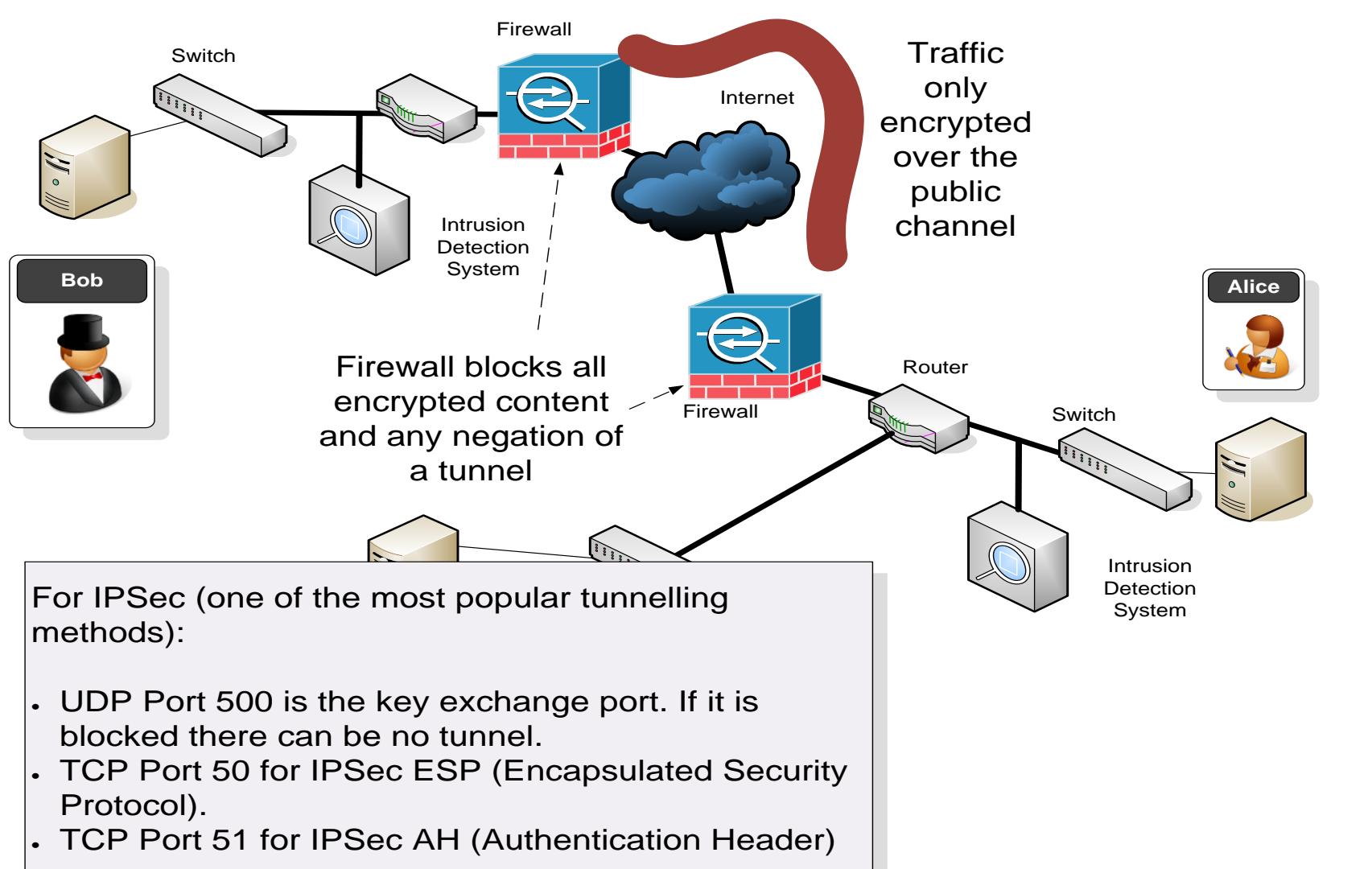
PPTP (Point-to-point Tunneling Protocol). Created by Microsoft and is routable. It uses MPPE (Microsoft Point-to-point Encryption) and user authentication.

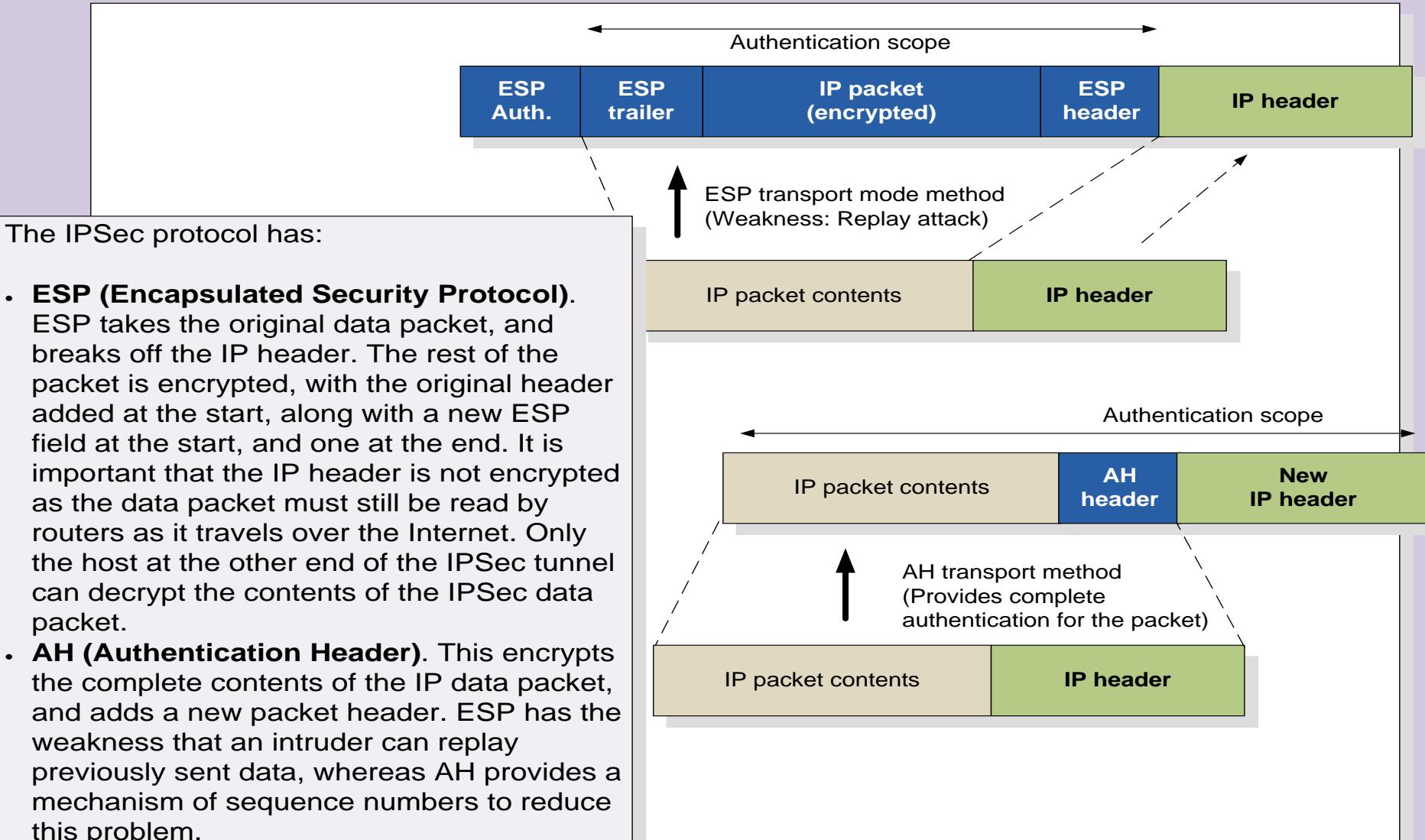
L2TP (Layer 2 Tunneling Protocol). Works at Layer 2 to Forward IP, IPX and AppleTalk (RFC2661). Cisco, Microsoft, Ascent and 3Com developed it. User and machine authentication, but no encryption (but can be used with L2TP over IPSec).

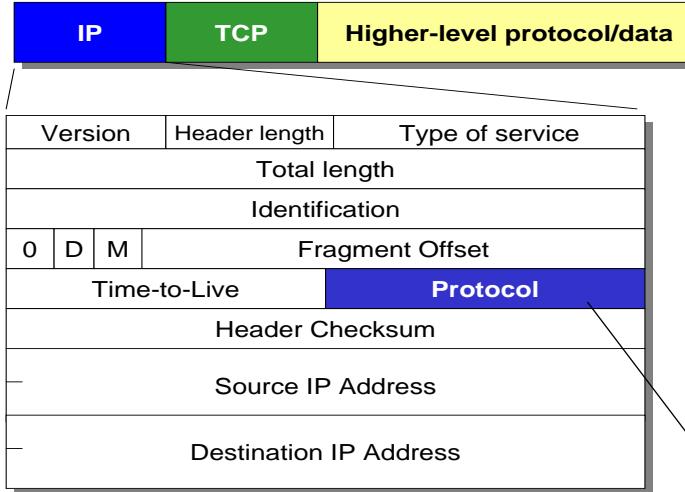
IPSec. An open standard. Includes both encryption and Authentication.



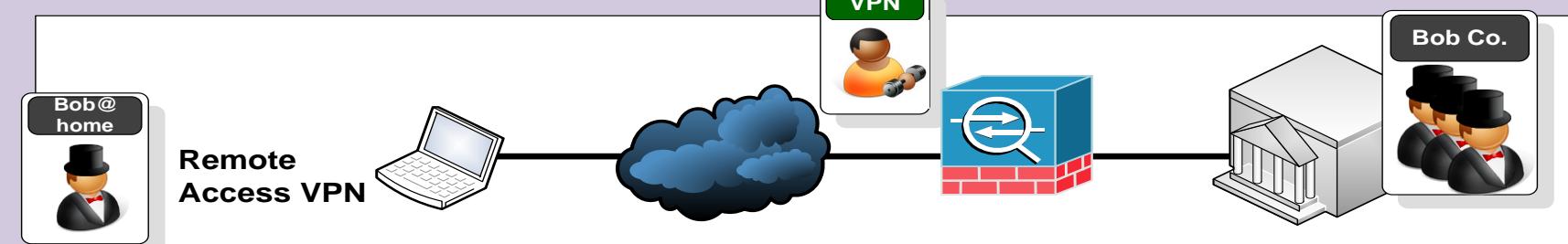








- 1 ICMP Internet Control Message [RFC792]
- 6 TCP Transmission Control [RFC793]
- 8 EGP Exterior Gateway Protocol [RFC888]
- 9 IGP any private interior gateway [IANA]
- 47 GRE General Routing Encapsulation (PPTP)**
- 50 ESP Encap Security Payload [RFC2406]**
- 51 AH Authentication Header [RFC2402]**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

Phase 2

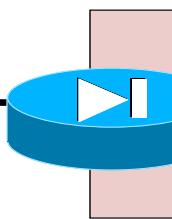
Defines the policies for transform sets, peer IP addresses/hostnames and lifetime settings.

Crypto maps are exchanged

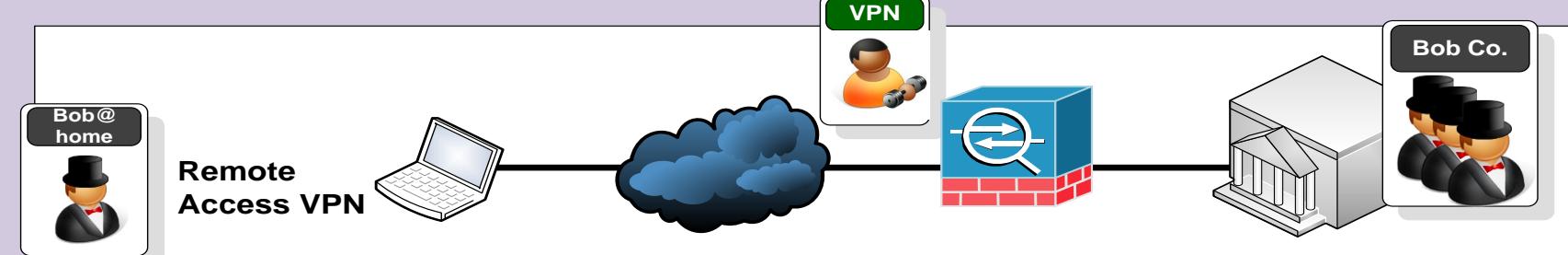
- AH, ESP (or both)
- Encryption (DES, 3DES)
- ESP (tunnel or transport)
- Authentication (SHA/MD5)
- SA lifetimes defined
- Define the traffic of interest

```
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
```

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

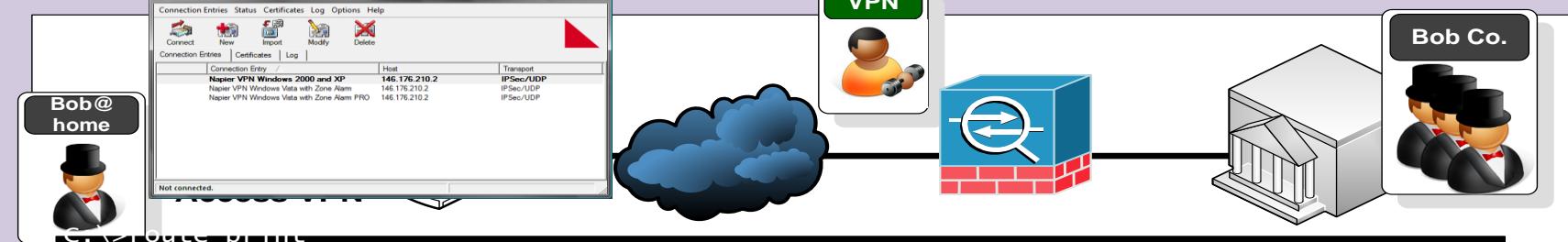
Network Security

```
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
```



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

=====

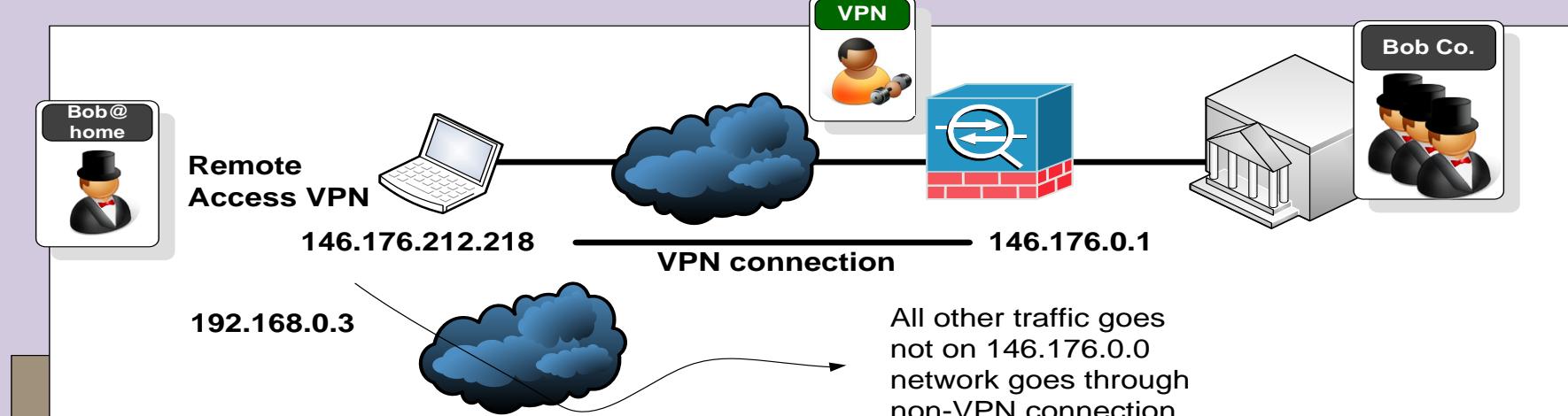
Active Routes:

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

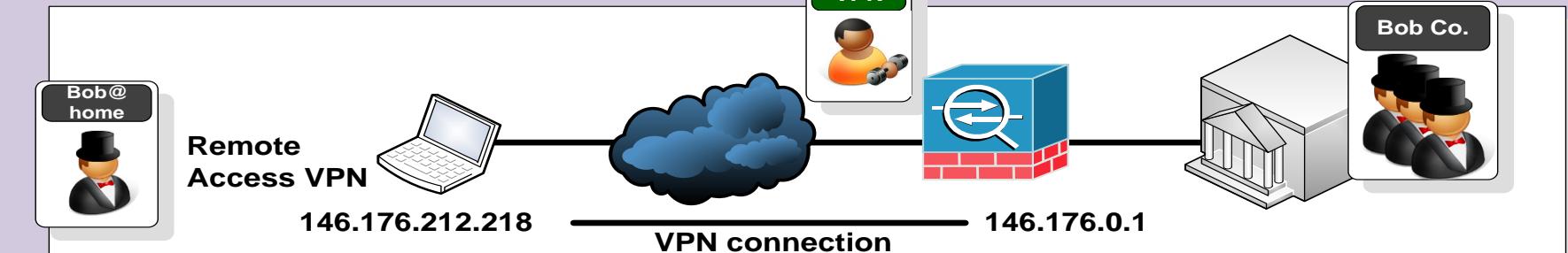


```

=====
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
...
=====

Persist
After connecting to the VPN
  
```



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

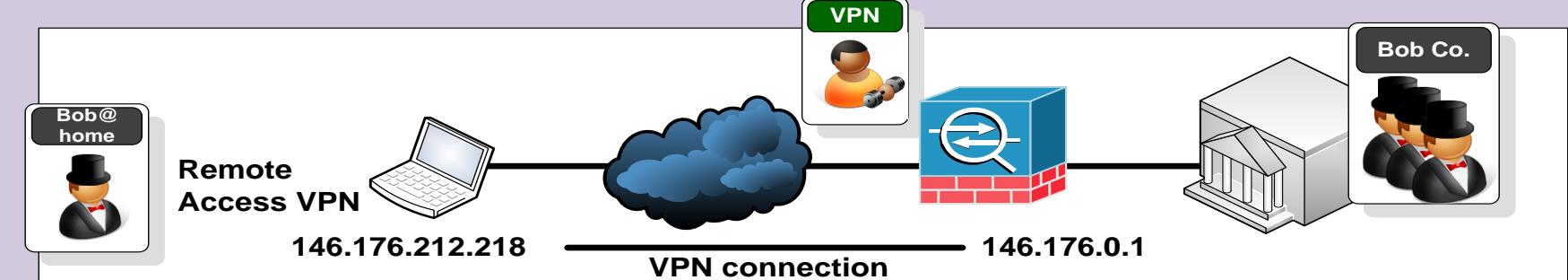
Tracing route to www.napier.ac.uk [146.176.222.174]
over a maximum of 30 hops:

1	2 ms	2 ms	6 ms	192.168.0.1	Before VPN connection
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					

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	After VPN connection
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]	



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