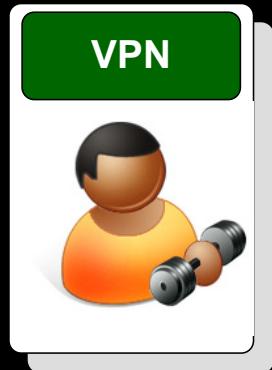
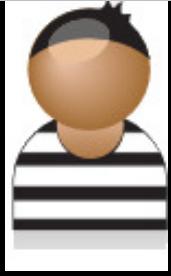


Network Security

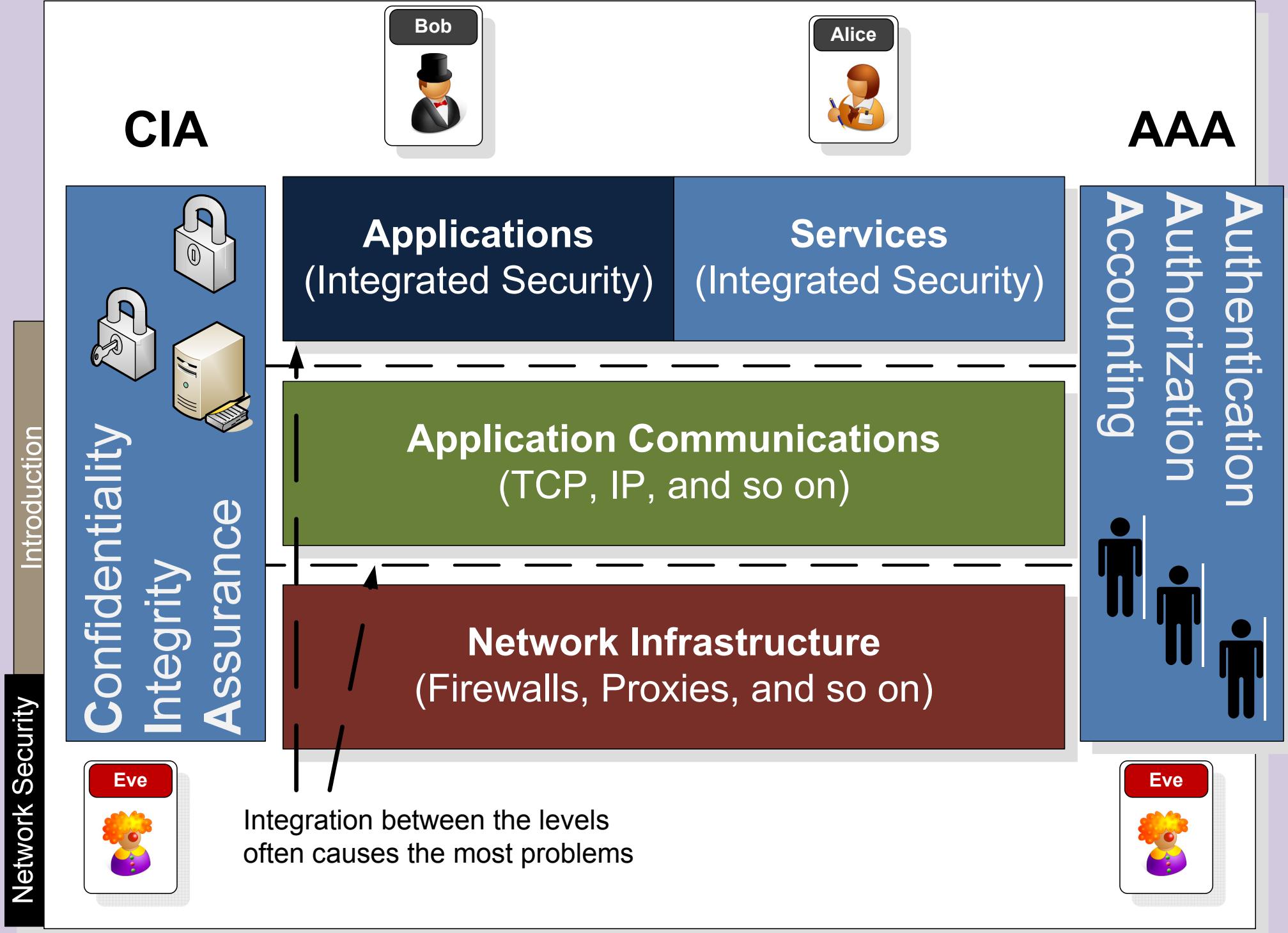
Introduction
Screening Firewalls
NAT
Stateful Firewalls
PIX/ASA Firewall
Proxies
VPN
Tunnelling



Network Security

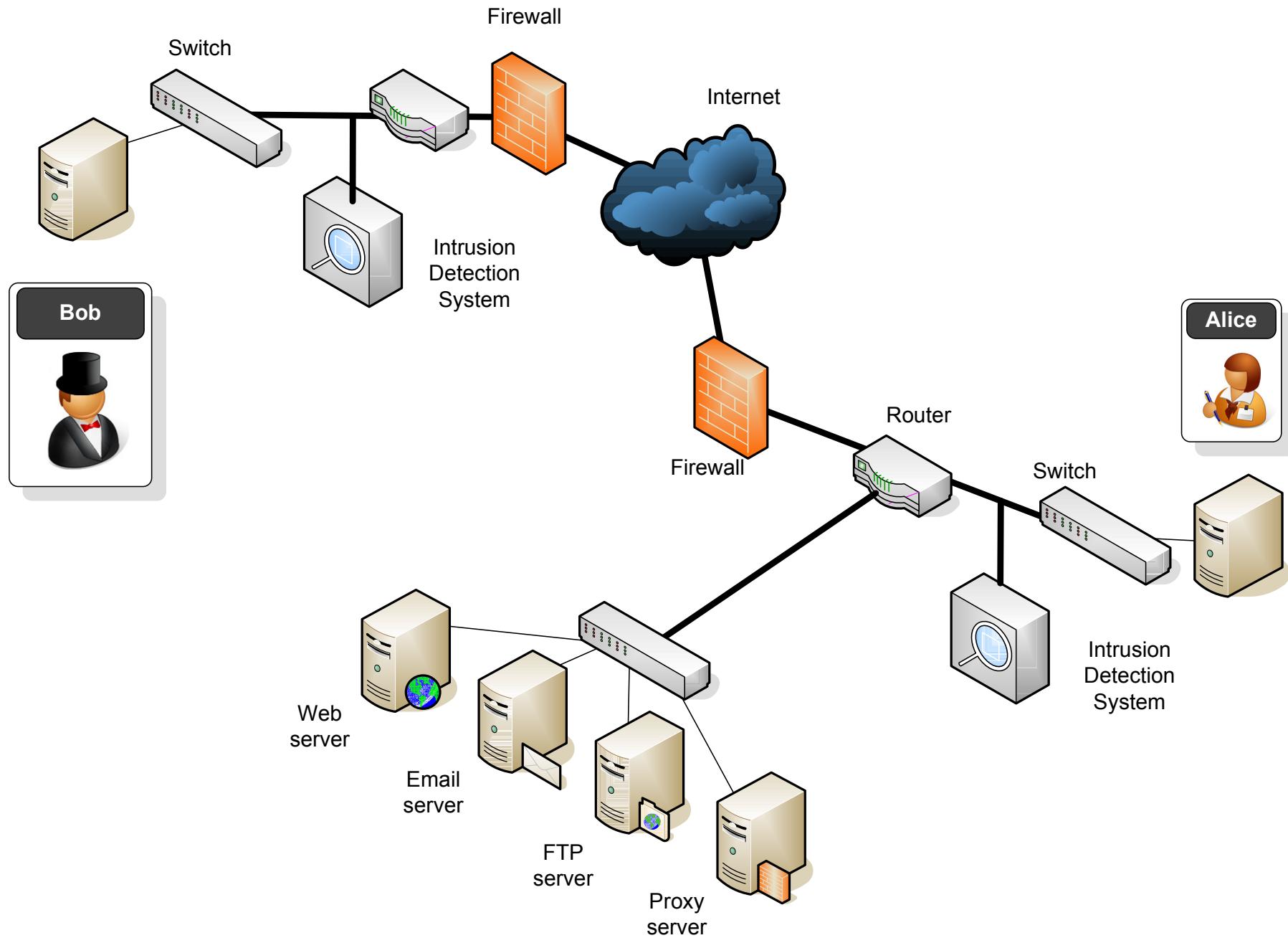


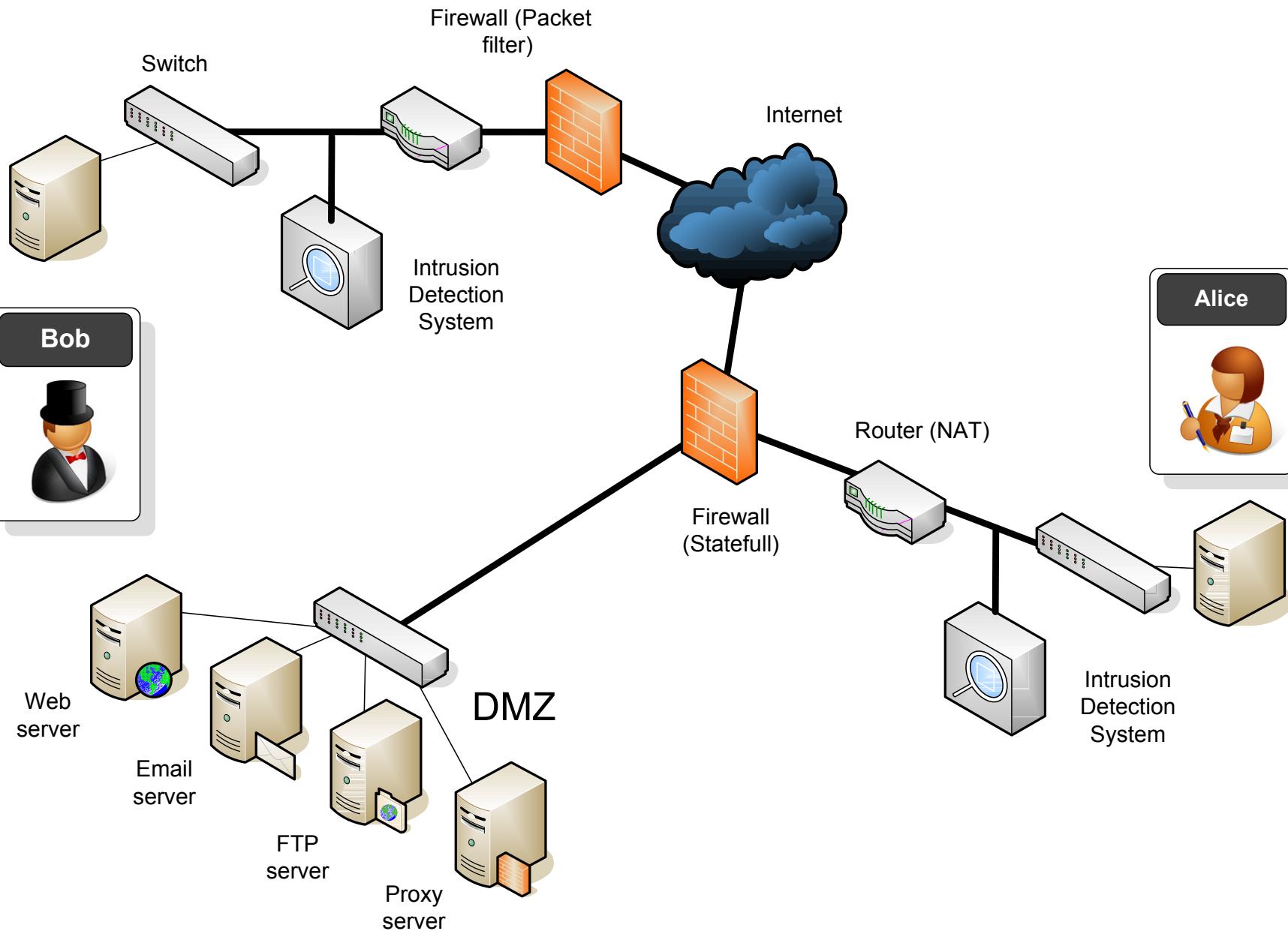
Introduction



Network Security

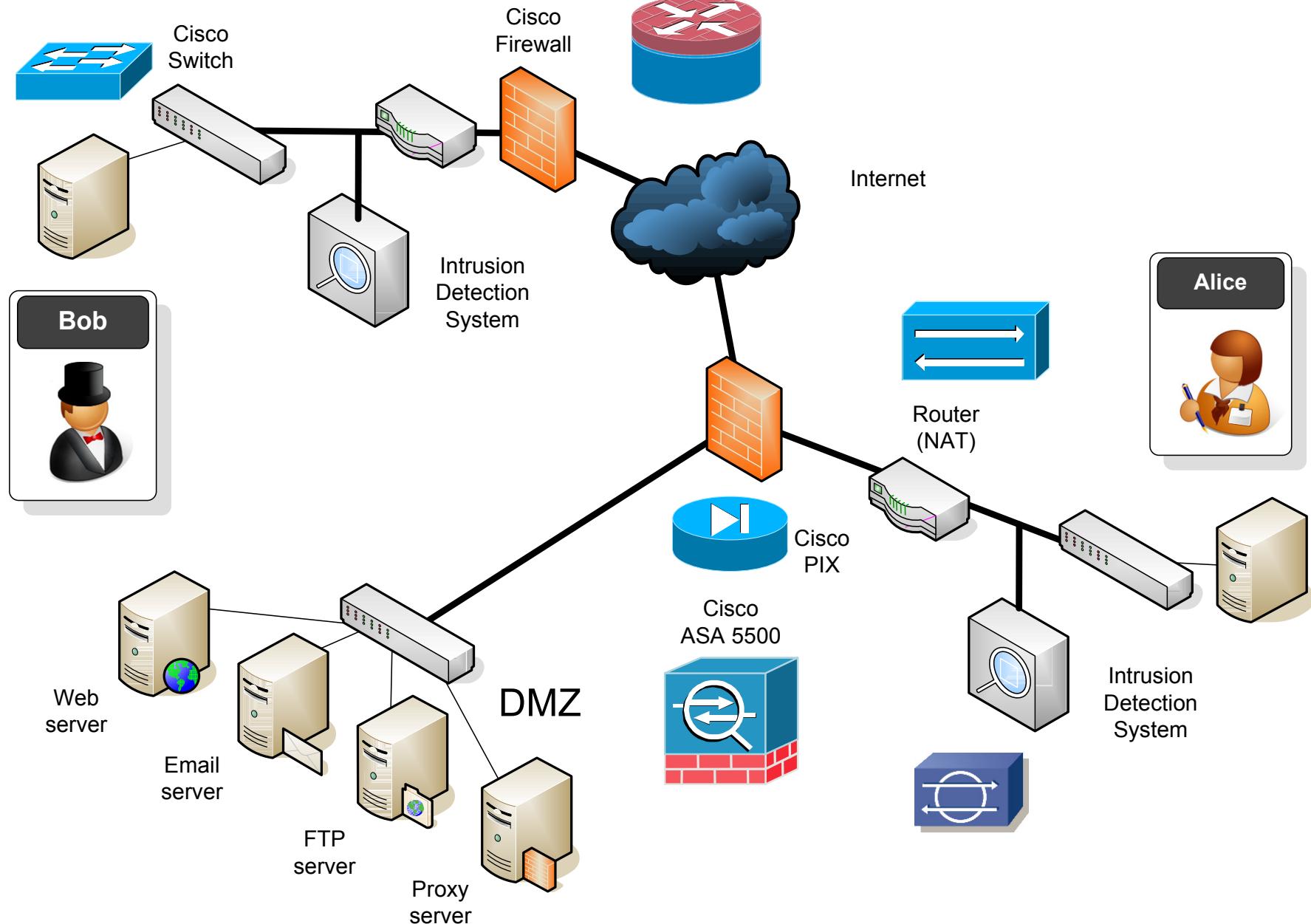
Introduction

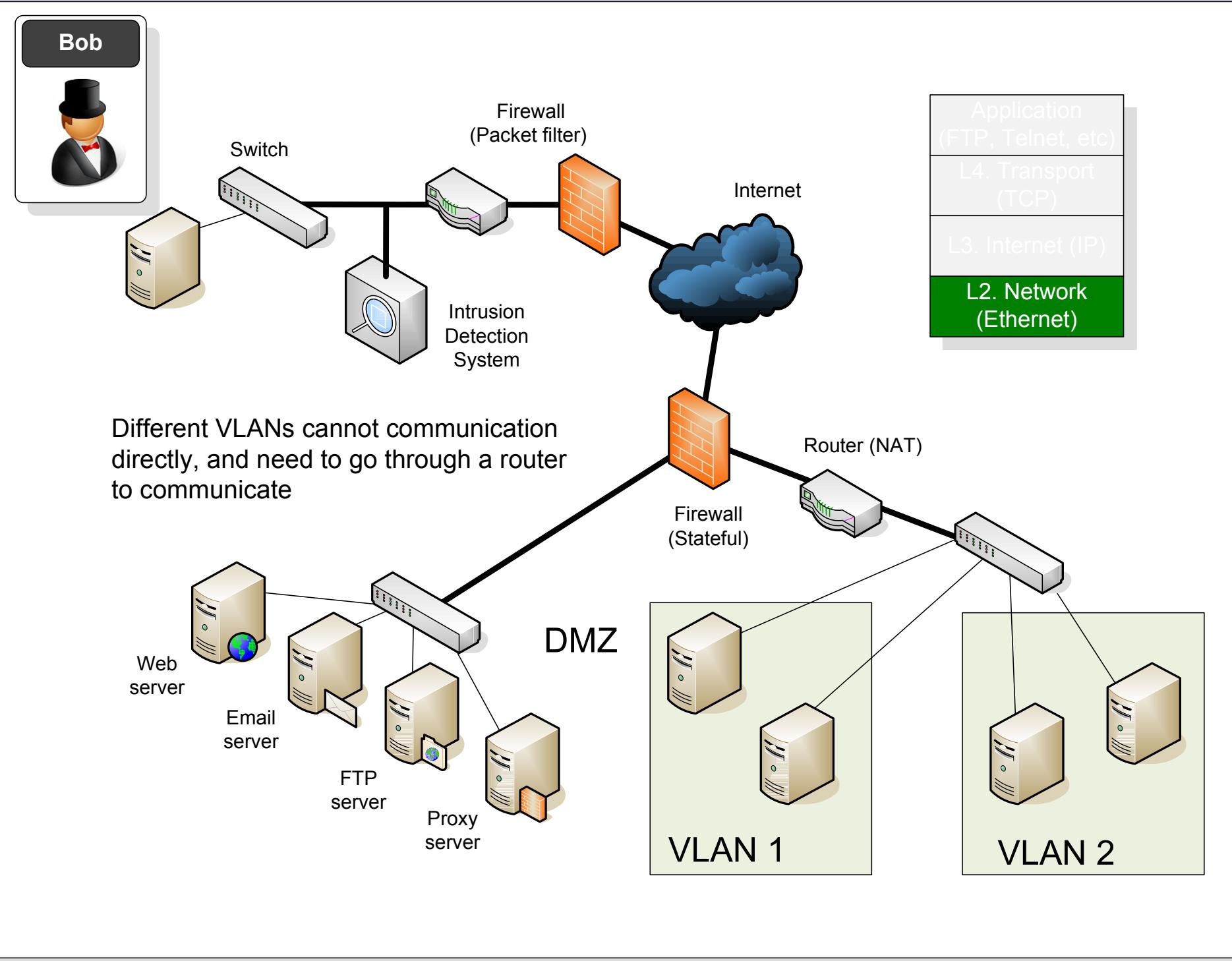


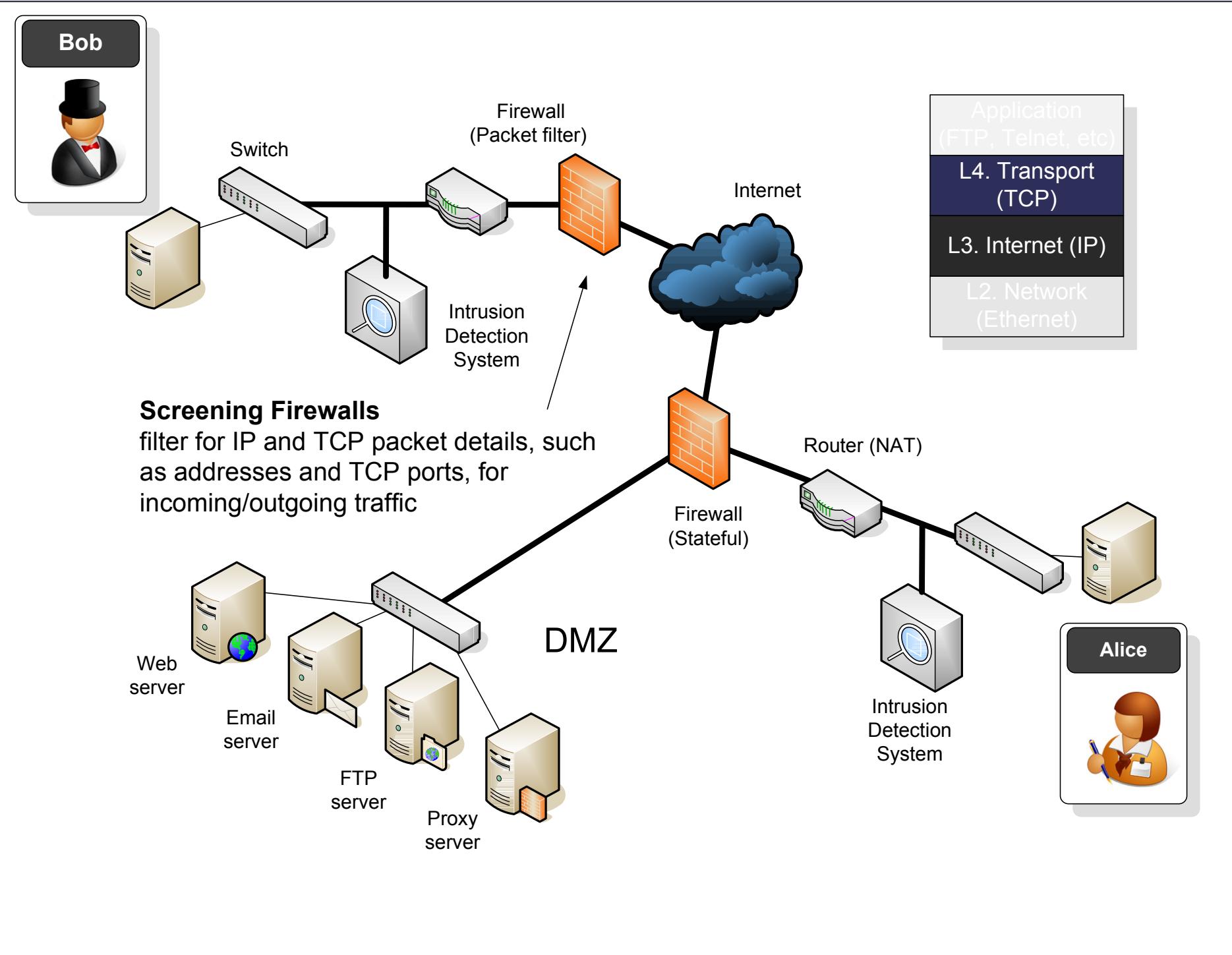


Network Security

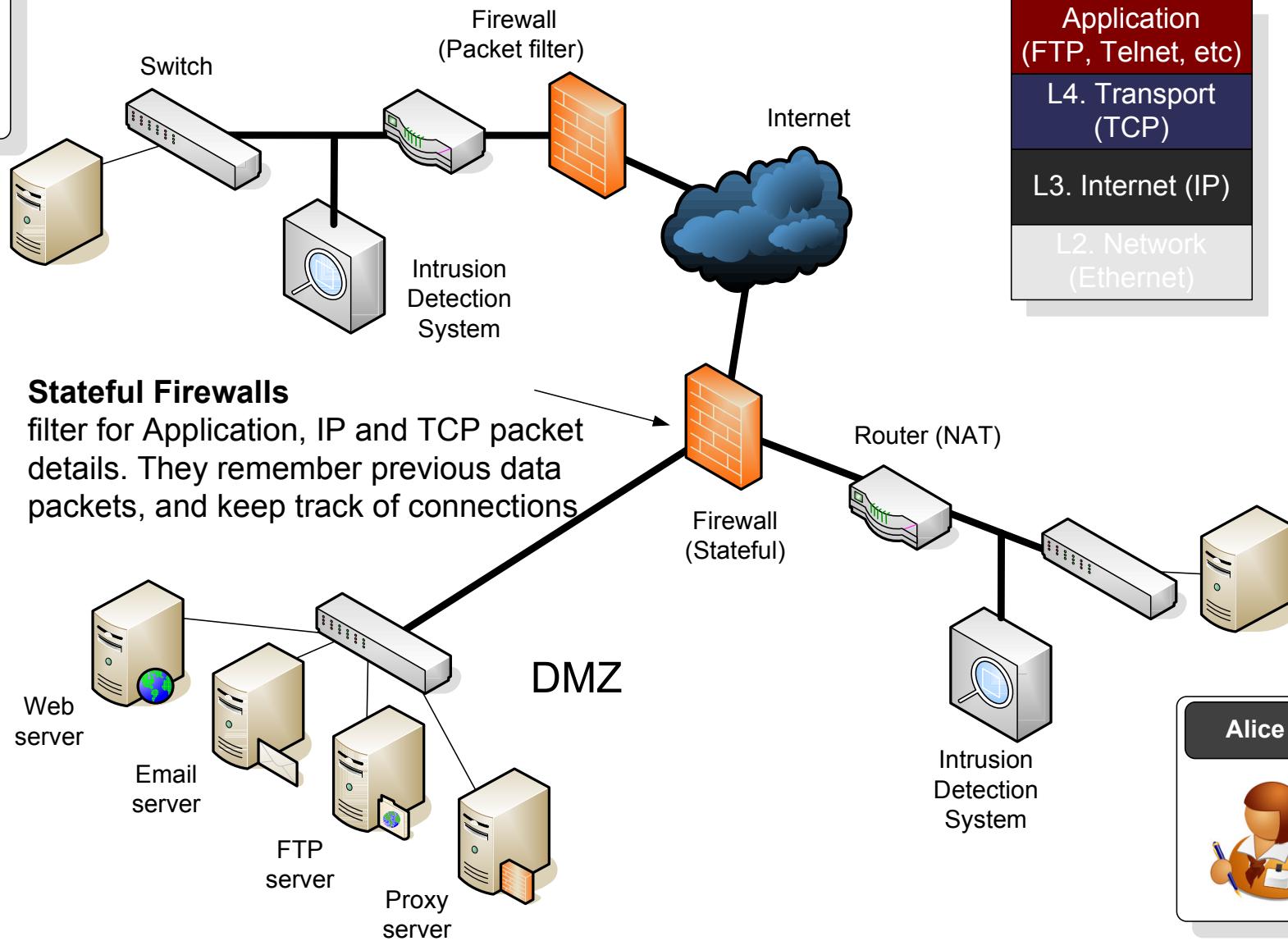
Introduction

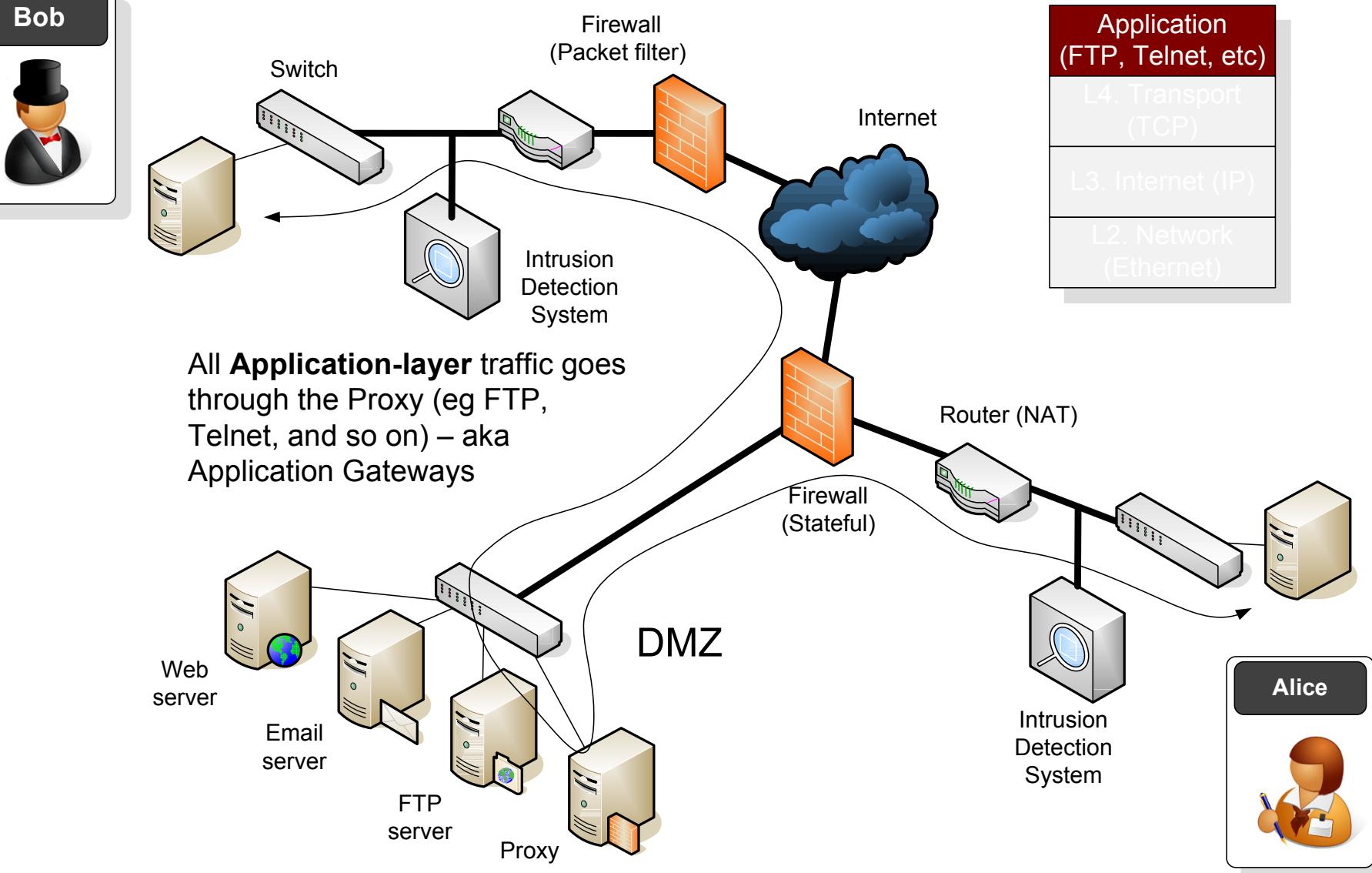




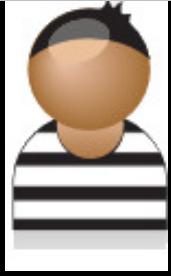


Bob





Network Security

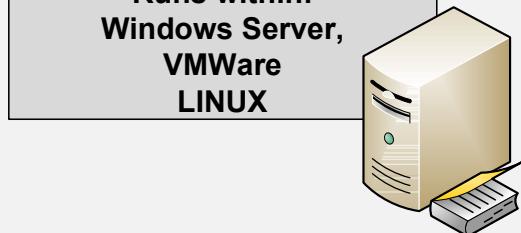


Screening Firewalls



CheckPoint firewall (software)

Runs within:
Windows Server,
VMWare
LINUX



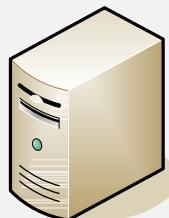
CheckPoint firewall (dedicated) Nokia

Software firewall

Host-based: Zone alarm



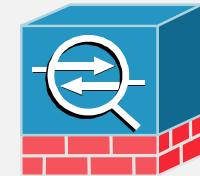
LINUX iptables



Hardware firewall



Cisco router With firewall (non-stateful)



Cisco PIX/ASA (stateful)

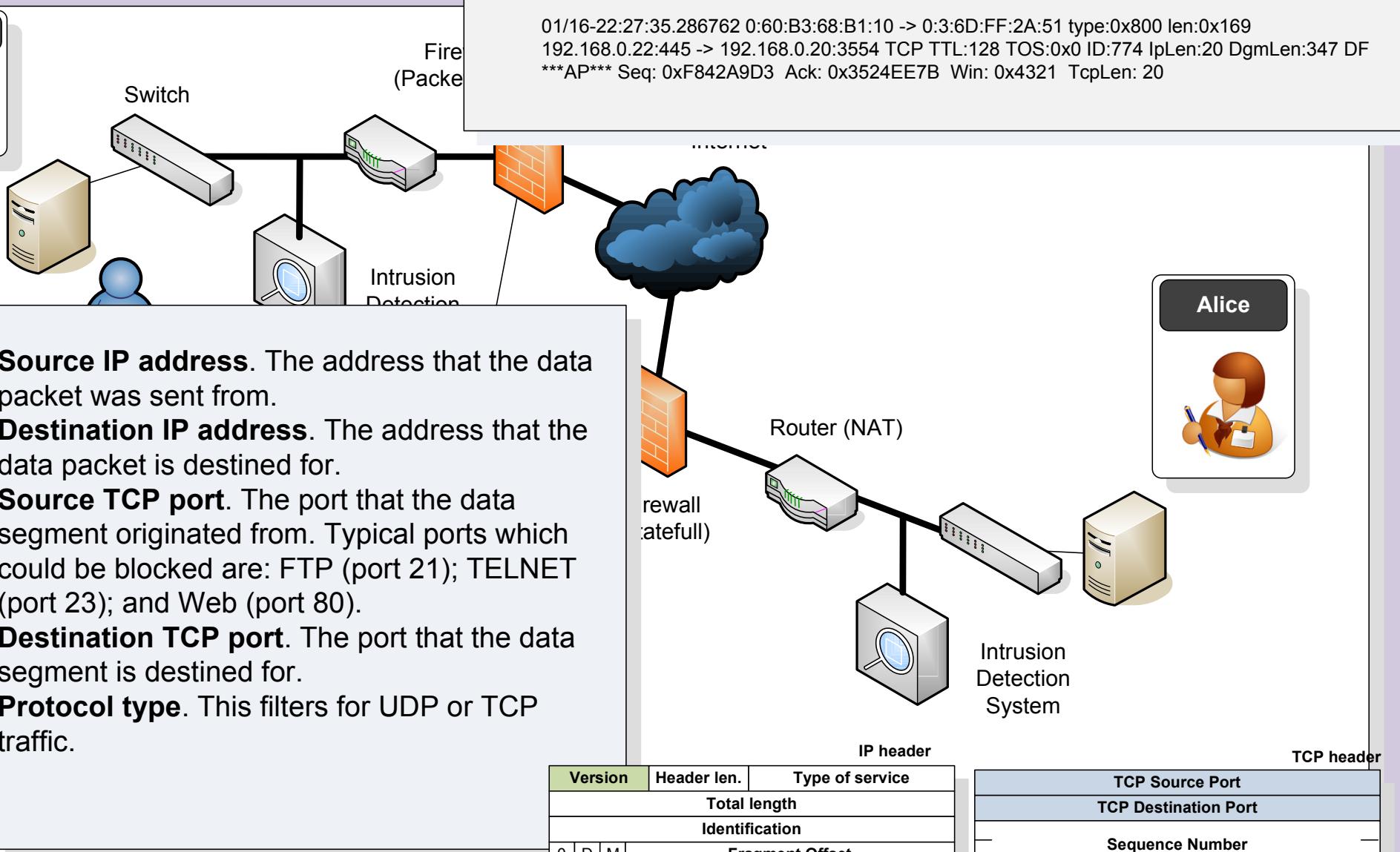


Software firewall:

- Easy to reconfigure
- Slower
- Less expensive
- Can be used with a range of computers/OSs

Hardware firewall:

- Optimized engine/architecture
- Copes better with large traffic conditions
- Improved failover



Source IP address. The address that the data packet was sent from.

Destination IP address. The address that the data packet is destined for.

Source TCP port. The port that the data segment originated from. Typical ports which could be blocked are: FTP (port 21); TELNET (port 23); and Web (port 80).

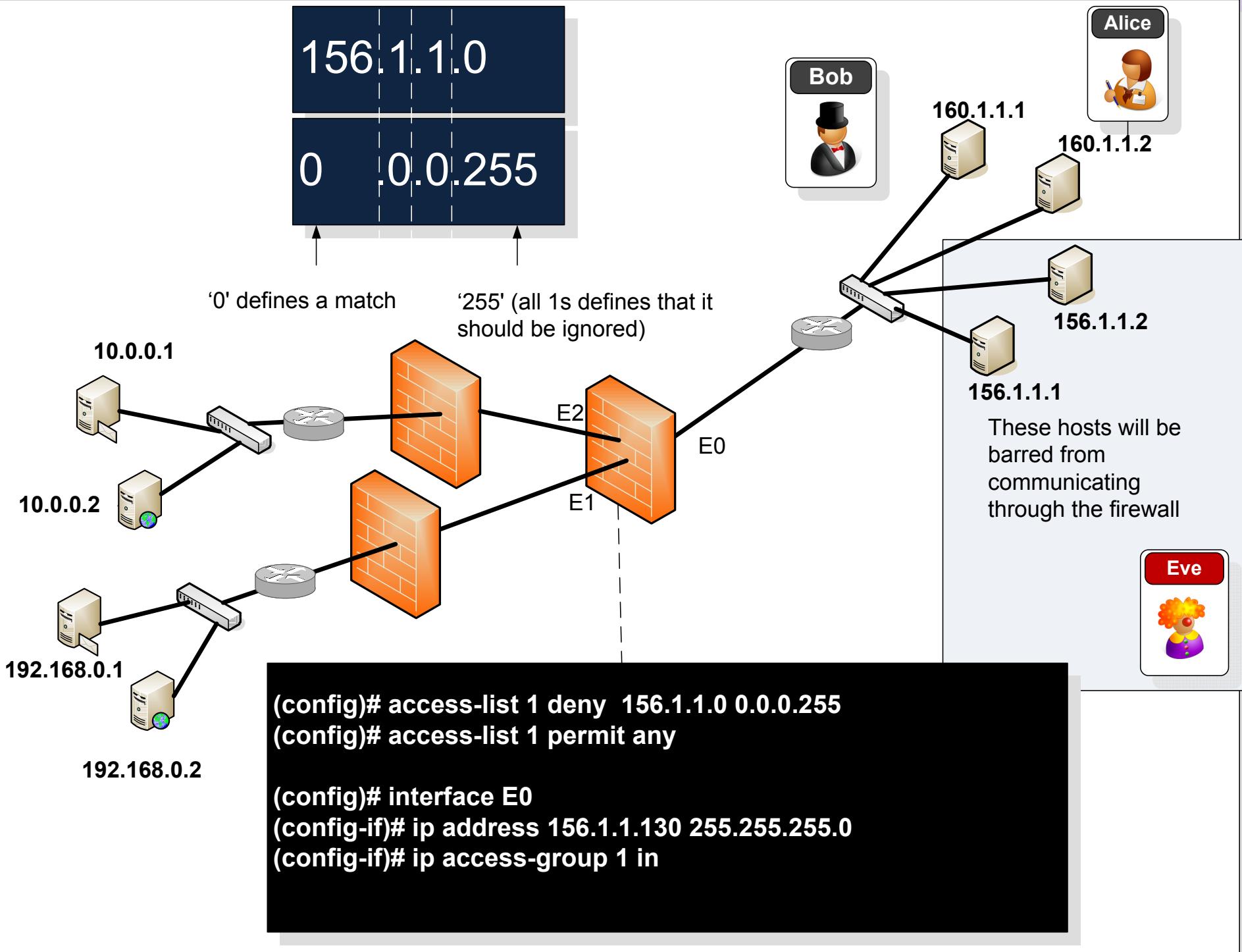
Destination TCP port. The port that the data segment is destined for.

Protocol type. This filters for UDP or TCP traffic.

Version	Header len.	Type of service
		Total length
		Identification
0	D	M
		Fragment Offset
		Time-to-live (TTL)
		Protocol
		Header Checksum
		Source IP Address
		Destination IP Address

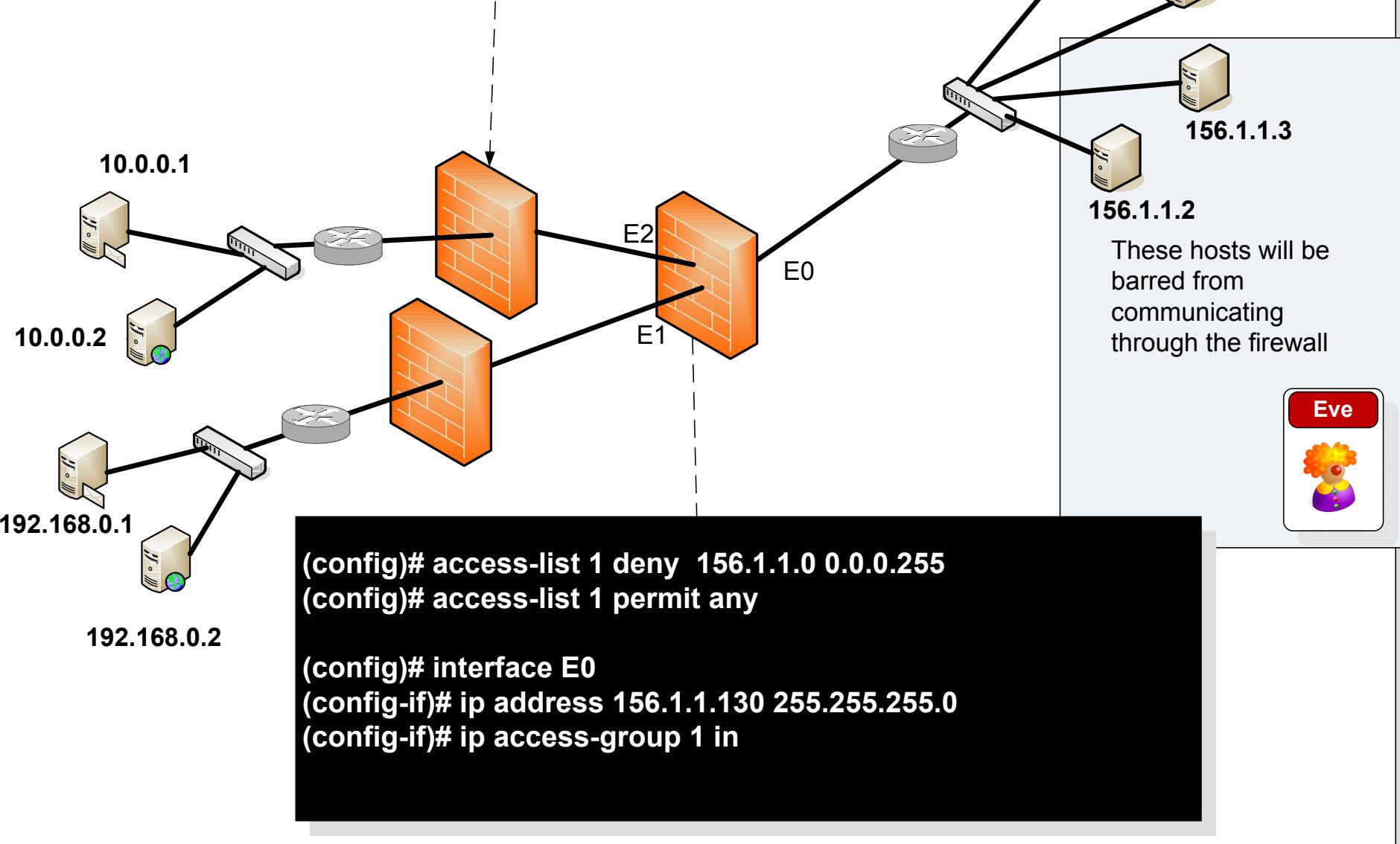
TCP header	
TCP Source Port	
TCP Destination Port	
Sequence Number	
Acknowledgement Number	
Data Offset	Flags/Reserved
Window	
Checksum	
Urgent Pointer	





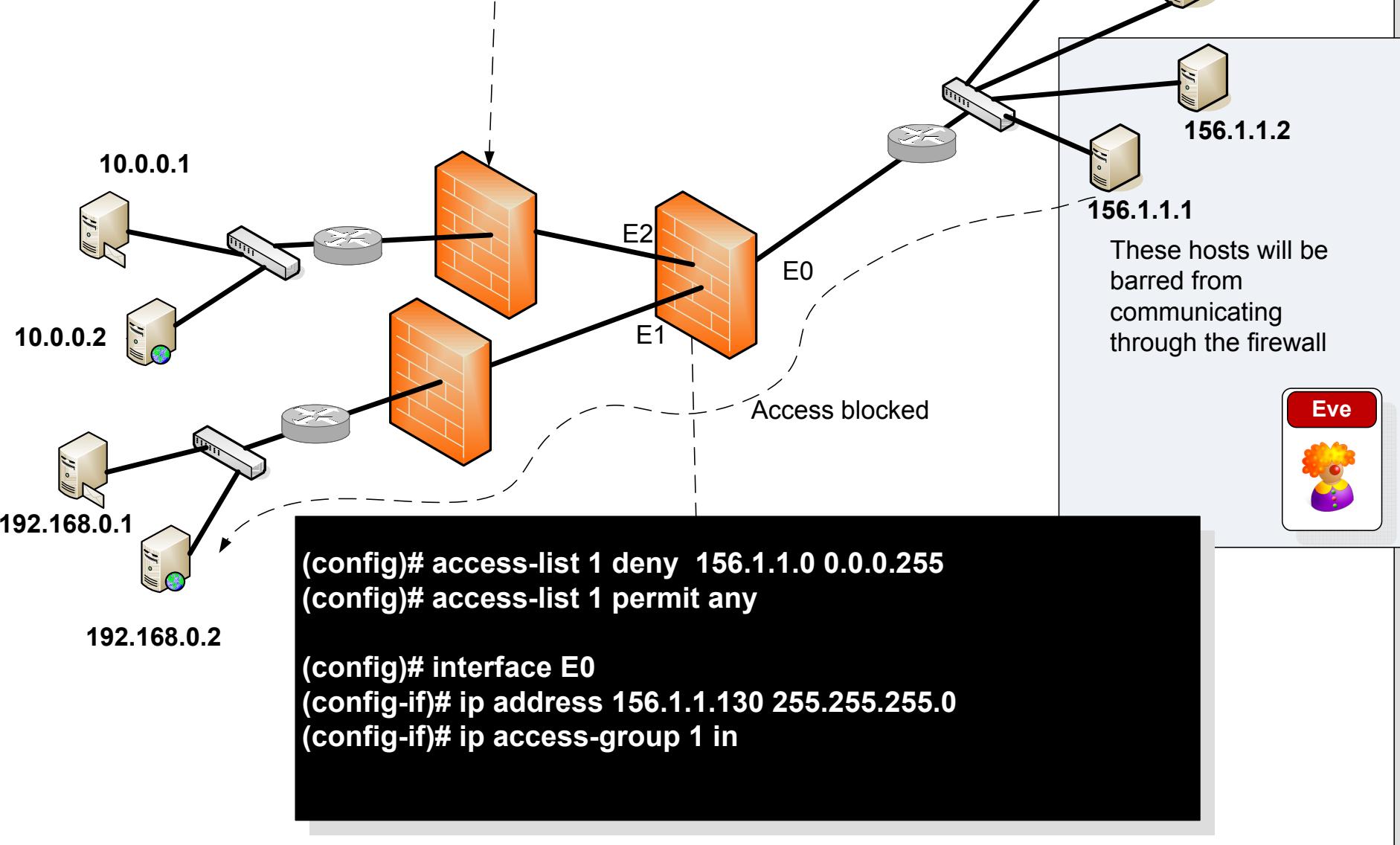
Network Security

Screening Firewalls

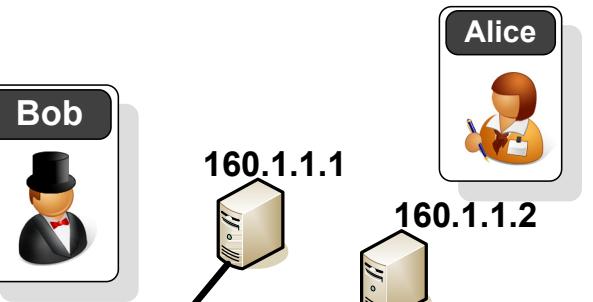


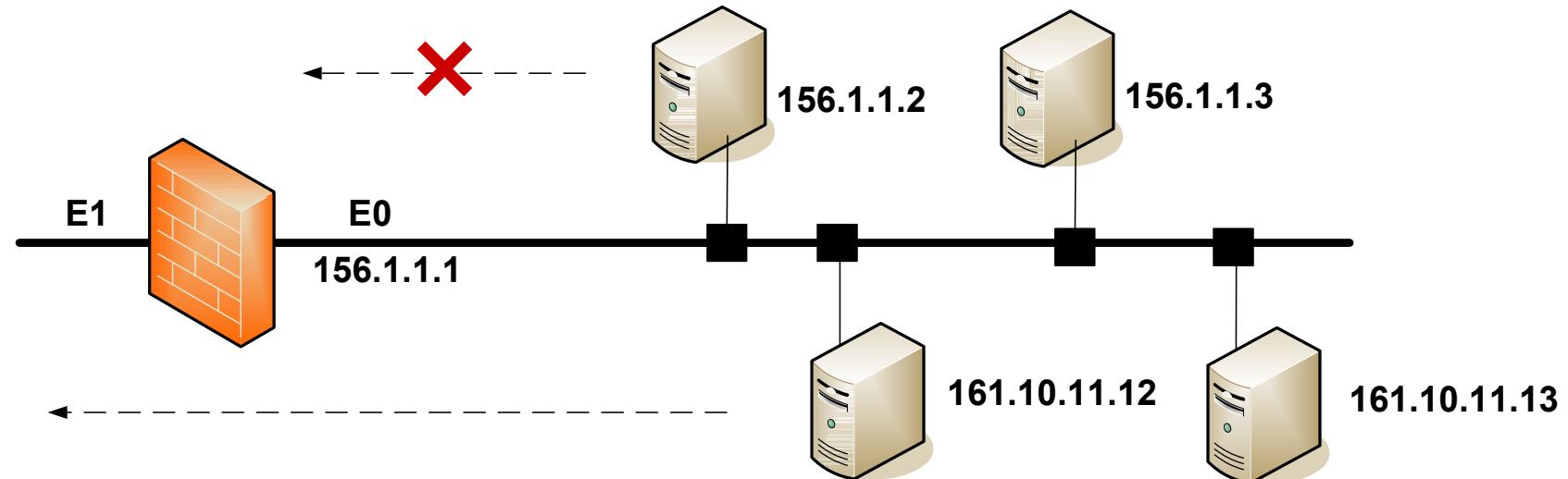
Network Security

Screening Firewalls



Standard ACLs are applied as near to the **destination** as possible, so that they do not affect any other traffic





```
Router(config)#access-list 100 deny ip host 156.1.1.2 70.1.2.0 0.0.0.255  
Router(config)#access-list 100 permit ip any any
```

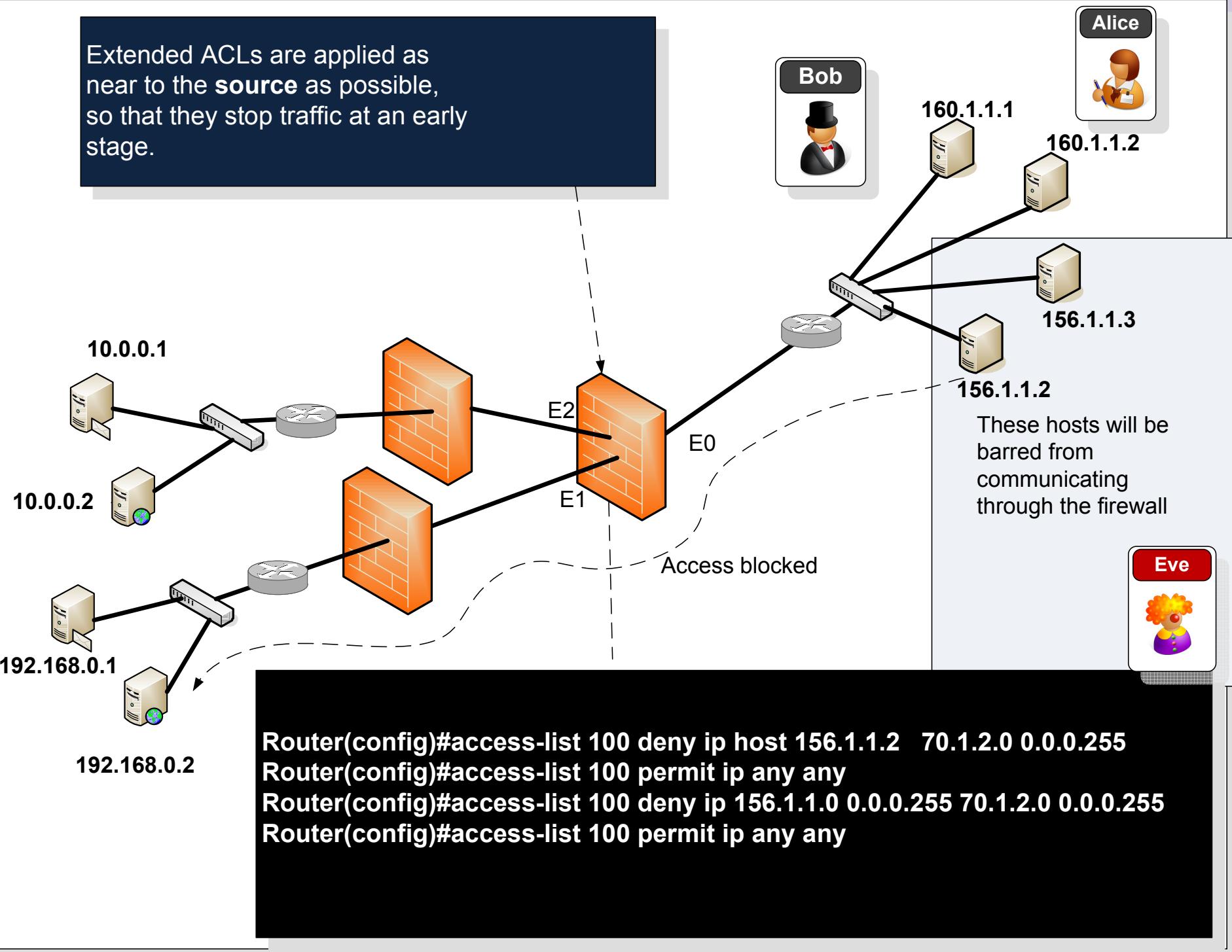
Denies traffic from 156.1.1.2 to the 70.1.2.0 network

```
Router(config)#access-list 100 deny ip 156.1.1.0 0.0.0.255 70.1.2.0 0.0.0.255  
Router(config)#access-list 100 permit ip any any
```

Denies traffic from any host on 156.1.1.0 to the 70.1.2.0 network

Network Security

Screening Firewalls



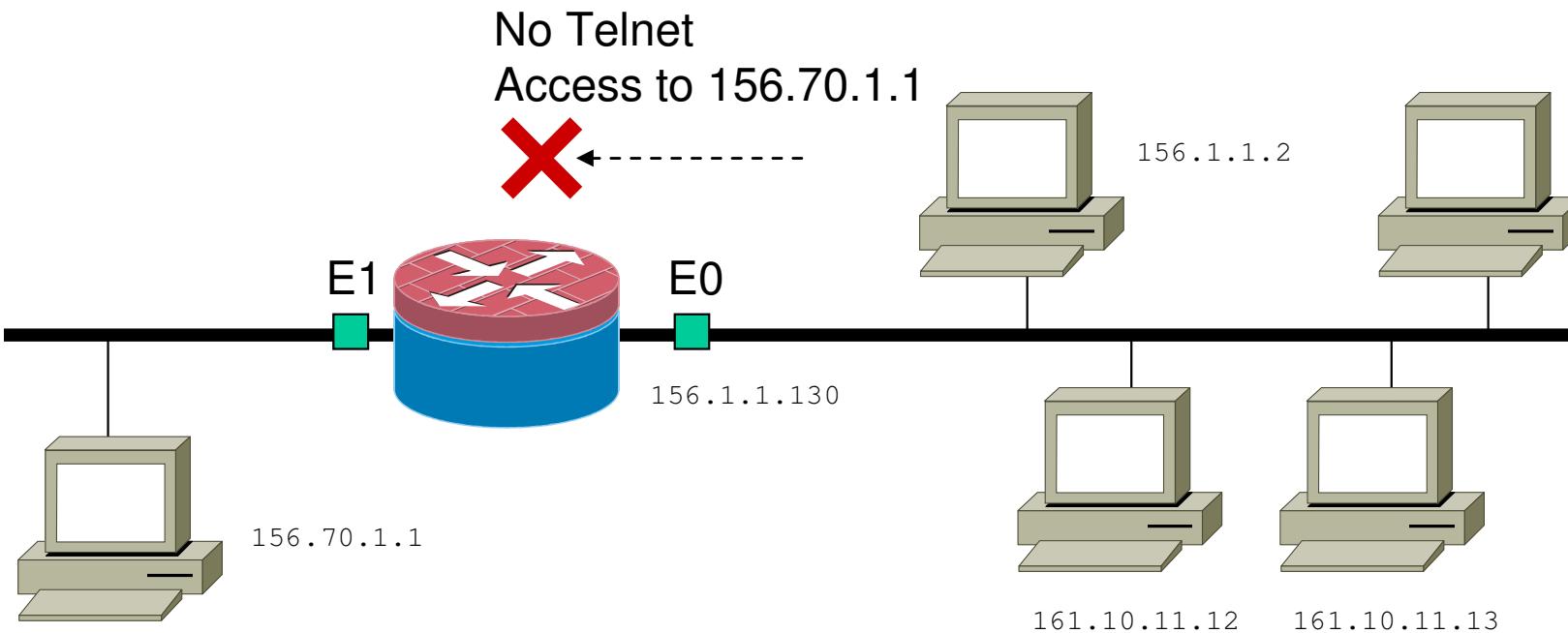
Extended ACL – can select a source and destination

An extended ACLs can also filter for TCP/UDP traffic, such as:

```
Router(config)#access-list access-list-value { permit | deny } {tcp | udp  
| igrp} source source-mask destination destination-mask {eq | neq | lt |  
gt} port
```

Optional field
in brackets

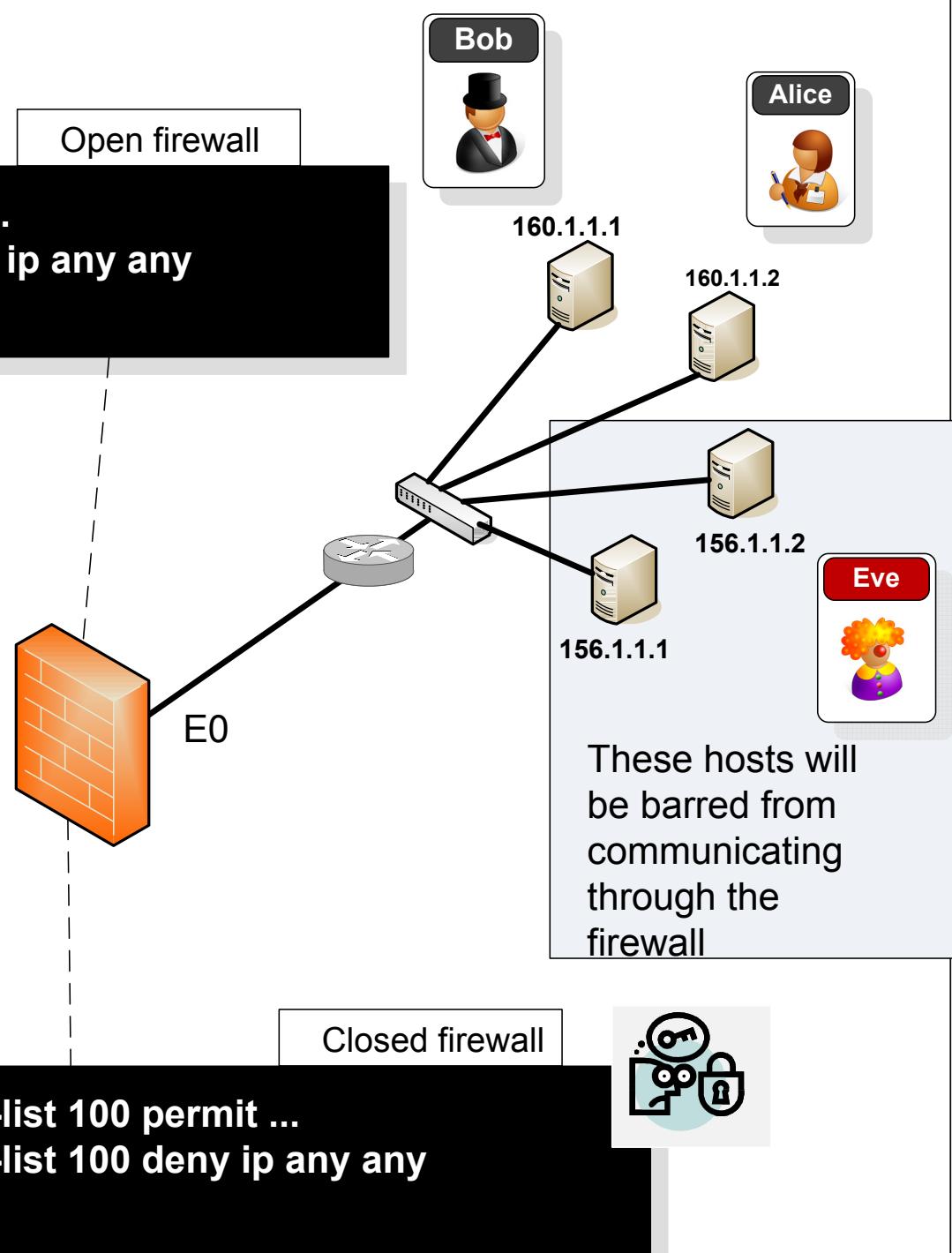
```
access-list 101 deny tcp 156.1.1.0 0.0.0.255 eq any host 156.70.1.1 eq telnet  
access-list 101 permit ip any any
```



```
Router(config)# access-list 100 deny ...
Router(config)# access-list 100 permit ip any any
```



Open firewall



Closed firewall

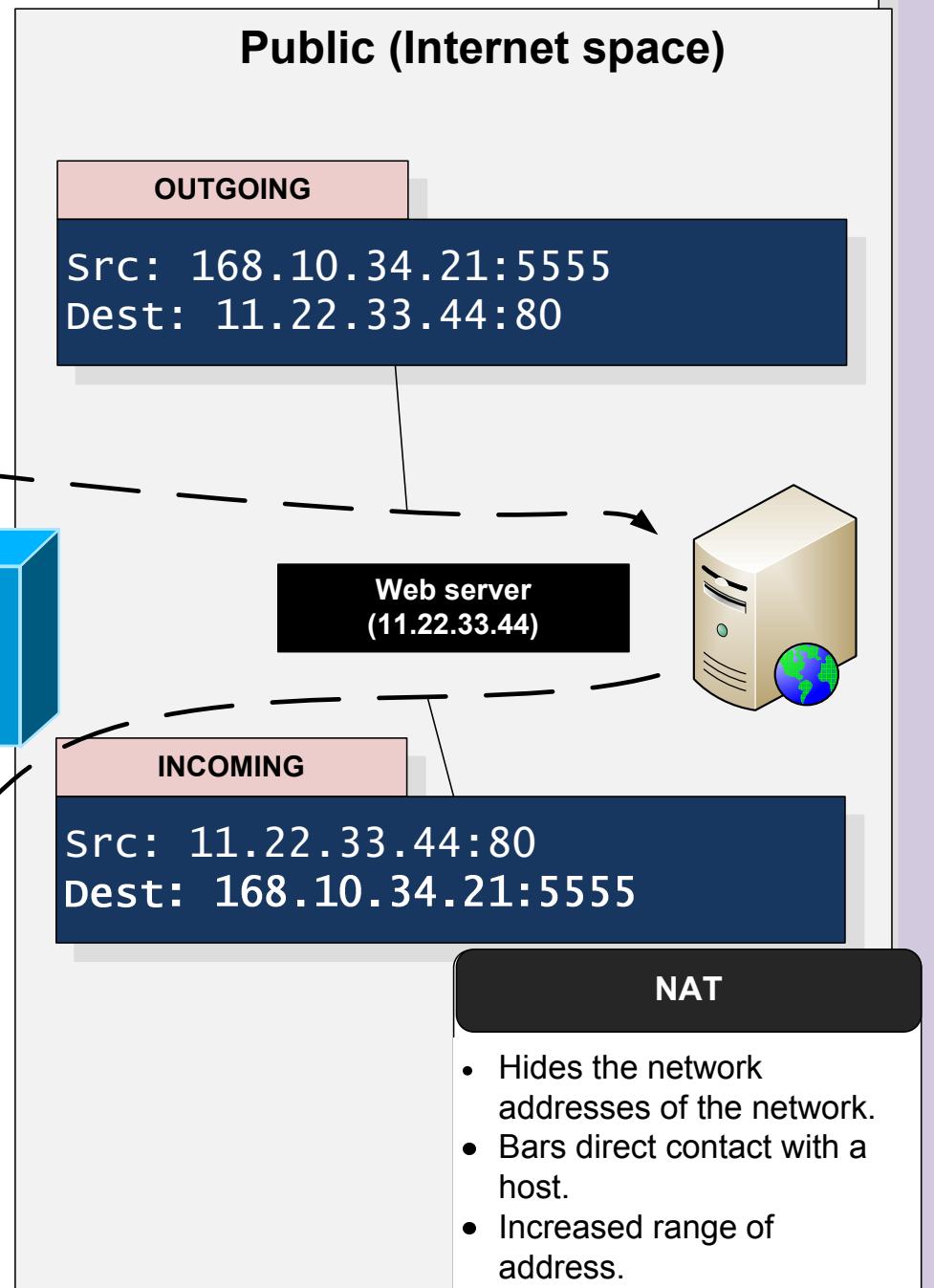
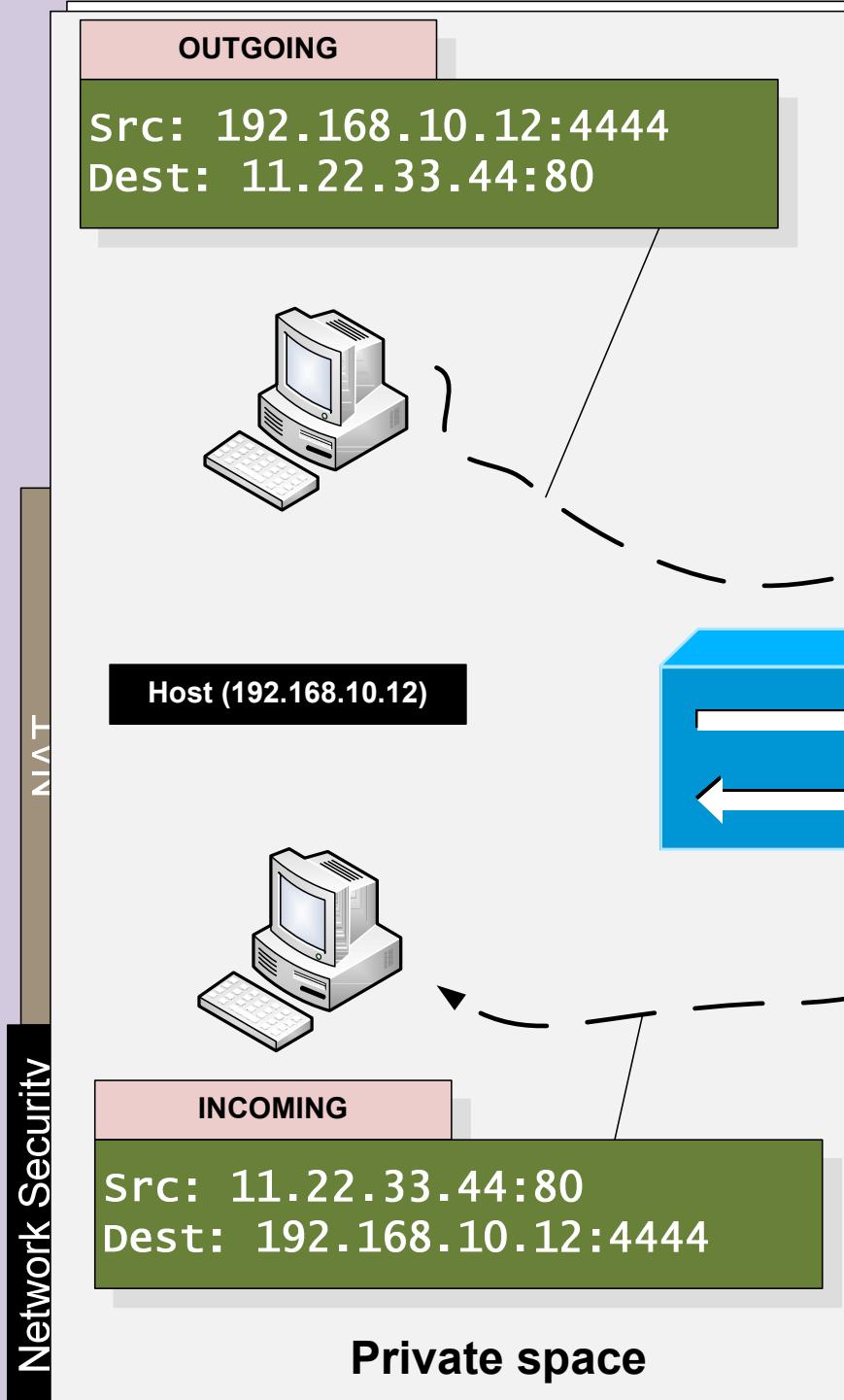


```
Router(config)# access-list 100 permit ...
Router(config)# access-list 100 deny ip any any
```

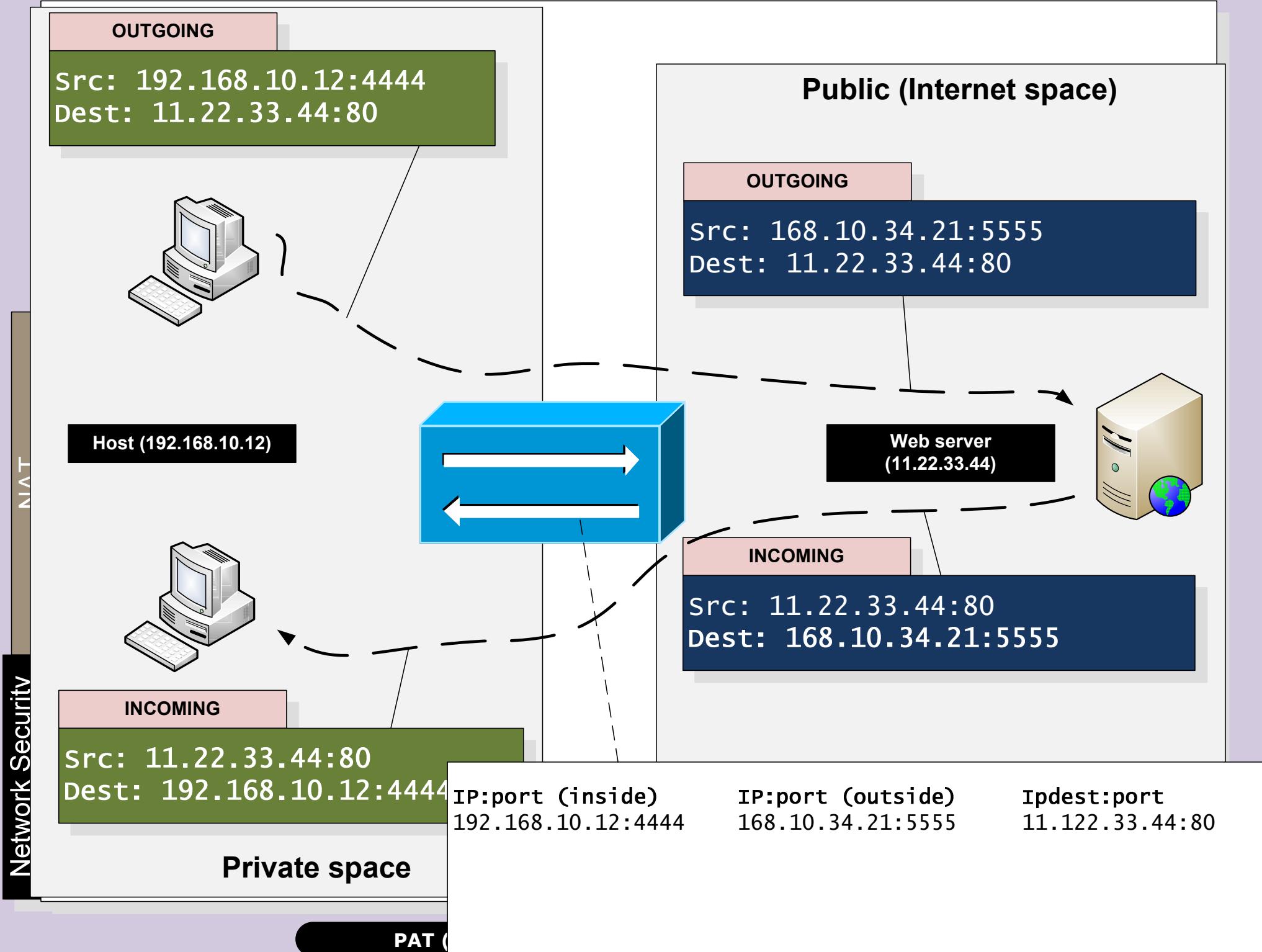
Network Security

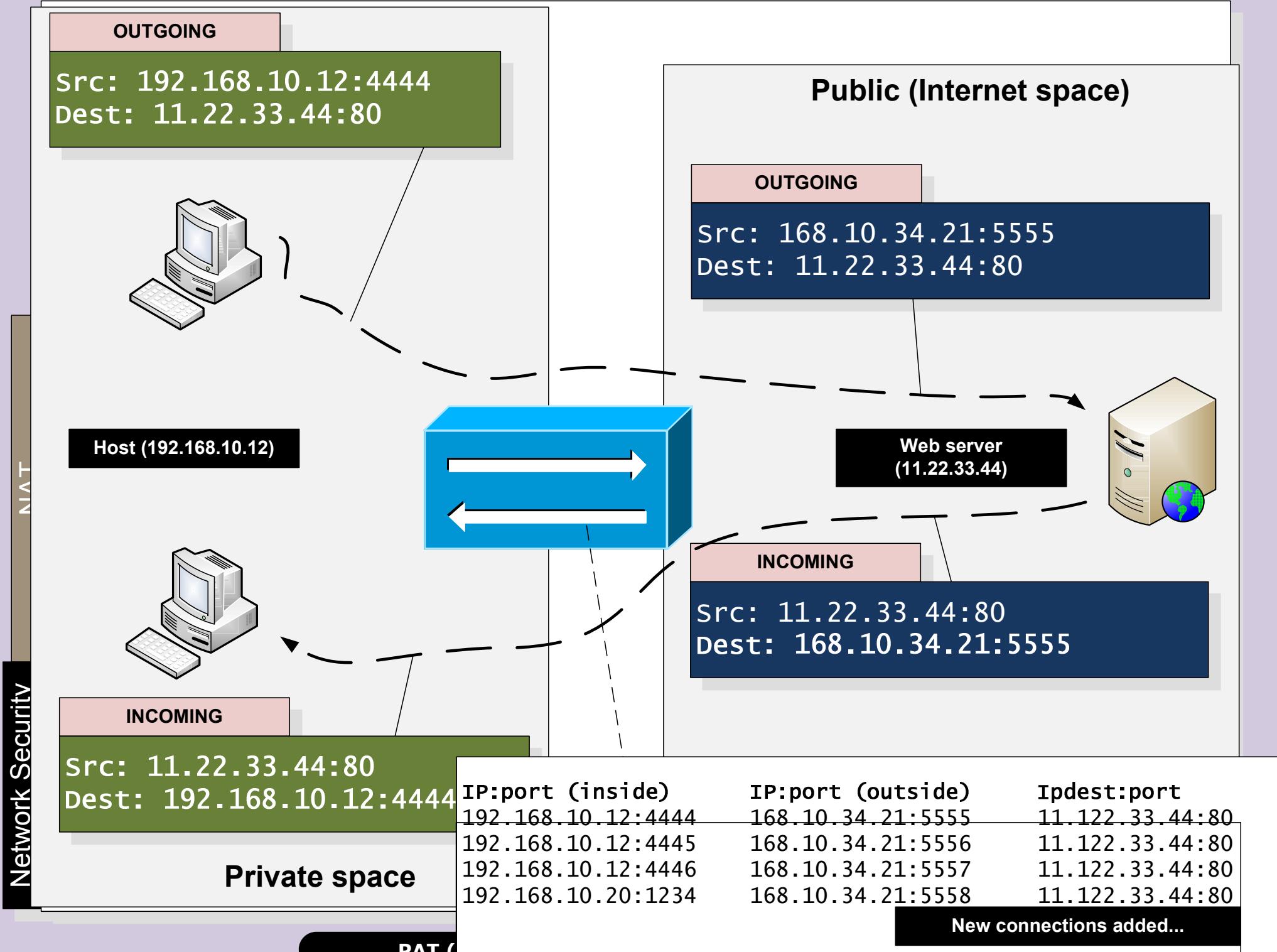


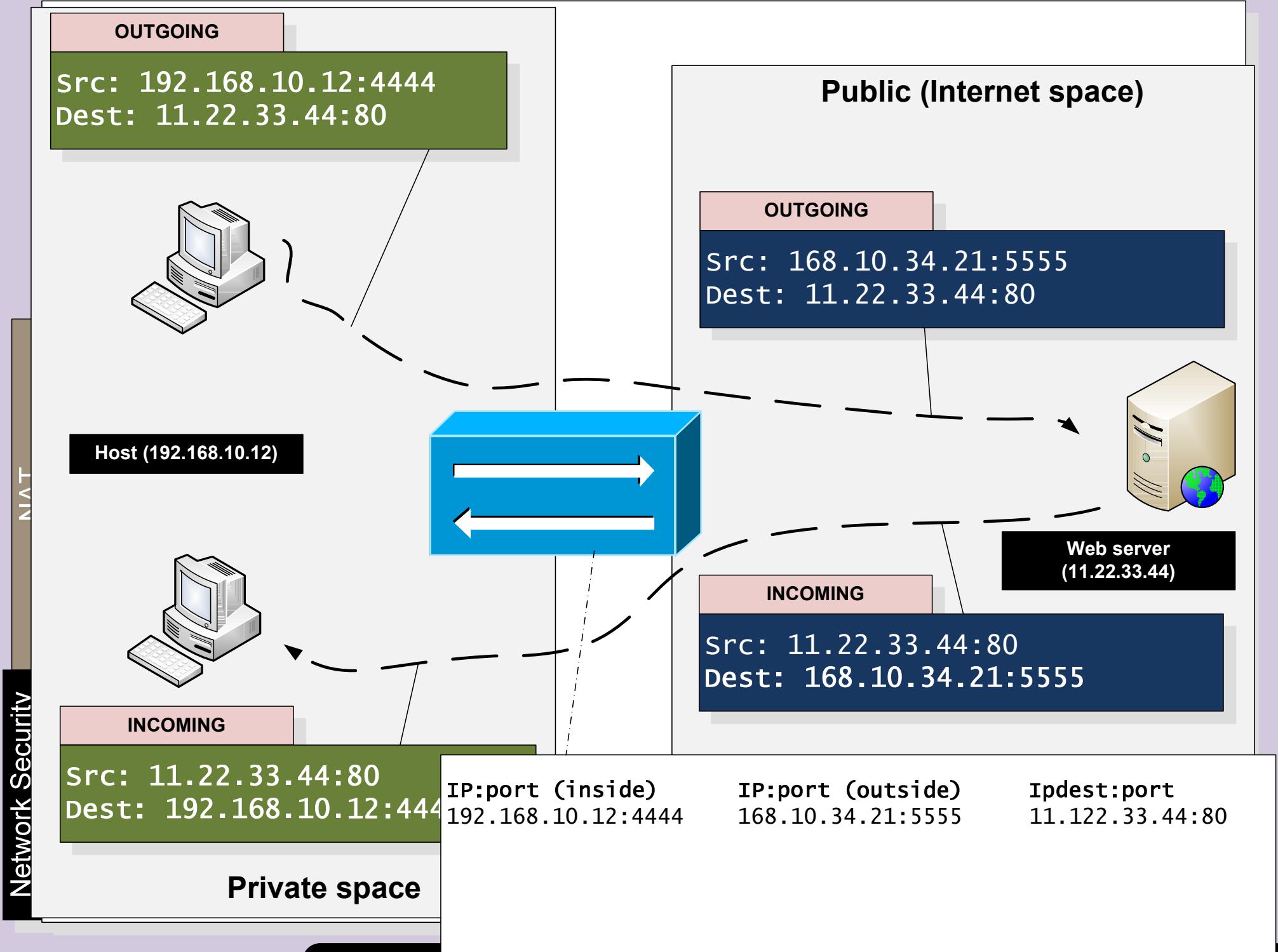
NAT

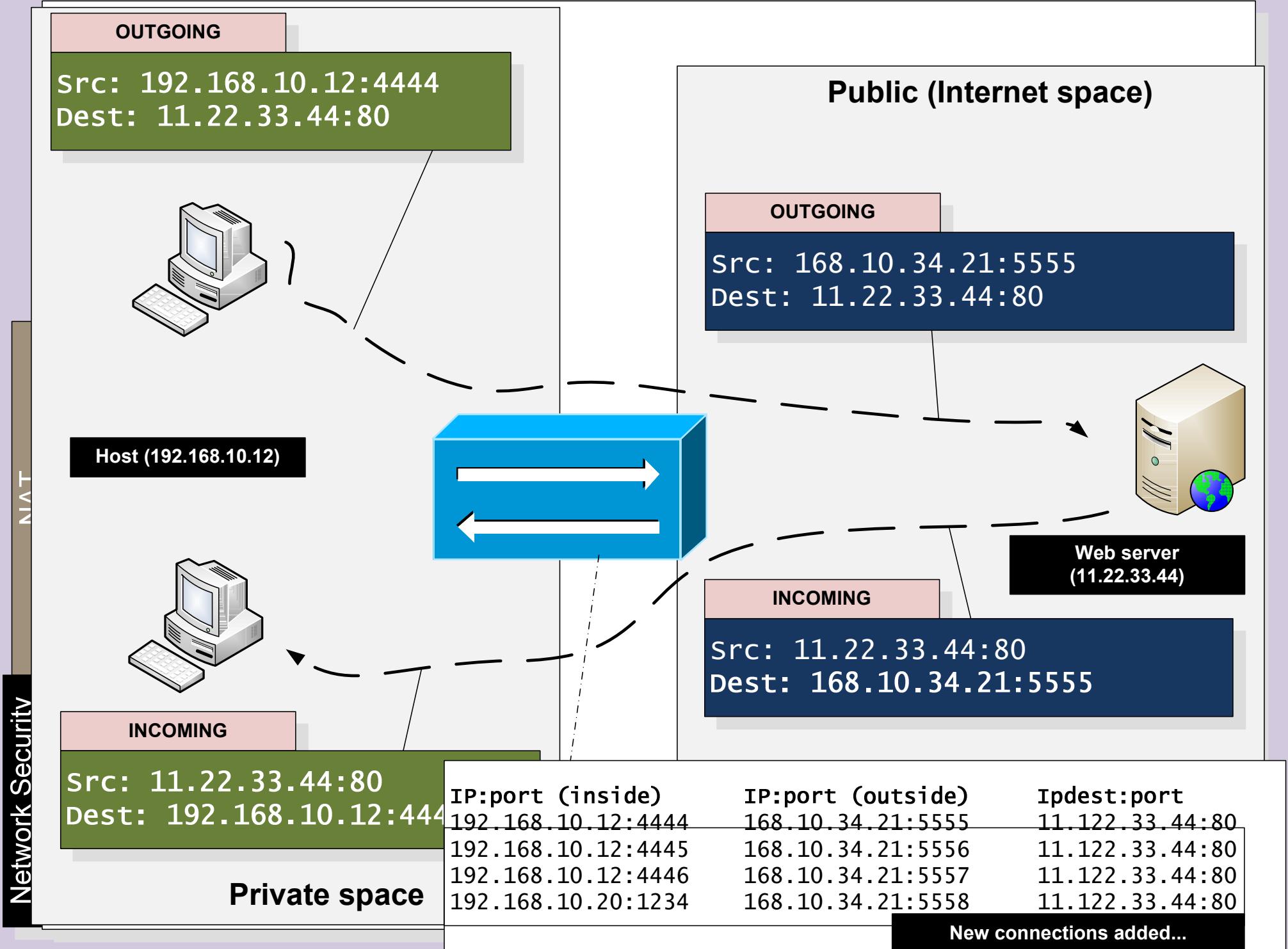


PAT (Port address translation) – Maps many addressees





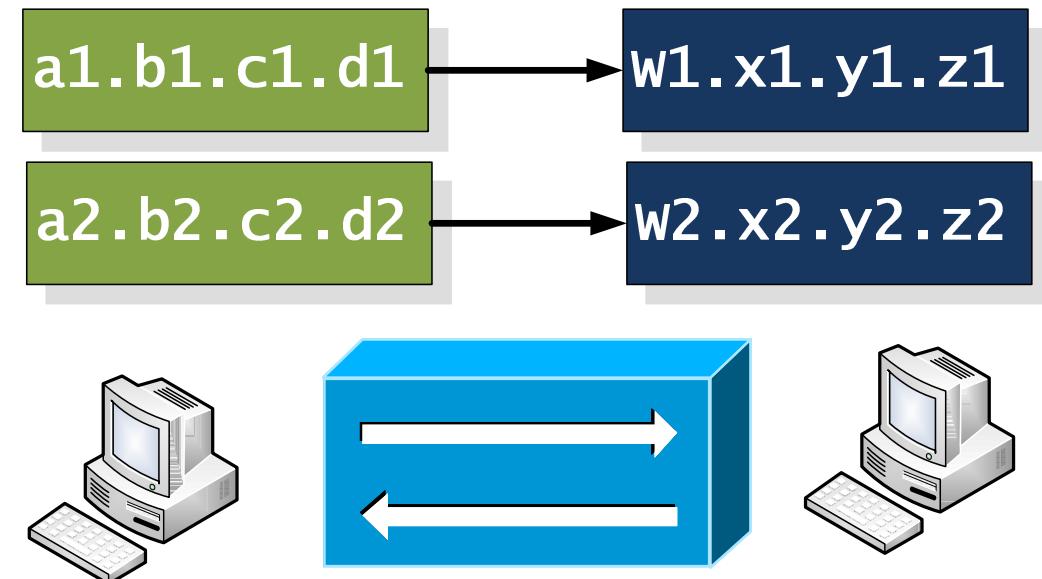




Network Security

Static translation.

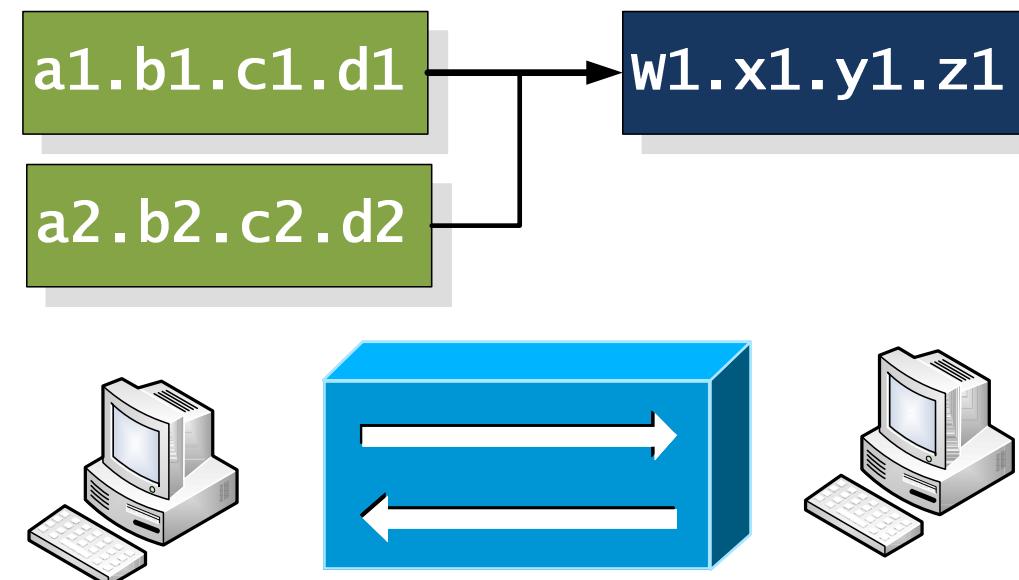
Each public IP address translates to a private one through a static table. Good for security/logging/traceability. Bad, as it does not hide the internal network.



NAT

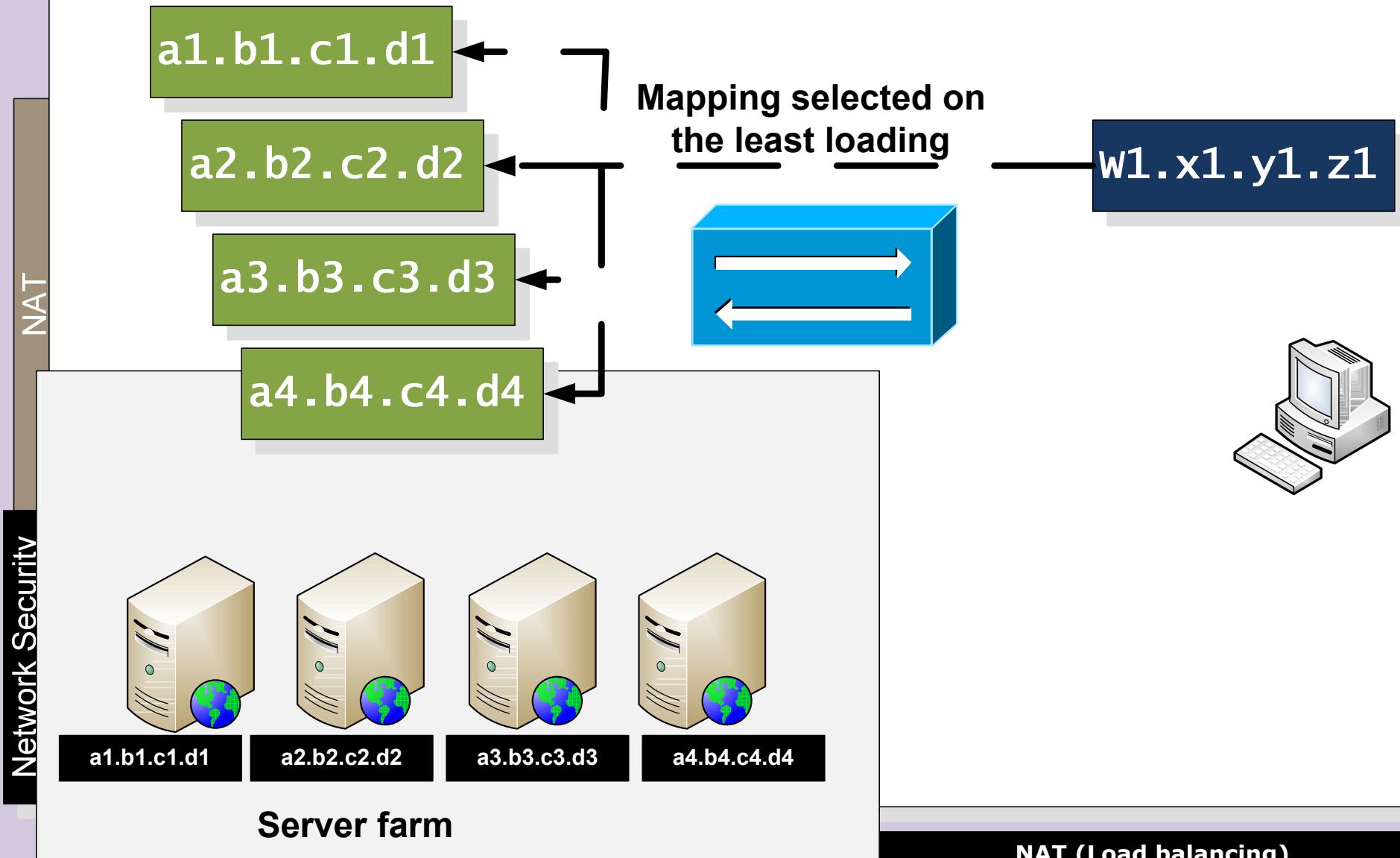
IP Masquerading (Dynamic Translation).

A single public IP address is used for the whole network. The table is thus dynamic.

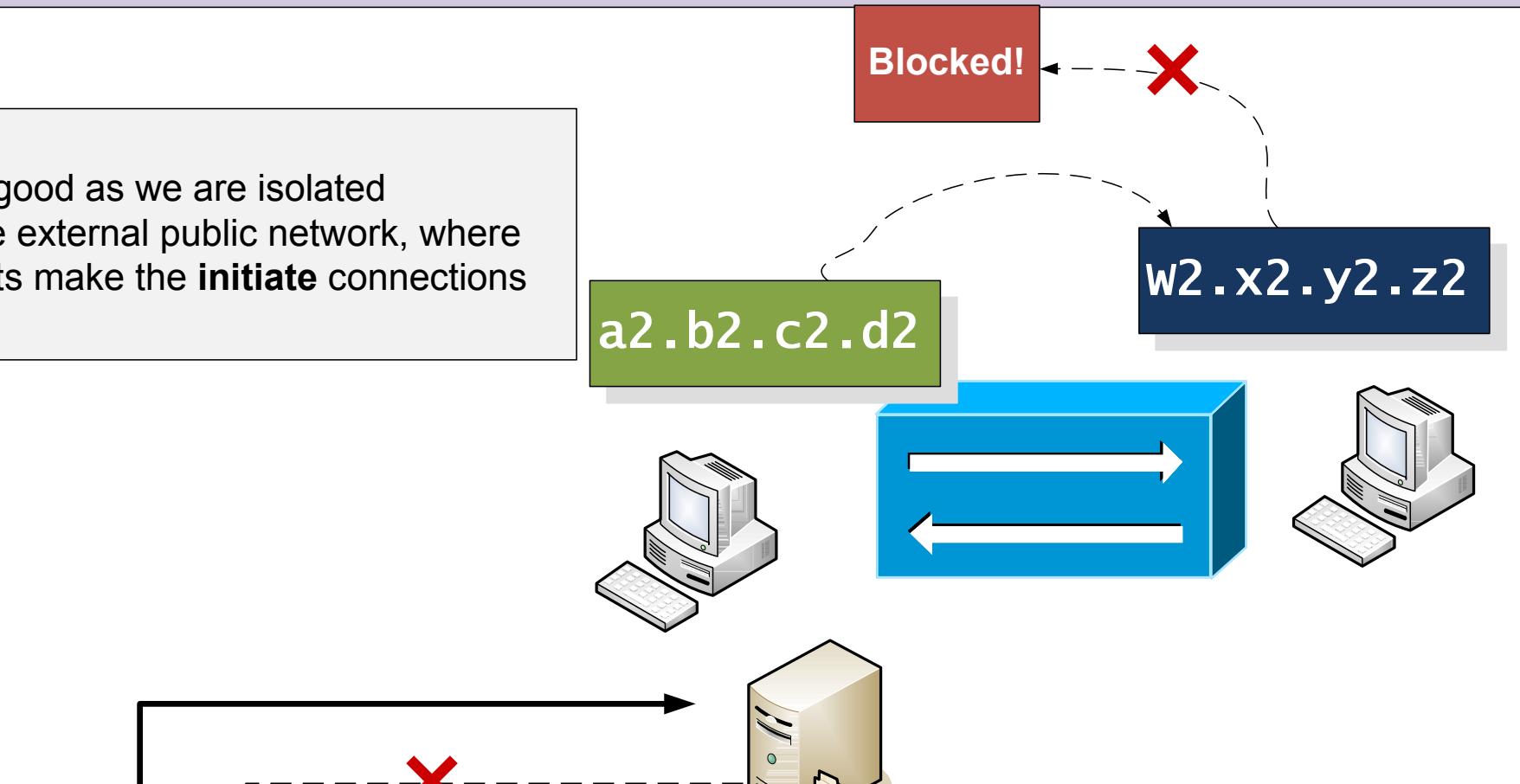


Load Balancing Translation.

With this, a request is made to a resource, such as to a WWW server, the NAT device then looks at the current loading of the systems, and forwards the request to the one which is most lightly used...



NAT is good as we are isolated from the external public network, where our hosts make the **initiate** connections



FTP creates a local server port

... but what happens if we use applications which create connections in the reverse direction, such as with FTP and IRC?

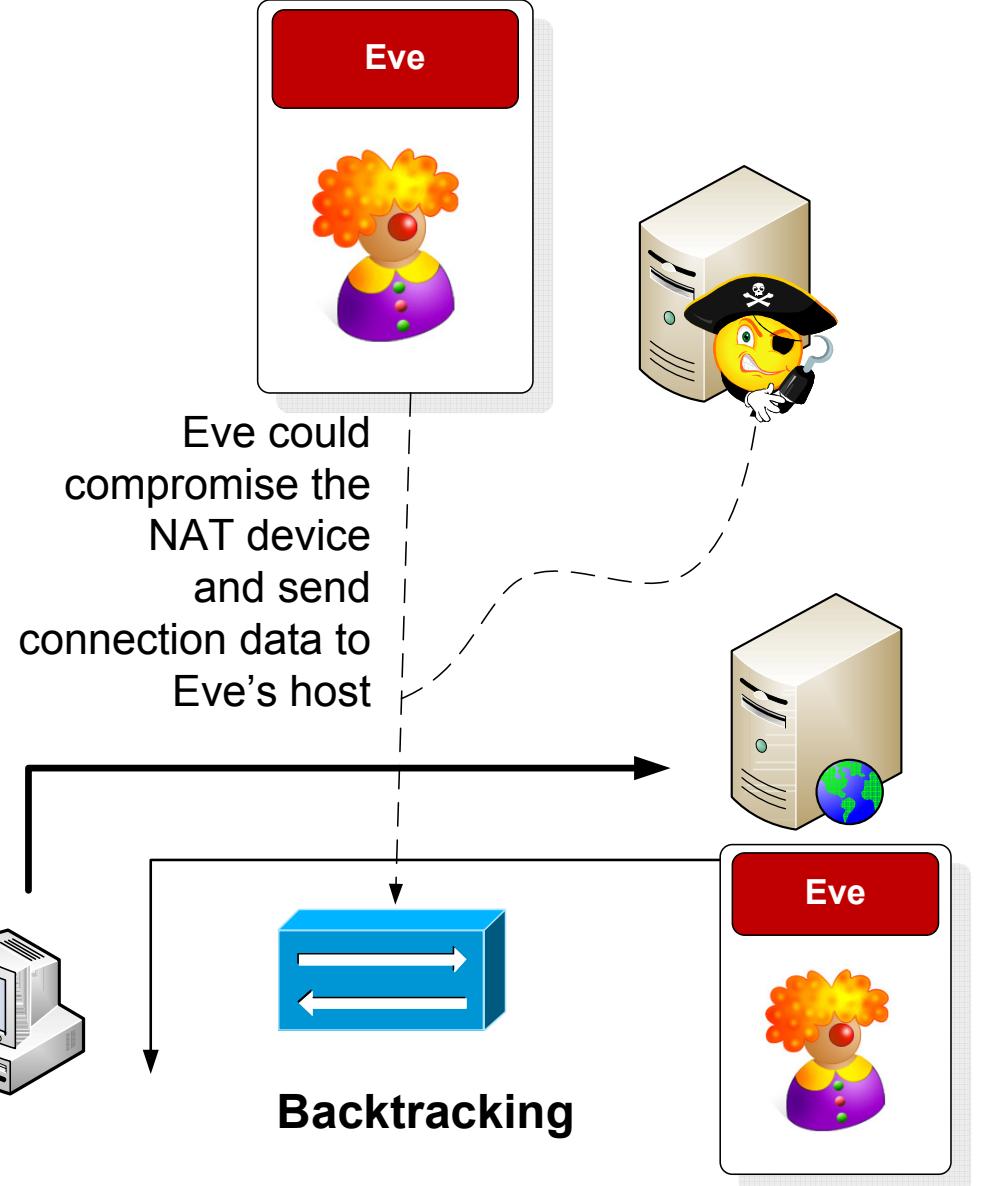
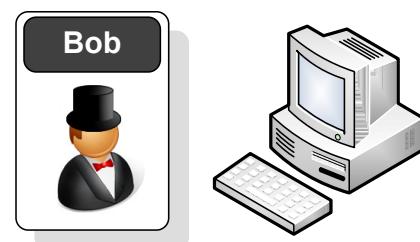
.. we thus need some form of **backtracking** of connections in the NAT device. Where the NAT device remembers the initial connection, and then allows direct connections to the initiator.

Static NAT is poor for security, as it does not hide the network. This is because there is a one-to-one mapping.

Dynamic NAT is good for security, as it hides the network. Unfortunately it has two major weaknesses:

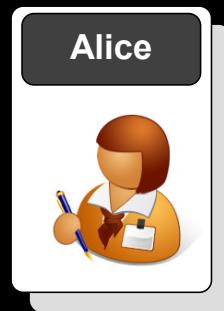
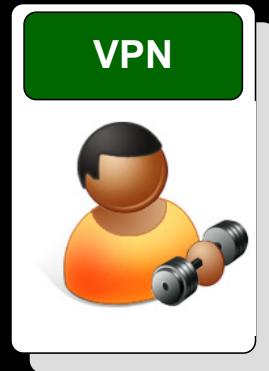
- *Backtracking* allows external parties to trace back a connection.
- If the NAT device become compromised the external party can redirect traffic.

Network Security



Eve gets Bob to connect to a server, and then backtracks into his host

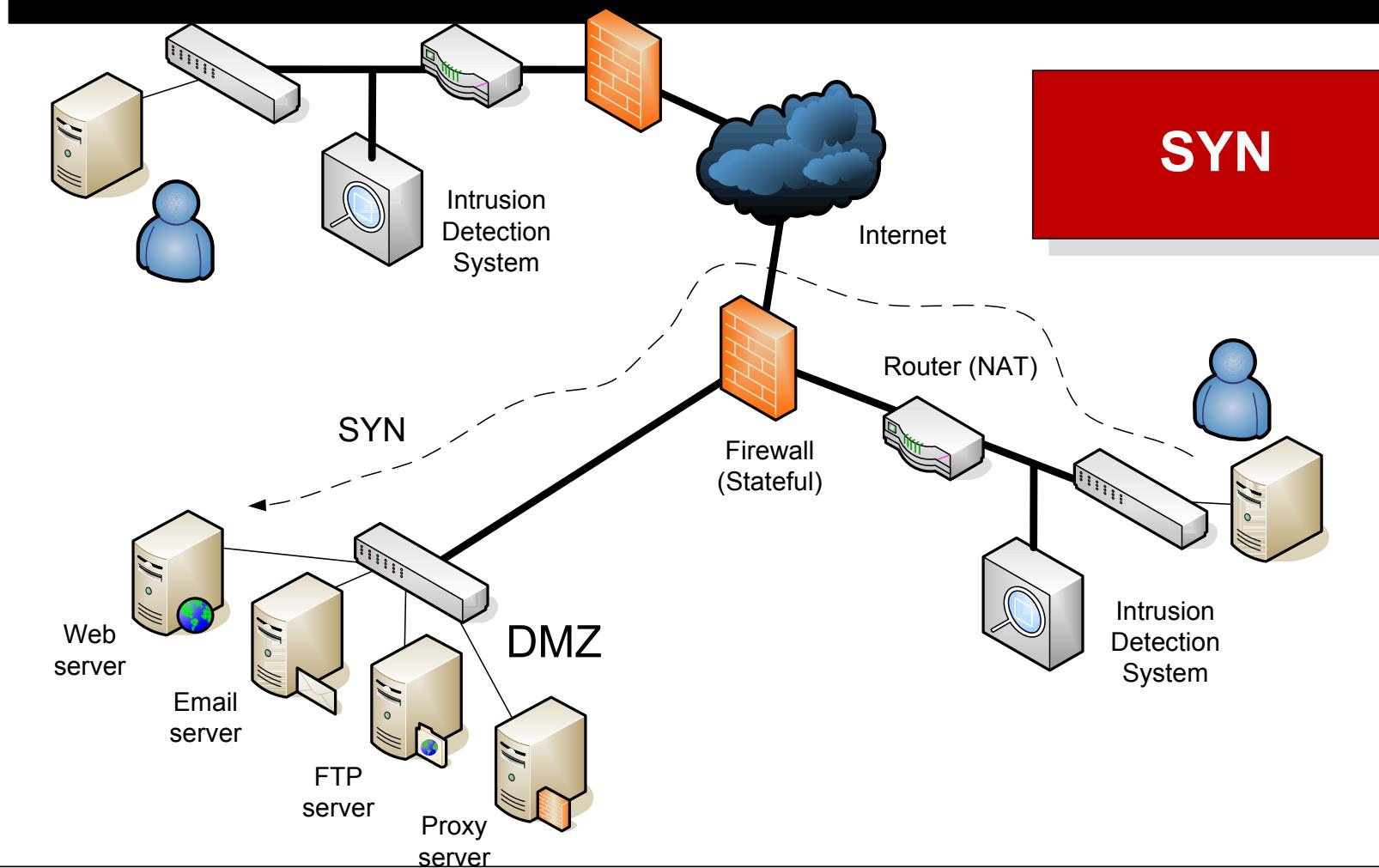
Network Security



Stateful Firewalls

Network Security

Stateful firewall



Originator

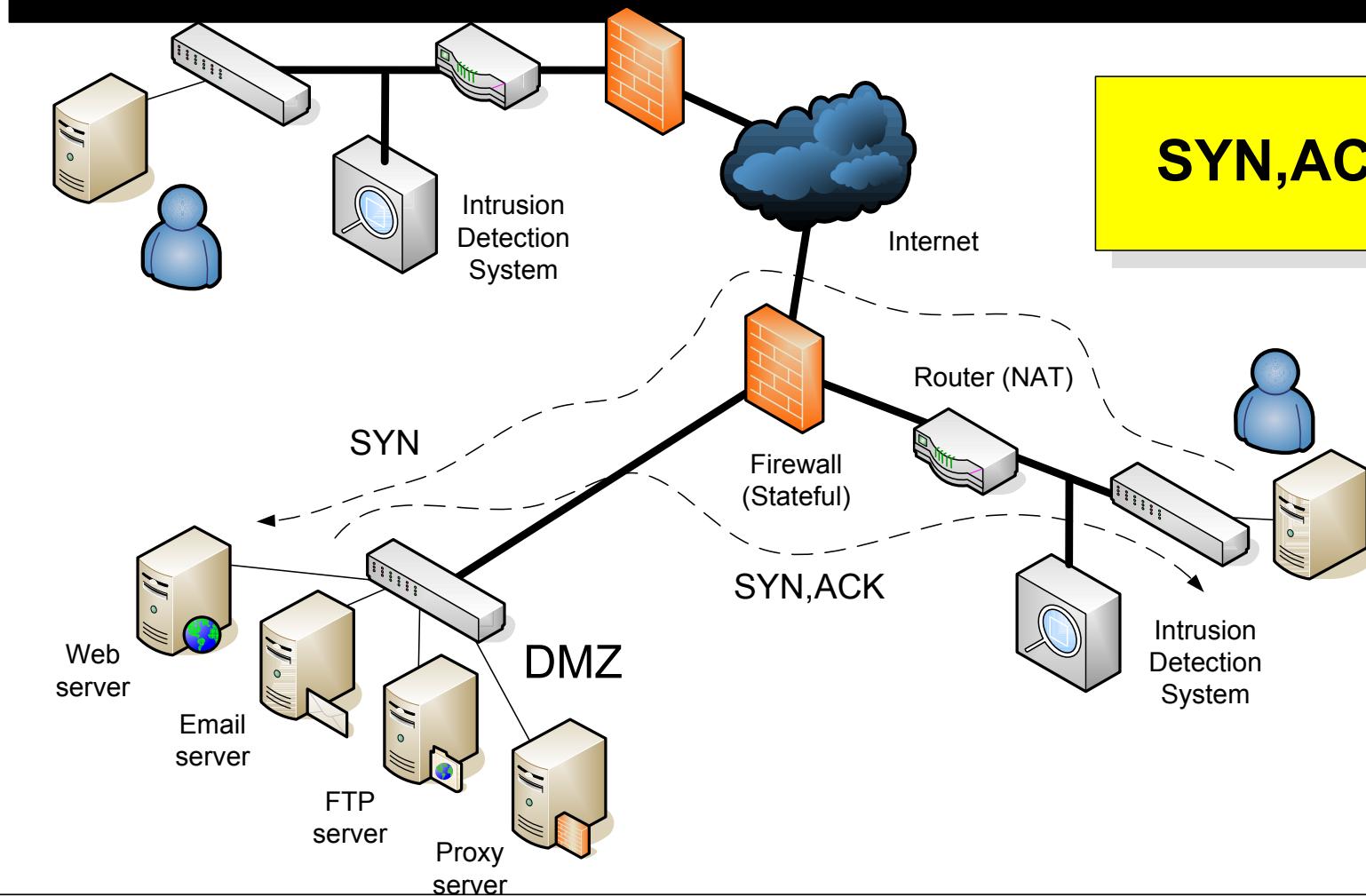
1. CLOSED
2. **SYN-SENT** <SEQ=999><CTL=SYN>
3. ESTABLISHED <SEQ=100><ACK=1000><CTL=SYN,ACK>
4. ESTABLISHED <SEQ=1000><ACK=101><CTL=ACK>
5. ESTABLISHED <SEQ=1000><ACK=101><CTL=ACK><DATA>

Recipient

LISTEN	
SYN-RECEIVED	SYN
SYN-RECEIVED	
ESTABLISHED	
ESTABLISHED	

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

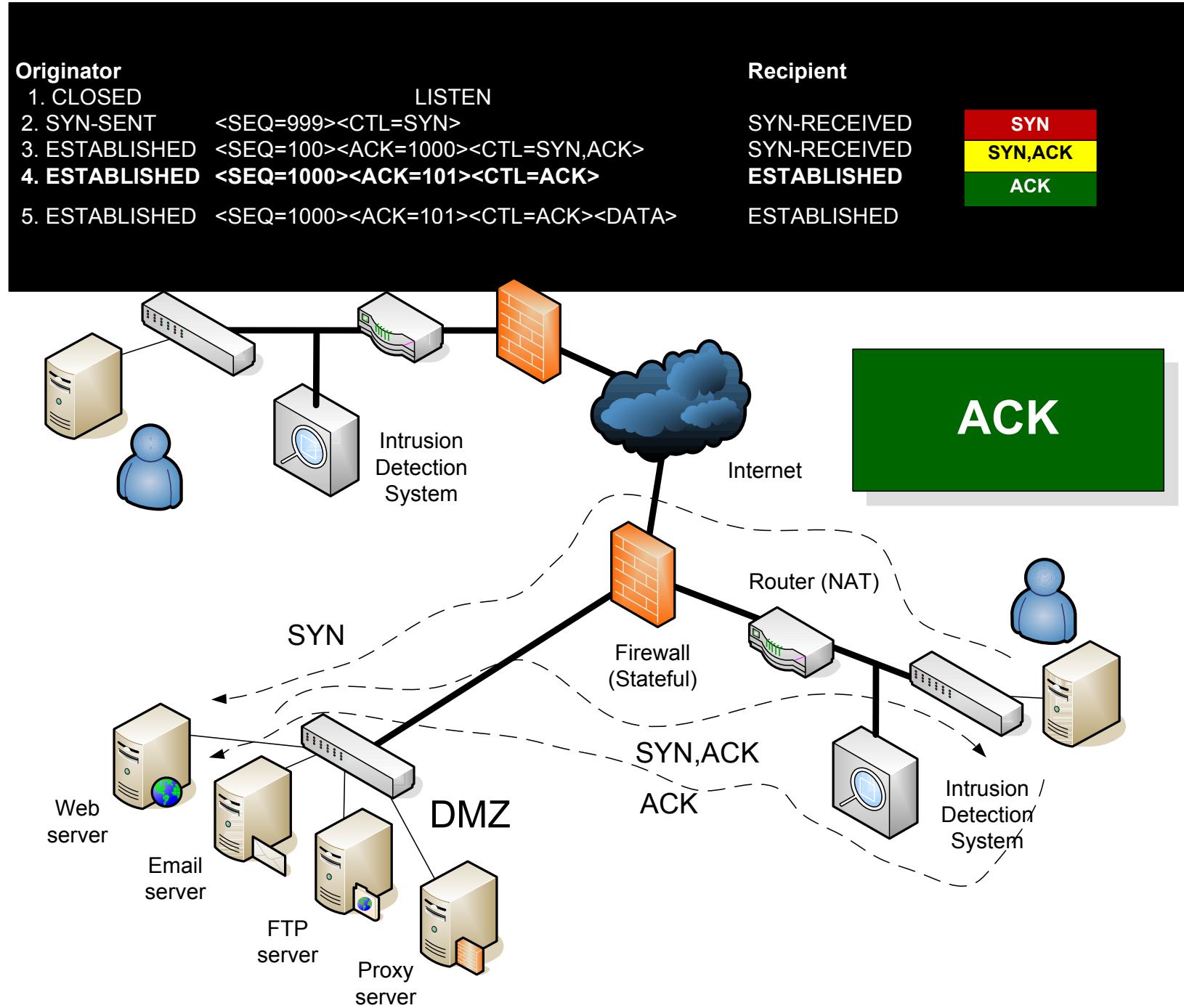
LISTEN
SYN-RECEIVED
SYN-RECEIVED
ESTABLISHED
ESTABLISHED

SYN
SYN,ACK

SYN,ACK

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	SMP	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)

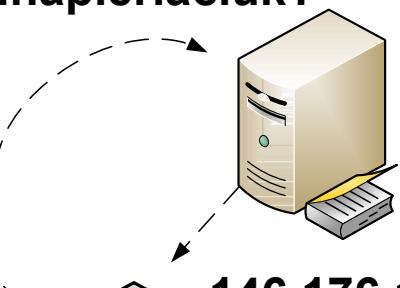
SYN

Stateful fir

Network Security

www.napier.ac.uk?

DNS server



146.176.1.188

SYN
Src Port=4213, Dest Port=80



TCP port=4213

TCP port=80



192.168.1.101

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) ←
window size: 16384
Checksum: 0xa97c (correct)
Options: (8 bytes)

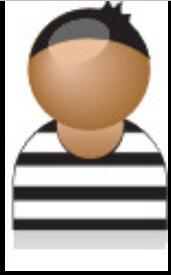
SYN,ACK

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

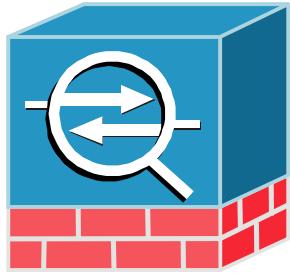
Name 75 (54 bytes on wire, 54 bytes captured)
Ethernet II, Src: 00:15:00:34:02:f0, Dst: 00:0c:41:f5:23:d5
Internet Protocol, Src Addr: 192.168.1.101 (192.168.1.101), Dst Addr: www.napier.ac.uk (146.176.1.188)
Transmission Control Protocol, Src Port: 4213 (4213), Dst Port: http (80), Seq: 1, Ack: 1, Len: 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) ←
window size: 17640
Checksum: 0xd0ec (correct)
[SEQ/ACK analysis]

ACK

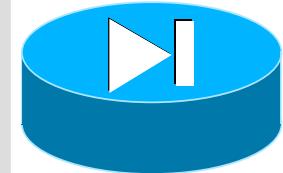
Network Security



PIX/ASA Firewalls



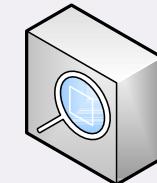
Firewall rules. These are contained within ACLs (using the **access-list** and **access-group** commands), and block or permit traffic. A key feature of this is the usage of **URL filtering** which defines the Web pages which are allowed and which are not.
Port blocking. These use the **fixup** command to change, enable or disable network services.



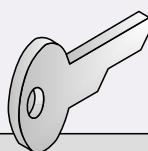
Cut-through proxy. This allows the definition of the users who are allowed services such as HTTP, Telnet and FTP. This authentication is a single initial authentication, which differs from the normal proxy operation which checks every single packet.



Intrusion detection. These use the **ip audit** command to detect intrusions.
Shunning. This, along with intrusion detection, allows a defined response to an intrusion.

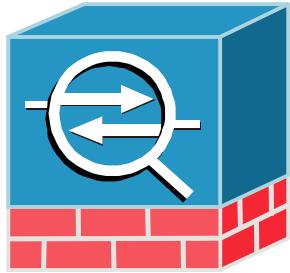


Encryption. This allows the PIX firewall to support enhanced encryption, such as being a server for VPN connections, typically with **IPSec** and tunnelling techniques such as **PPTP**.



Failover. This allows other devices to detect that a PIX device has crashed, and that another device needs to take its place.





Remote office – **PIX 506E**. This has a 300MHz processor with 32MB RAM, and handles a throughput of 20Mbps for a maximum of 25,000 connections. It does not support failover, and has two connections.

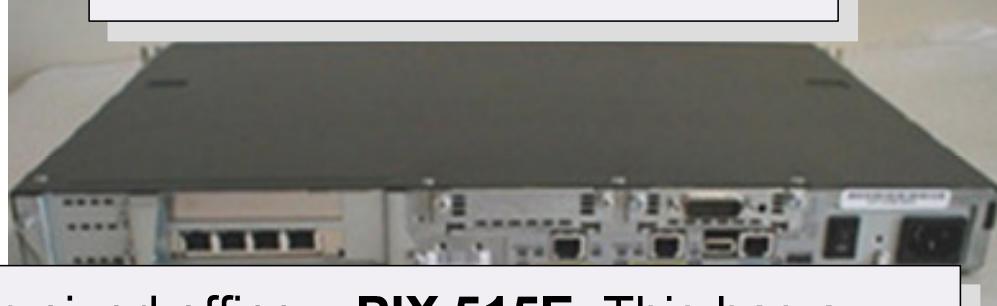


515E – R

515E – U

- Integrated accelerator
- Failover support.
- More LAN.
- VPN acceleration.

Small office – **PIX 501**. This has a 133MHz processor with 16MB RAM, and handles a throughput of 10Mbps for a maximum of 7,500 connections. It does not support failover, and has one external connection, and a switch for inside connections.



Medium-sized office – **PIX 515E**. This has a 433MHz processor with 32/64MB RAM, and handles a throughput of 188Mbps for a maximum of 130,000 connections. It supports failover, and has the support for up to six connections.

Max throughput: 188Mbps, 3-DES Throughput: 22Mbps
AES Throughput: 63Mbps (100Mbps - accell)
Access: VPN Accellerator (DES/3DES), Failover cable, 4-port FE (PCI), 1-port GE (PCI).





Enterprise – **PIX 535**. This has a 1GHz processor with 1GB RAM, and handles a throughput of 1Gbps for a maximum of 500,000 connections. It supports failover, and has the support for up to ten network interfaces.



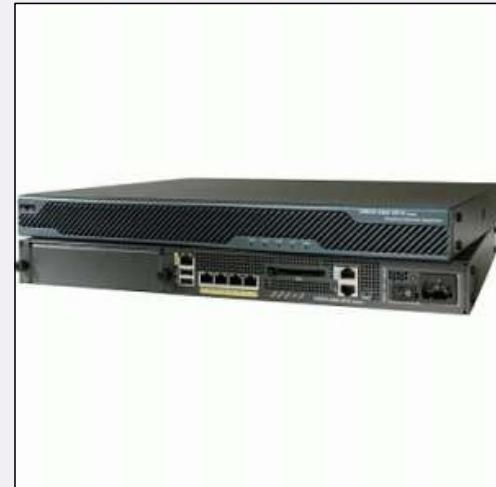
Enterprise – **PIX 525**. This has a 600MHz processor with 256MB RAM, and handles a throughput of 360Mbps for a maximum of 280,000 connections. It supports failover, and has the support for up to eight connections.



ASA 5520

Intel Pentium 4, 2GHz
512MB RAM
PIX 7.x, ASA 8.x IOS
8 interfaces
Integrated VPN
SSL VPN

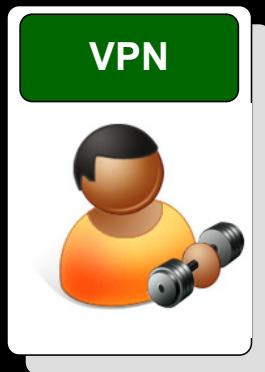
Throughput: 450Mbps
3DES: 225Mbps
Max conn: 280,000
VPN peers: 750



Network Security



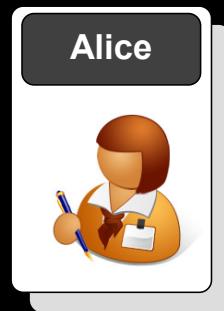
Proxy



VPN



Bob



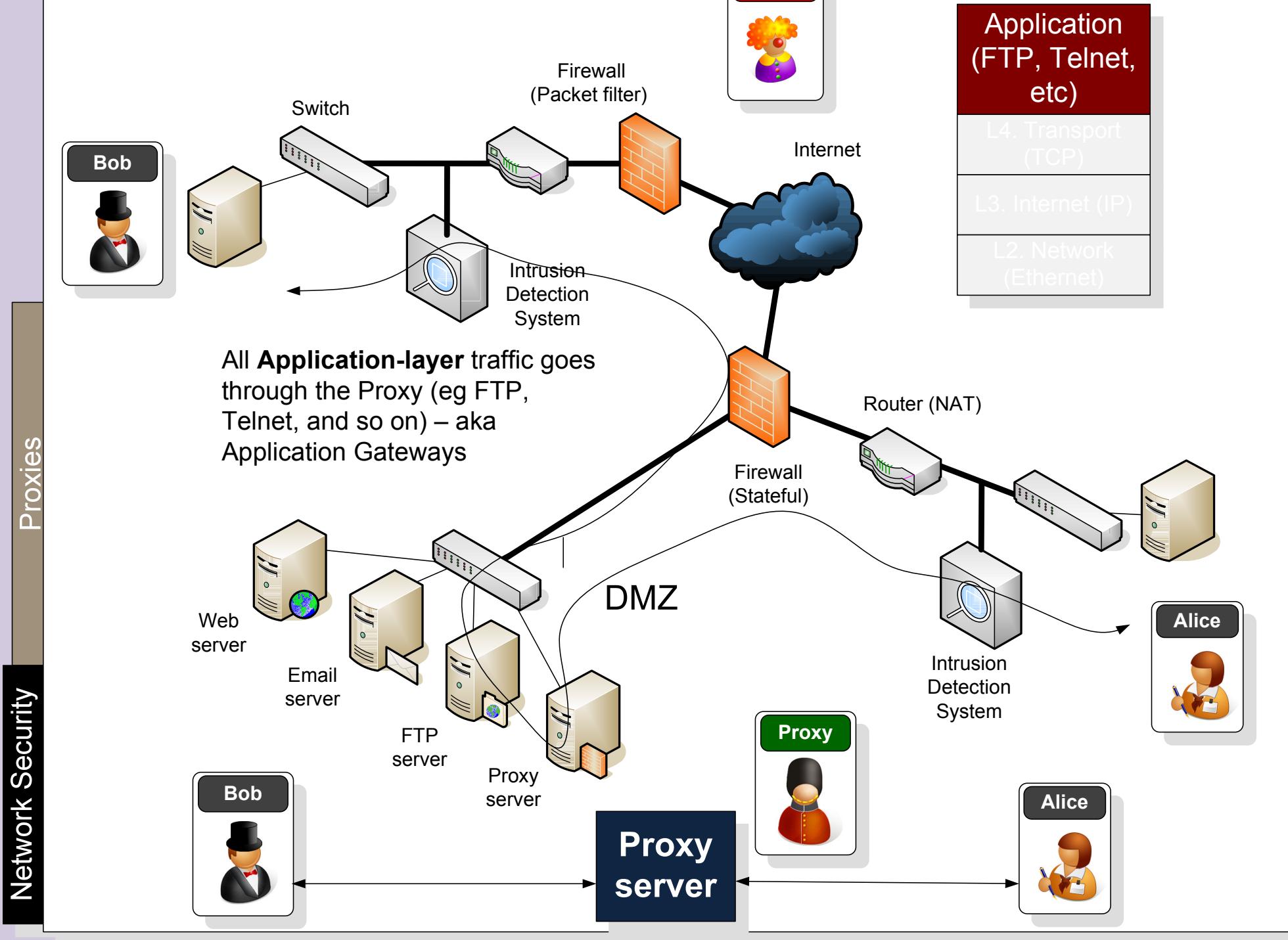
Alice



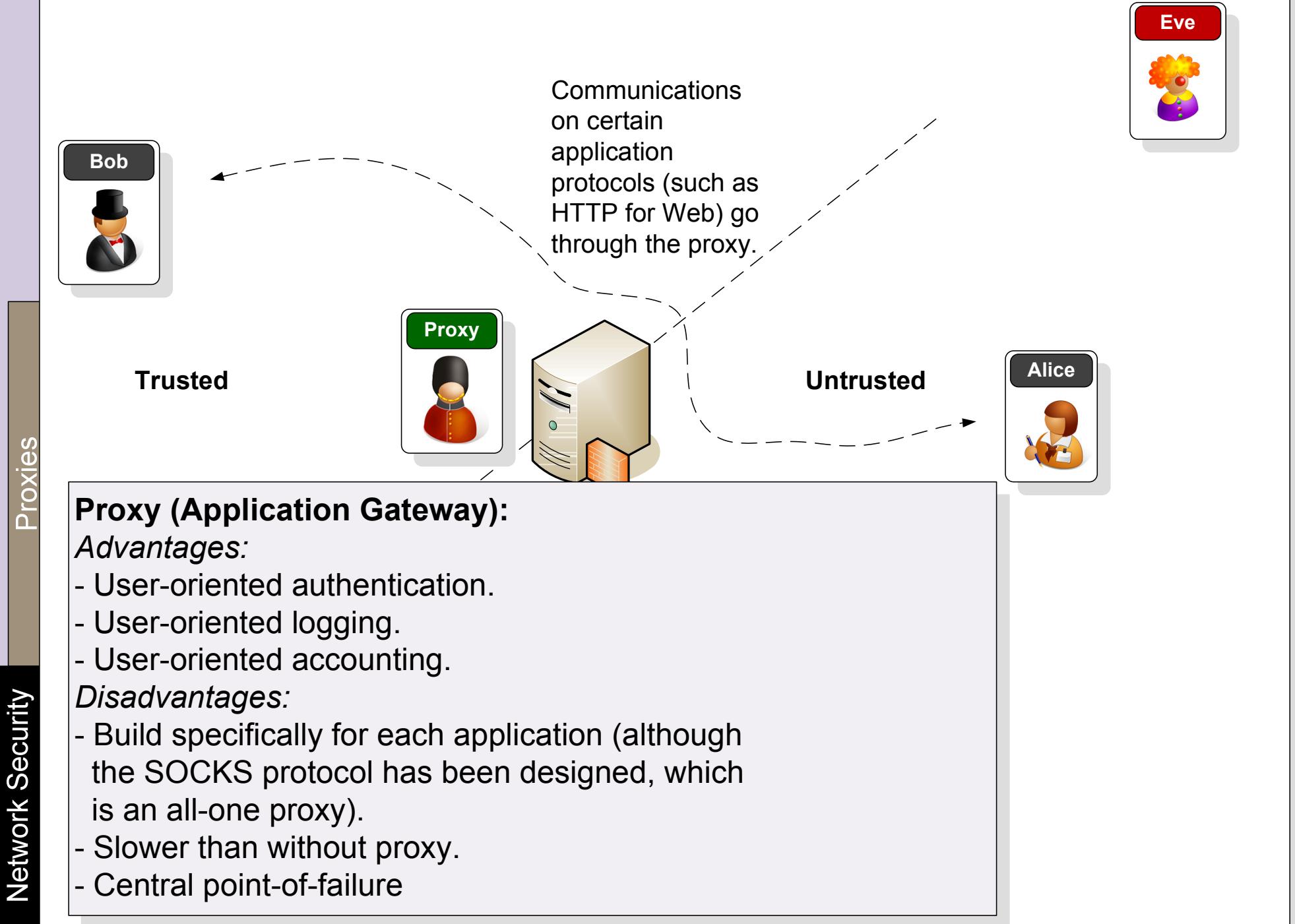
Eve

Proxies

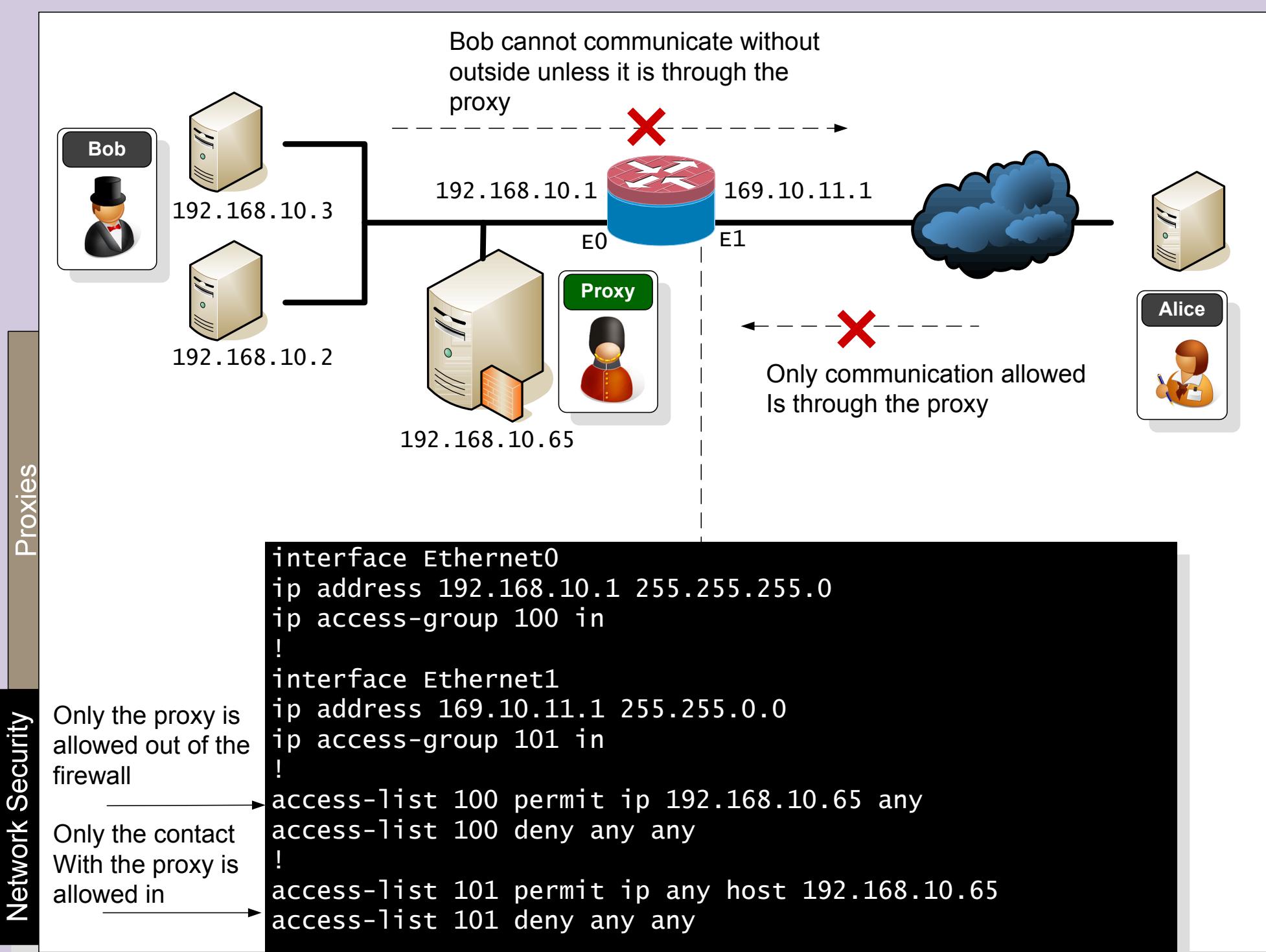
Network Security



Application gateways/proxy servers

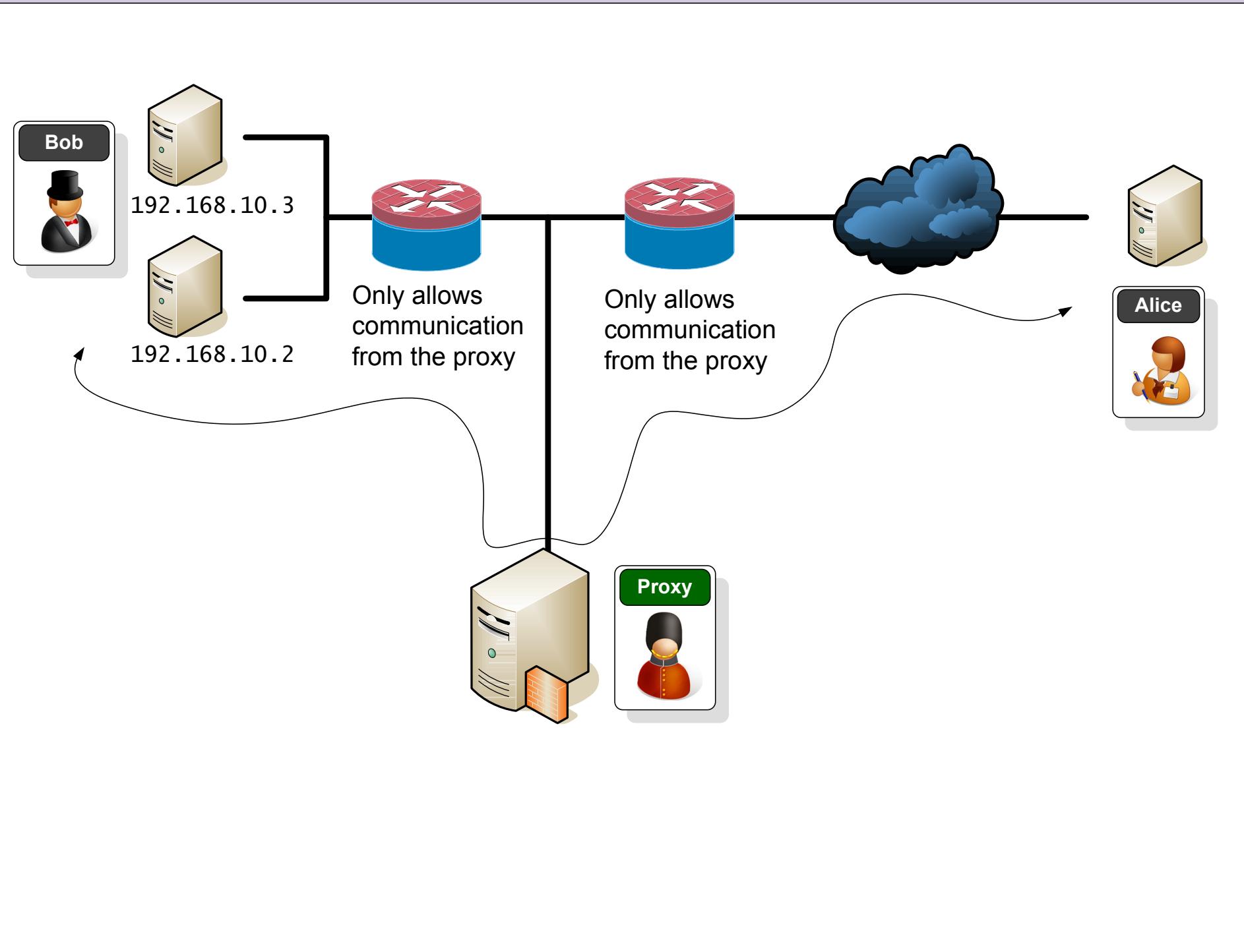


Network Security



Network Security

Proxies



Network Security

The diagram illustrates a network architecture involving a proxy server. On the left, a user icon labeled 'Bob' is connected to a server with IP 192.168.10.3. A second server with IP 192.168.10.2 is also connected. A central 'Proxy' server with IP 192.168.10.65 is shown. Solid lines represent direct connections between Bob's computer and the proxy, and between the proxy and the external network (represented by a cloud). Dashed lines show the path of 'Web traffic' from Bob's computer through the proxy to the external network. The proxy itself has two interfaces: E0 (connected to the internal network) and E1 (connected to the external network).

Proxy Settings

Type	Proxy address to use	Port
HTTP:	192.168.0.65	: 6588
Secure:	192.168.0.65	: 6588
FTP:	192.168.0.65	: 21
Gopher:		
Socks:	192.168.0.65	: 1080

Use the same proxy server for all protocols

Exceptions

Do not use proxy server for addresses beginning with:
[Empty list box]
Use semicolons (;) to separate entries.

Configure Proxy...

Services	Logging:
HTTP	Enabled
FTP	On
NNTP	On
SMTP	On
POP3	On
Socks	On

News server address:
Proxy Binding:
192.168.0.65

Configure Email Alias's
Check if proxy is in Open mode
Ok

Web traffic goes on port 6588

Web traffic goes out on port 80

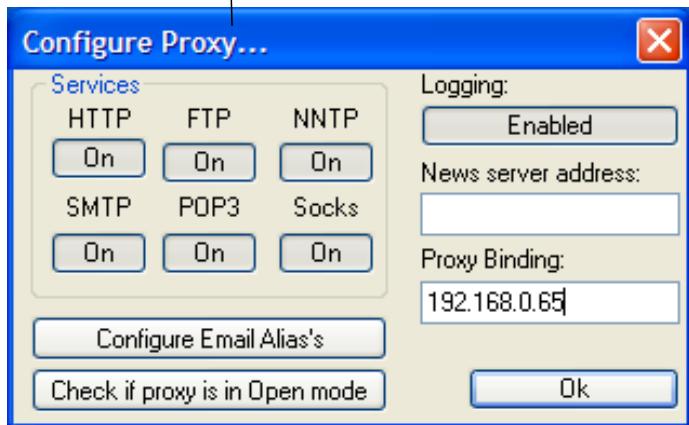
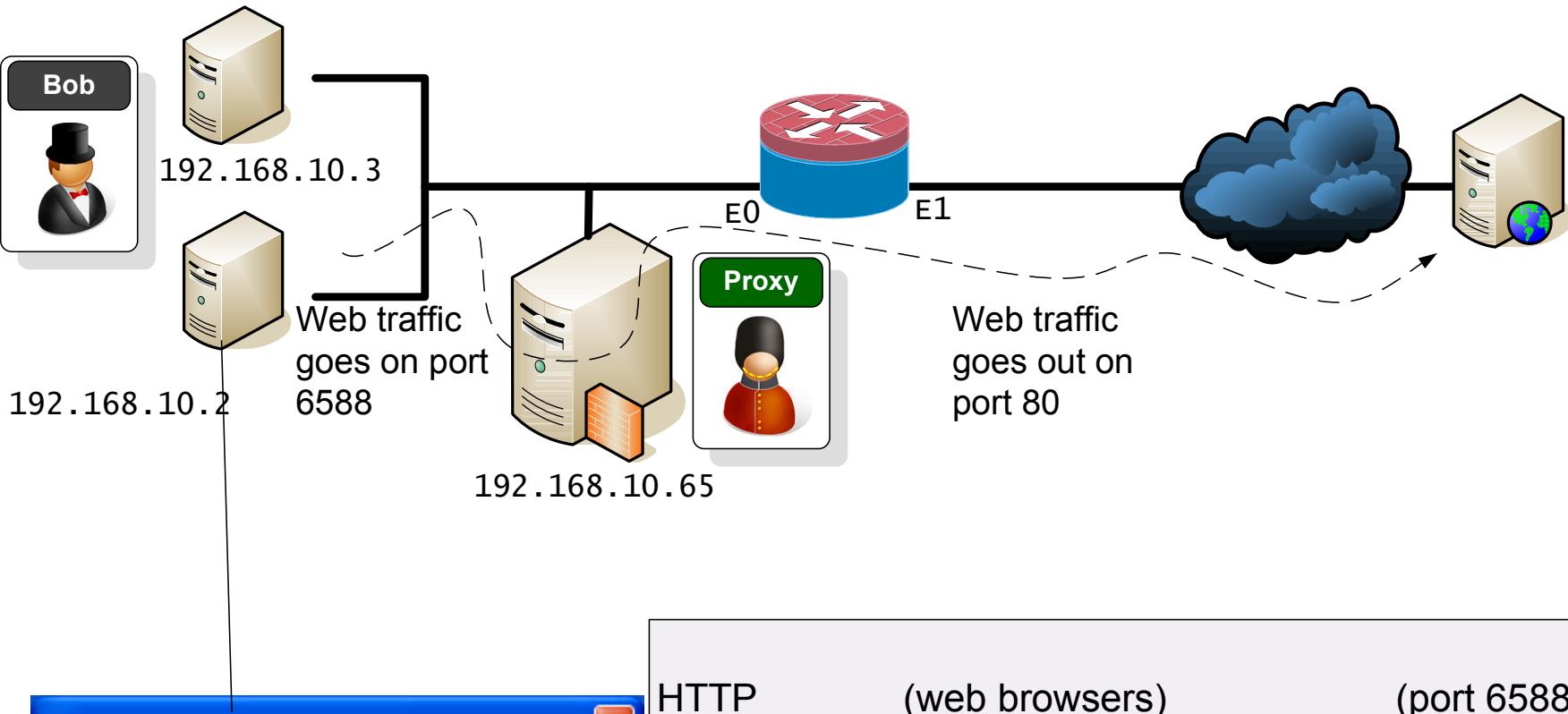
Agent proxy enabled

Web traffic goes To port 6588 on the proxy

Application gateways/proxy servers

Network Security

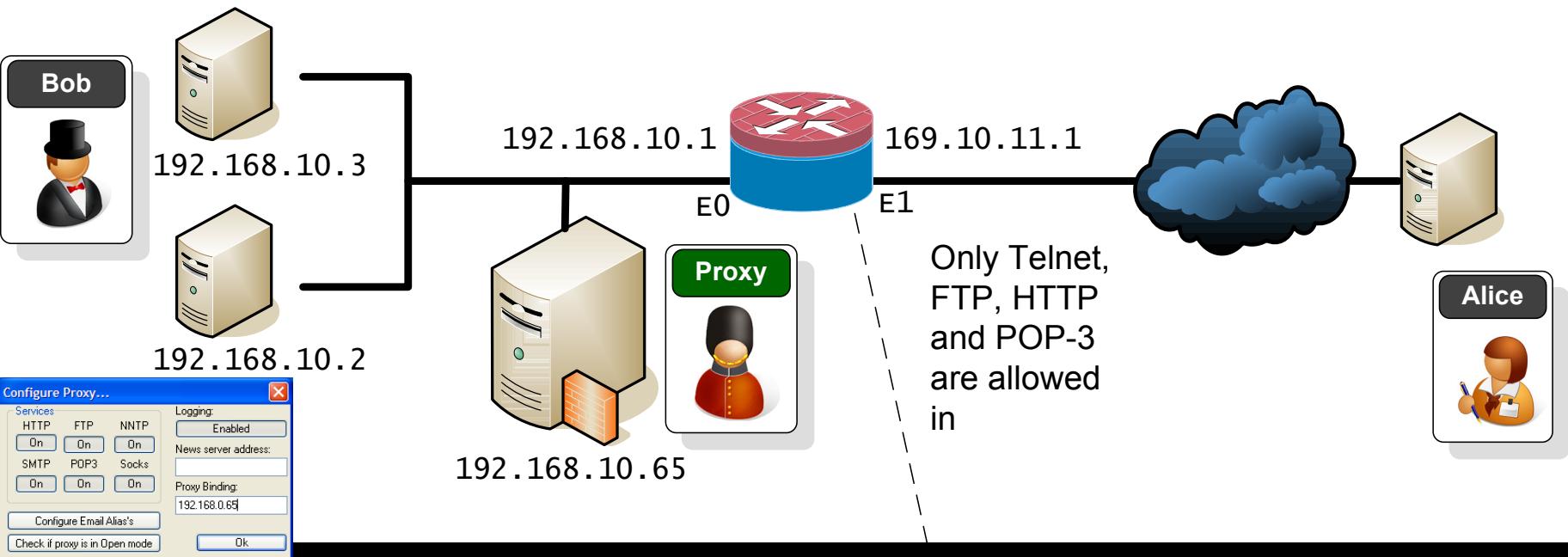
Proxies



Agent proxy
enabled

HTTP	(web browsers)	(port 6588)
HTTPS	(secure web browsers)	(port 6588)
SOCKS4	(TCP proxying)	(port 1080)
SOCKS4a	(TCP proxying w/ DNS lookups)	(port 1080)
SOCKS5	(only partial support, no UDP)	(port 1080)
NNTP	(usenet newsgroups)	(port 119)
POP3	(receiving email)	(port 110)
SMTP	(sending email)	(port 25)
FTP	(file transfers)	(port 21)

Typical proxy ports

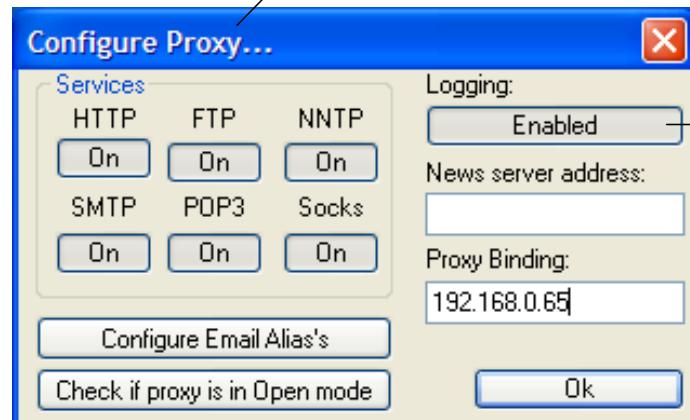
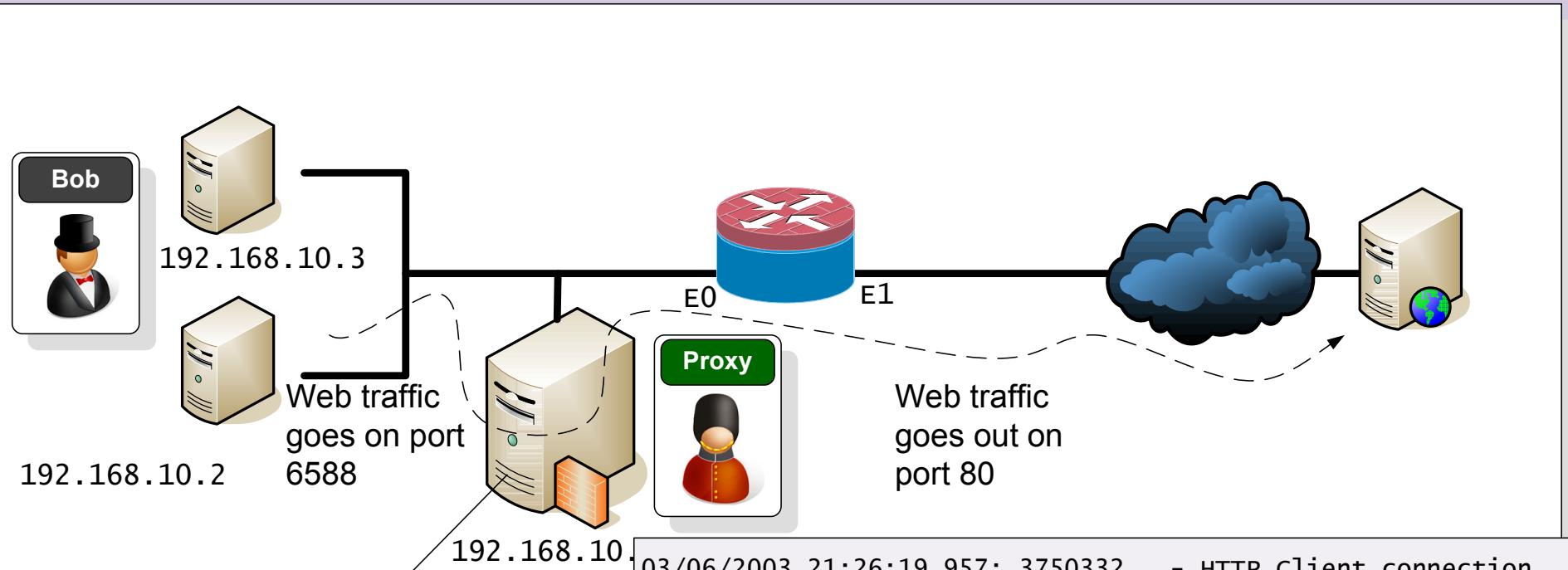


Only traffic on certain ports are allowed, and only if they are destined for the proxy

```
interface Ethernet1
ip address 169.10.11.1 255.255.0.0
ip access-group 101 in
!
access-list 101 permit tcp any any eq telnet host 192.168.10.65
access-list 101 permit tcp any any eq ftp host 192.168.10.65
access-list 101 permit tcp any any eq http host 192.168.10.65
access-list 101 permit tcp any any eq pop3 host 192.168.10.65
access-list 101 deny any any
```

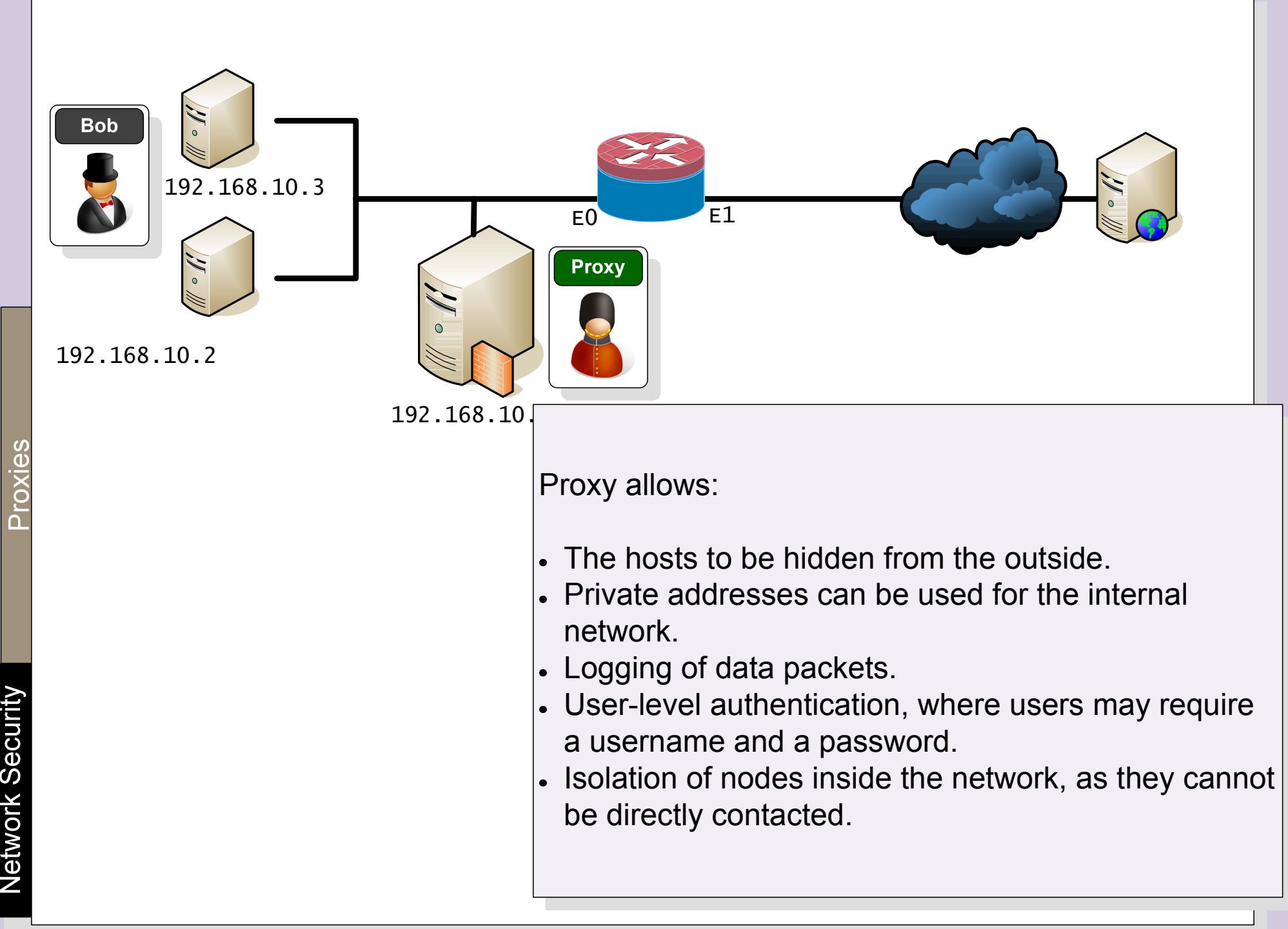
Network Security

Proxies



Agent proxy
enabled

03/06/2003 21:26:19.957: 3750332 - HTTP Client connection
accepted from 192.168.0.20
03/06/2003 21:26:21.620: 3773004 - HTTP Client connection
accepted from 192.168.0.20
03/06/2003 21:26:23.232: 3773004 - HTTP Closing socket (2)
03/06/2003 21:26:23.863: 3773004 - HTTP Client connection
accepted from 192.168.0.20
03/06/2003 21:26:26.527: 3773004 - HTTP Closing socket (2)
03/06/2003 21:26:26.737: 3773004 - HTTP Client connection
accepted from 192.168.0.20
03/06/2003 21:26:29.091: 3773004 - HTTP Closing socket (2)
03/06/2003 21:26:29.371: 3773004 - HTTP Client connection
accepted from 192.168.0.20
03/06/2003 21:26:29.431: 3750332 - HTTP Closing socket (2)
03/06/2003 21:26:30.453: 3773004 - HTTP Closing socket (1)
03/06/2003 21:26:31.644: 3750332 - HTTP Client connection
accepted from 192.168.0.20
03/06/2003 21:26:32.786: 3750332 - HTTP Closing socket (1)
03/06/2003 21:26:33.126: 3750332 - HTTP Client connection
accepted from 192.168.0.20



Network Security



VPNs

What is required is:

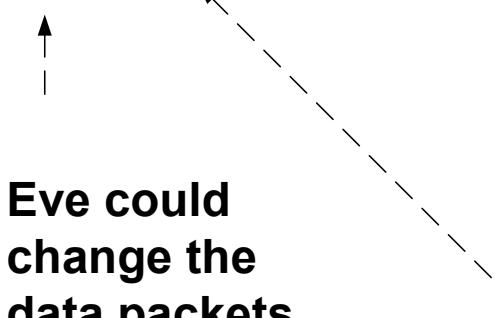
- Encryption.
- Authentication of devices (to overcome spoofing)
- Authentication of packets (for integrity)



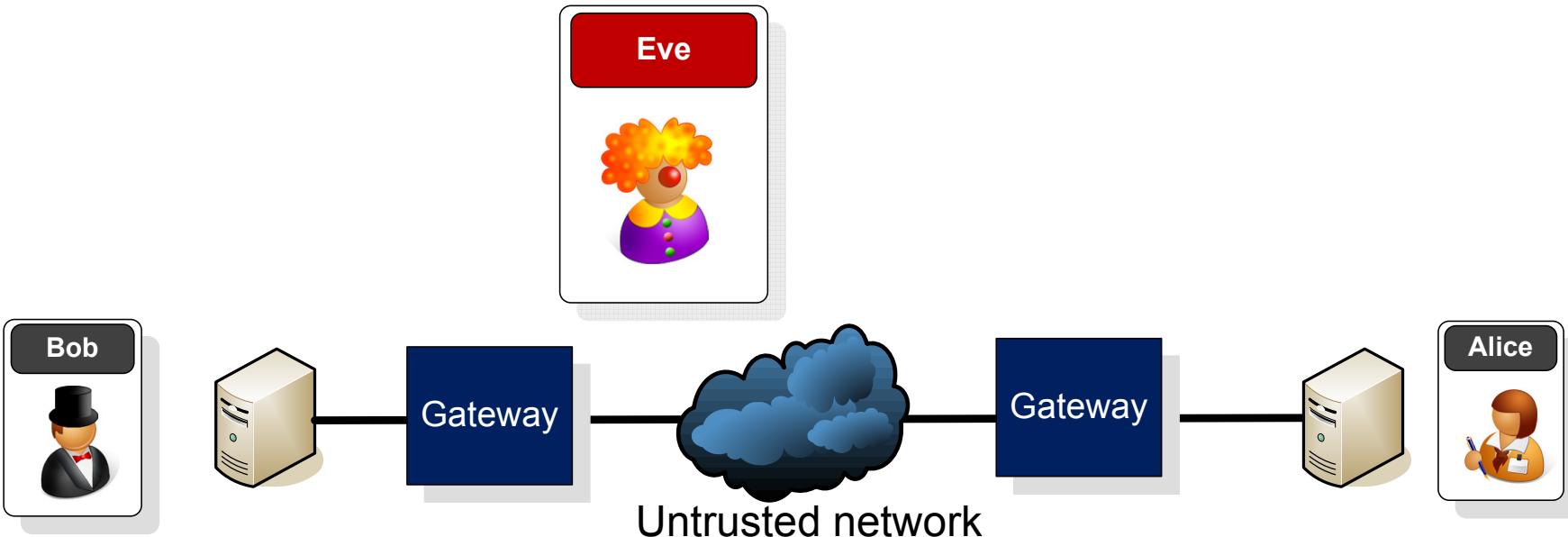
Eve could eavesdrop on the public communications



Eve could change the data packets



Eve could setup an alternative gateway



What is required is:

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

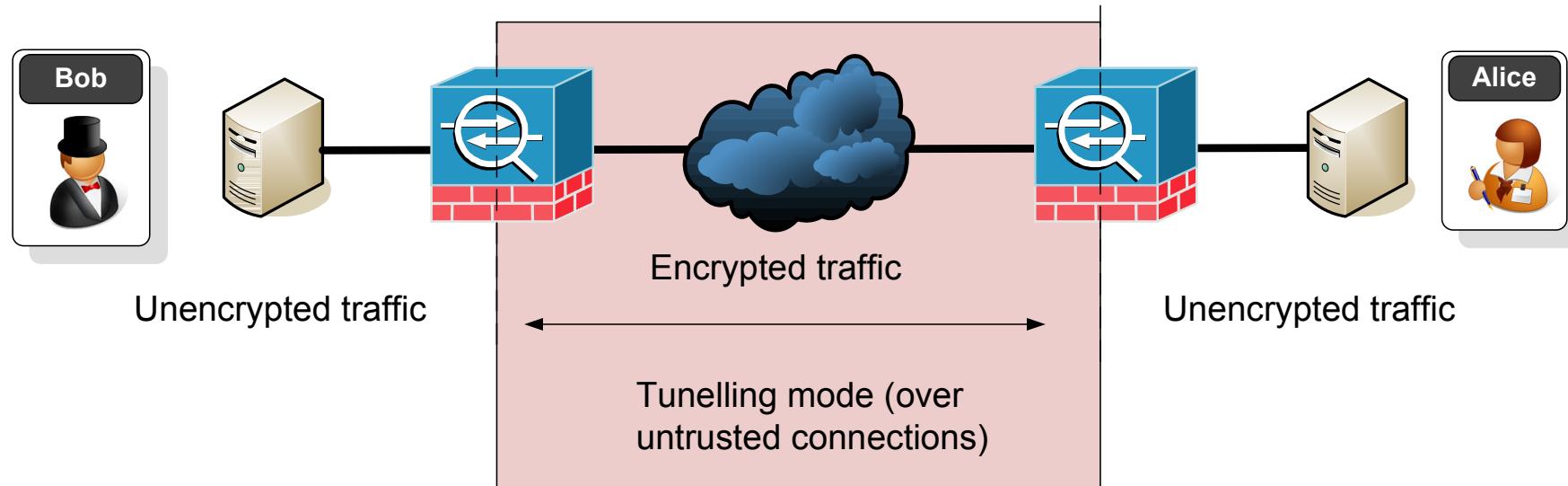
PPTP (Point-to-point Tunneling Protocol). Created by Microsoft and is routable. It uses MPPE (Microsoft Point-to-point Encryption) and user authentication.

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).

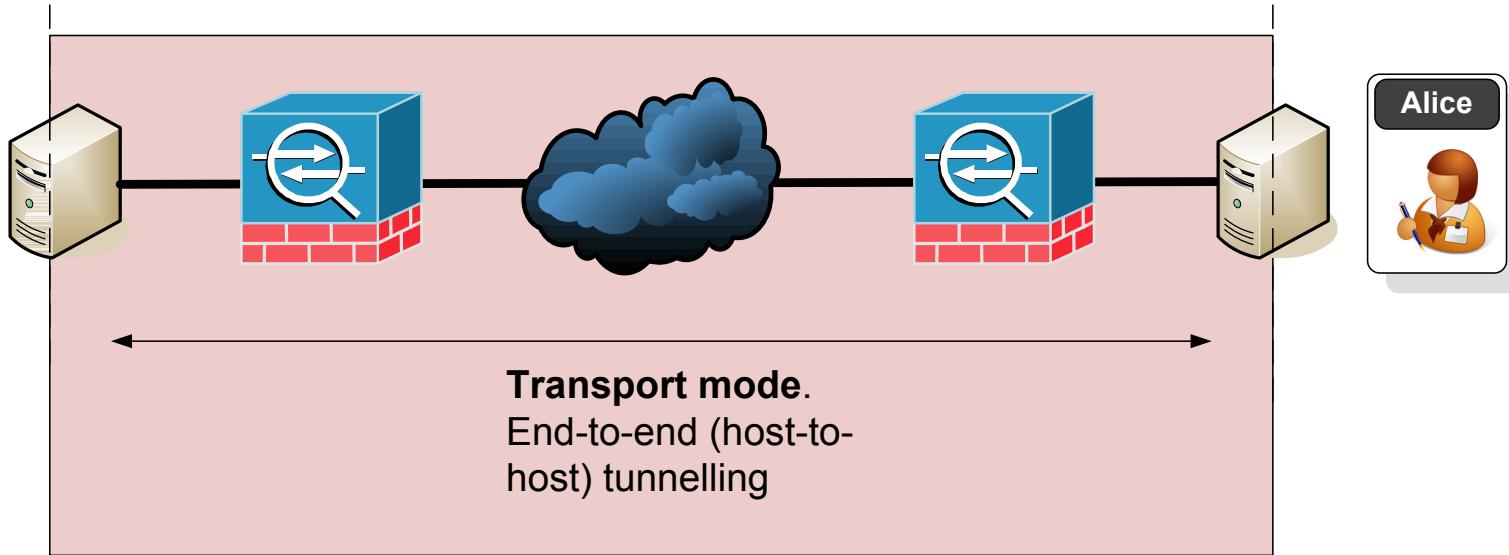
IPSec. An open standard. Includes both encryption and Authentication.

Network Security

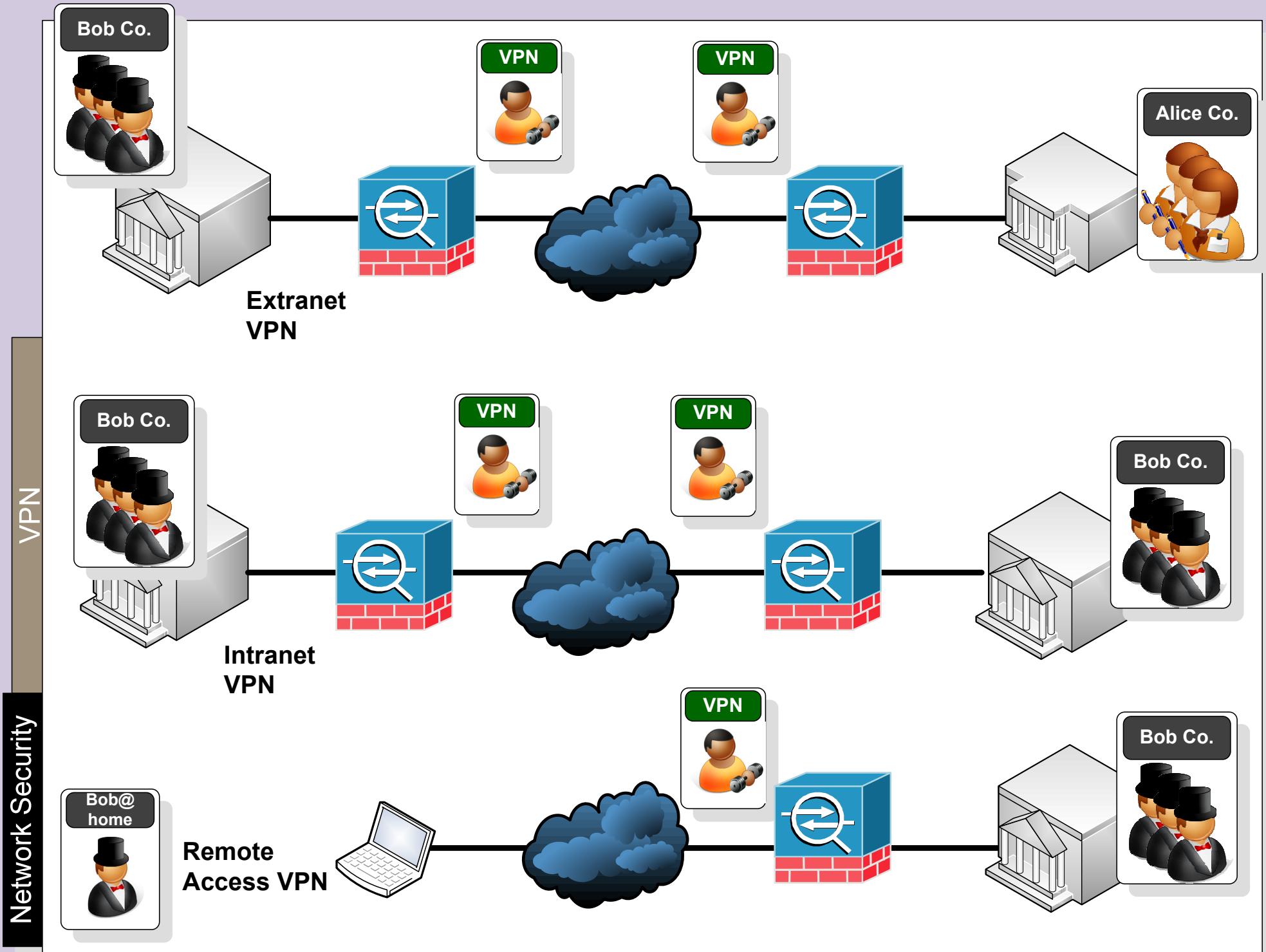
VPN



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



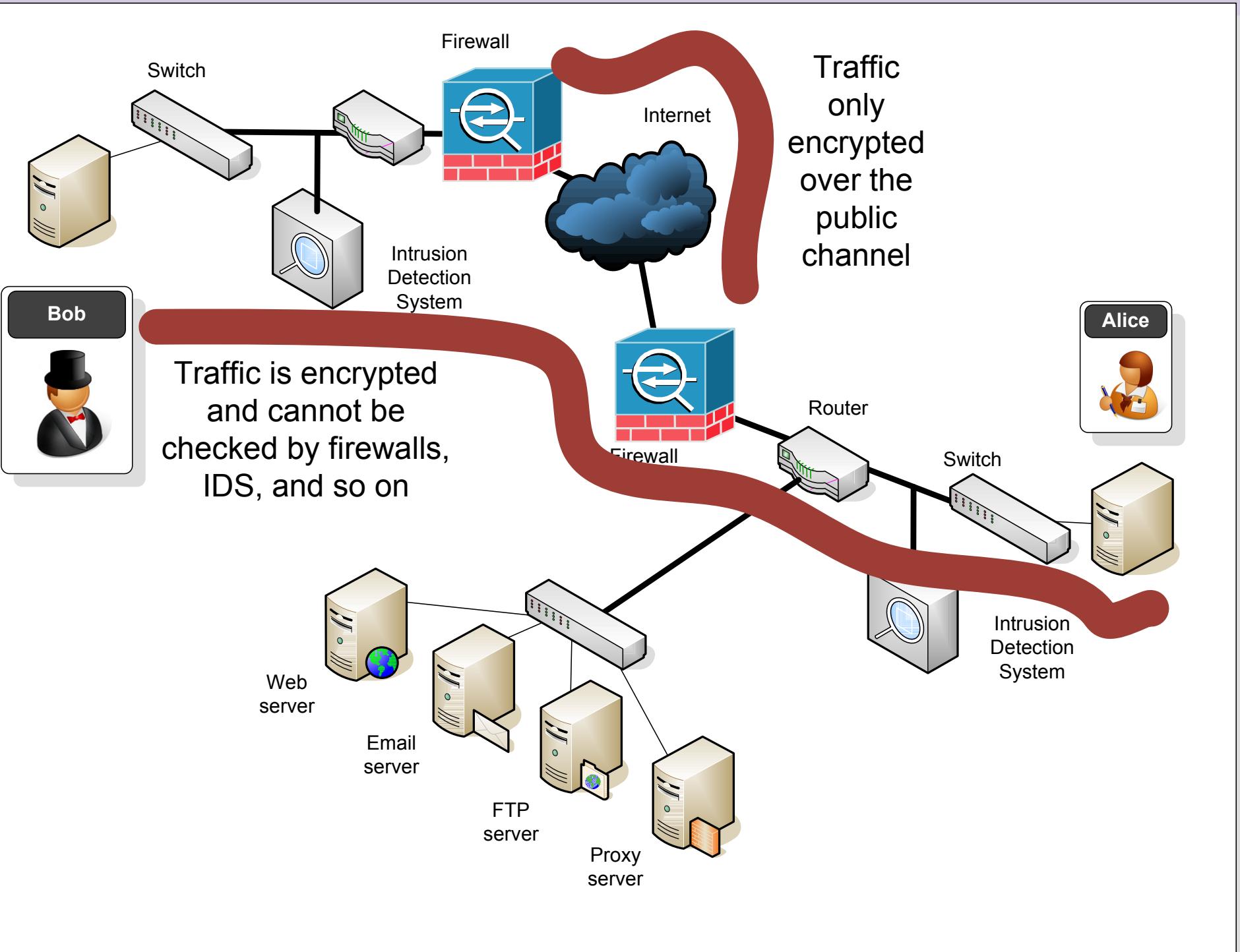
Tunnelling mode or transport mode

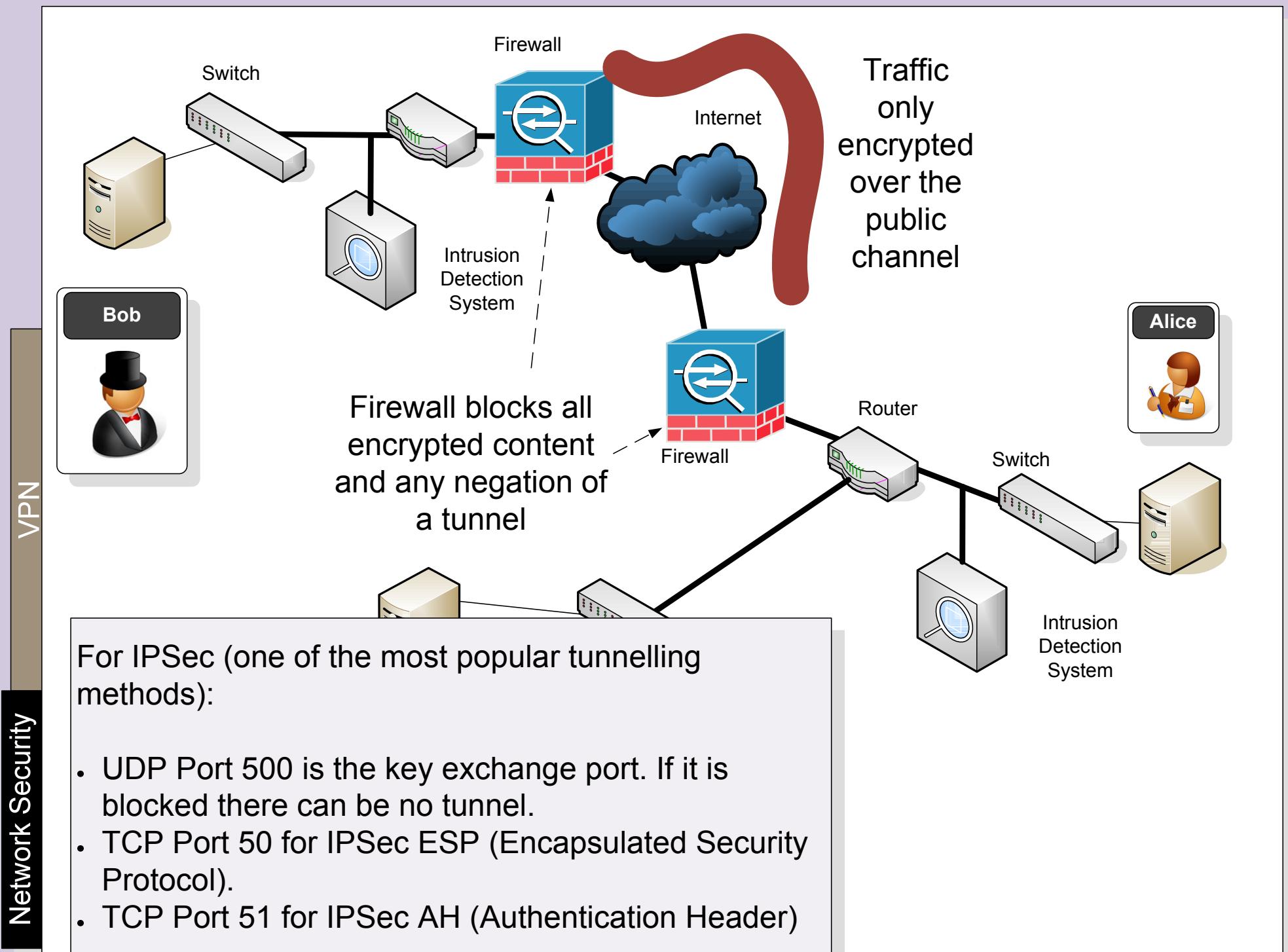


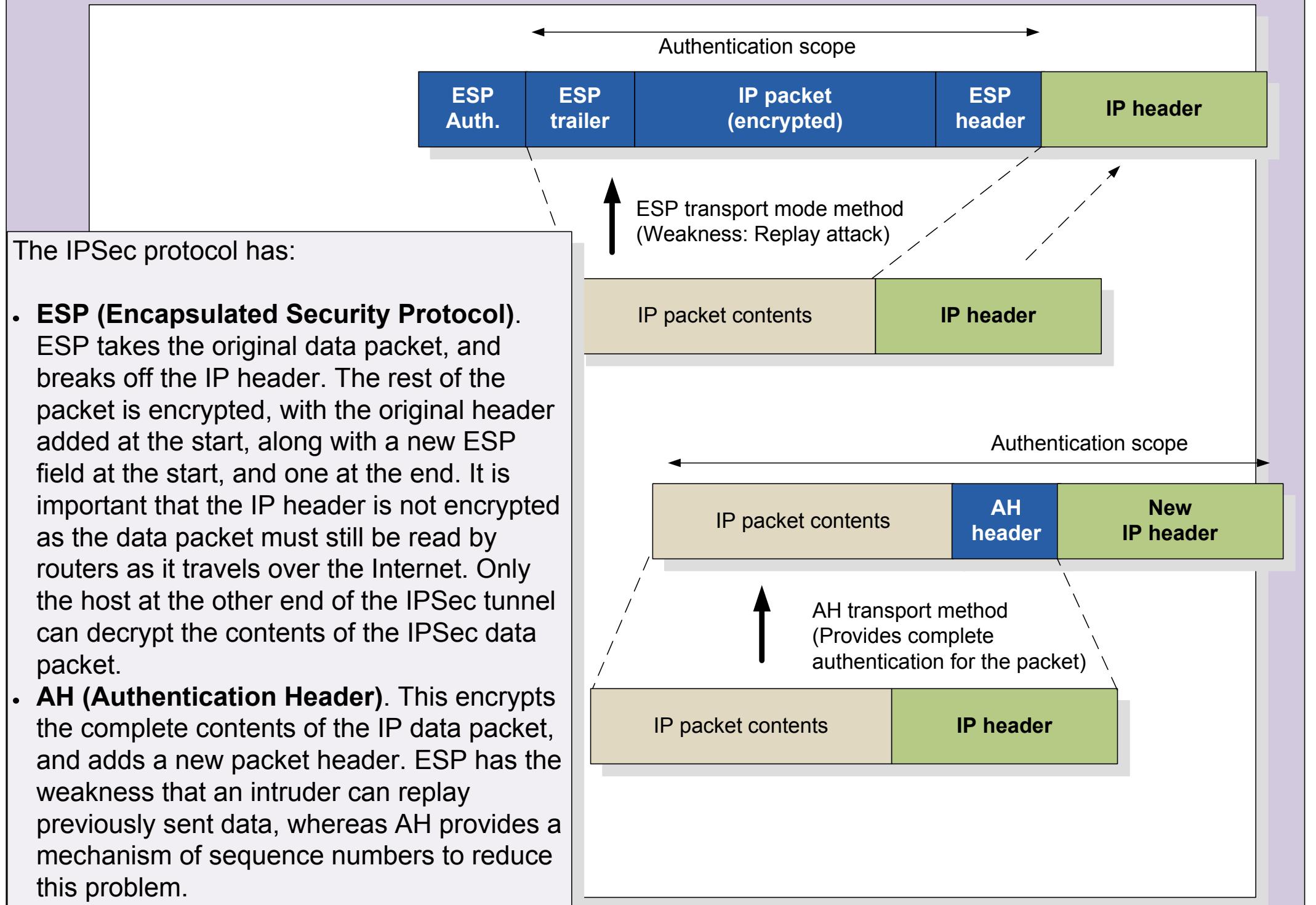
VPN types

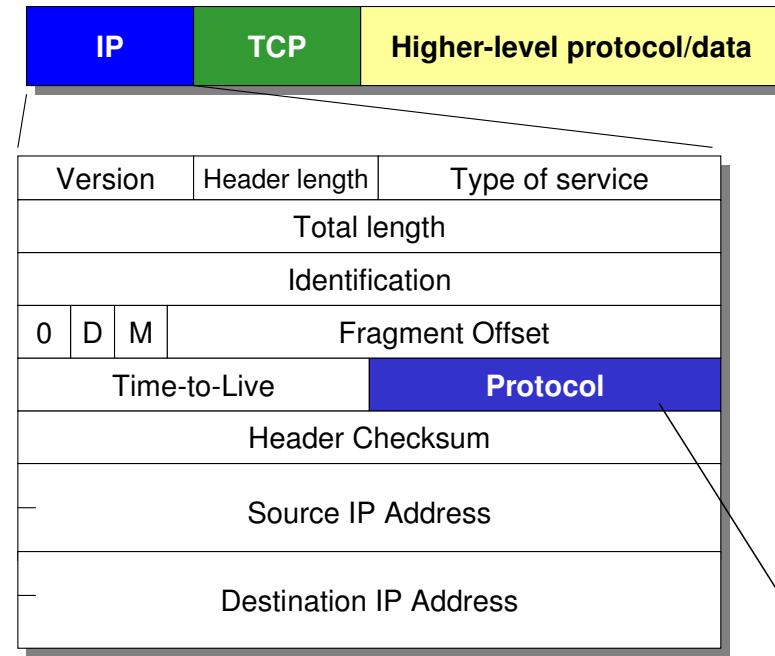
Network Security

VPN

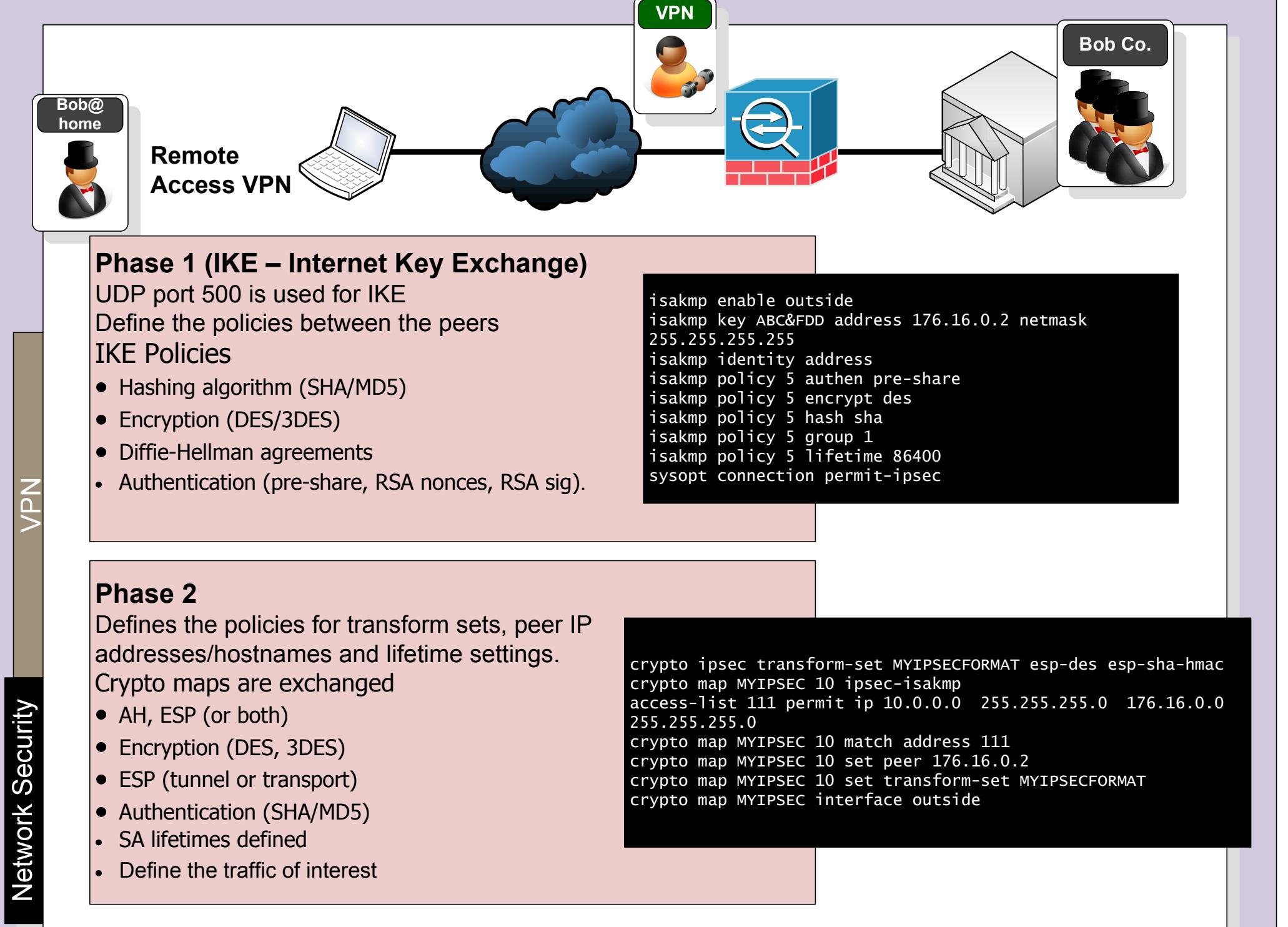


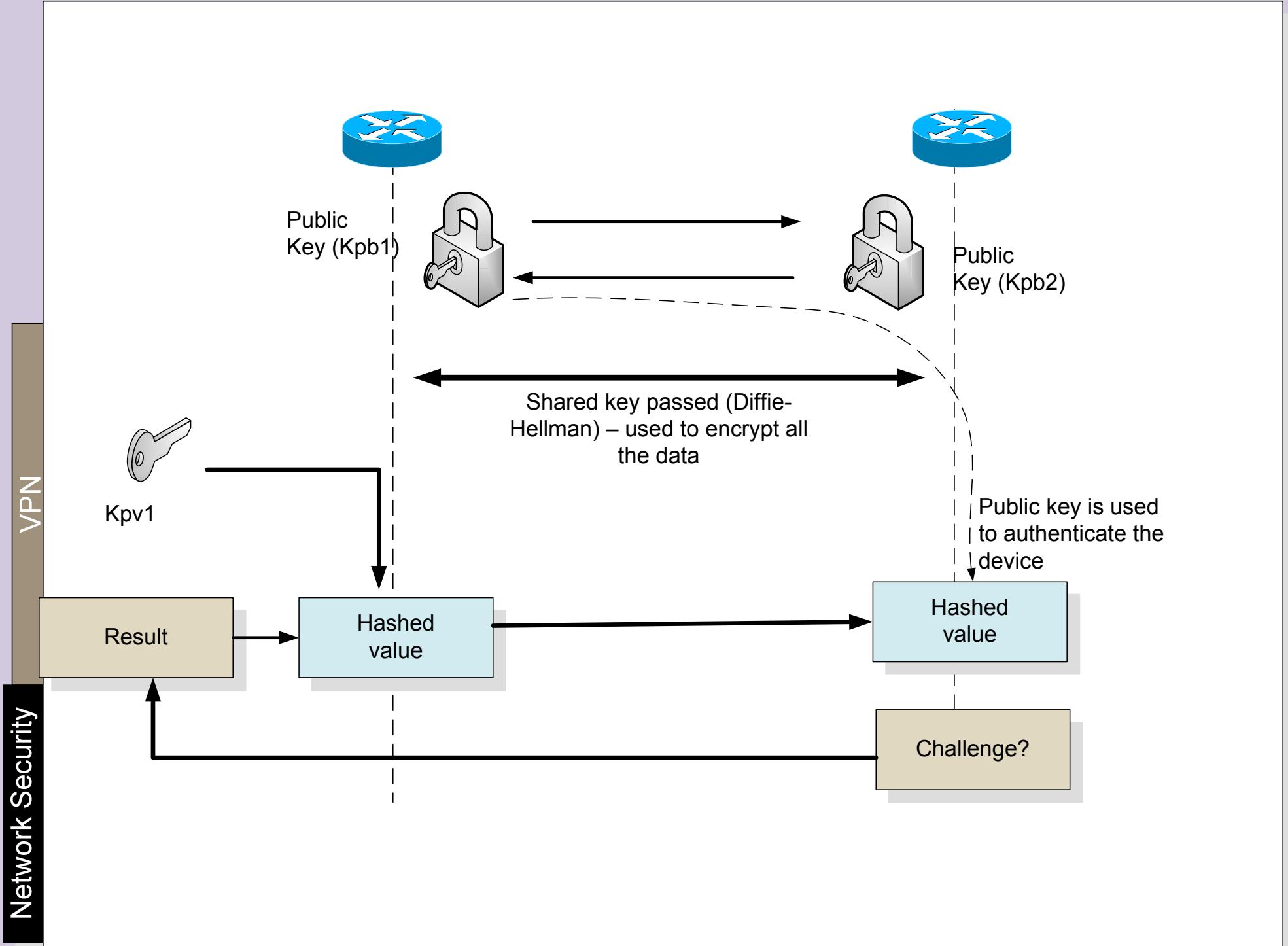


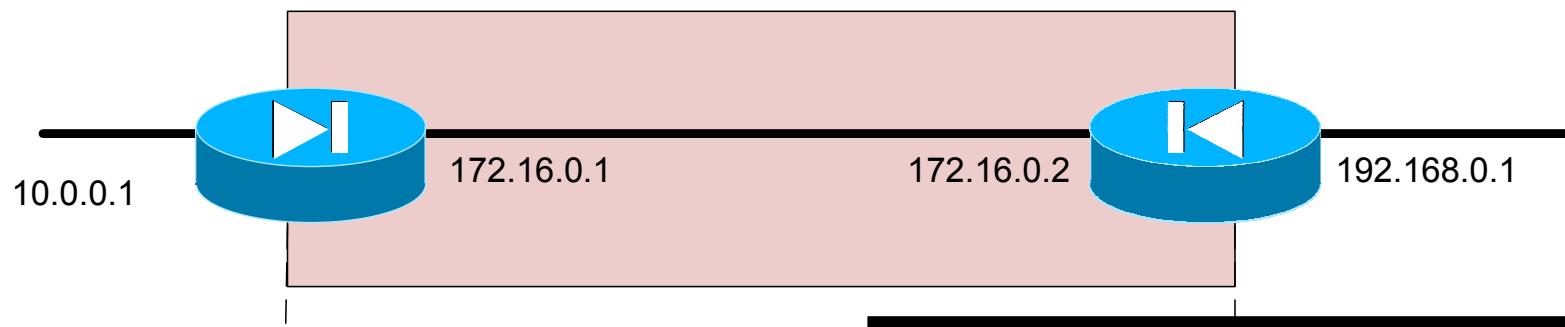




- 1 ICMP Internet Control Message [RFC792]
- 6 TCP Transmission Control [RFC793]
- 8 EGP Exterior Gateway Protocol [RFC888]
- 9 IGP any private interior gateway [IANA]
- 47 GRE General Routing Encapsulation (PPTP)**
- 50 ESP Encap Security Payload [RFC2406]**
- 51 AH Authentication Header [RFC2402]**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







```

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

crypto ipsec transform-set MYIPSECFORMAT esp-des esp-
sha-hmac
access-list 111 permit ip 10.0.0.0 255.255.255.0
192.168.0.0 255.255.255.0
crypto map MYIPSEC 10 ipsec-isakmp
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

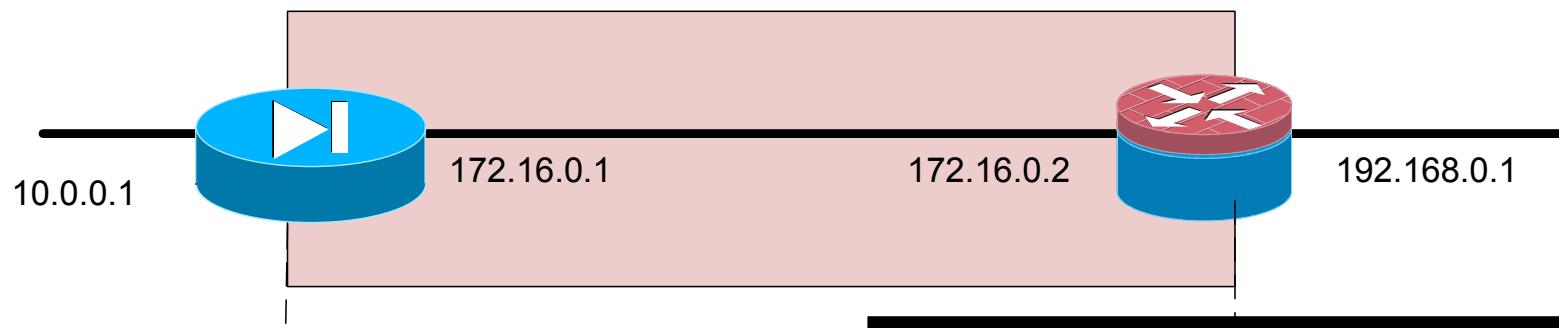
```

```

isakmp enable outside
isakmp key ABC&FDD address 176.16.0.1 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

crypto ipsec transform-set MYIPSECFORMAT esp-des esp-
sha-hmac
access-list 111 permit ip 192.168.0.0
255.255.255.0 10.0.0.0 255.255.255.0
crypto map MYIPSEC 10 ipsec-isakmp
crypto map MYIPSEC 10 match address 111
crypto map MYIPSEC 10 set peer 176.16.0.1
crypto map MYIPSEC 10 set transform-set
MYIPSECFORMAT
crypto map MYIPSEC interface outside

```



```

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

crypto ipsec transform-set MYIPSECFORMAT esp-des esp-
sha-hmac
access-list 111 permit ip 10.0.0.0 255.255.255.0
192.168.0.0 255.255.255.0
crypto map MYIPSEC 10 ipsec-isakmp
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

```

```

crypto isakmp policy 1
  hash sha
  authentication pre-share
  group 1
  lifetime 86400
  encryption des
crypto isakmp key ABC&FDD address 172.16.0.1
crypto ipsec transform-set rtpset esp-des esp-md5-
hmac
crypto identity address

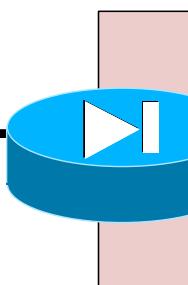
crypto map mymap 1 ipsec-isakmp
  set peer 172.16.0.1
  set transform-set rtpset
  match address 115

interface FastEthernet0/0
  ip address 172.16.0.2 255.255.255.0
  crypto map mymap

access-list 115 permit ip 192.168.0.0 0.0.0.255
10.0.0.0 0.0.0.255

```

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)

Network Security

VPN

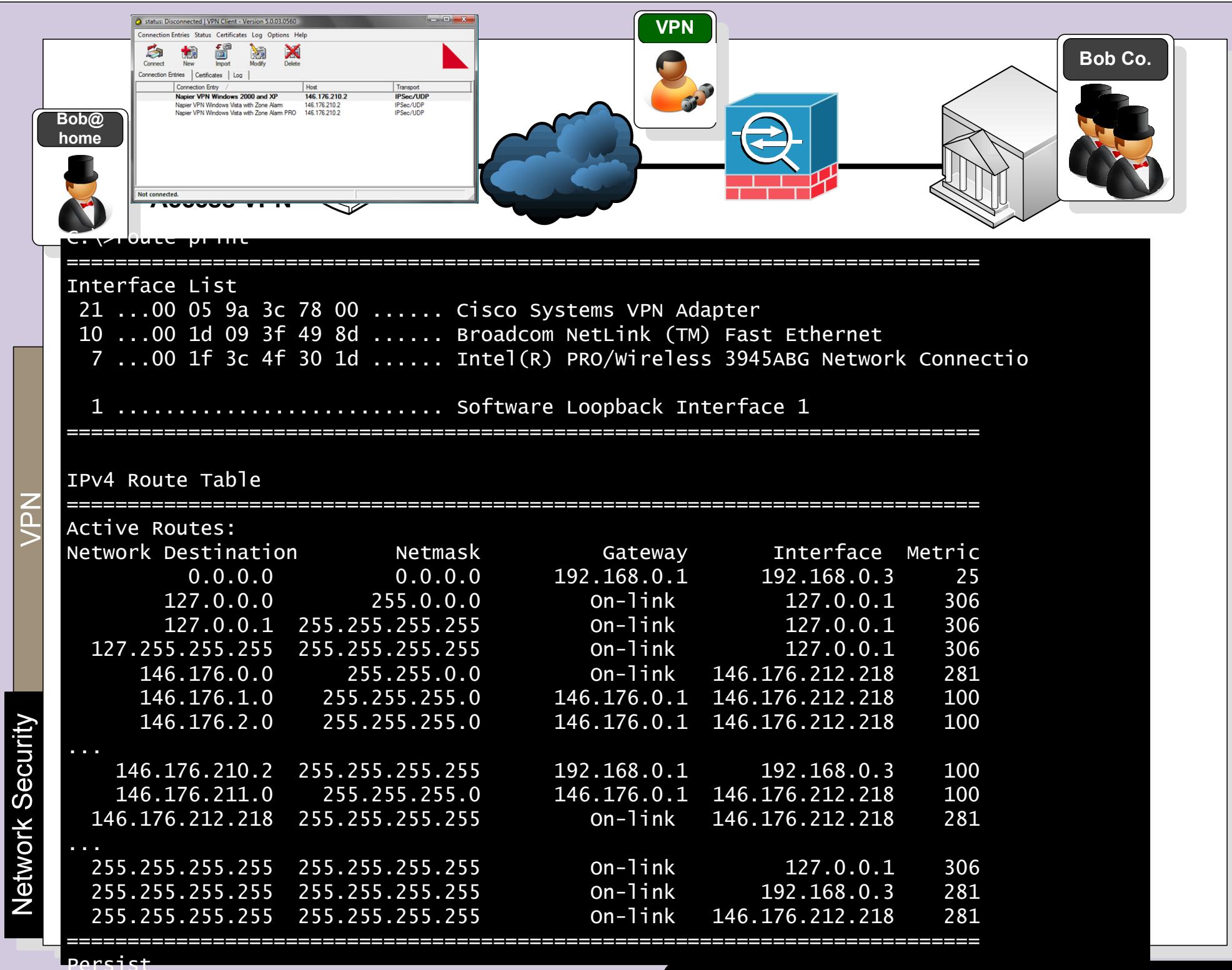
Remote Access VPN

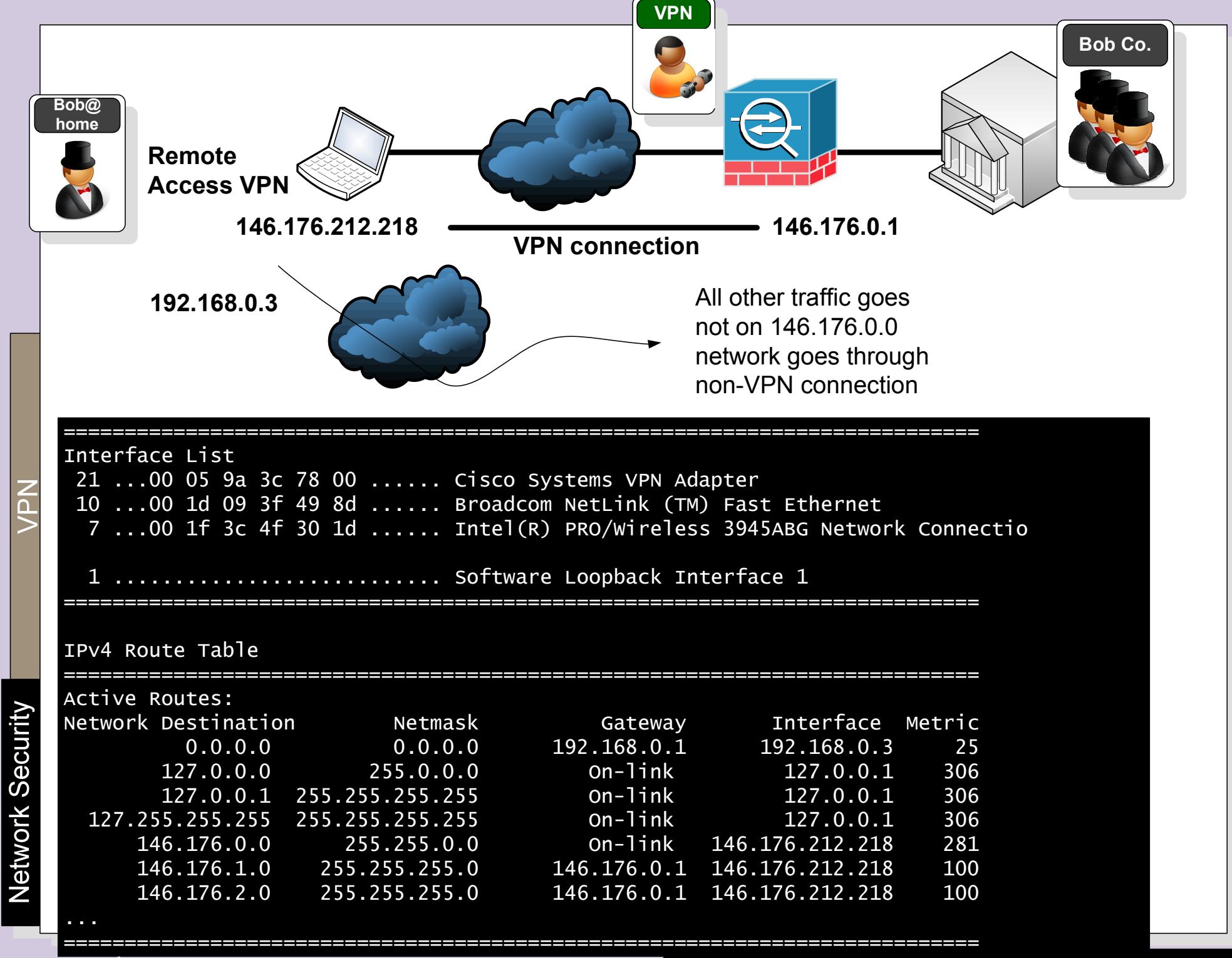
```
C:\>route print
=====
Interface List
10 ...00 1d 09 3f 49 8d ..... Broadcom NetLink (TM) Fast Ethernet
 7 ...00 1f 3c 4f 30 1d ..... Intel(R) PRO/Wireless 3945ABG Network Connection

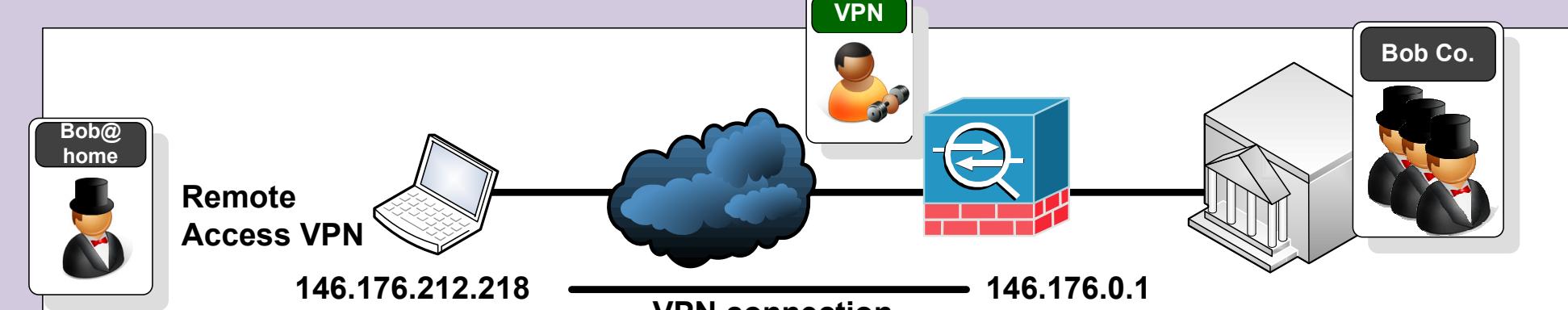
 1 ..... Software Loopback Interface 1
=====

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
```

Before connecting to the VPN







VPN

Network Security

```
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				

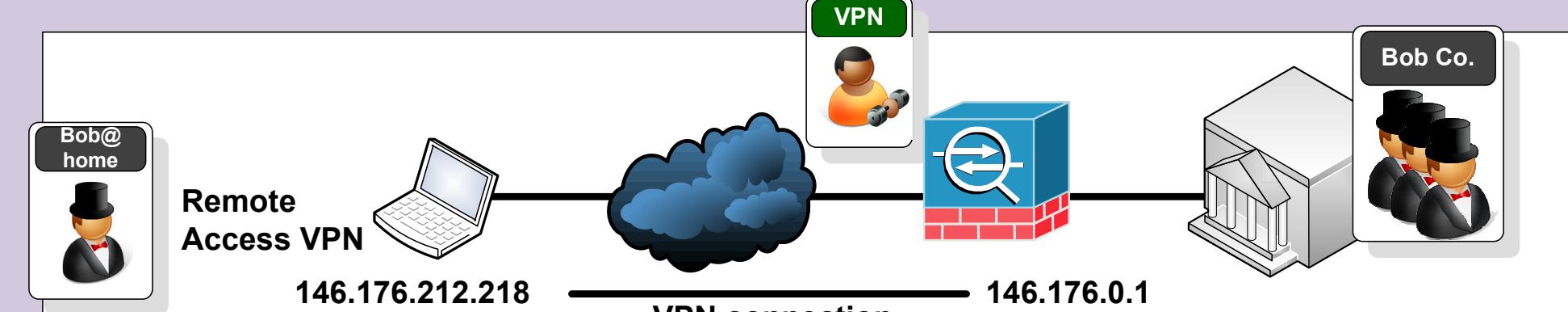
Before VPN connection

```
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



VPN

Network Security

```
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:

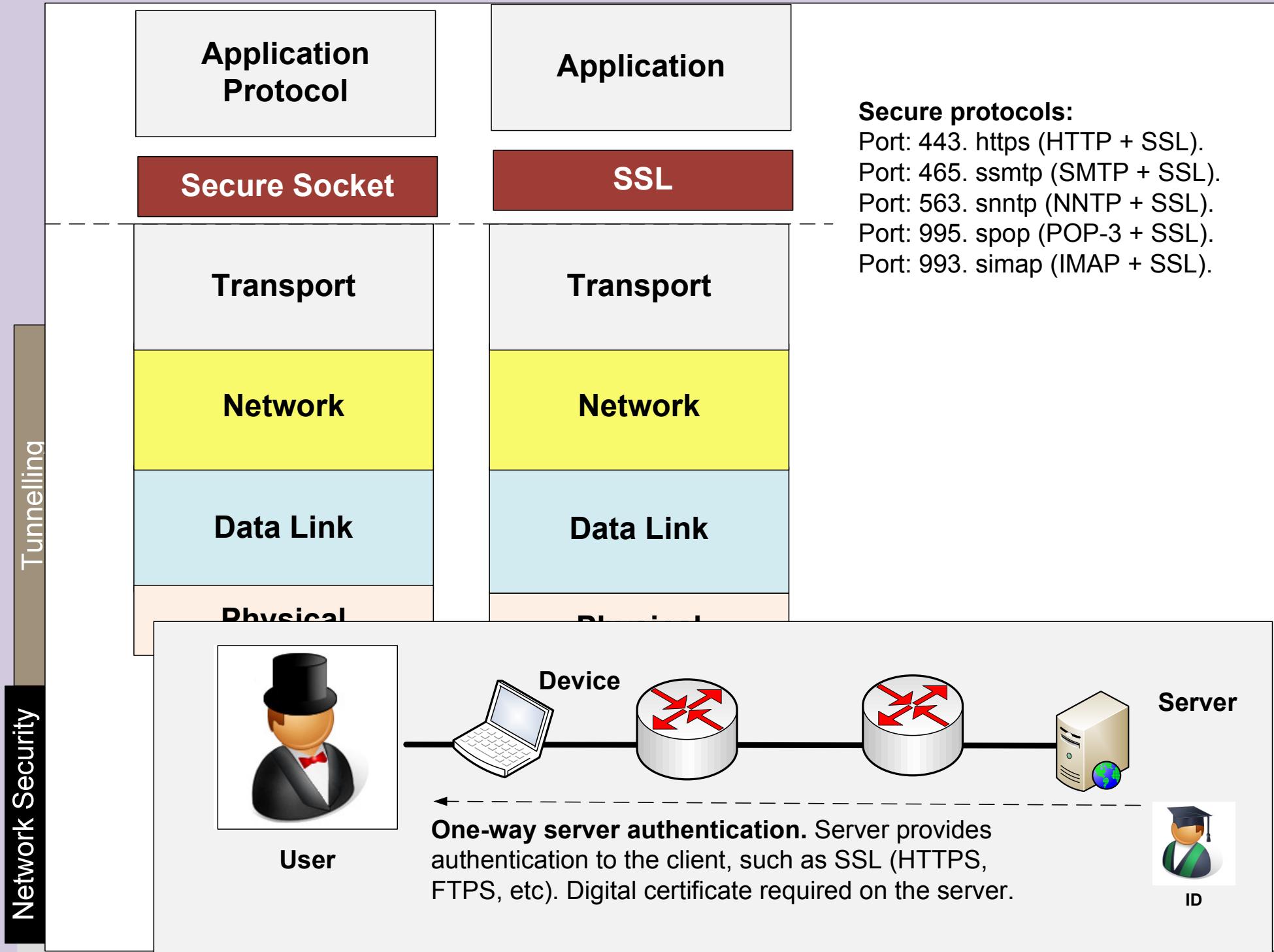
1	3 ms	1 ms	1 ms	192.168.0.1
2	35 ms	43 ms	36 ms	cr0.escra.uk.easynet.net [87.87.249.224]
3	32 ms	31 ms	32 ms	ip-87-87-146-129.easynet.co.uk [87.87.146.129]
4	46 ms	45 ms	45 ms	te7-0-0.sr0.enlcs.ov.easynet.net [89.200.132.109]
5	46 ms	47 ms	47 ms	5adff621.bb.sky.com [90.223.246.33]

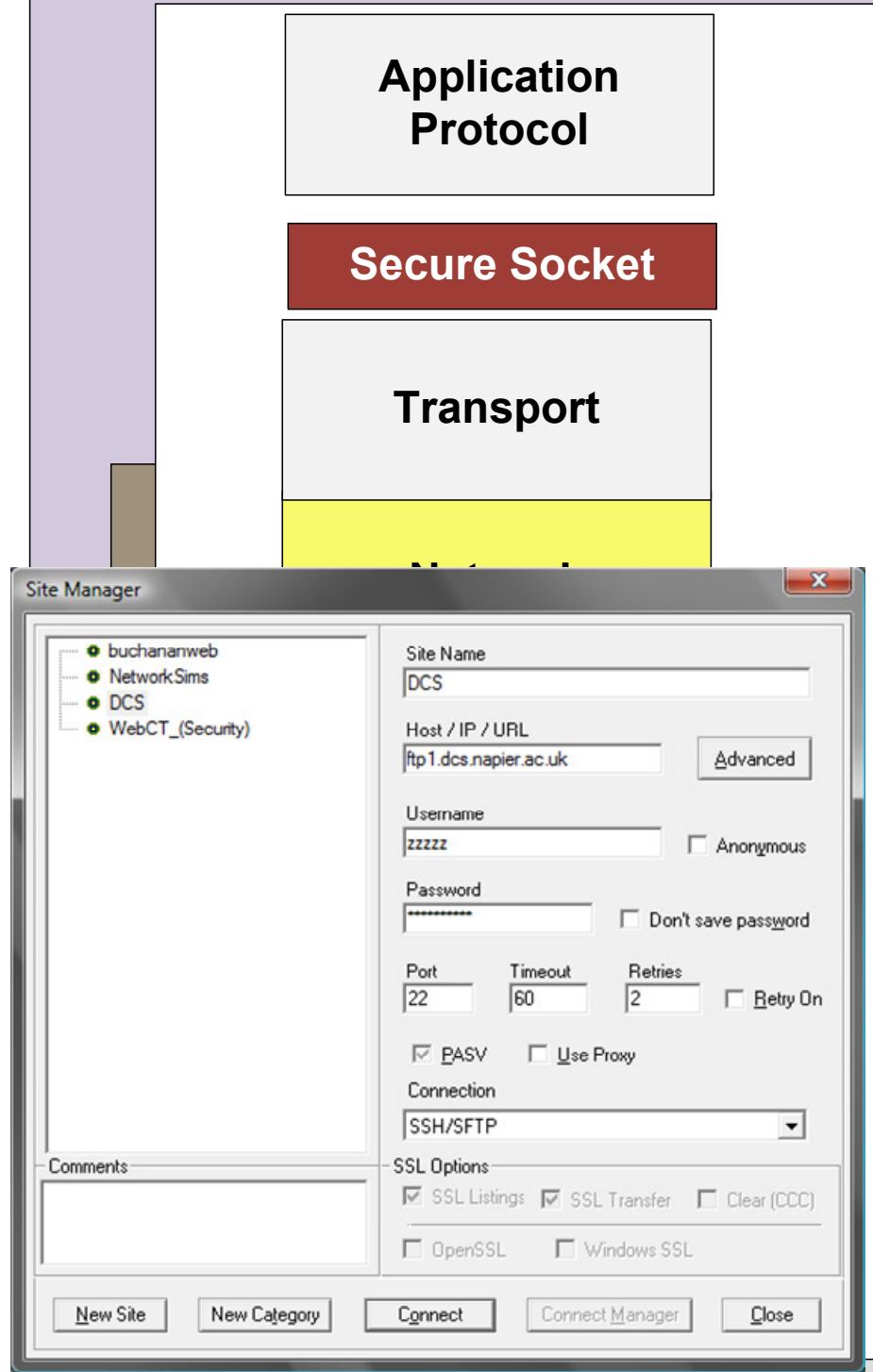
After VPN connection

Network Security



Tunnelling





Enter Remote Host: **ftp1.dcs.napier.ac.uk**
Enter Username: **zzAA**
Enter Password: **abcde**

Connecting... Details:

MAC-hmac-md5

Port: 22

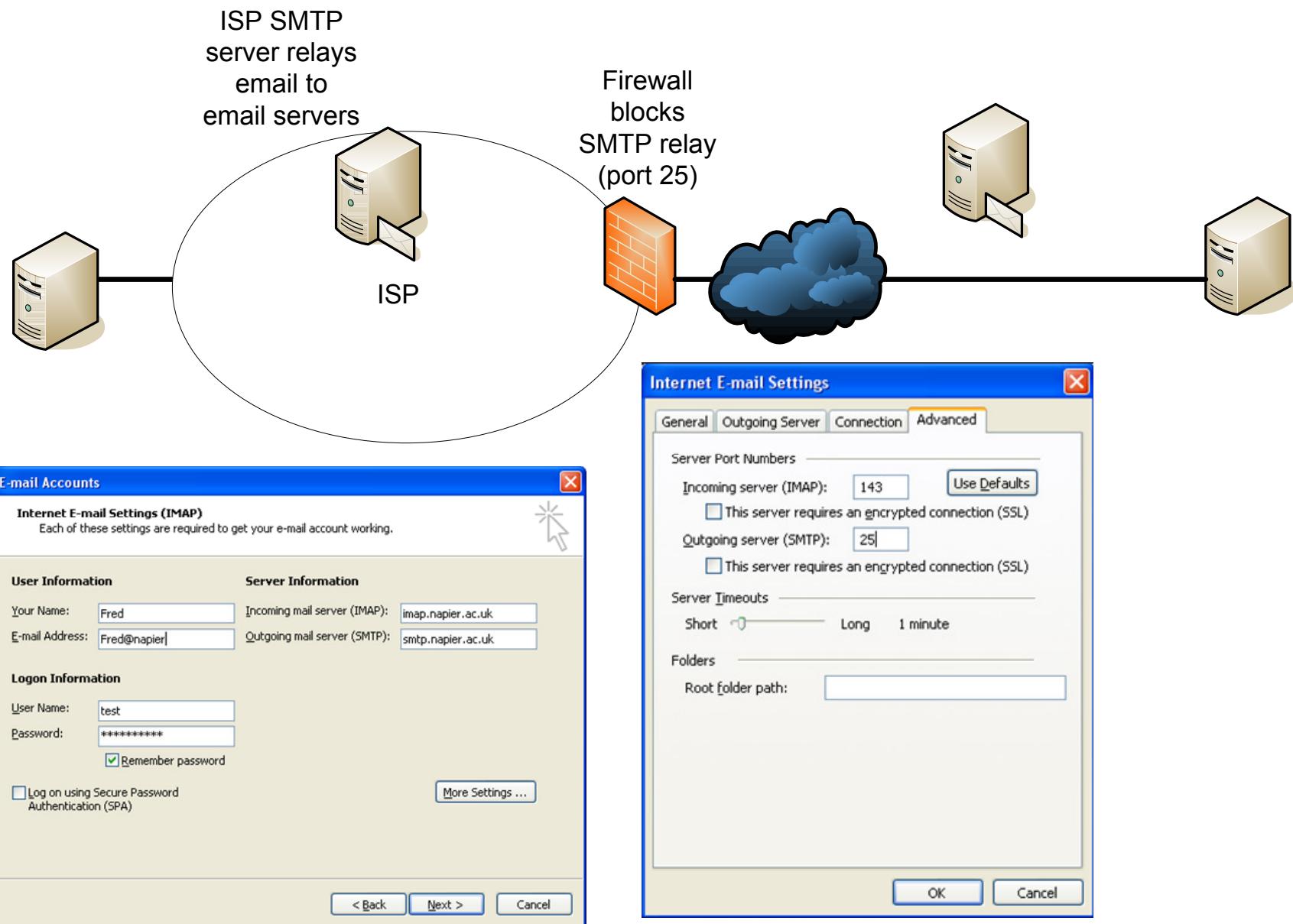
Cipher: 3des-cbc

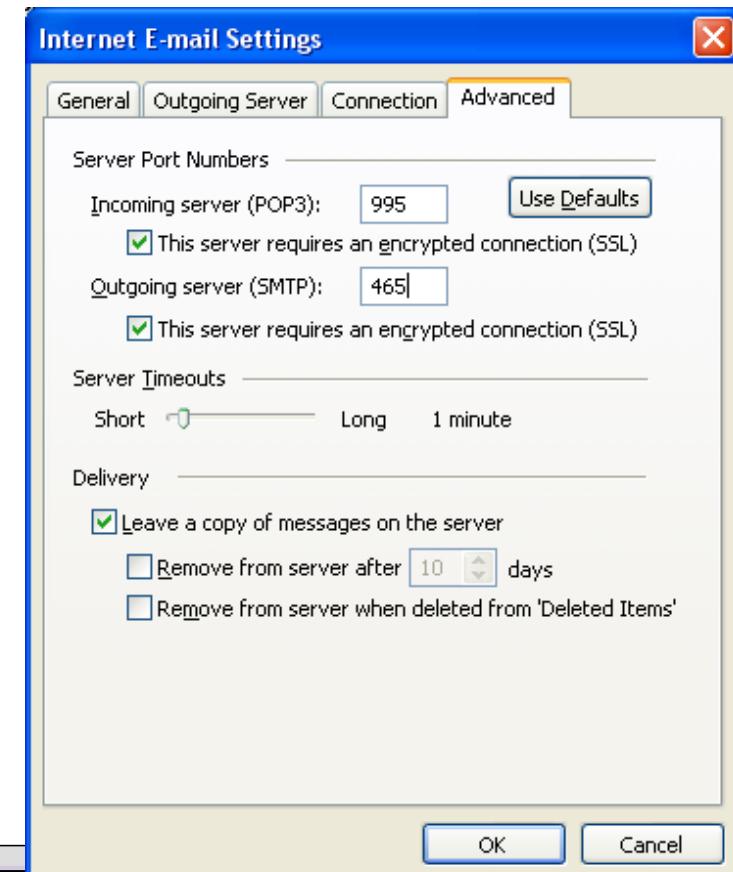
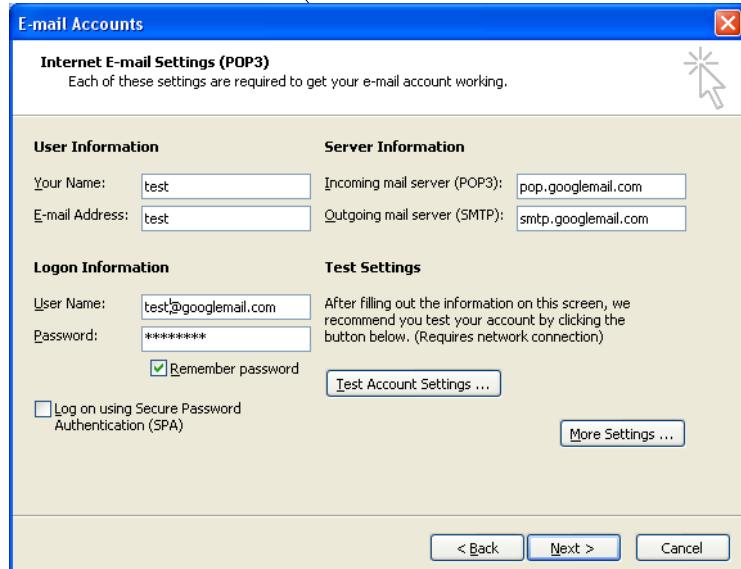
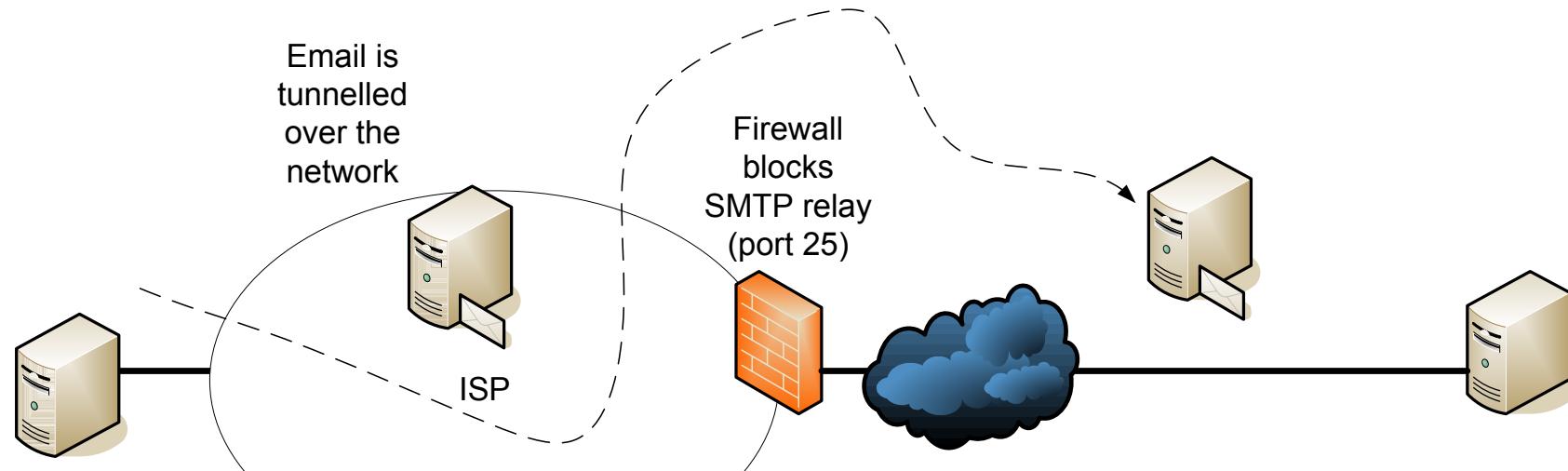
Last login: Tue Jan 23 21:15:43 2007 from user-514da235.12.c1.ds1.pol.co.uk

Directory: /home/cs72

Tue Jan 23 21:19:30 GMT 2007

socweb1:~> ls





Secure protocols:

- Port: 443. https (HTTP + SSL).
- Port: 465. ssmtp (SMTP + SSL).
- Port: 563. snntp (NNTP + SSL).
- Port: 995. spop (POP-3 + SSL).
- Port: 993. simap (IMAP + SSL).

Intel(R) PRO/Wireless 2200BG Network Connection (Microsoft's Packet Scheduler) : Capturing - Ethernet

File Edit View Go Capture Analyze Statistics Help

Filter: (ip.addr eq 192.168.1.101 and ip.addr eq 146.176.165.229) and (Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	1.268236	pc165229.napier.ac.uk	telnet[13]	TELNET	Telnet Data ...
28	1.268236	pc165229.napier.ac	192.168.1.101	TCP	telnet > 1508 [ACK] Seq=0 Ack=1 wIn=5840 Len=0
39	1.268388	pc165229.napier.ac	192.168.1.101	TELNET	Telnet Data ...
48	1.393798	192.168.1.101	pc165229.napier.ac	TCP	1508 > telnet [ACK] Seq=1 Ack=1 wIn=17499 Len=0
58	1.367366	192.168.1.101	pc165229.napier.ac	TELNET	Telnet Data ...
63	1.431317	pc165229.napier.ac	192.168.1.101	TELNET	Telnet Data ...
81	1.7946212	192.168.1.101	pc165229.napier.ac	TCP	1508 > telnet [ACK] Seq=2 Ack=2 wIn=17498 Len=0
101	2.080087	192.168.1.101	pc165229.napier.ac	TELNET	Telnet Data ...
112	2.167048	pc165229.napier.ac	192.168.1.101	TELNET	Telnet Data ...
117	2.299159	192.168.1.101	pc165229.napier.ac	TCP	1508 > telnet [ACK] Seq=3 Ack=3 wIn=17495 Len=0
119	2.314791	192.168.1.101	pc165229.napier.ac	TELNET	Telnet Data ...
125	2.376102	pc165229.napier.ac	192.168.1.101	TELNET	Telnet Data ...
138	2.500319	192.168.1.101	pc165229.napier.ac	TCP	1508 > telnet [ACK] Seq=4 Ack=4 wIn=17494 Len=0
139	2.5122898	192.168.1.101	pc165229.napier.ac	TELNET	Telnet Data ...
131	2.643422	pc165229.napier.ac	192.168.1.101	TELNET	Telnet Data ...
138	2.700027	192.168.1.101	pc165229.napier.ac	TELNET	Telnet Data ...
160	2.739947	pc165229.napier.ac	192.168.1.101	TELNET	Telnet Data ...
173	2.902644	192.168.1.101	pc165229.napier.ac	TCP	1508 > telnet [ACK] Seq=6 Ack=6 wIn=17492 Len=0
180	2.957809	192.168.1.101	pc165229.napier.ac	TELNET	Telnet Data ...
181	3.001930	pc165229.napier.ac	192.168.1.101	TELNET	Telnet Data ...
184	3.103867	192.168.1.101	pc165229.napier.ac	TCP	1508 > telnet [ACK] Seq=7 Ack=7 wIn=17491 Len=0
188	3.248610	192.168.1.101	pc165229.napier.ac	TELNET	Telnet Data ...
190	3.283807	pc165229.napier.ac	192.168.1.101	TELNET	Telnet Data ...
193	3.405649	192.168.1.101	pc165229.napier.ac	TCP	1508 > telnet [ACK] Seq=8 Ack=8 wIn=17490 Len=0
194	3.406671	192.168.1.101	pc165229.napier.ac	TELNET	Telnet Data ...
195	3.443667	pc165229.napier.ac	192.168.1.101	TELNET	Telnet Data ...

```

# Frame 32 (33 bytes on wire, 33 bytes captured)
# Ethernet II, Src: IntelCor_14:02:f0 (00:15:00:14:02:f0), Dst: Linksys_53:21:d0 (00:0c:a1:f3:21:d0)
# Internet Protocol Version 4, Src: 192.168.1.101 (192.168.1.101), Dst: pc165229.napier.ac.uk (146.176.165.229)
# Transmission Control Protocol, Src Port: 1508 (1508), Dst Port: telnet (23), Seq: 0, Ack: 0, Len: 1
# Telnet
    Data: 0

```

0000	00	0c	a1	f3	23	d5	00	11	00	34	02	f0	08	00	43	00	.A.	#	..	4	..	E.
0010	00	29	76	dc	49	00	80	06	89	37	c0	48	01	61	92	b0	.J	v.	B,	.	W,	..B.
0020	43	e3	03	64	00	17	3a	6c	51	b3	f3	24	d2	af	50	18	21	Q,	..P,		
0030	44	5c	b6	dc	00	00	42										D\,,	B			

Intel(R) PRO/Wireless 2200BG Network Connection (Microsoft's Packet Scheduler) : drive capture in progress> File: C:\DOCUMENTS AND SETTINGS\NOLLA\DESKTOP\PROBLEMS\TELNET.CAP | P: 4660 D: 147 M: 0

Intel(R) PRO/Wireless 2200BG Network Connection (Microsoft's Packet Scheduler) : Capturing - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: tcp.port==443 ▾ Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
118361	2317.3130	192.168.1.101	www.amazon.co.uk	TCP	1619 > https [SYN] Seq=0 Len=0 MSS=1260
118363	2317.3548	www.amazon.co.uk	192.168.1.101	TCP	https > 1619 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1460
118364	2317.3549	192.168.1.101	www.amazon.co.uk	TCP	1619 > https [ACK] Seq=1 Ack=1 Win=17640 Len=0
118365	2317.3552	192.168.1.101	www.amazon.co.uk	TLS	Client Hello
118366	2317.4077	www.amazon.co.uk	192.168.1.101	TLS	Server Hello, Certificate, Server Hello Done
118367	2317.4096	192.168.1.101	www.amazon.co.uk	TLS	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
118368	2317.4551	www.amazon.co.uk	192.168.1.101	TCP	https > 1619 [ACK] Seq=1051 Ack=332 Win=8190 Len=0
118369	2317.4565	www.amazon.co.uk	192.168.1.101	TLS	Change Cipher Spec, Encrypted Handshake Message
118370	2317.4568	192.168.1.101	www.amazon.co.uk	TLS	Application Data
118372	2317.5287	www.amazon.co.uk	192.168.1.101	TCP	https > 1619 [ACK] Seq=1094 Ack=1318 Win=8190 Len=0
118373	2317.5288	192.168.1.101	www.amazon.co.uk	TLS	Application Data, Application Data, Application Data
118376	2317.7929	www.amazon.co.uk	192.168.1.101	TCP	https > 1619 [ACK] Seq=1094 Ack=2049 Win=32768 Len=0
118401	2320.1362	www.amazon.co.uk	192.168.1.101	TCP	[TCP segment of a reassembled PDU]
118402	2320.1420	www.amazon.co.uk	192.168.1.101	TCP	[TCP segment of a reassembled PDU]
118403	2320.1422	192.168.1.101	www.amazon.co.uk	TCP	1619 > https [ACK] Seq=2049 Ack=4014 Win=17640 Len=0
118404	2320.1483	www.amazon.co.uk	192.168.1.101	TCP	[TCP segment of a reassembled PDU]
118405	2320.1495	www.amazon.co.uk	192.168.1.101	TCP	[TCP Previous segment lost] [TCP segment of a reassembled PDU]
118406	2320.1496	192.168.1.101	www.amazon.co.uk	TCP	1619 > https [ACK] Seq=2049 Ack=5474 Win=17640 Len=0
118407	2320.1565	www.amazon.co.uk	192.168.1.101	TCP	[TCP Retransmission] [TCP segment of a reassembled PDU]
118408	2320.1566	192.168.1.101	www.amazon.co.uk	TCP	1619 > https [ACK] Seq=2049 Ack=7457 Win=17640 Len=0
118414	2320.3573	192.168.1.101	e265.1.akamaiedge.	TCP	1620 > https [SYN] Seq=0 Len=0 MSS=1260
118416	2320.3836	e265.1.akamaiedge.	192.168.1.101	TCP	https > 1620 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
118417	2320.3837	192.168.1.101	e265.1.akamaiedge.	TCP	1620 > https [ACK] Seq=1 Ack=1 Win=17640 Len=0
118418	2320.4271	192.168.1.101	e265.1.akamaiedge.	TCP	1621 > https [SYN] Seq=0 Len=0 MSS=1260
118419	2320.4277	192.168.1.101	e265.1.akamaiedge.	TLS	client Hello
118420	2320.4510	e265.1.akamaiedge.	192.168.1.101	TCP	https > 1621 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460

+ Frame 118361 (62 bytes on wire, 62 bytes captured)
+ Ethernet II, Src: IntelCor_34:02:f0 (00:15:00:34:02:f0), Dst: LinksysG_f5:23:d5 (00:0c:41:f5:23:d5)
+ Internet Protocol, Src: 192.168.1.101 (192.168.1.101), Dst: www.amazon.co.uk (87.238.81.129)
+ Transmission Control Protocol, src Port: 1619 (1619), dst Port: https (443), seq: 0, Len: 0
Source port: 1619 (1619)
Destination port: https (443)
Sequence number: 0 (relative sequence number)
Header length: 28 bytes
+ Flags: 0x0002 (SYN)
Window size: 16384
Checksum: 0x7cc7 [correct]
+ Options: (8 bytes)

```
0000 00 0c 41 f5 23 d5 00 15 00 34 02 f0 08 00 45 00 ..A.#....4....E.  

0010 00 30 9e 21 40 00 80 06 f1 29 c0 a8 01 65 57 ee .0.!@....).ew.  

0020 51 81 06 53 01 bb 71 3f e2 55 00 00 00 70 02 Q..S..q? .U....p.  

0030 40 00 7c c7 00 00 02 04 04 ec 01 01 04 02 @.|.....
```

Intel(R) PRO/Wireless 2200BG Network Connection (Microsoft's Packet Scheduler) : <live capture in progress> File: C:\DOCUMENTS\WILLIA\LO... | P: 129764 D: 297 M: 0

Network

HTTPS Example

Network Security

Introduction
Screening Firewalls
NAT
Stateful Firewalls
PIX/ASA Firewall
Proxies
VPN
Tunnelling

