Network Security

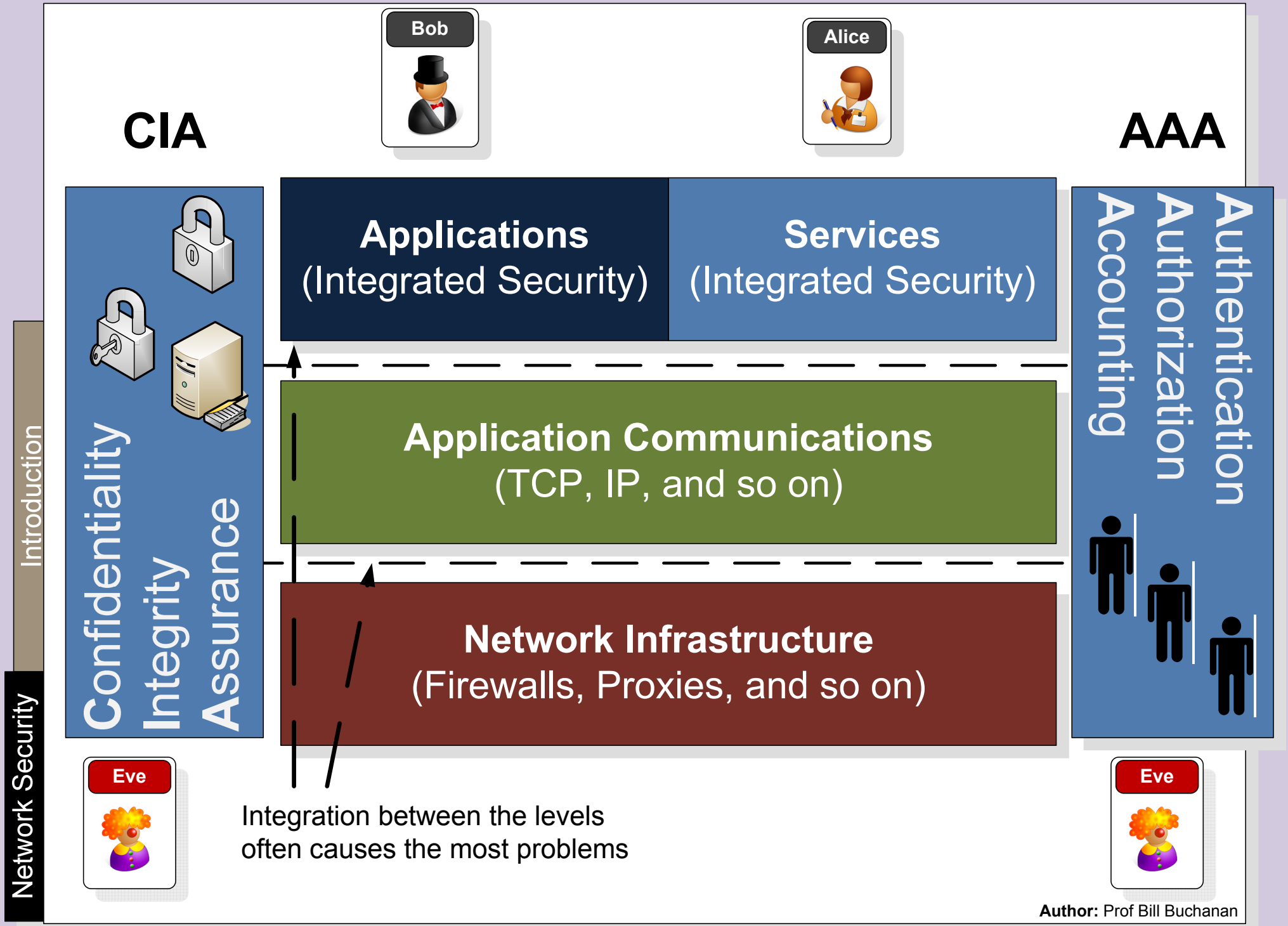
Introduction
Screening Firewalls
NAT
Stateful Firewalls
PIX/ASA Firewall
Proxies
VPN
Tunnelling

Author: Prof Bill Buchanan

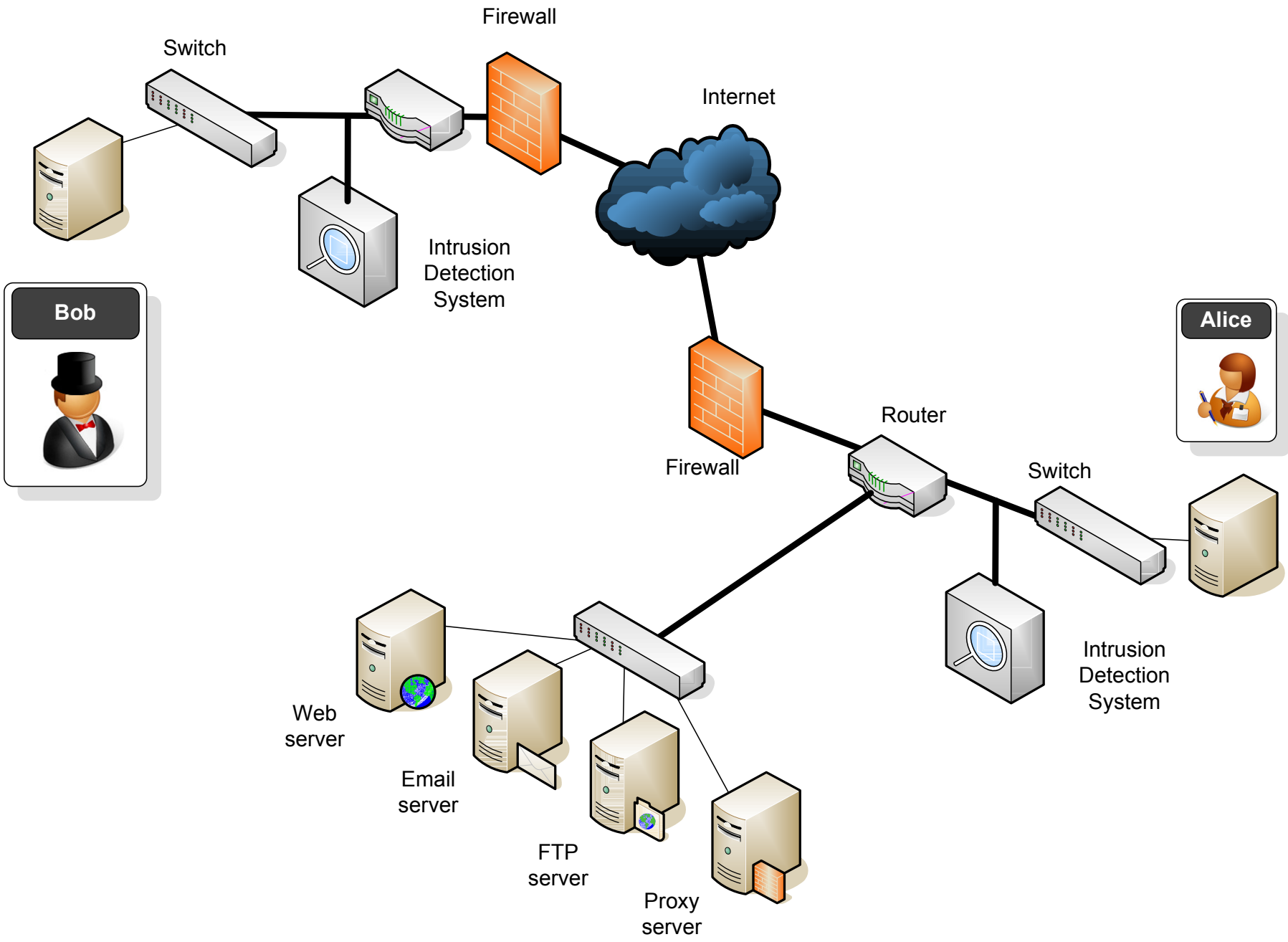
Network Security

Introduction

Author: Prof Bill Buchanan

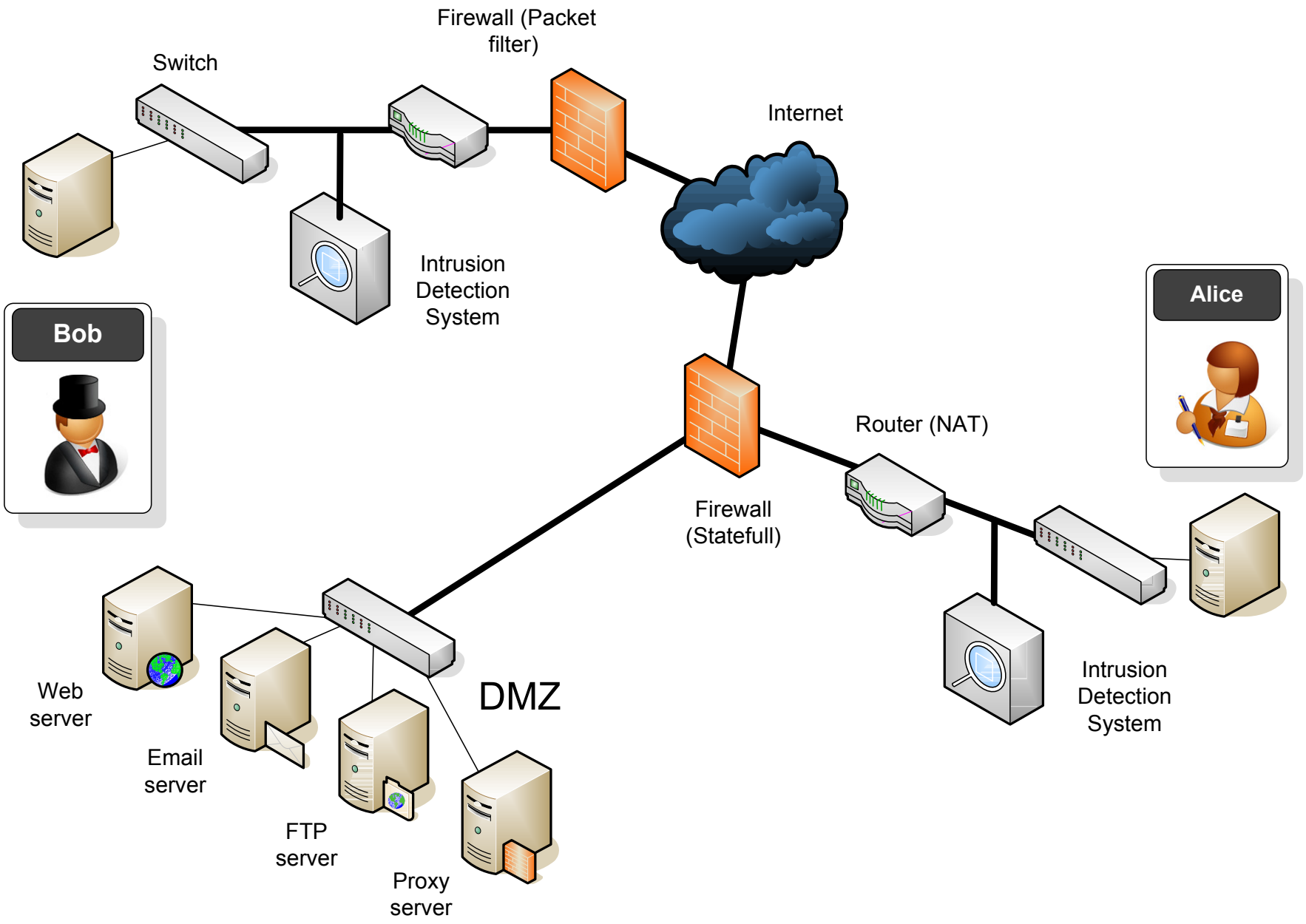

Bob
Alice
CIA
AAA
Applications
(Integrated Security)
Services
(Integrated Security)
Application Communications
(TCP, IP, and so on)
Network Infrastructure
(Firewalls, Proxies, and so on)
Confidentiality
Integrity
Assurance
Authentication
Authorization
Accounting
Eve
Eve
Integration between the levels
often causes the most problems
Author: Prof Bill Buchanan

CIA and AAA



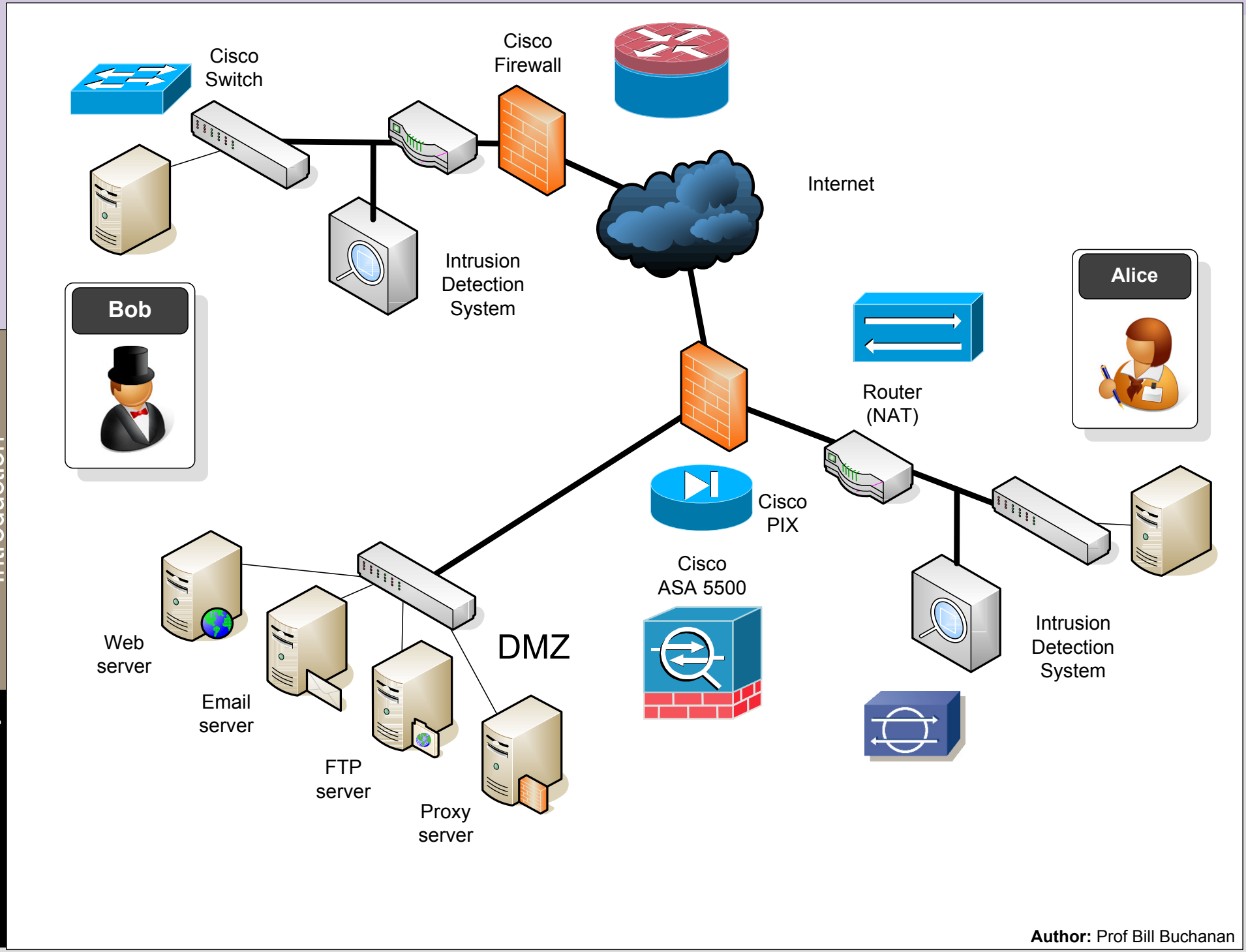
Author: Prof Bill Buchanan

Example Infrastructure



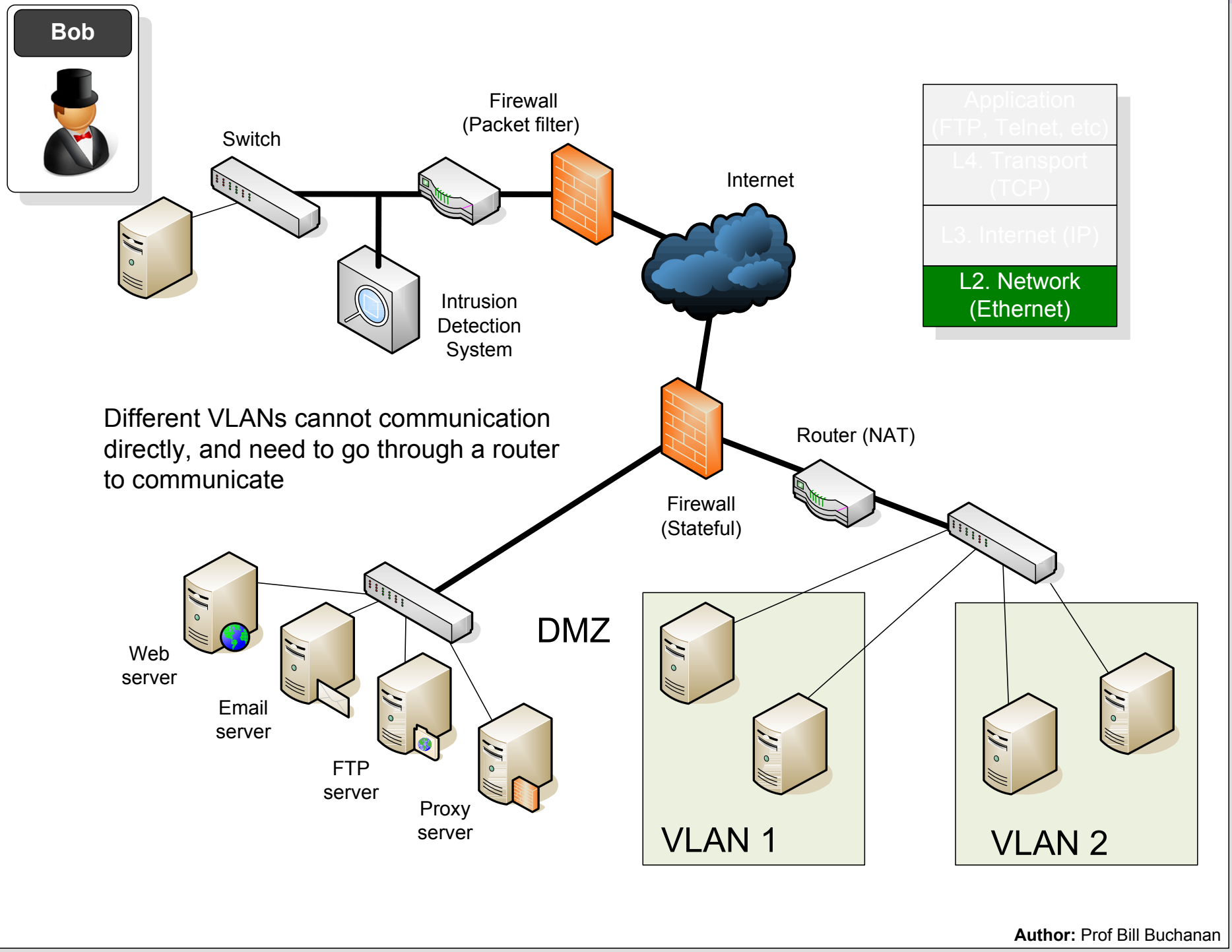
Author: Prof Bill Buchanan

Example Infrastructure



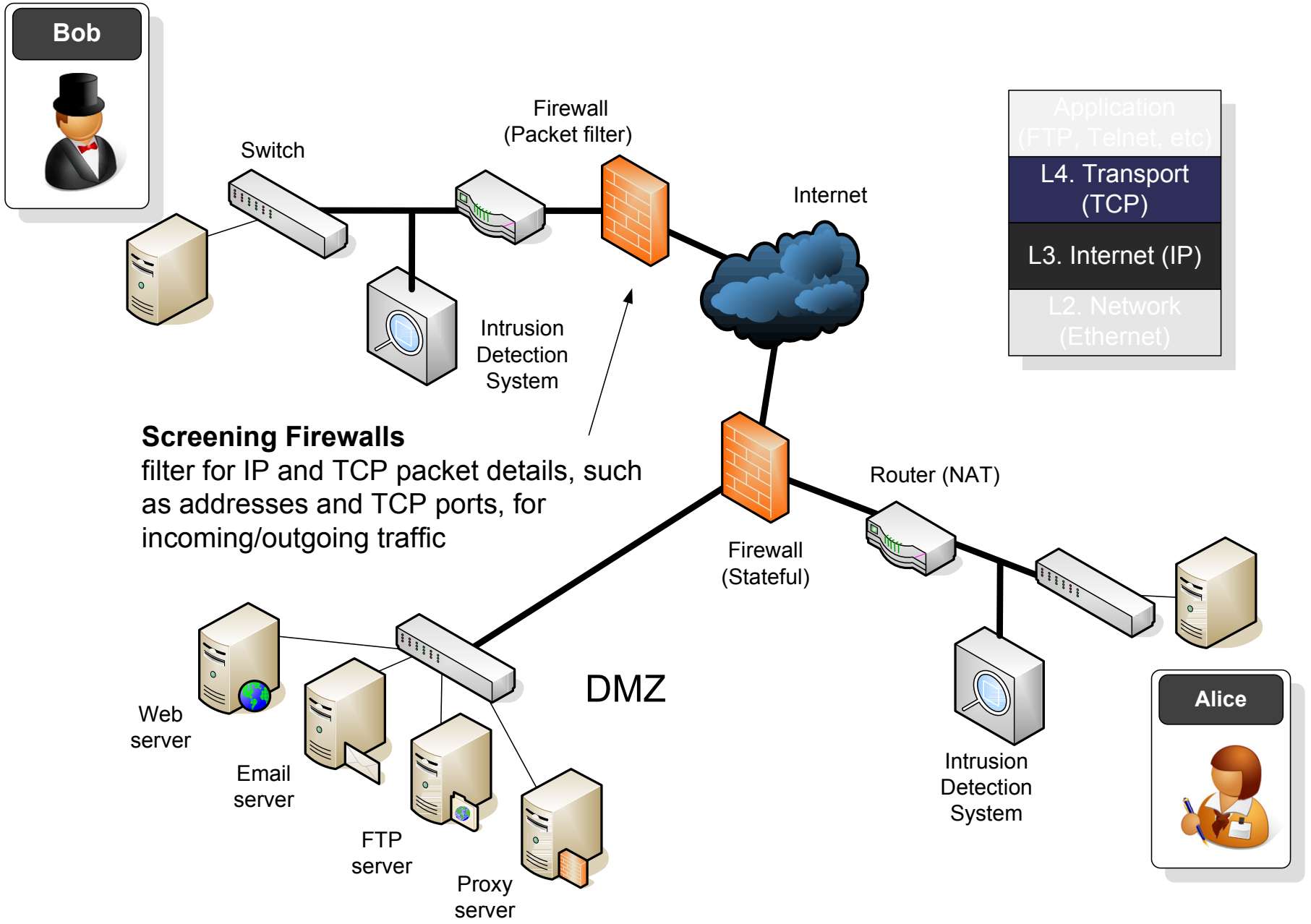
Author: Prof Bill Buchanan

Example Infrastructure

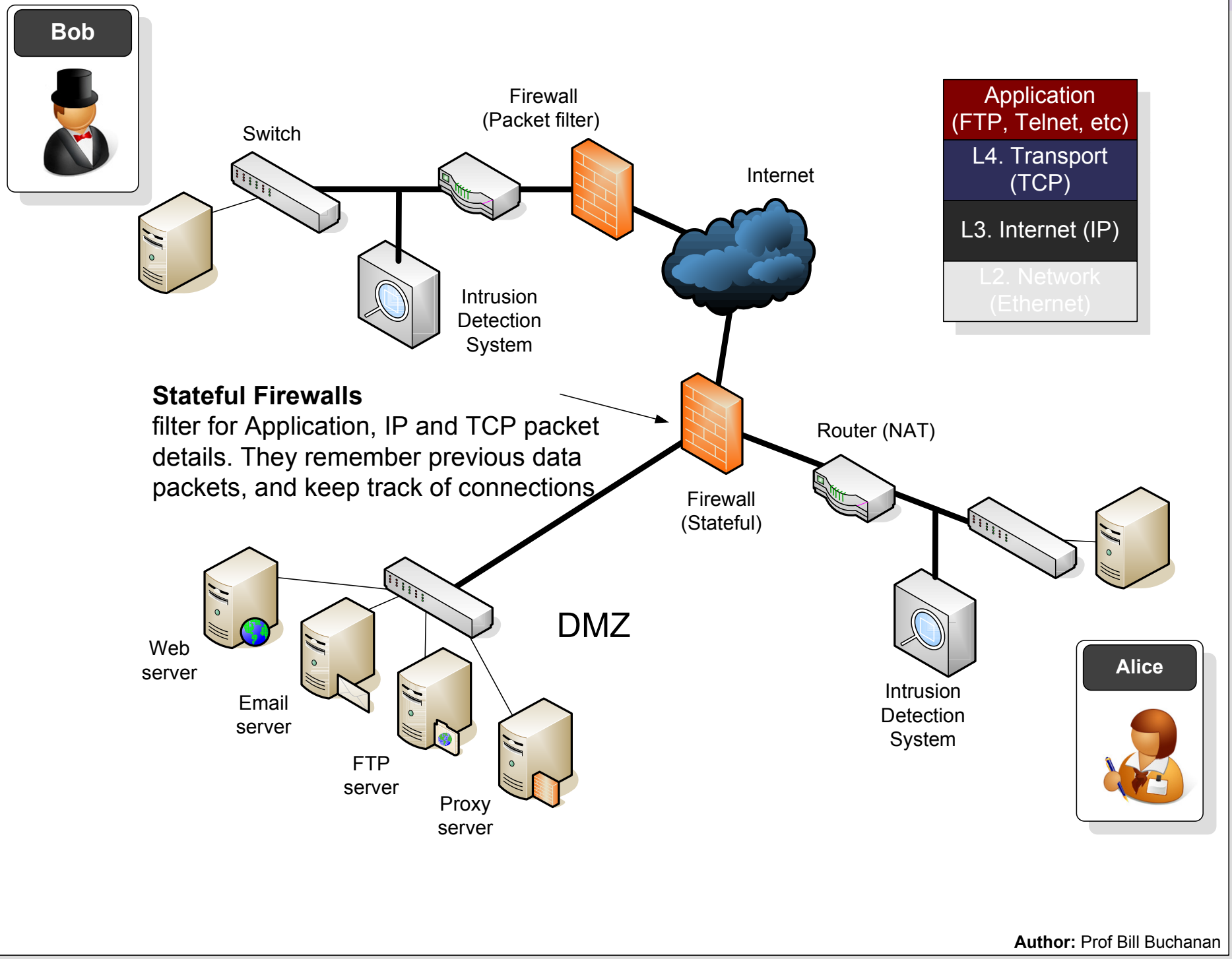


Author: Prof Bill Buchanan

Example Infrastructure

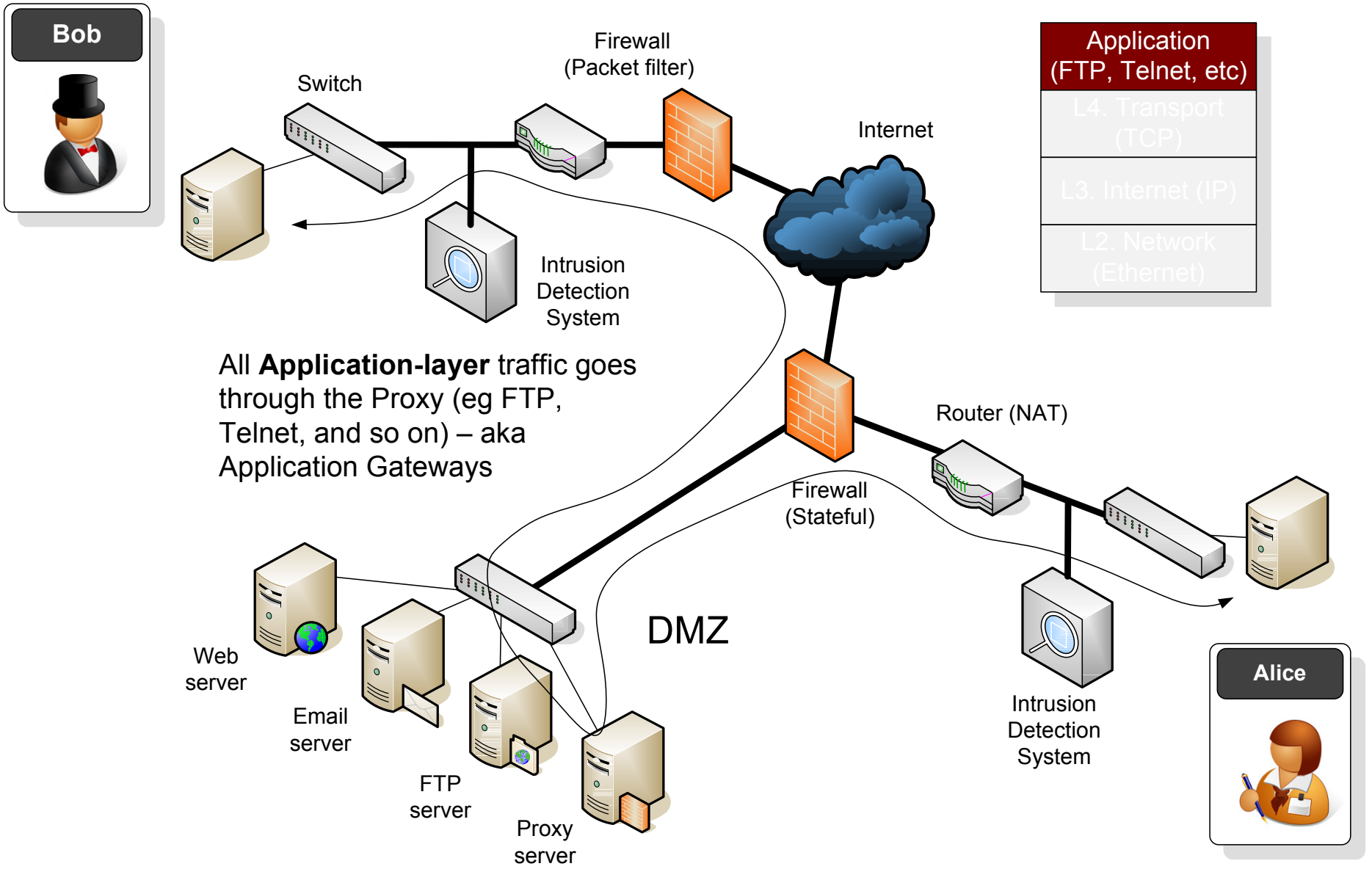


Author: Prof Bill Buchanan



Author: Prof Bill Buchanan

Example Infrastructure



Author: Prof Bill Buchanan

Example Infrastructure

Network Security

Screening Firewalls

Author: Prof Bill Buchanan

Software firewall

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet

Host-based: Zone alarm

ZONEALARM
FOR YOUR HOME AND SMALL BUSINESS

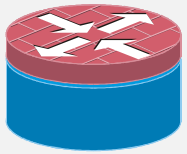
CheckPoint firewall (software)

Runs within: Windows Server, VMWare LINUX

CheckPoint firewall (dedicated) Nokia

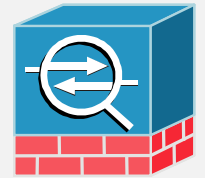
LINUX iptables

Hardware firewall



Cisco router With firewall (non-stateful)

Cisco PIX/ASA (stateful)



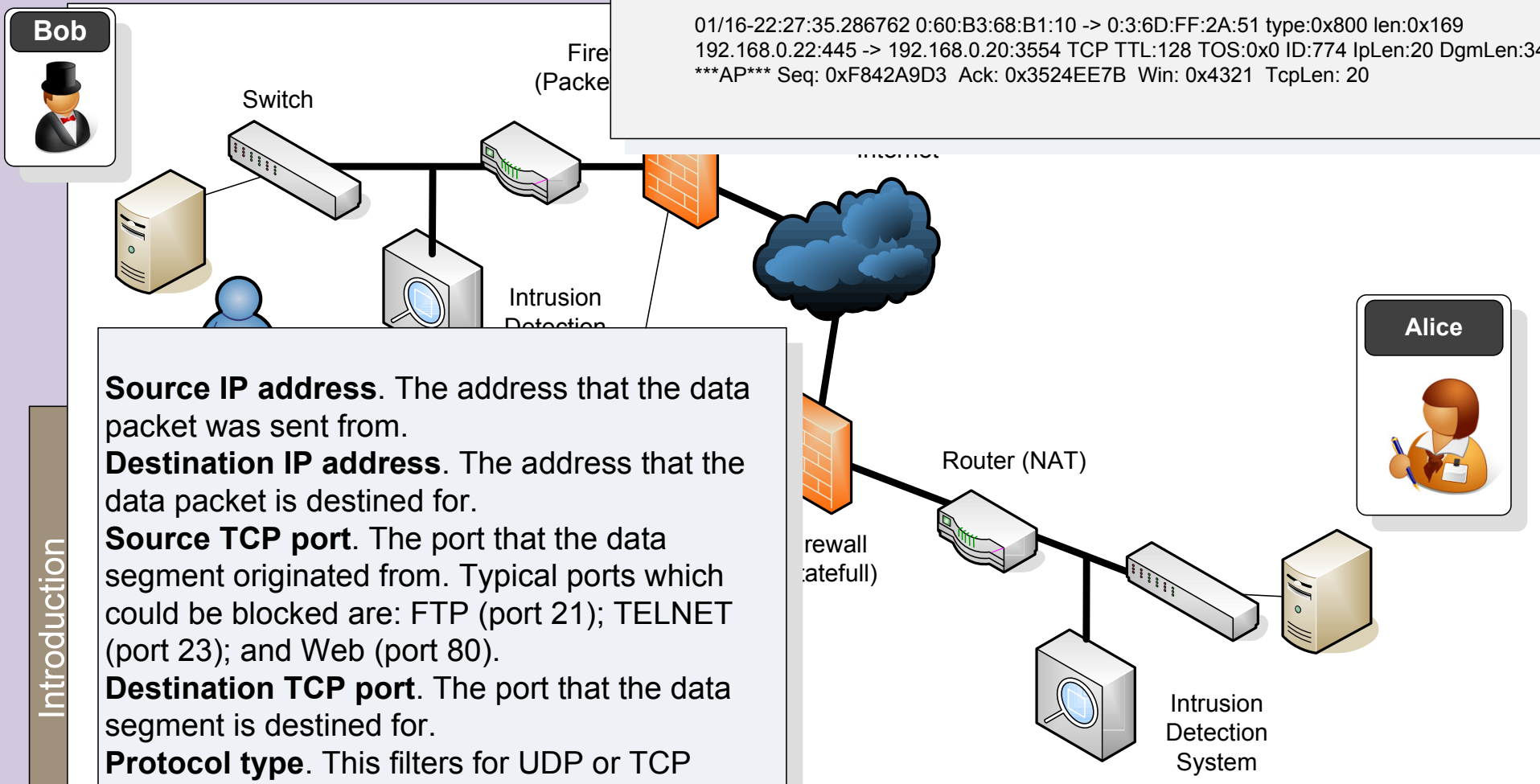
Software firewall:

- 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

01/16-22:27:35.286762 0:60:B3:68:B1:10 -> 0:3:6D:FF:2A:51 type:0x800 len:0x169
192.168.0.22:445 -> 192.168.0.20:3554 TCP TTL:128 TOS:0x0 ID:774 IpLen:20 DgmLen:347 DF
AP Seq: 0xF842A9D3 Ack: 0x3524EE7B Win: 0x4321 TcpLen: 20



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.

IP header

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		

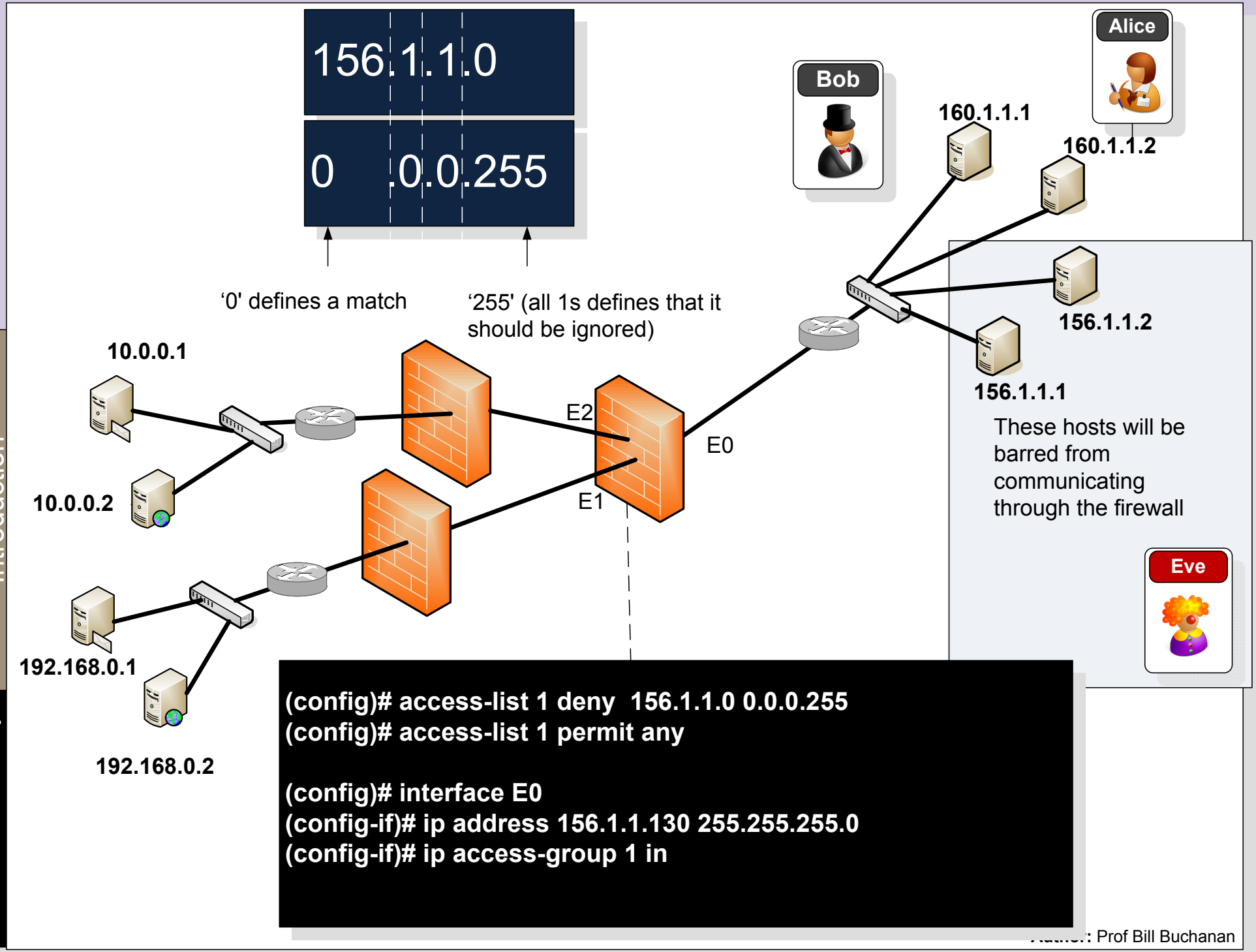
TCP header

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

Ethernet frame

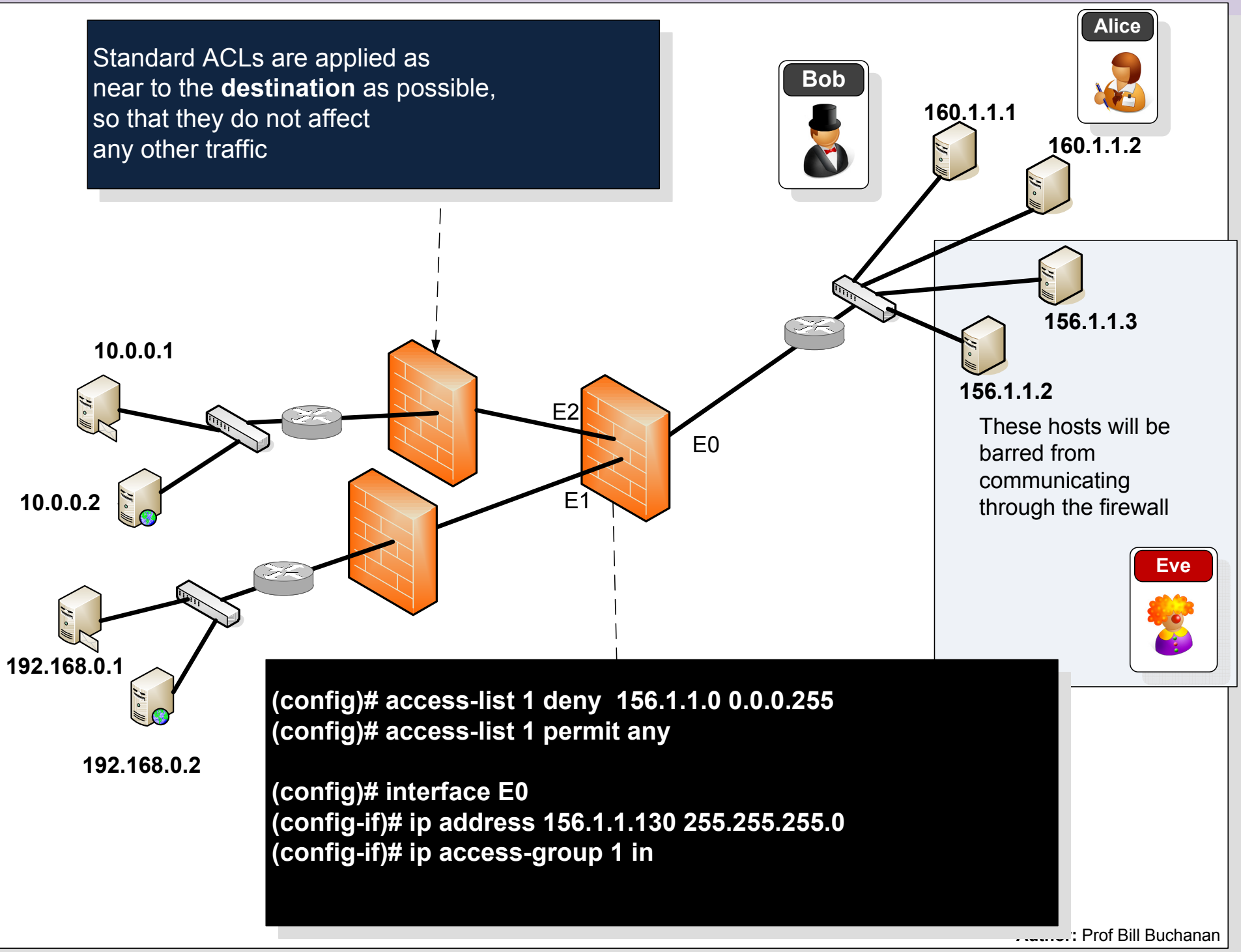
	Src MAC address	Dest. MAC address	Type	Length	IP header	TCP header	Data	

Author: Prof Bill Buchanan



Author: Prof Bill Buchanan

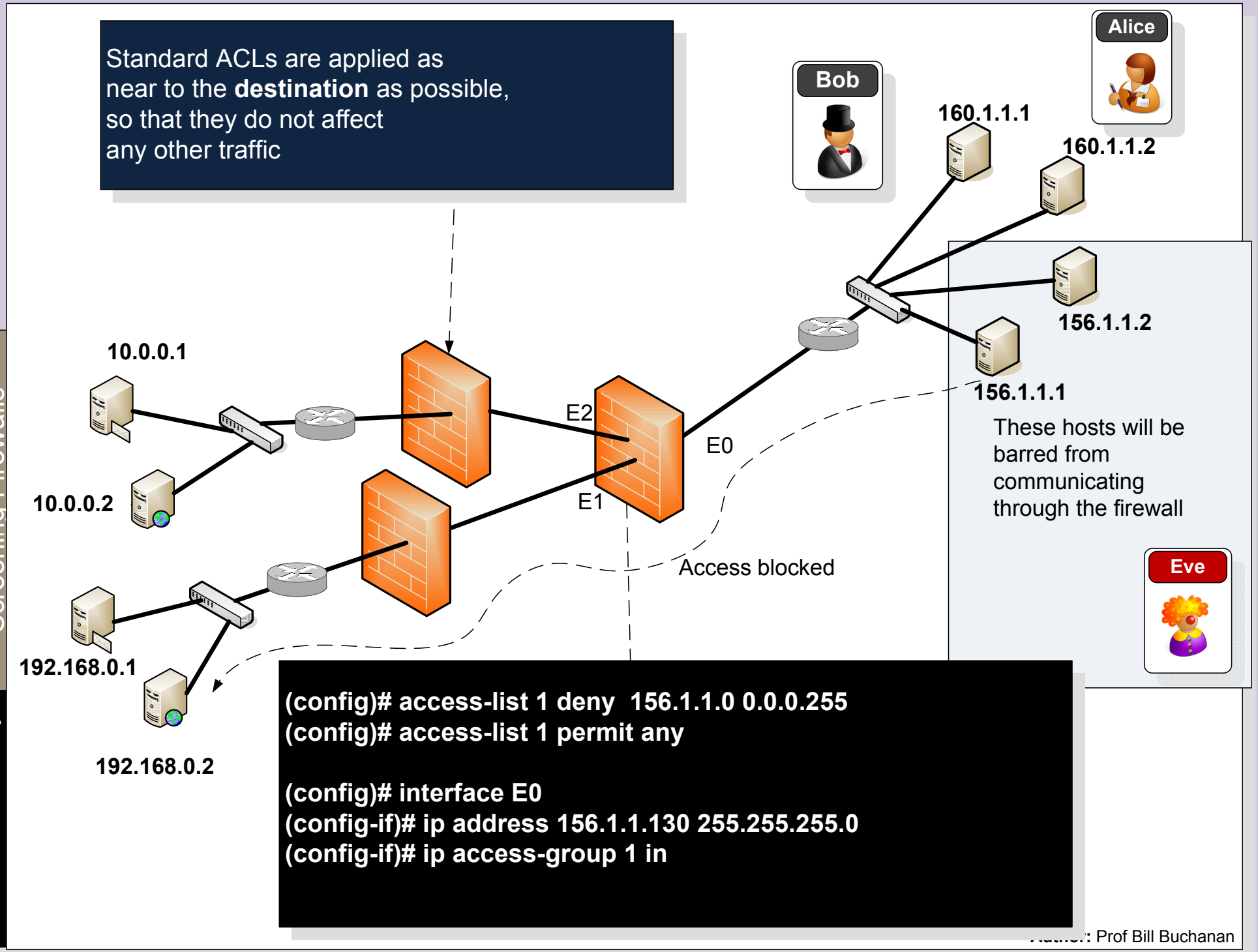
Standard ACLs are applied as near to the **destination** as possible, so that they do not affect any other traffic




```
(config)# access-list 1 deny  156.1.1.0 0.0.0.255
(config)# access-list 1 permit any

(config)# interface E0
(config-if)# ip address 156.1.1.130 255.255.255.0
(config-if)# ip access-group 1 in
```

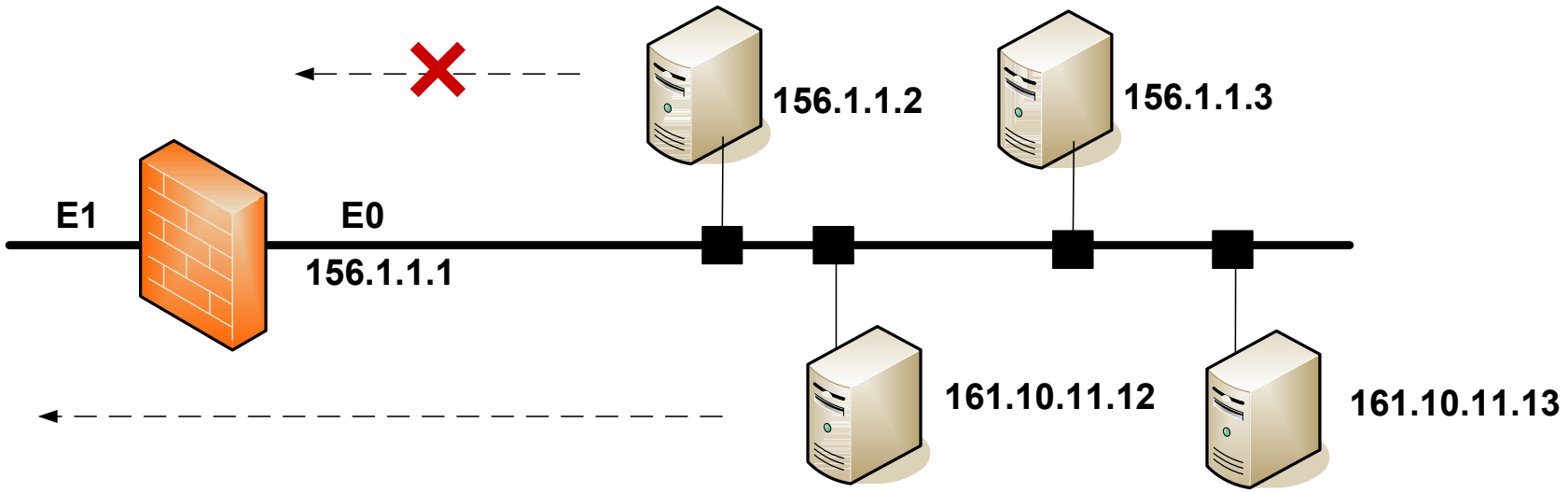
Author: Prof Bill Buchanan

Standard Access-Control List (ACL)



Author: Prof Bill Buchanan

Standard Access-Control List (ACL)




```
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

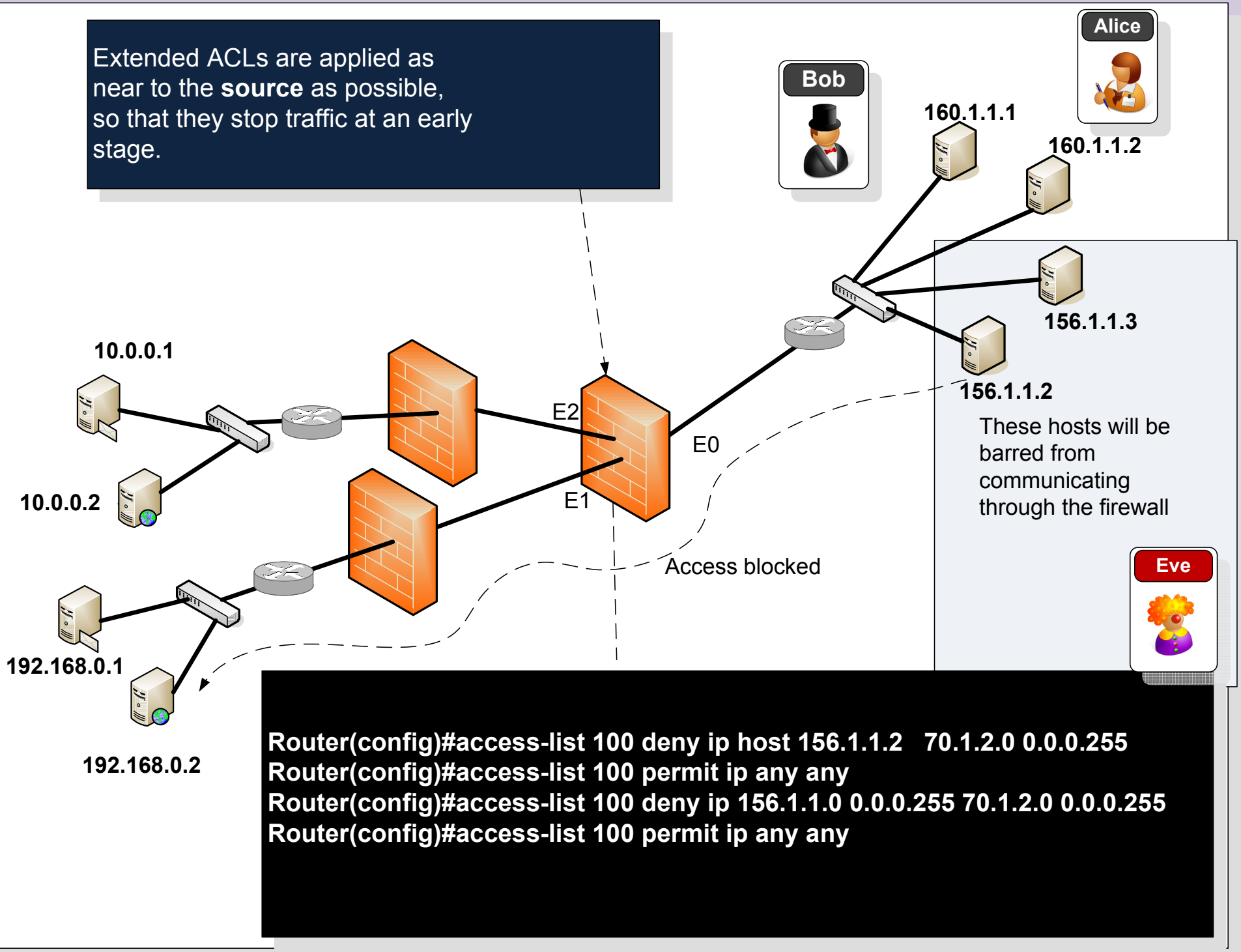
```
Router(config)#access-list 100 deny ip 156.1.1.0 0.0.0.255 70.1.2.0 0.0.0.255
Router(config)#access-list 100 permit ip any any
```

Denies traffic from any host on 156.1.1.0 to the 70.1.2.0 network

Author: Prof Bill Buchanan

Extended ACL – can select a source and destination

Extended ACLs are applied as near to the **source** as possible, so that they stop traffic at an early stage.




```
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
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
```

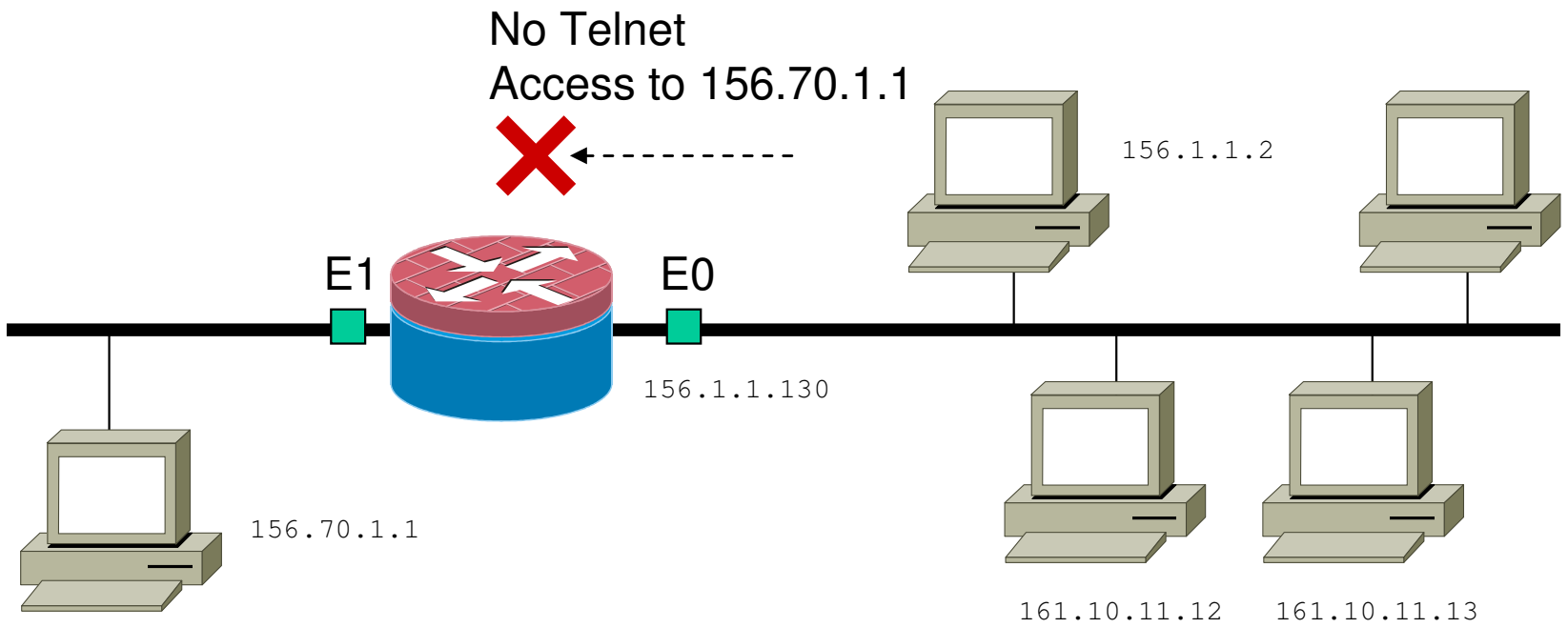
Extended ACL – can select a source and destination

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

Optional field in brackets

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

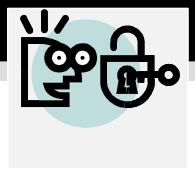
```
access-list 101 deny tcp 156.1.1.0 0.0.0.255 eq any host 156.70.1.1 eq telnet
access-list 101 permit ip any any
```

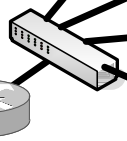


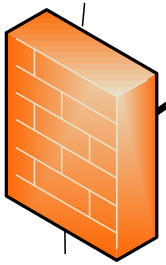
Author: Prof Bill Buchanan

Open firewall

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







E0

These hosts will be barred from communicating through the firewall

Closed firewall

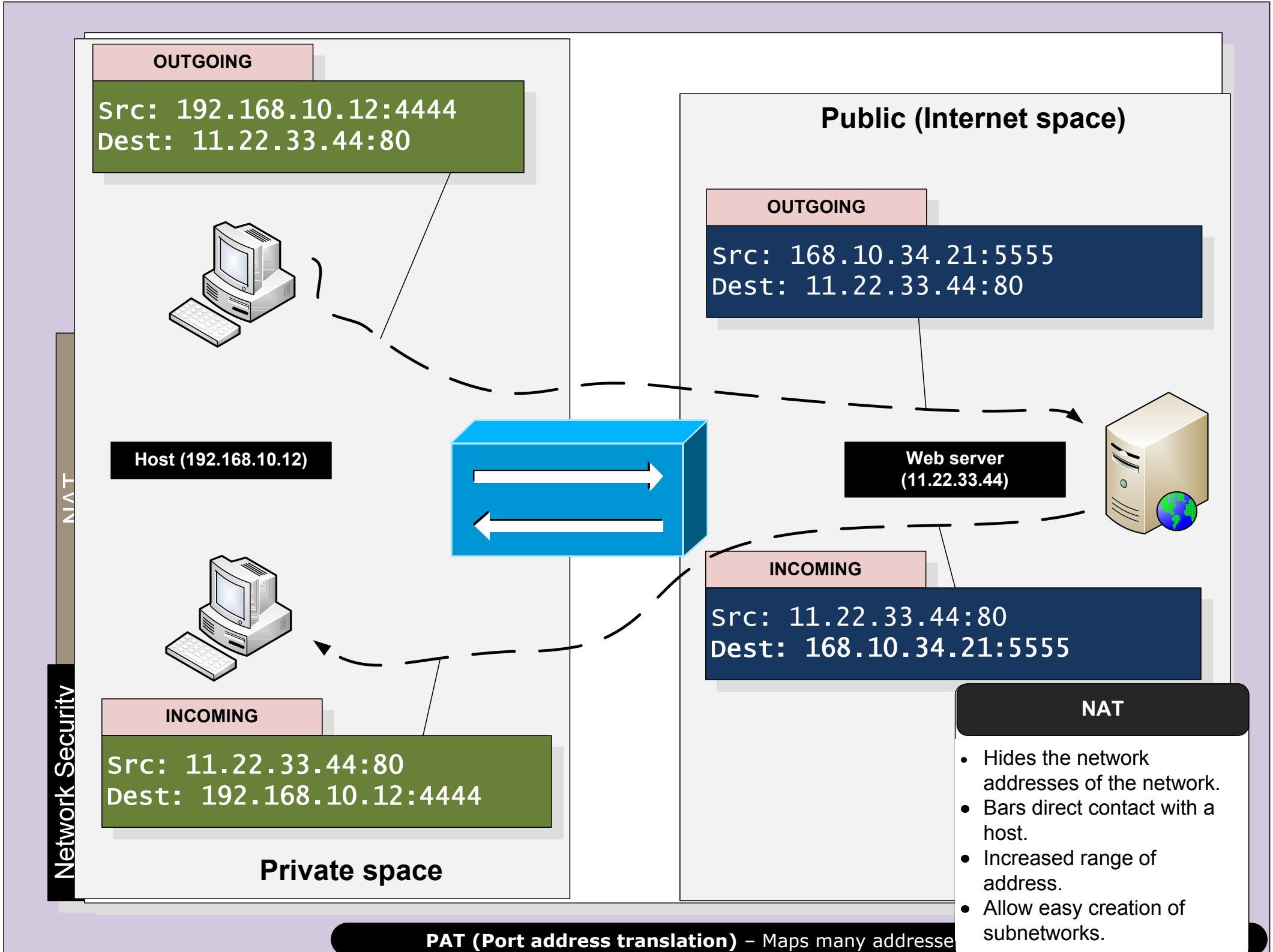
```
Router(config)# access-list 100 permit ...
Router(config)# access-list 100 deny ip any any
```

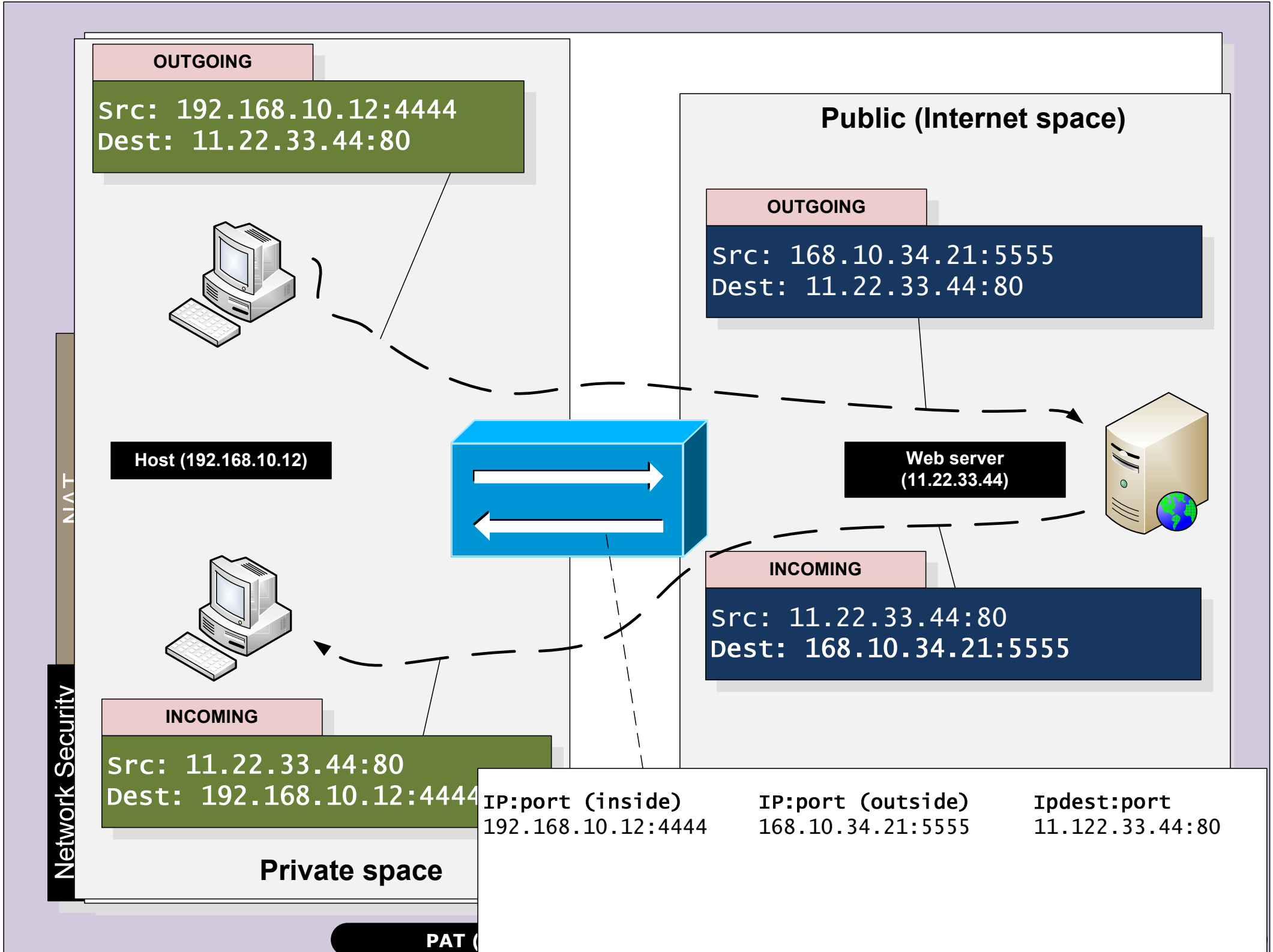
Author: Prof Bill Buchanan

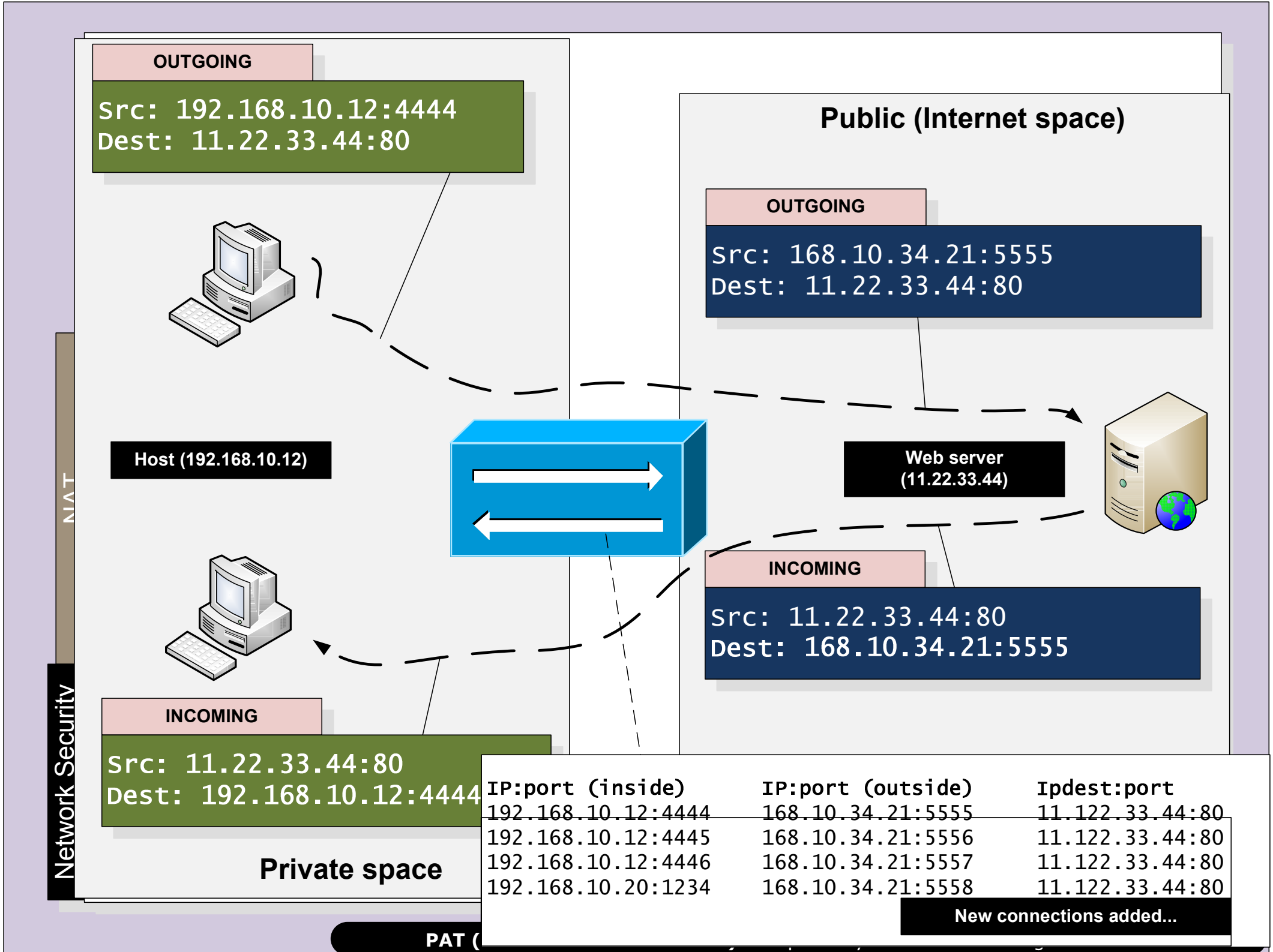
Network Security

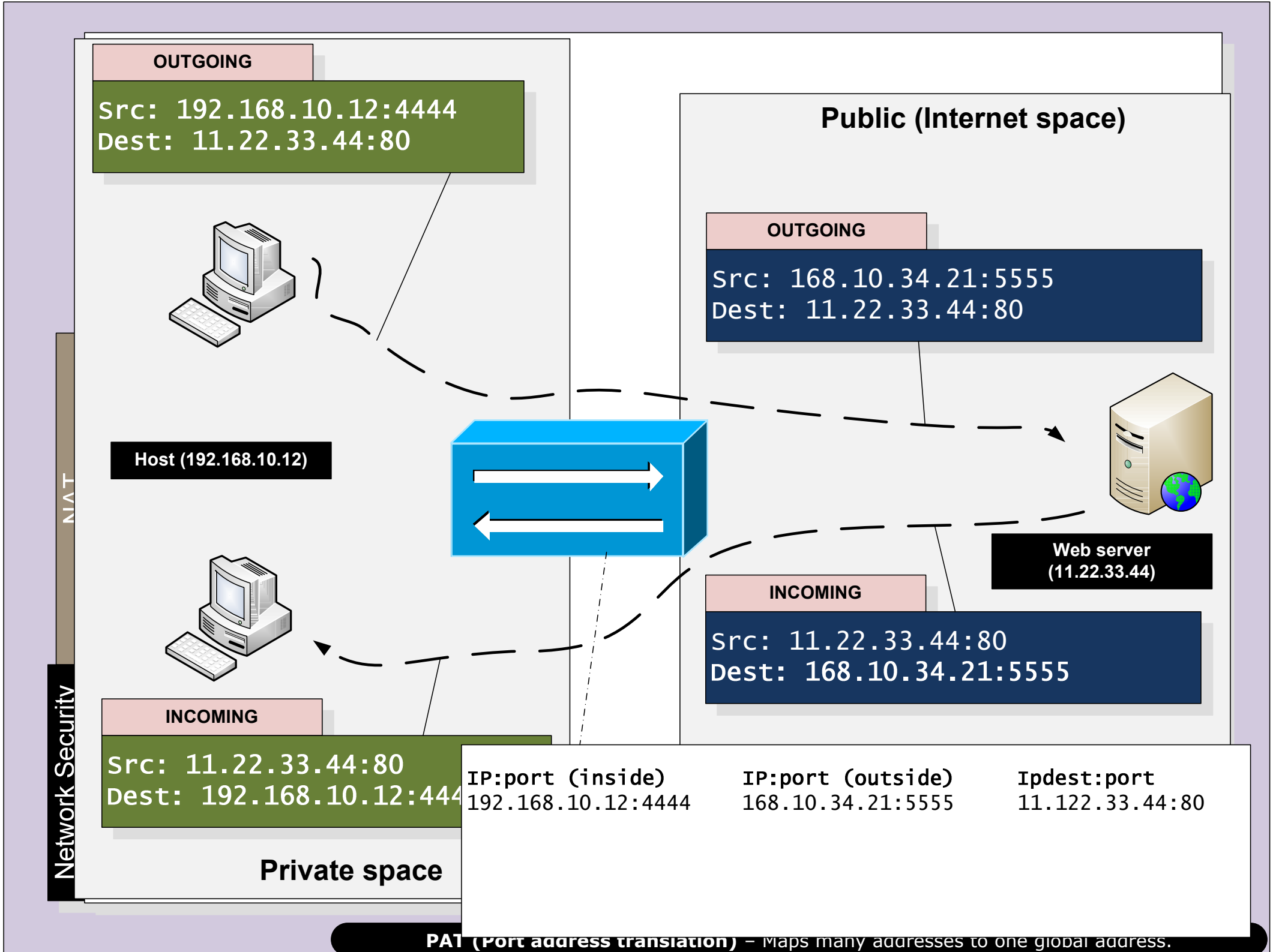
NAT

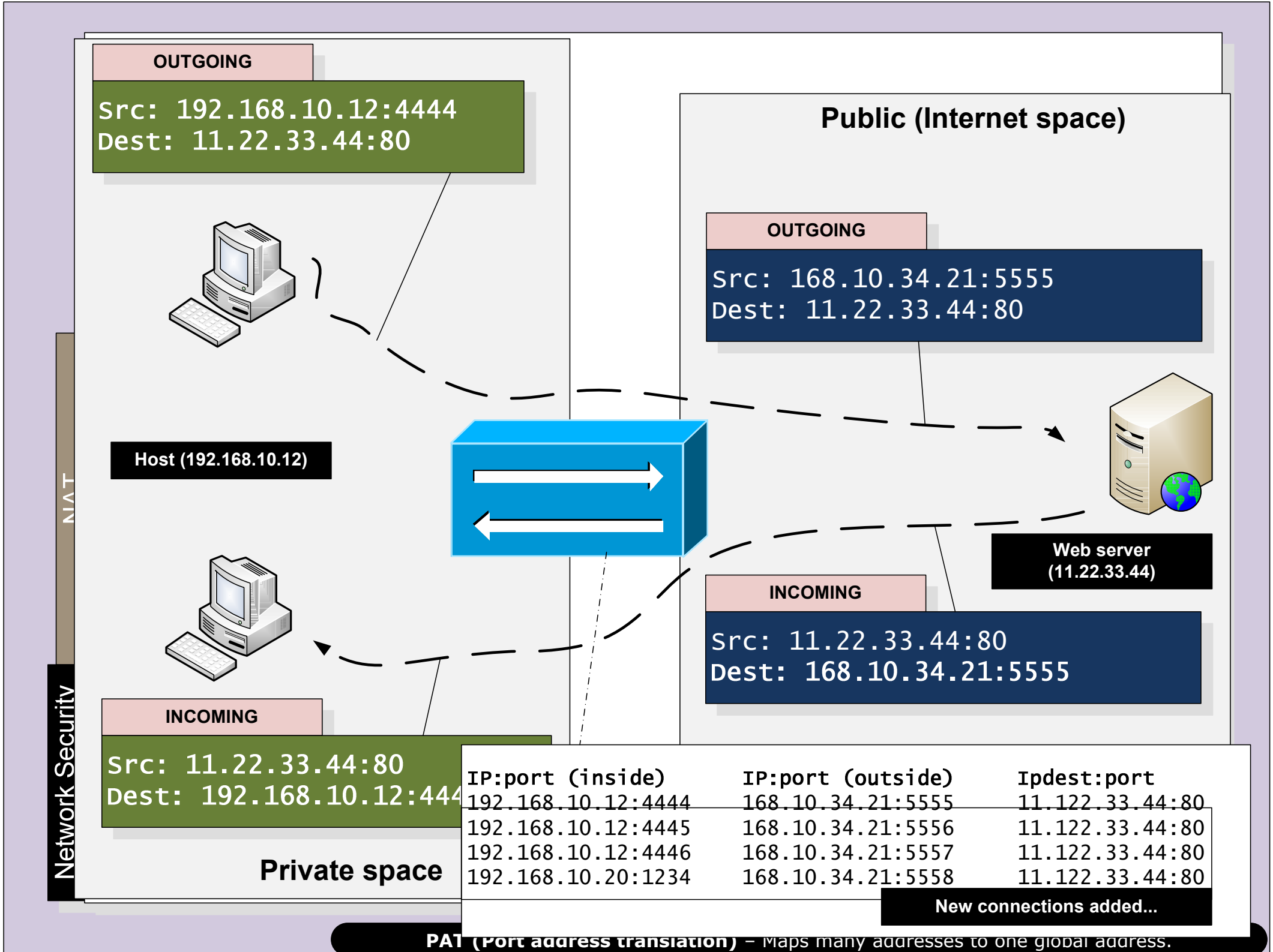
Author: Prof Bill Buchanan


OUTGOING
Src: 192.168.10.12:4444
Dest: 11.22.33.44:80
Public (Internet space)
OUTGOING
Src: 168.10.34.21:5555
Dest: 11.22.33.44:80
Host (192.168.10.12)
Web server
(11.22.33.44)
INCOMING
Src: 11.22.33.44:80
Dest: 168.10.34.21:5555
NAT
Network Security
INCOMING
Src: 11.22.33.44:80
Dest: 192.168.10.12:4444
Private space
NAT
Hides the network addresses of the network.
Bars direct contact with a host.
Increased range of address.
Allow easy creation of subnetworks.
PAT (Port address translation) – Maps many addresse

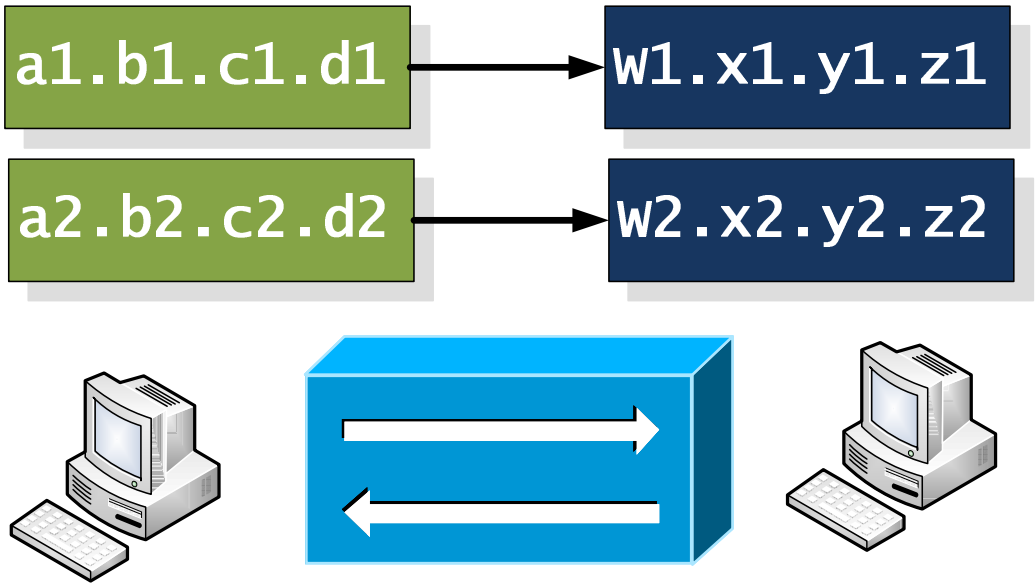

OUTGOING
Src: 192.168.10.12:4444
Dest: 11.22.33.44:80
Public (Internet space)
OUTGOING
Src: 168.10.34.21:5555
Dest: 11.22.33.44:80
Host (192.168.10.12)
Web server
(11.22.33.44)
INCOMING
Src: 11.22.33.44:80
Dest: 168.10.34.21:5555
NAT
Network Security
INCOMING
Src: 11.22.33.44:80
Dest: 192.168.10.12:4444
Private space
IP:port (inside)
192.168.10.12:4444
IP:port (outside)
168.10.34.21:5555
Ipdest:port
11.122.33.44:80
PAT (


OUTGOING
Src: 192.168.10.12:4444
Dest: 11.22.33.44:80
Public (Internet space)
OUTGOING
Src: 168.10.34.21:5555
Dest: 11.22.33.44:80
Host (192.168.10.12)
Web server
(11.22.33.44)
INCOMING
Src: 11.22.33.44:80
Dest: 168.10.34.21:5555
NAT
Network Security
INCOMING
Src: 11.22.33.44:80
Dest: 192.168.10.12:4444
Private space
IP:port (inside) IP:port (outside) Ipdest:port
192.168.10.12:4444 168.10.34.21:5555 11.122.33.44:80
192.168.10.12:4445 168.10.34.21:5556 11.122.33.44:80
192.168.10.12:4446 168.10.34.21:5557 11.122.33.44:80
192.168.10.20:1234 168.10.34.21:5558 11.122.33.44:80
New connections added...
PAT (

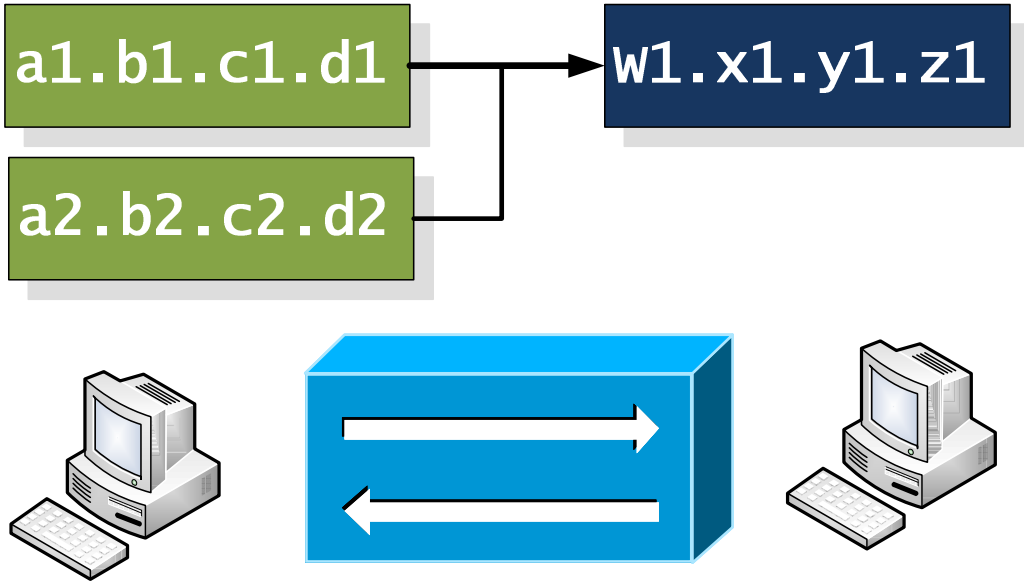

OUTGOING
Src: 192.168.10.12:4444
Dest: 11.22.33.44:80
Public (Internet space)
OUTGOING
Src: 168.10.34.21:5555
Dest: 11.22.33.44:80
Host (192.168.10.12)
Web server
(11.22.33.44)
INCOMING
Src: 11.22.33.44:80
Dest: 168.10.34.21:5555
NAT
Network Security
INCOMING
Src: 11.22.33.44:80
Dest: 192.168.10.12:444
Private space
IP:port (inside)
192.168.10.12:4444
IP:port (outside)
168.10.34.21:5555
Ipdest:port
11.122.33.44:80
PAT (Port address translation) – Maps many addresses to one global address.


OUTGOING
Src: 192.168.10.12:4444
Dest: 11.22.33.44:80
Public (Internet space)
OUTGOING
Src: 168.10.34.21:5555
Dest: 11.22.33.44:80
Host (192.168.10.12)
Web server
(11.22.33.44)
INCOMING
Src: 11.22.33.44:80
Dest: 168.10.34.21:5555
NAT
Network Security
INCOMING
Src: 11.22.33.44:80
Dest: 192.168.10.12:444
Private space
IP:port (inside) IP:port (outside) Ipdest:port
192.168.10.12:4444 168.10.34.21:5555 11.122.33.44:80
192.168.10.12:4445 168.10.34.21:5556 11.122.33.44:80
192.168.10.12:4446 168.10.34.21:5557 11.122.33.44:80
192.168.10.20:1234 168.10.34.21:5558 11.122.33.44:80
New connections added...
PAT (Port address translation) – Maps many addresses to one global address.

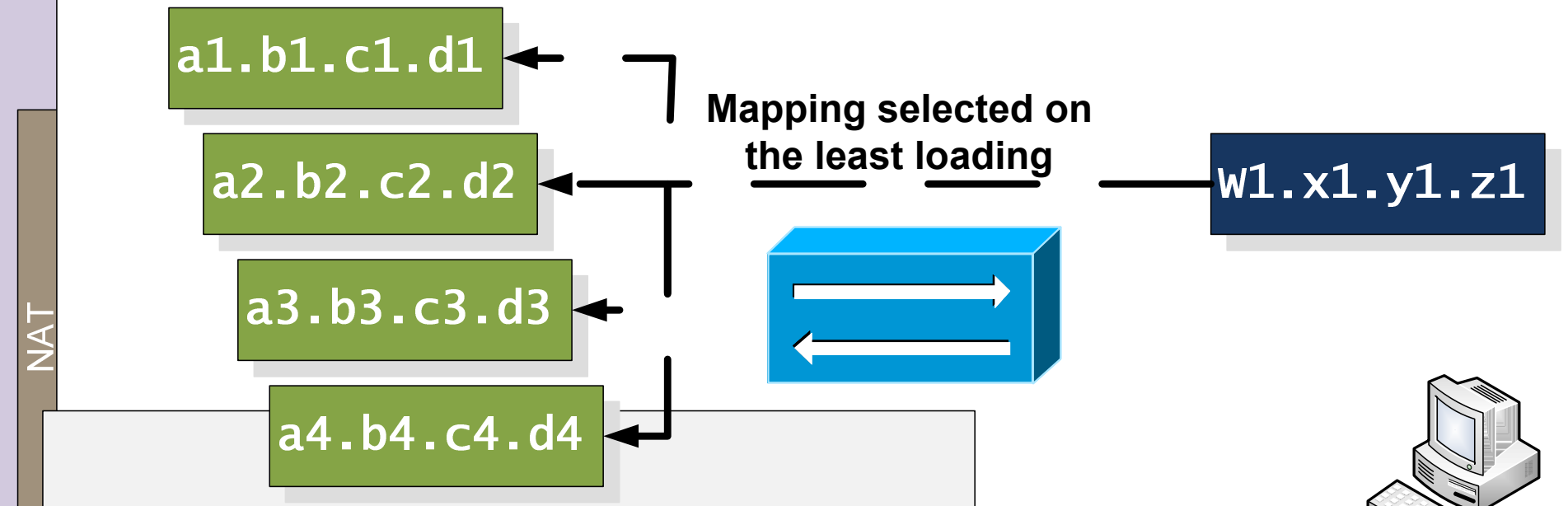
Static translation.
Each public IP address translates to a private one through a static table.
Good for security/logging/traceability.
Bad, as it does not hide the internal network.



IP Masquerading (Dynamic Translation).
A single public IP address is used for the whole network. The table is thus dynamic.

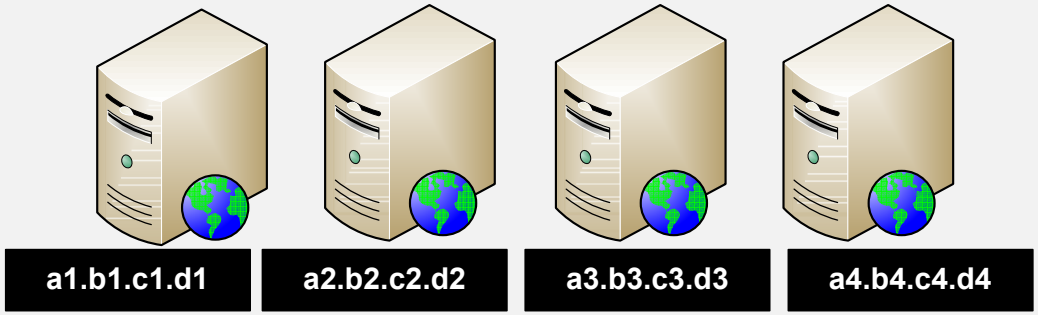


Load Balancing Translation.
With this, a request is made to a resource, such as to a WWW server, the NAT device then looks at the current loading of the systems, and forwards the request to the one which is most lightly used…



NAT

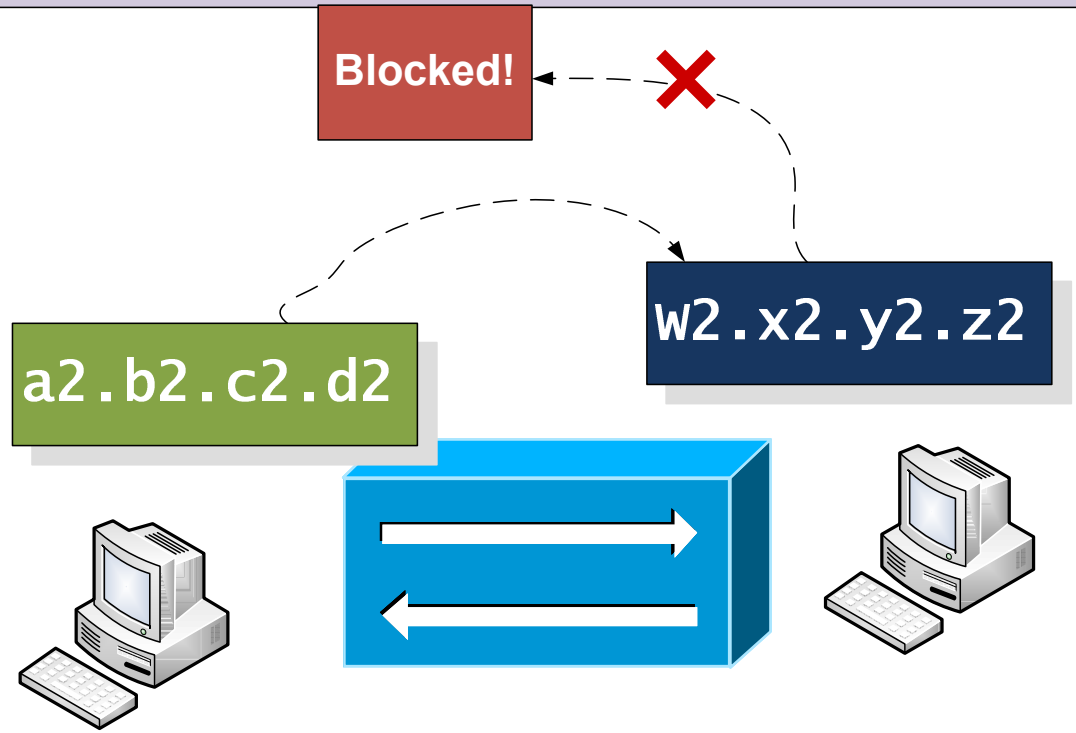
Network Security

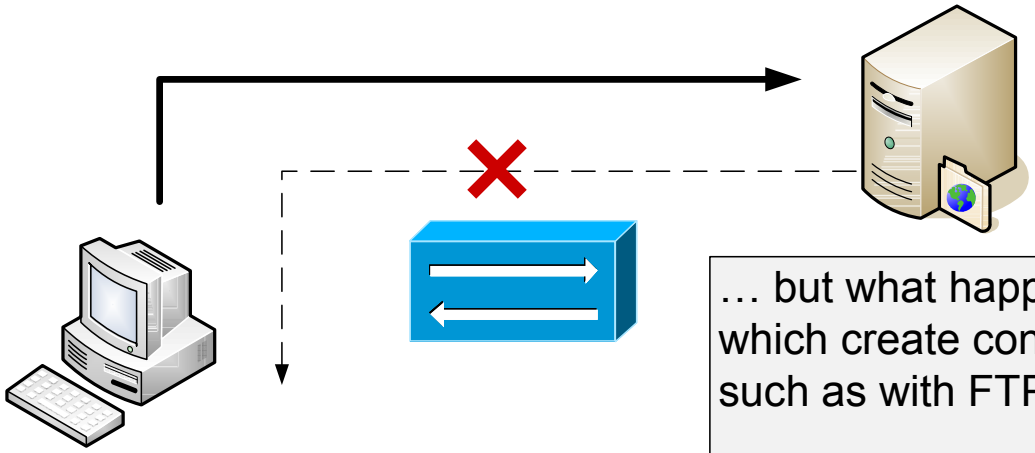


Server farm

NAT (Load balancing)

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

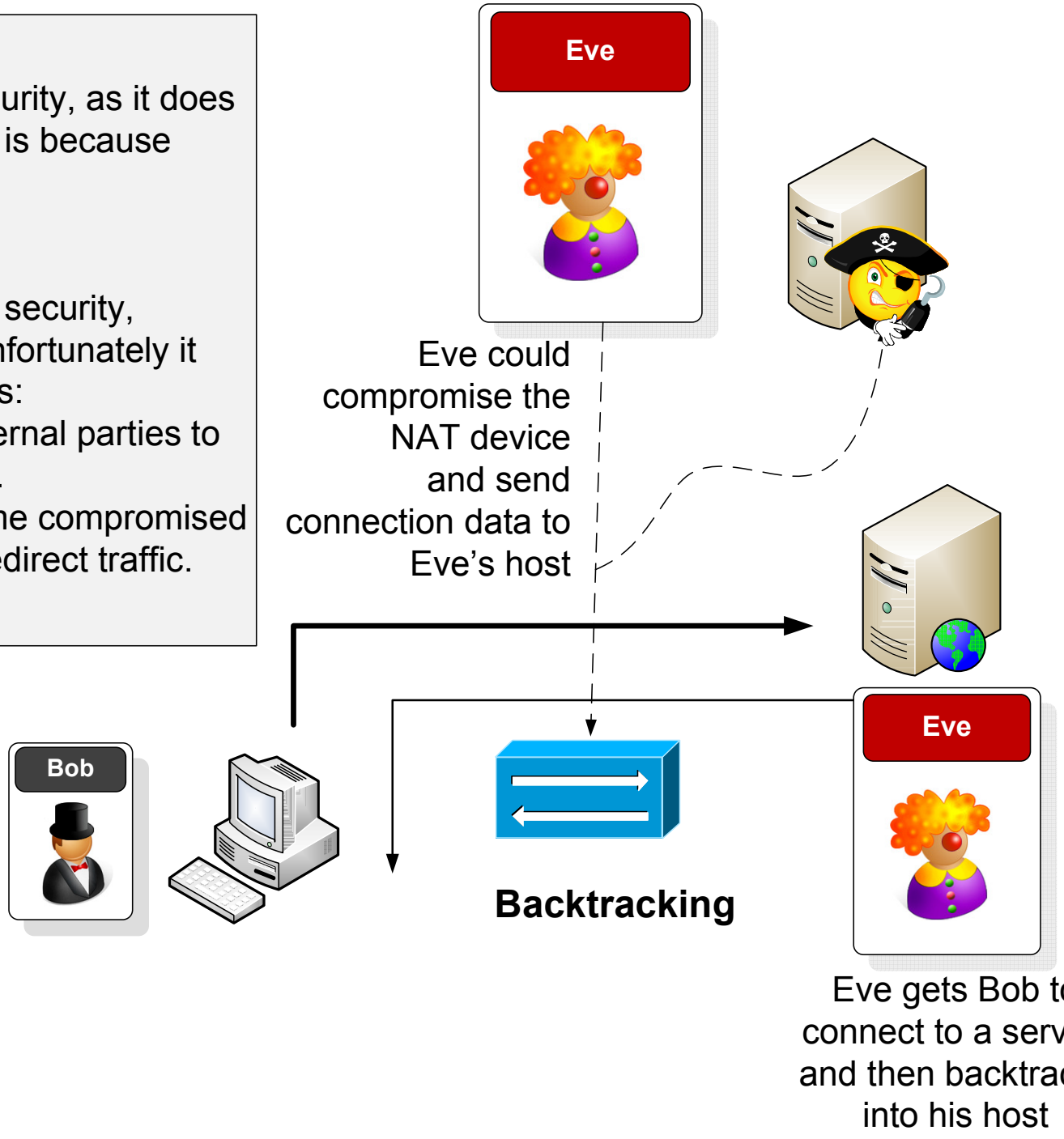
… but what happens if we use applications which create connections in the reverse direction, such as with FTP and IRC?

.. 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.

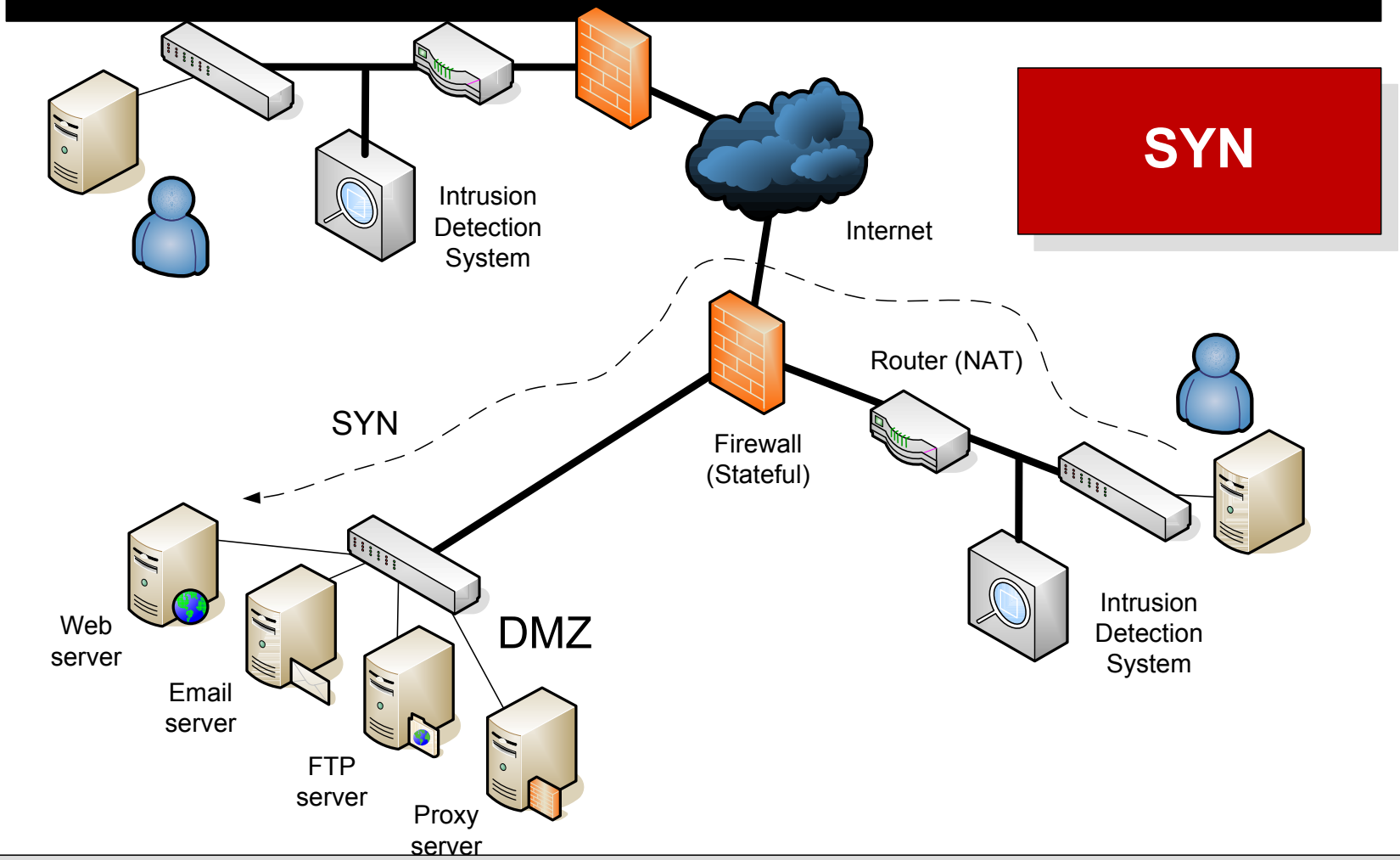


Network Security

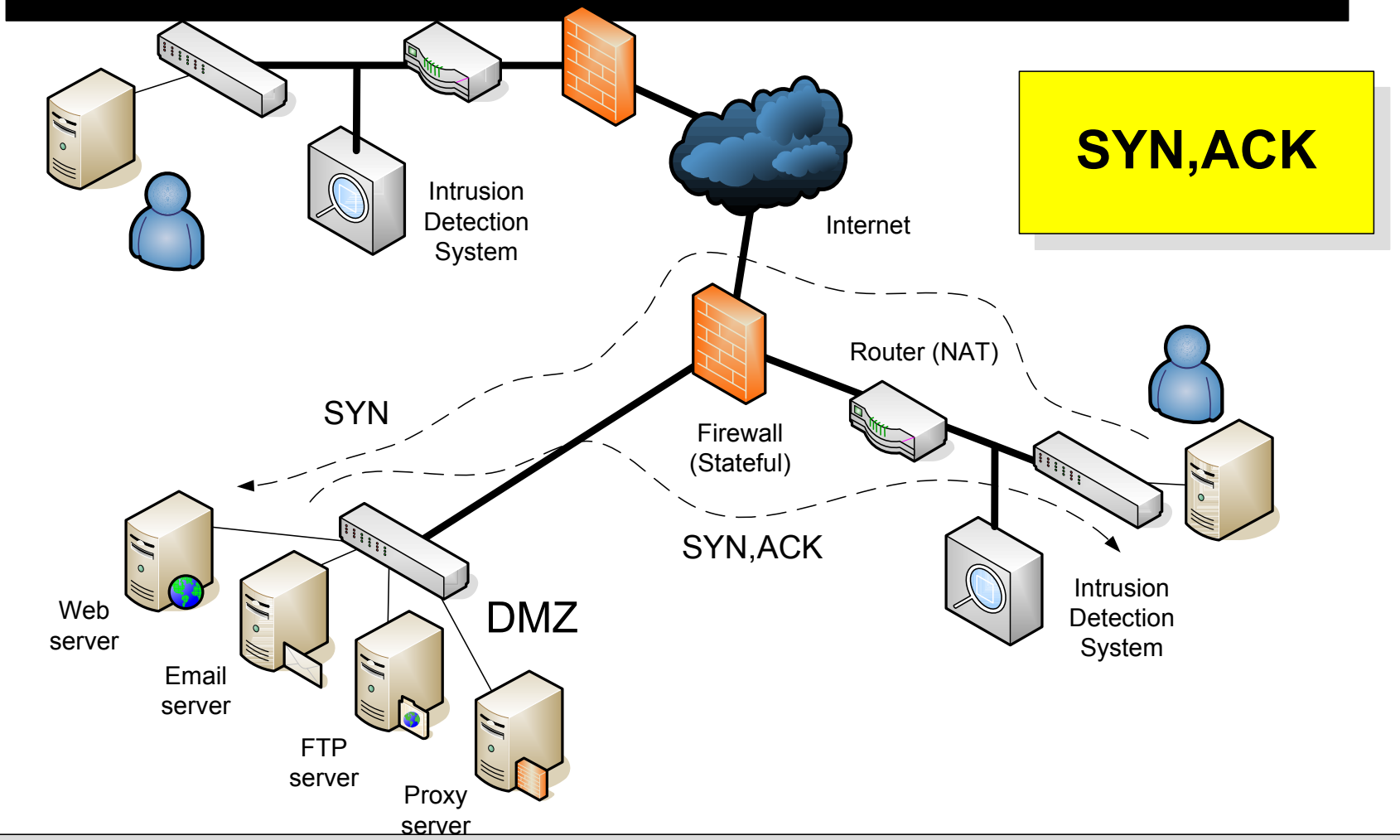
Stateful Firewalls

Author: Prof Bill Buchanan

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

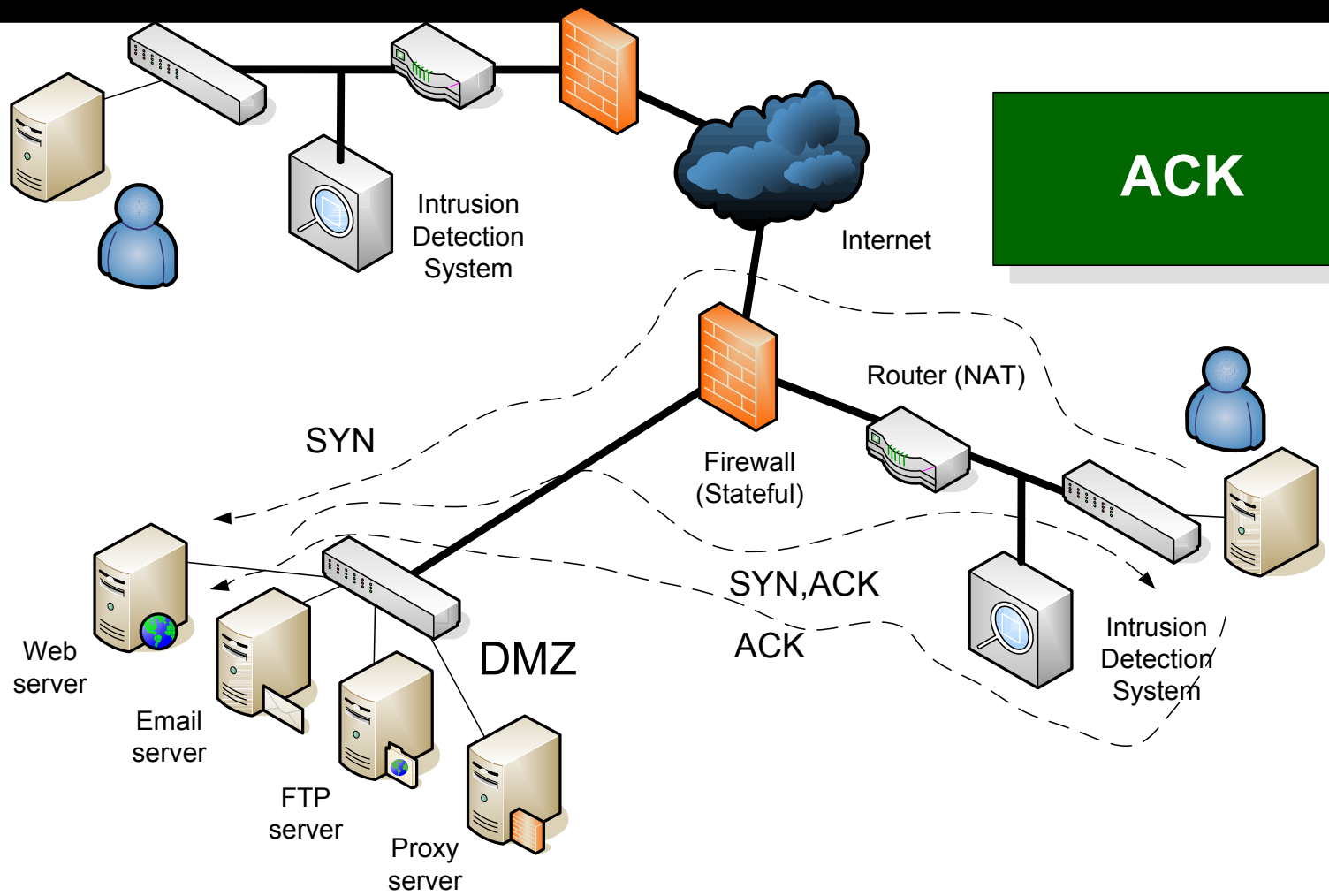


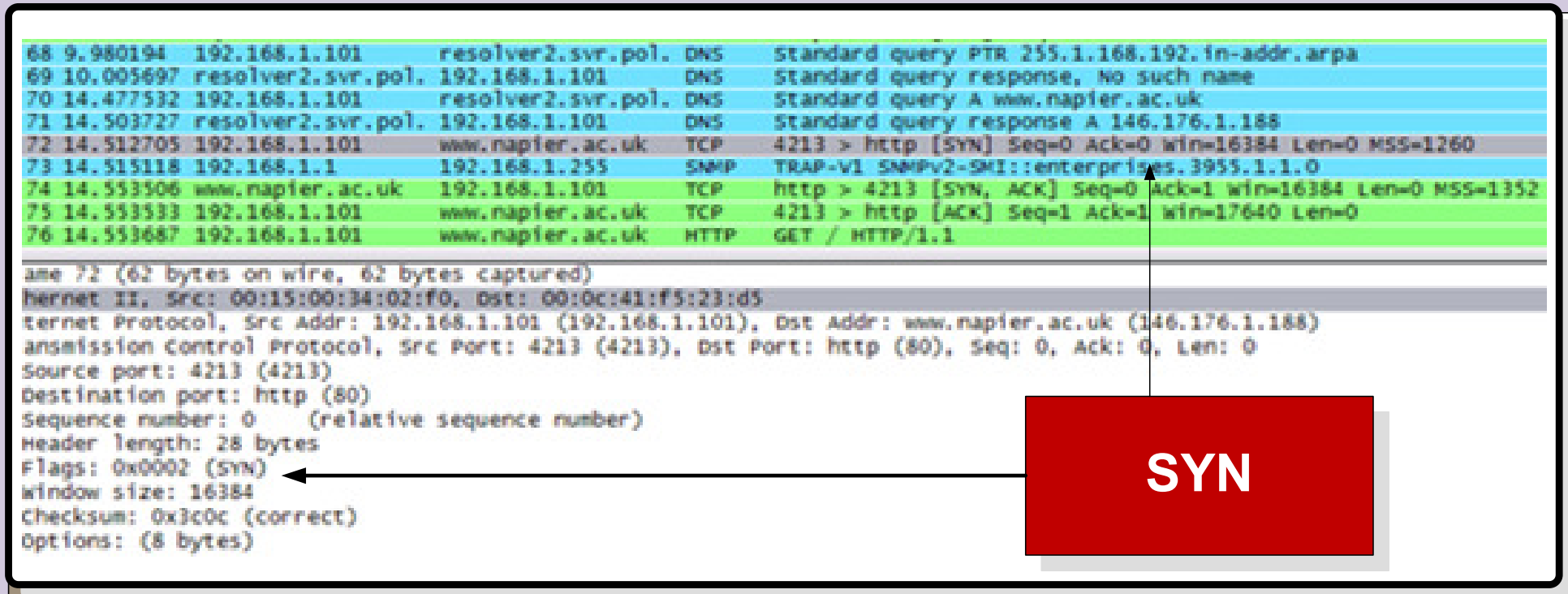
Originator		Recipient	
1. CLOSED		LISTEN	
2. SYN-SENT	<SEQ=999><CTL=SYN>	SYN-RECEIVED	SYN
3. ESTABLISHED	**<SEQ=100><ACK=1000><CTL=SYN,ACK>**	**SYN-RECEIVED**	**SYN,ACK**
4. ESTABLISHED	<SEQ=1000><ACK=101><CTL=ACK>	ESTABLISHED	
5. ESTABLISHED	<SEQ=1000><ACK=101><CTL=ACK><DATA>	ESTABLISHED	



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

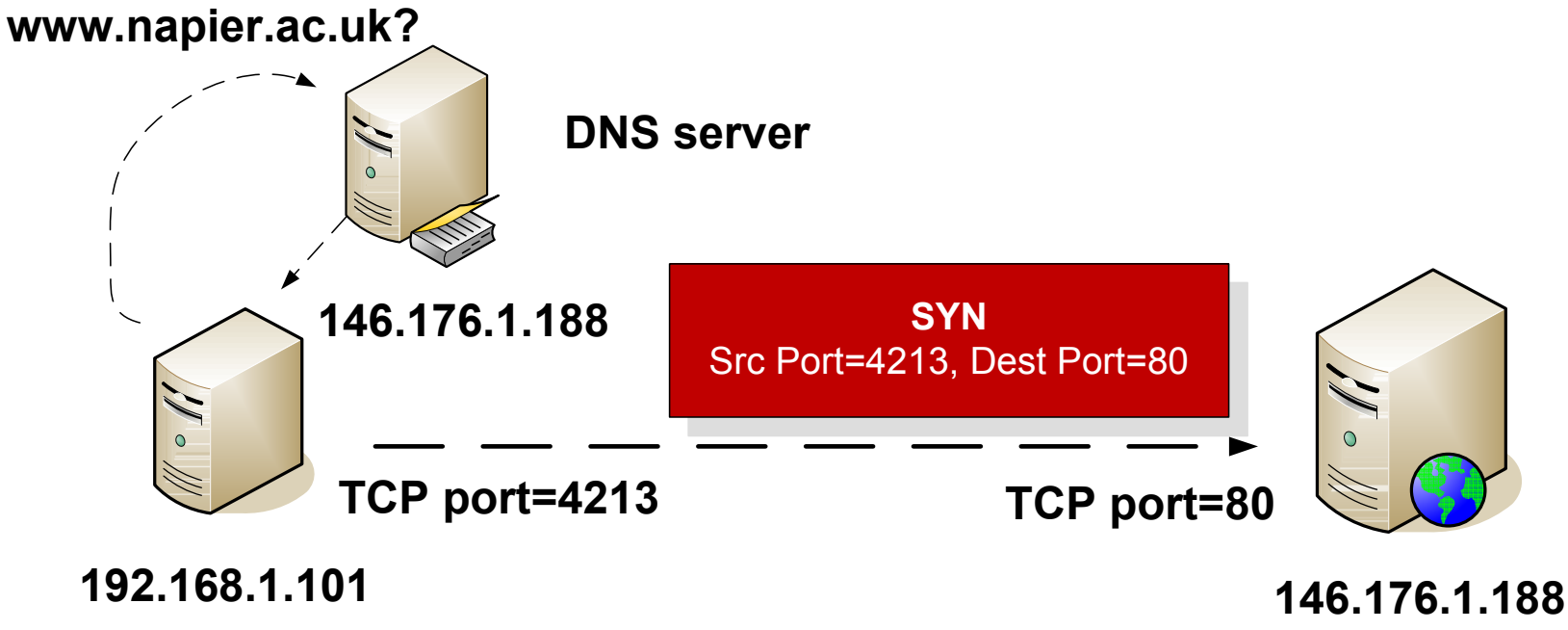
SYN
SYN,ACK
ACK

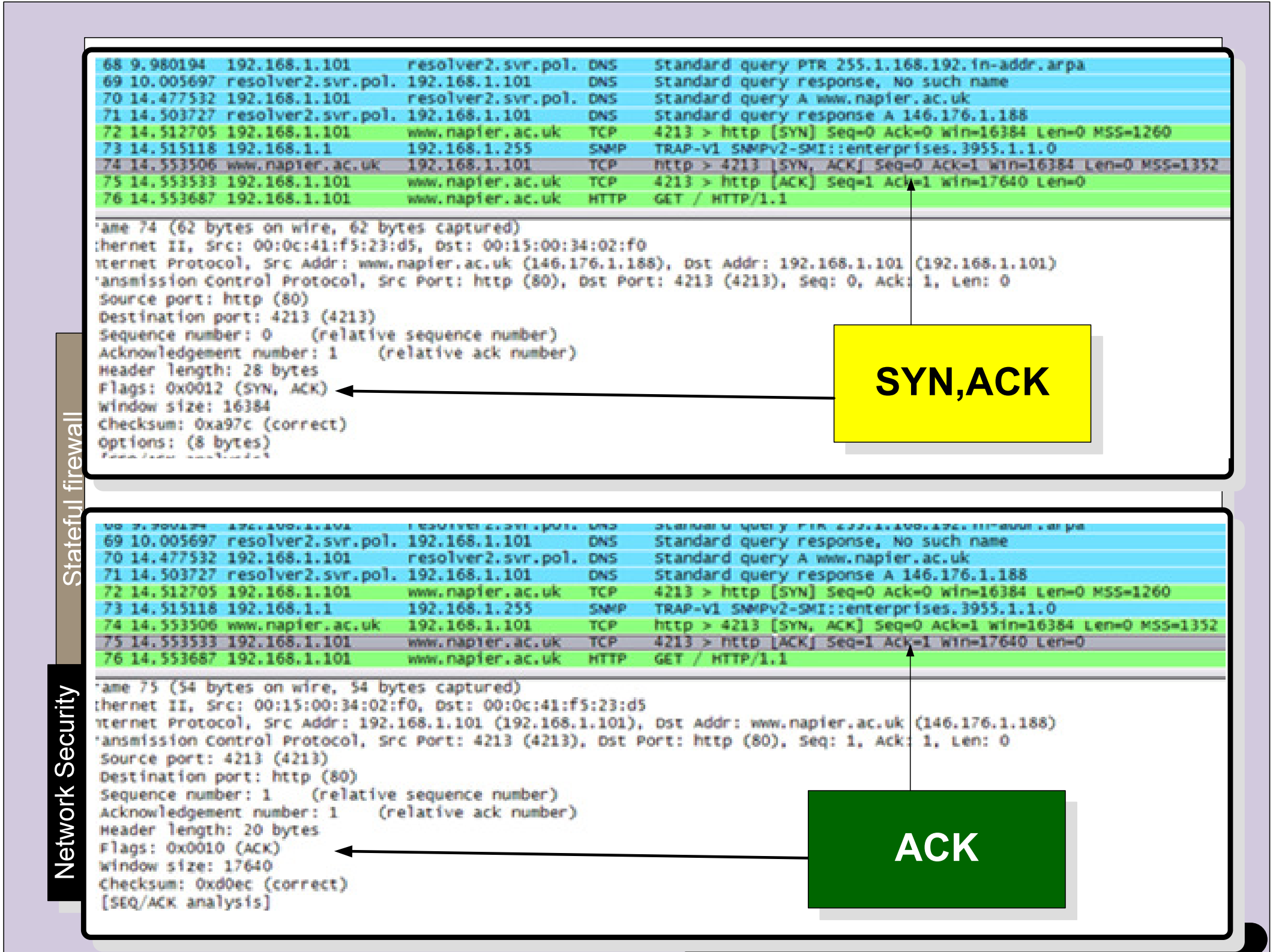




Stateful fi

Network Security

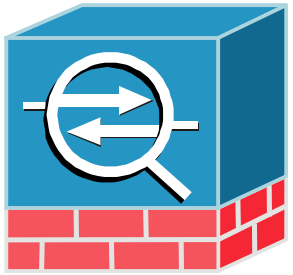



Stateful firewall
Network Security
68 9.980194 192.168.1.101 resolver2.svr.pol. DNS Standard query PTR 255.1.168.192.in-addr.arpa
69 10.005697 resolver2.svr.pol. 192.168.1.101 DNS Standard query response, No such name
70 14.477532 192.168.1.101 resolver2.svr.pol. DNS Standard query A www.napier.ac.uk
71 14.503727 resolver2.svr.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 74 (62 bytes on wire, 62 bytes captured)
thernet II, Src: 00:0c:41:f5:23:d5, Dst: 00:15:00:34:02:f0
nternet Protocol, Src Addr: www.napier.ac.uk (146.176.1.188), Dst Addr: 192.168.1.101 (192.168.1.101)
ansmission 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
69 10.005697 resolver2.svr.pol. 192.168.1.101 DNS Standard query response, No such name
70 14.477532 192.168.1.101 resolver2.svr.pol. DNS Standard query A www.napier.ac.uk
71 14.503727 resolver2.svr.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 75 (54 bytes on wire, 54 bytes captured)
thernet II, Src: 00:15:00:34:02:f0, Dst: 00:0c:41:f5:23:d5
nternet 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: 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

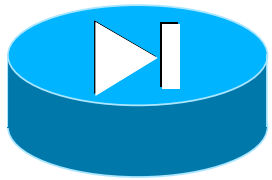
Network Security

PIX/ASA Firewalls

Author: Prof Bill Buchanan

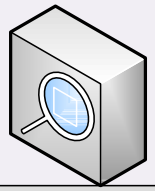


Firewall rules. These are contained within ACLs (using the **access-list** and **access-group** commands), and block or permit traffic. A key feature of this is the usage of **URL filtering** which defines the Web pages which are allowed and which are not.
Port blocking. These use the **fixup** command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

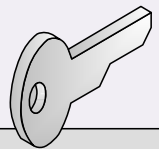


Cut-through proxy. This allows the definition of the users who are allowed services such as HTTP, Telnet and FTP. This authentication is a single initial authentication, which differs from the normal proxy operation which checks every single packet.

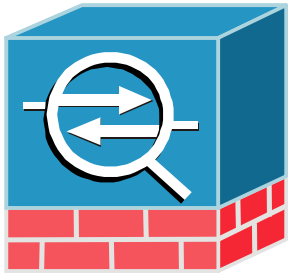
Intrusion detection. These use the **ip audit** command to detect intrusions.
Shunning. This, along with intrusion detection, allows a defined response to an intrusion.



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**.

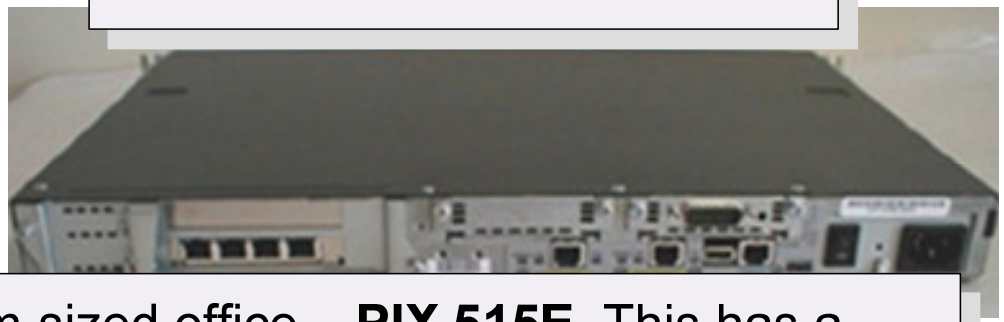


Failover. This allows other devices to detect that a PIX device has crashed, and that another device needs to take its place.



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.

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.



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).

515E – R
515E – U

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

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.

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.

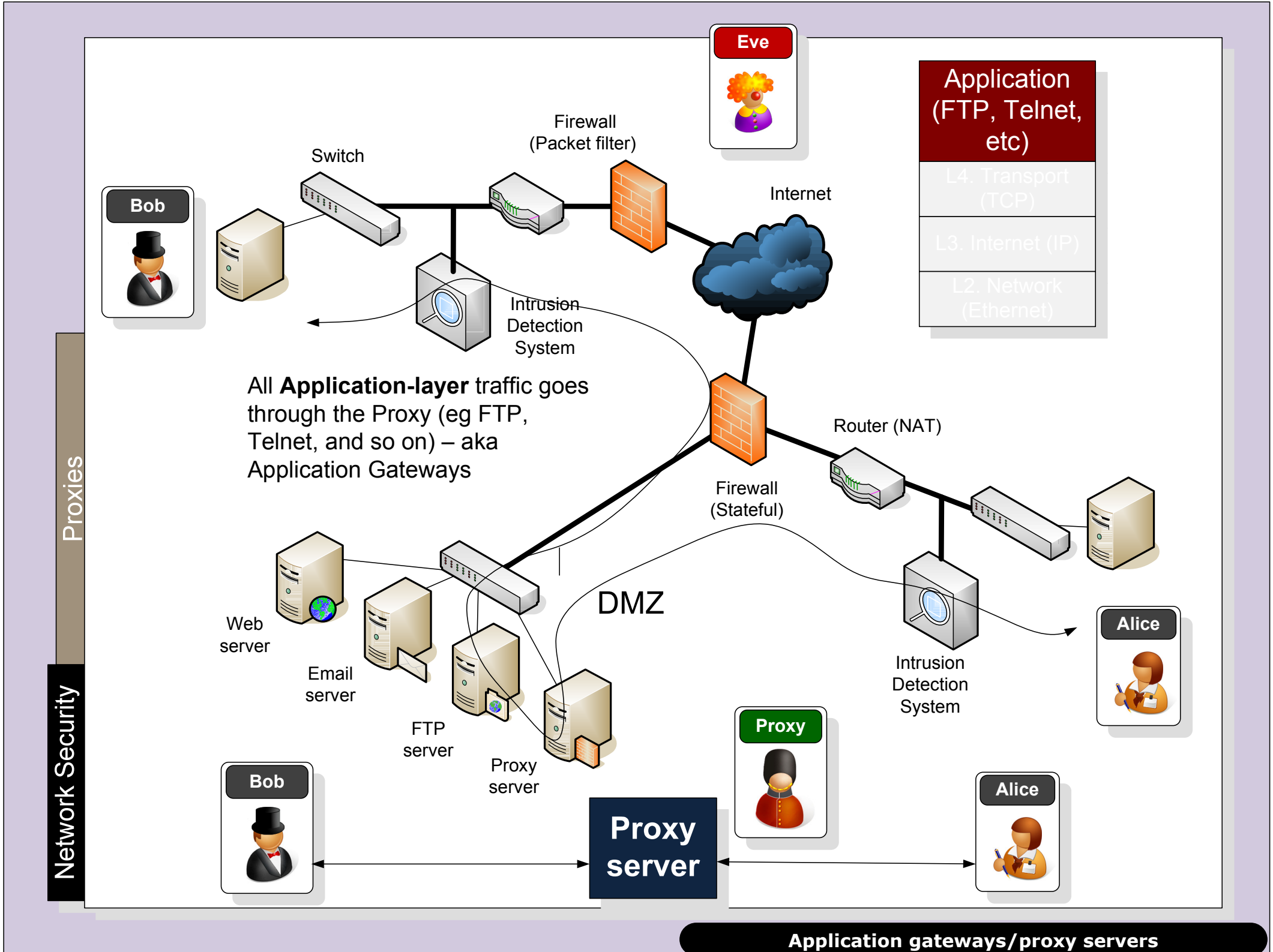
ASA 5520
Intel Pentium 4, 2GHz
512MB RAM
PIX 7.x, ASA 8.x IOS
8 interfaces
Integrated VPN
SSL VPN

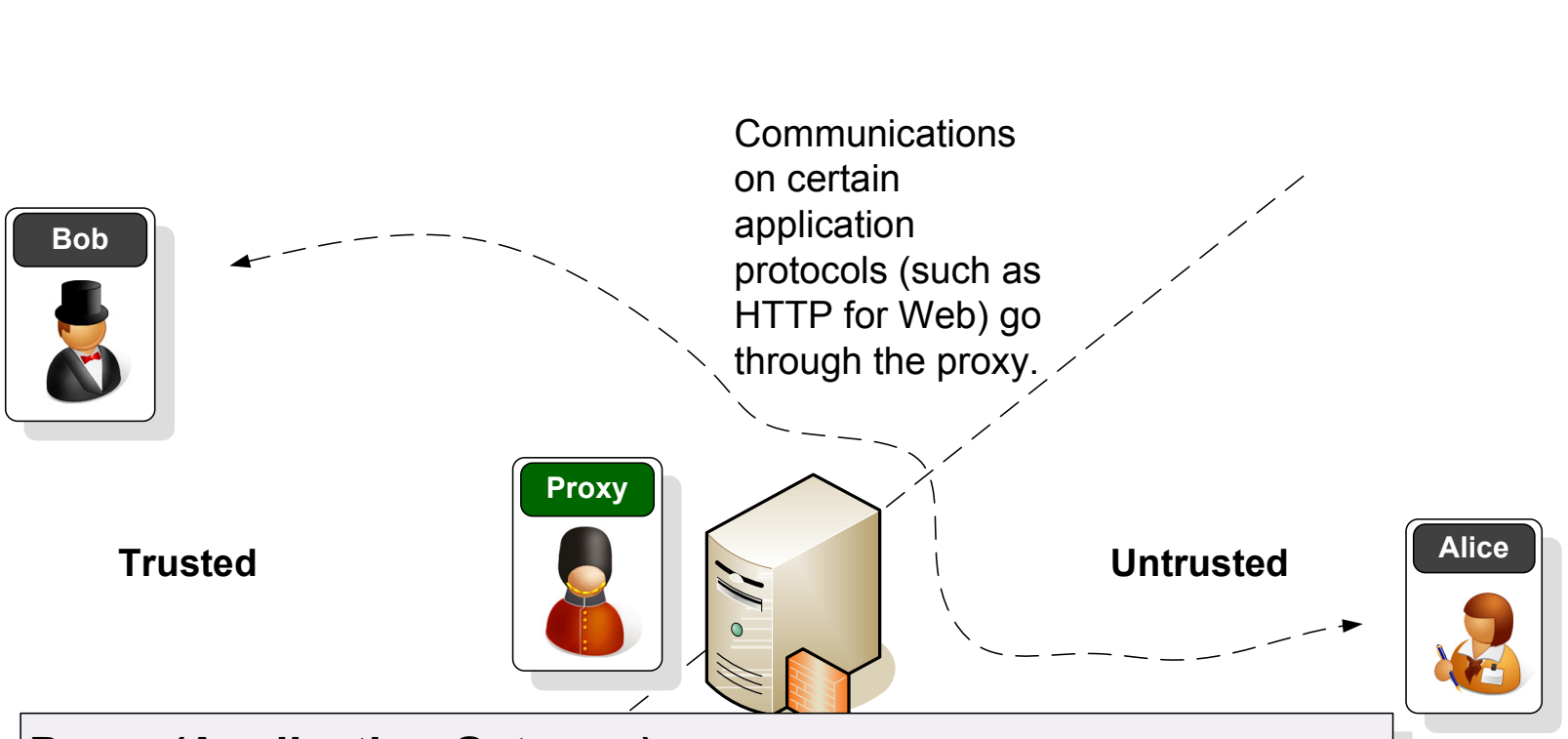
Throughput: 450Mbps
3DES: 225Mbps
Max conn: 280,000
VPN peers: 750

Network Security

Proxies

Author: Prof Bill Buchanan


Eve
Application (FTP, Telnet, etc)
L4. Transport (TCP)
L3. Internet (IP)
L2. Network (Ethernet)
Firewall (Packet filter)
Switch
Internet
Bob
Intrusion Detection System
All **Application-layer** traffic goes through the Proxy (eg FTP, Telnet, and so on) – aka Application Gateways
Router (NAT)
Firewall (Stateful)
Proxies
Network Security
DMZ
Web server
Email server
FTP server
Proxy server
Intrusion Detection System
Alice
Proxy
Bob
Proxy server
Alice
Application gateways/proxy servers



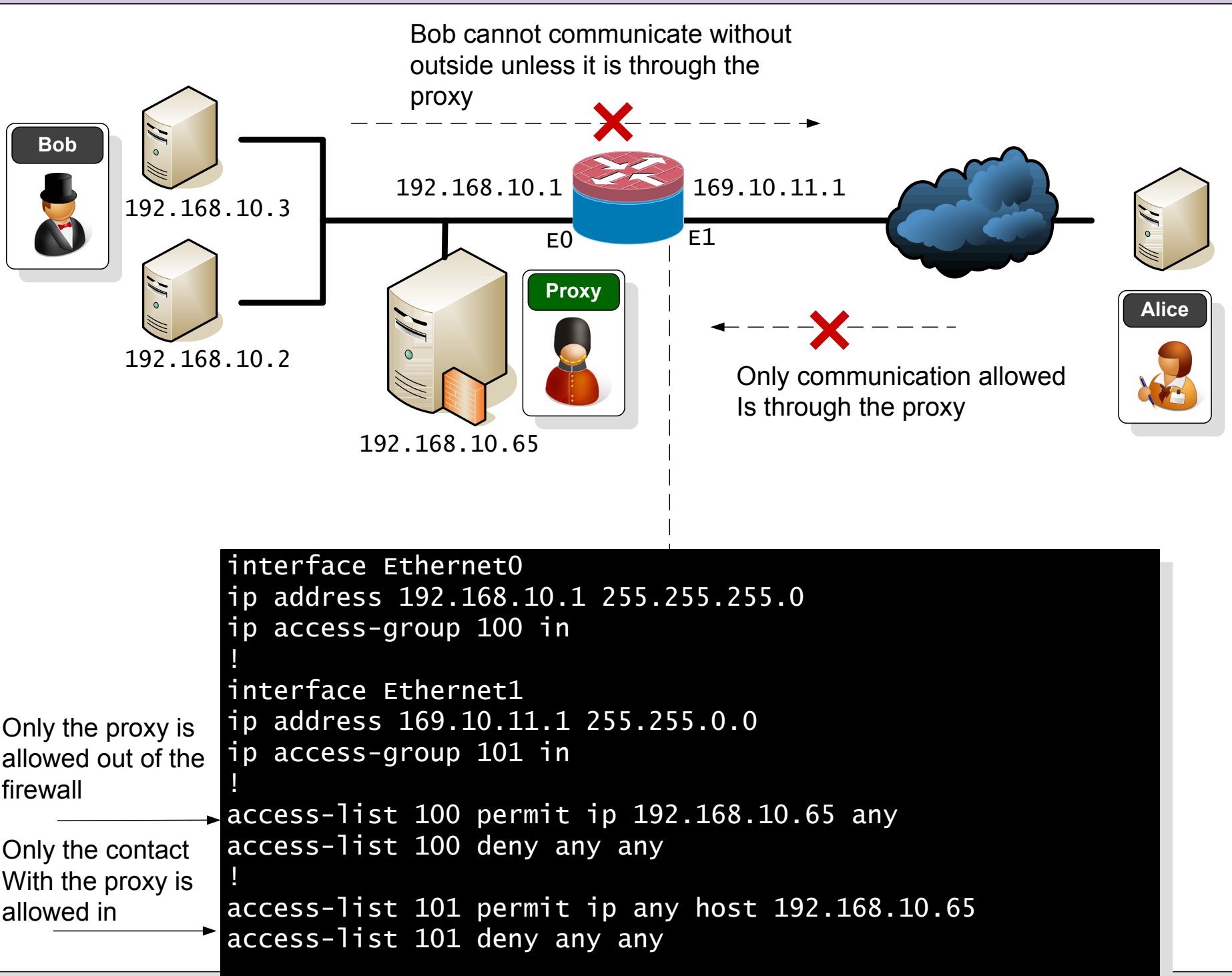
Proxy (Application Gateway):

Advantages:

- User-oriented authentication.
- User-oriented logging.
- User-oriented accounting.

Disadvantages:

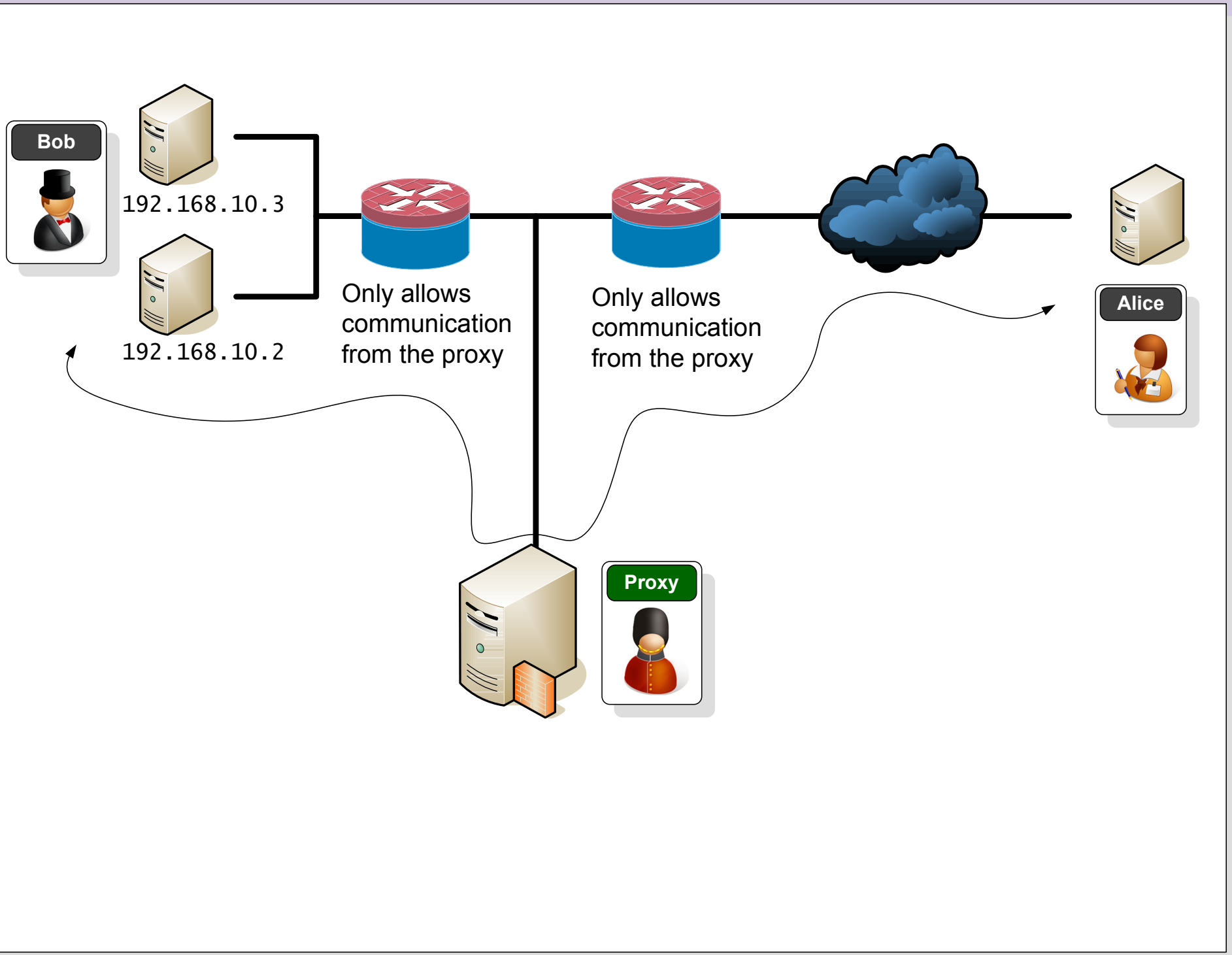
- Build specifically for each application (although the SOCKS protocol has been designed, which is an all-one proxy).
- Slower than without proxy.
- Central point-of-failure



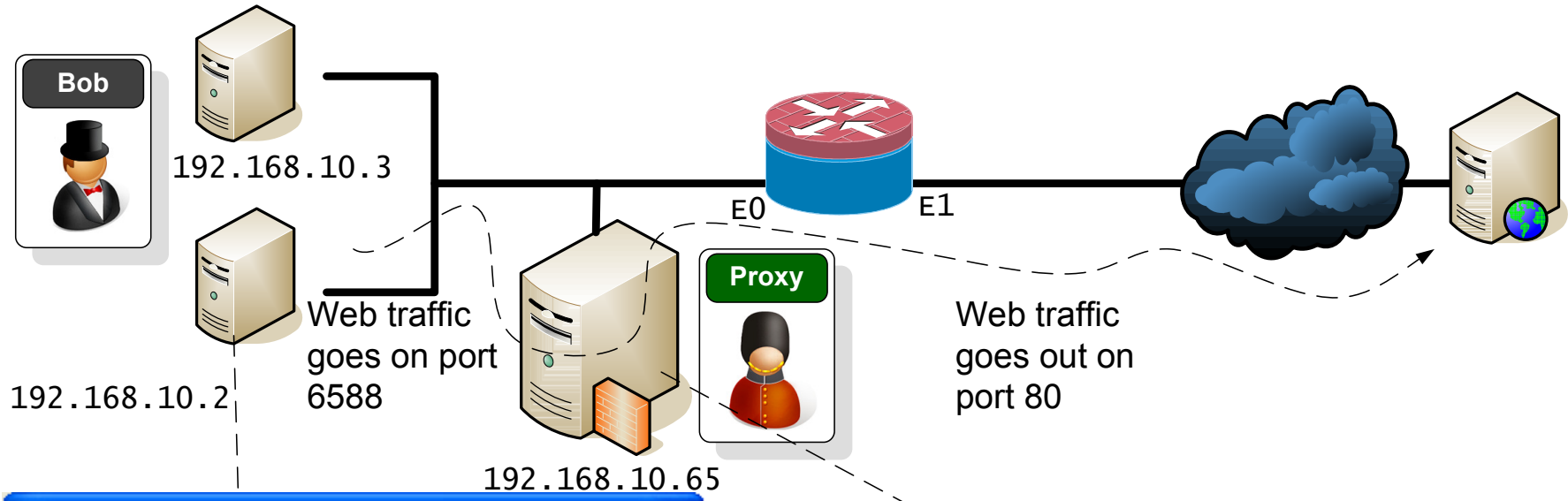
Only the proxy is allowed out of the firewall

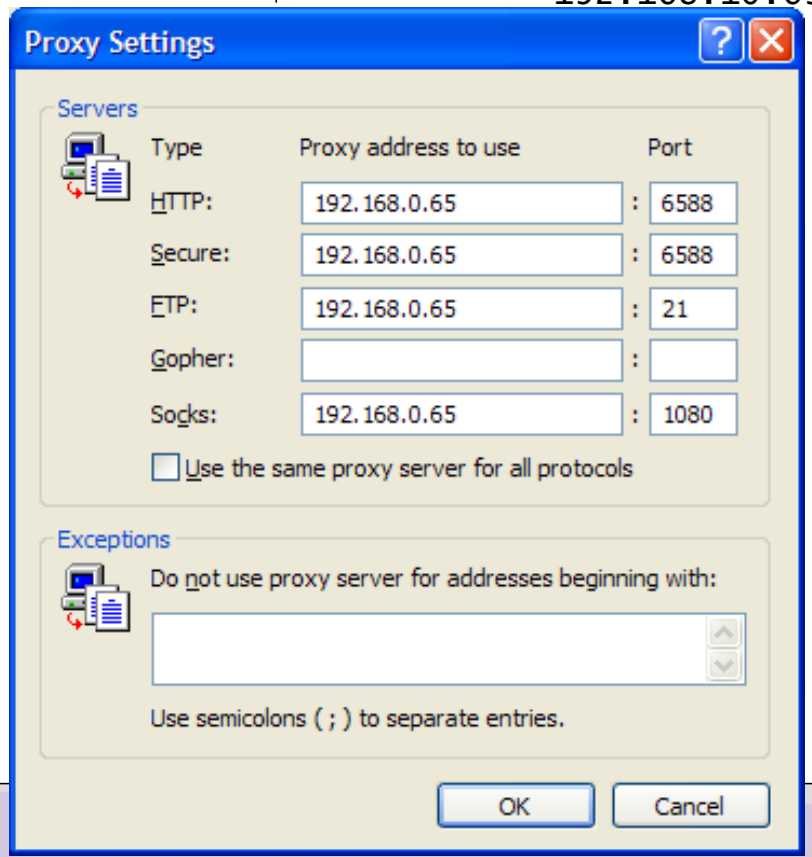
Only the contact With the proxy is allowed in

```
interface Ethernet0
ip address 192.168.10.1 255.255.255.0
ip access-group 100 in
!
interface Ethernet1
ip address 169.10.11.1 255.255.0.0
ip access-group 101 in
!
access-list 100 permit ip 192.168.10.65 any
access-list 100 deny any any
!
access-list 101 permit ip any host 192.168.10.65
access-list 101 deny any any
```



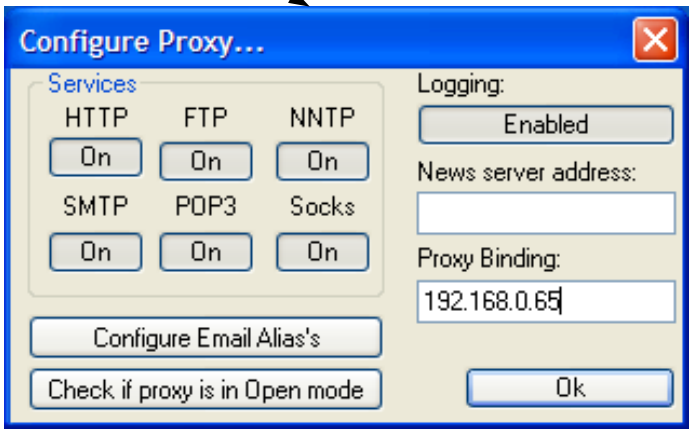
Dual homed proxy

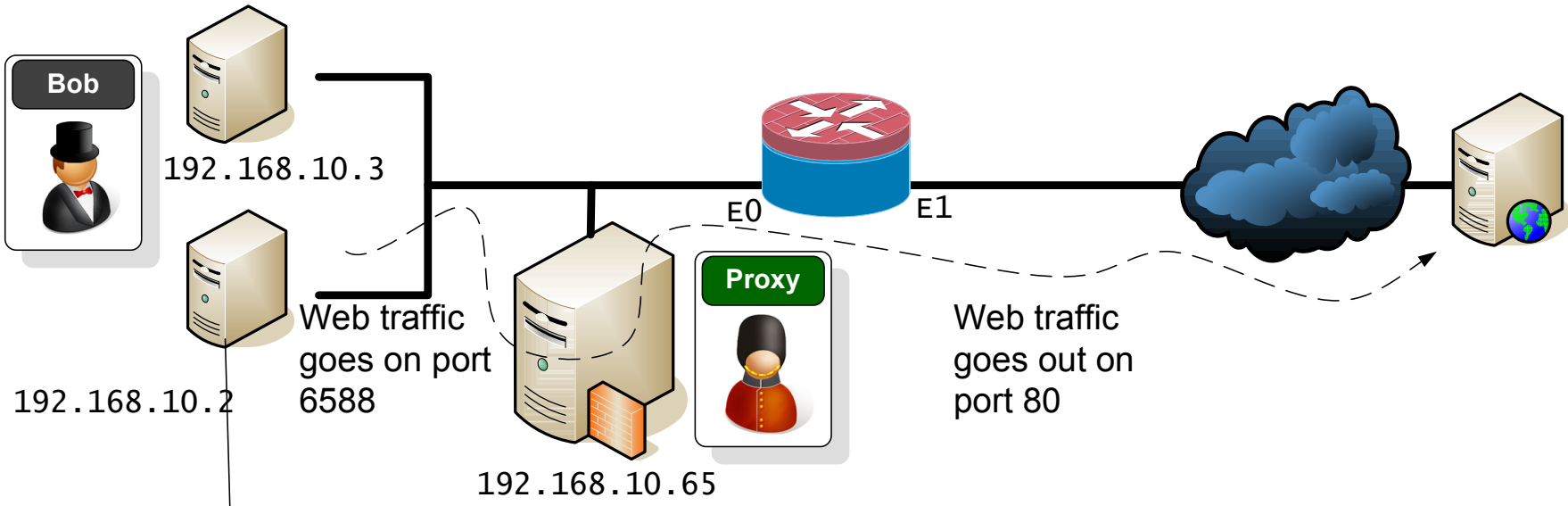


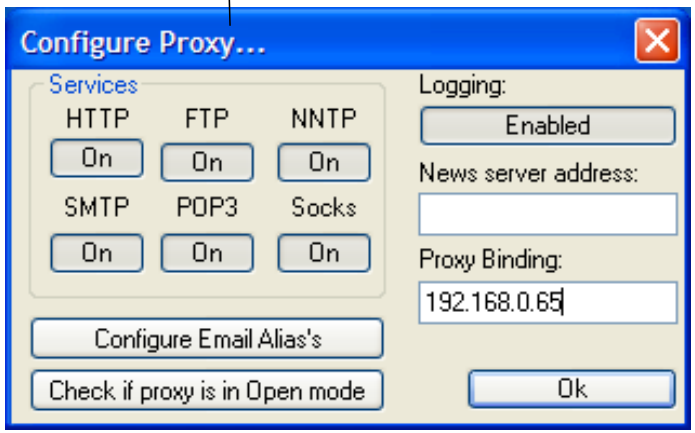


Web traffic goes To port 6588 on the proxy

Agent proxy enabled



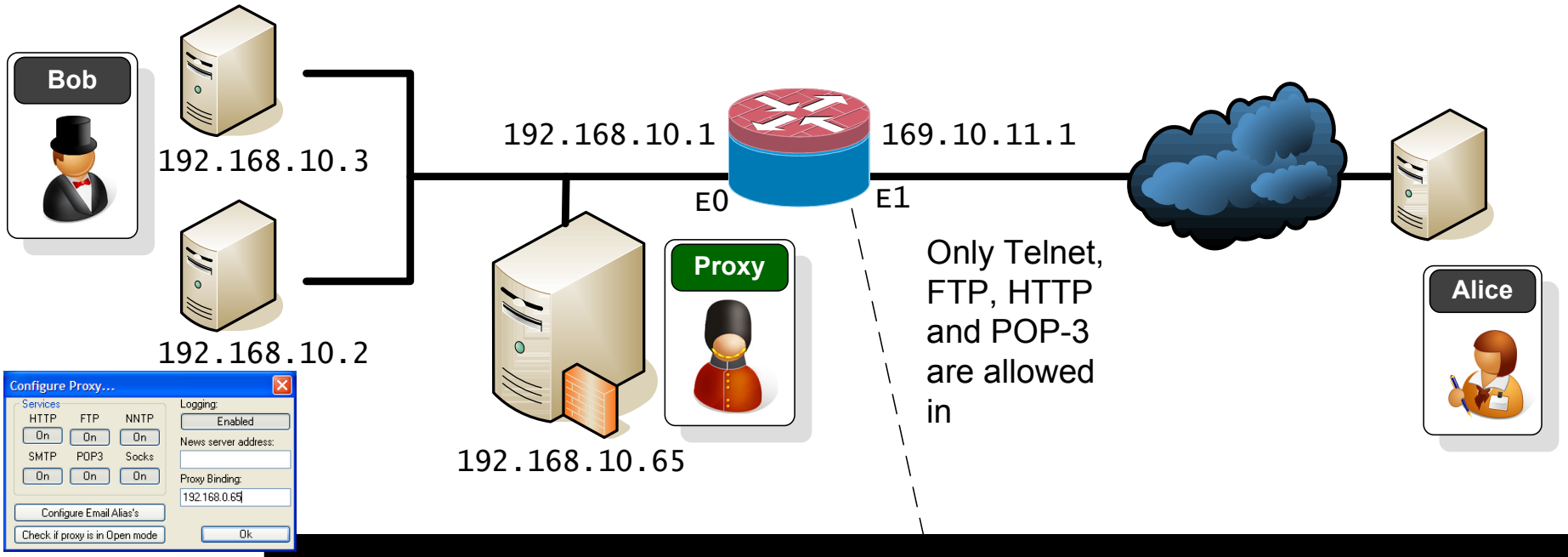




Agent proxy enabled

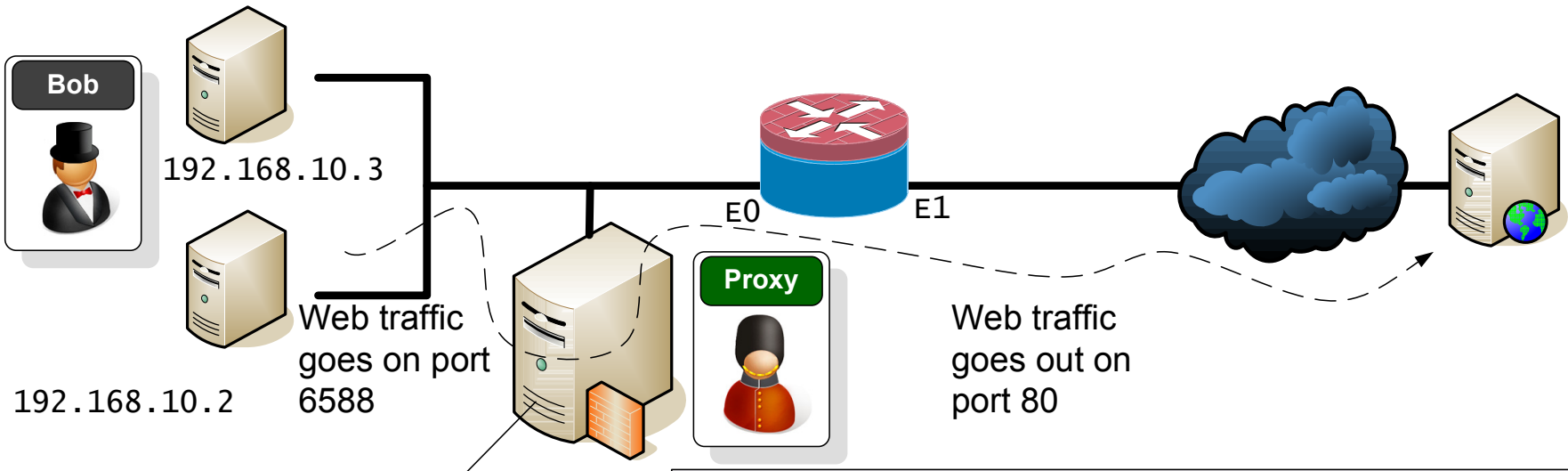
HTTP	(web browsers)	(port 6588)
HTTPS	(secure web browsers)	(port 6588)
SOCKS4	(TCP proxying)	(port 1080)
SOCKS4a	(TCP proxying w/ DNS lookups)	(port 1080)
SOCKS5	(only partial support, no UDP)	(port 1080)
NNTP	(usenet newsgroups)	(port 119)
POP3	(receiving email)	(port 110)
SMTP	(sending email)	(port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

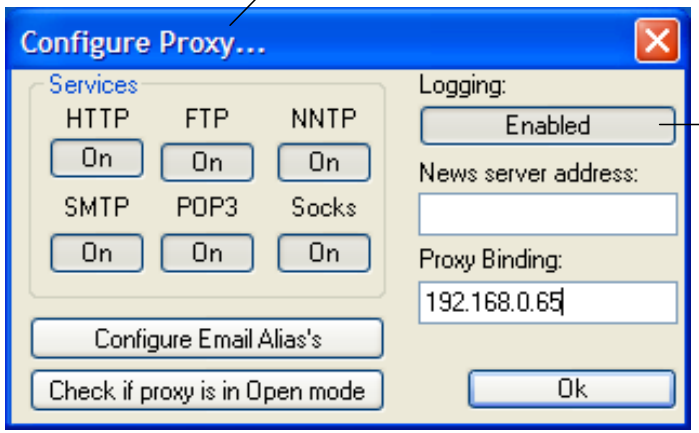
Typical proxy ports



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
```

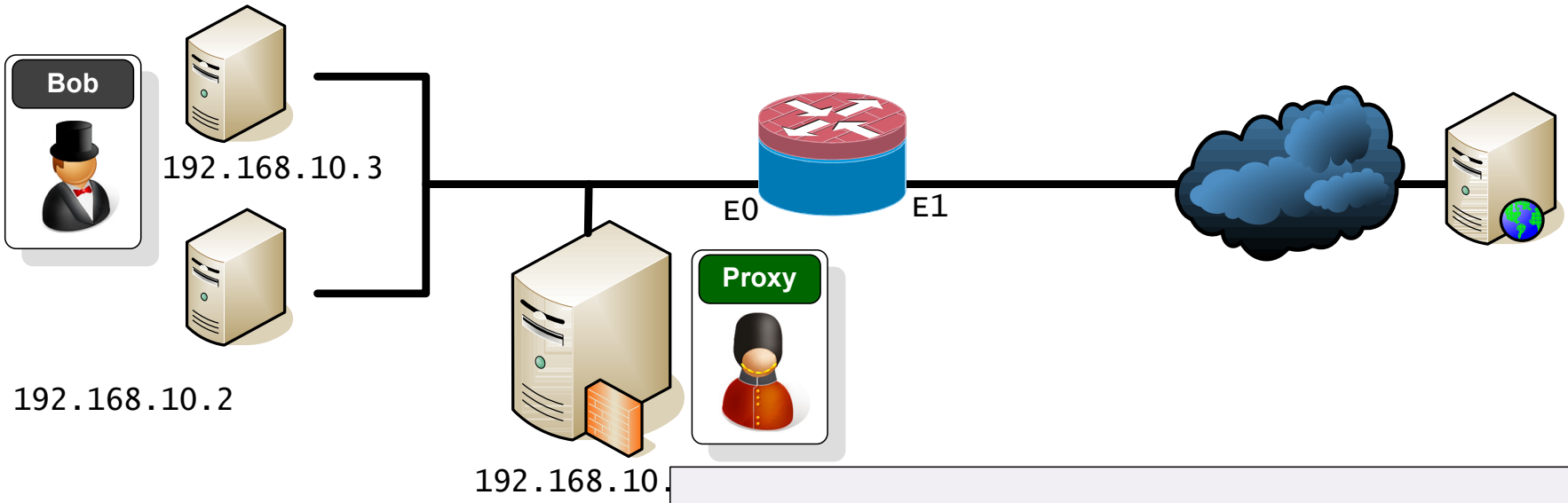




Agent proxy enabled

```
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
```

Logging from a proxy



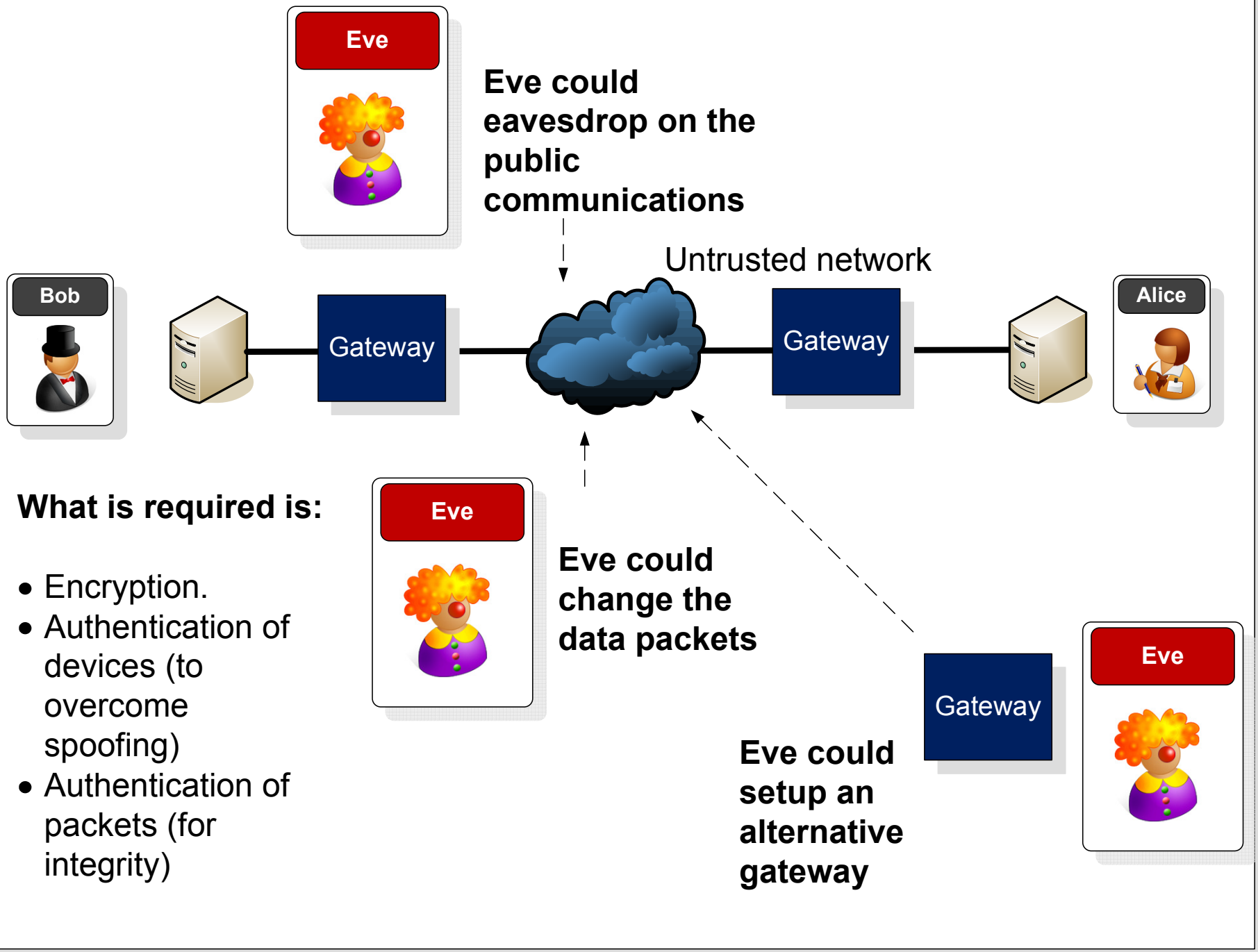
Proxy allows:

- The hosts to be hidden from the outside.
- Private addresses can be used for the internal network.
- Logging of data packets.
- User-level authentication, where users may require a username and a password.
- Isolation of nodes inside the network, as they cannot be directly contacted.

Network Security

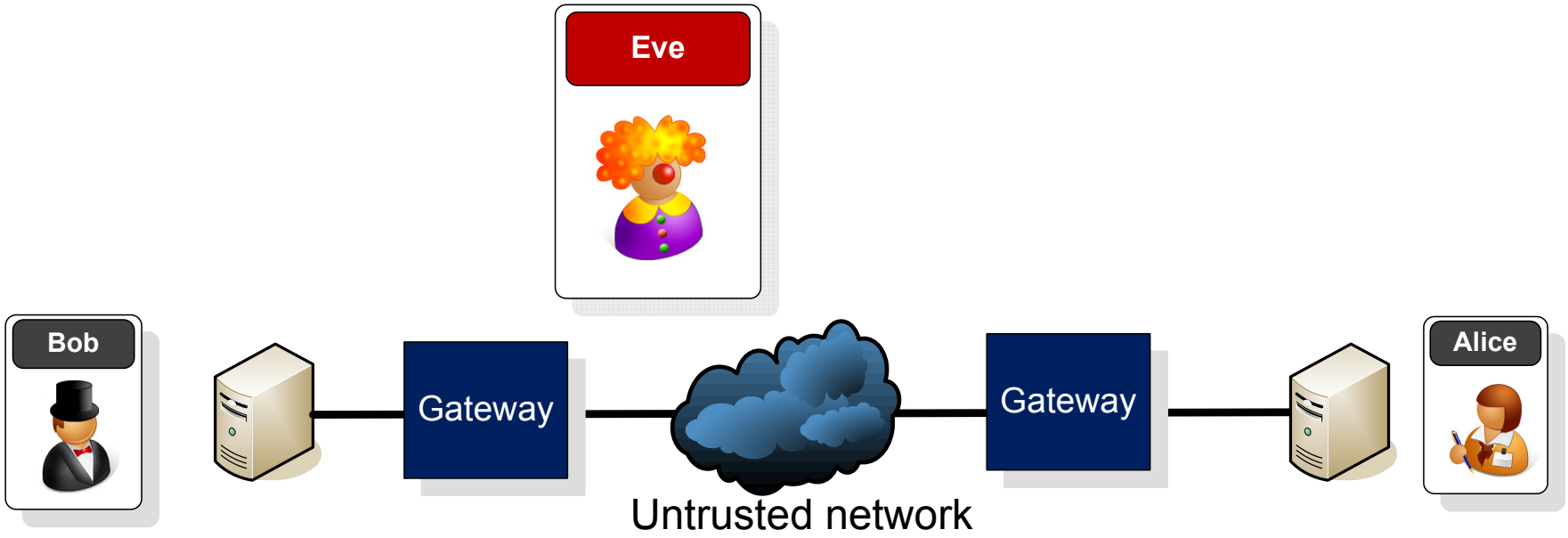
VPNs

Author: Prof Bill Buchanan



What is required is:

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



What is required is:

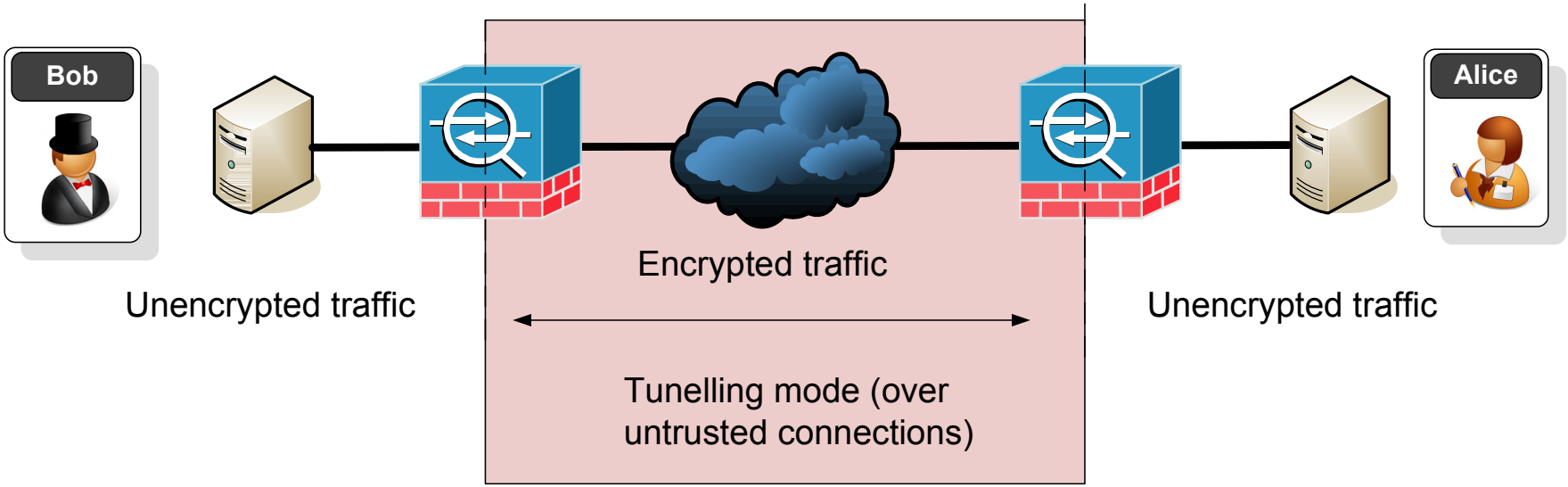
- Encryption.
- Authentication of devices (to overcome spoofing)
- Authentication of packets (for integrity)

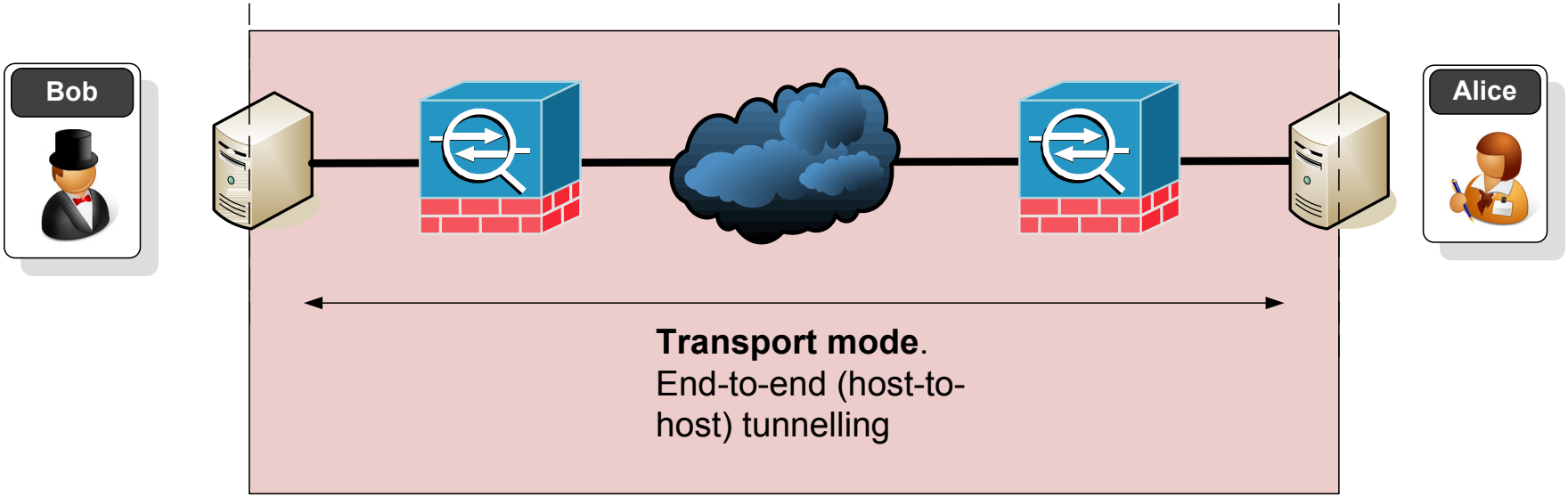
PPTP (Point-to-point Tunneling Protocol). Created by Microsoft and is routable. It uses MPPE (Microsoft Point-to-point Encryption) and user authentication.

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).

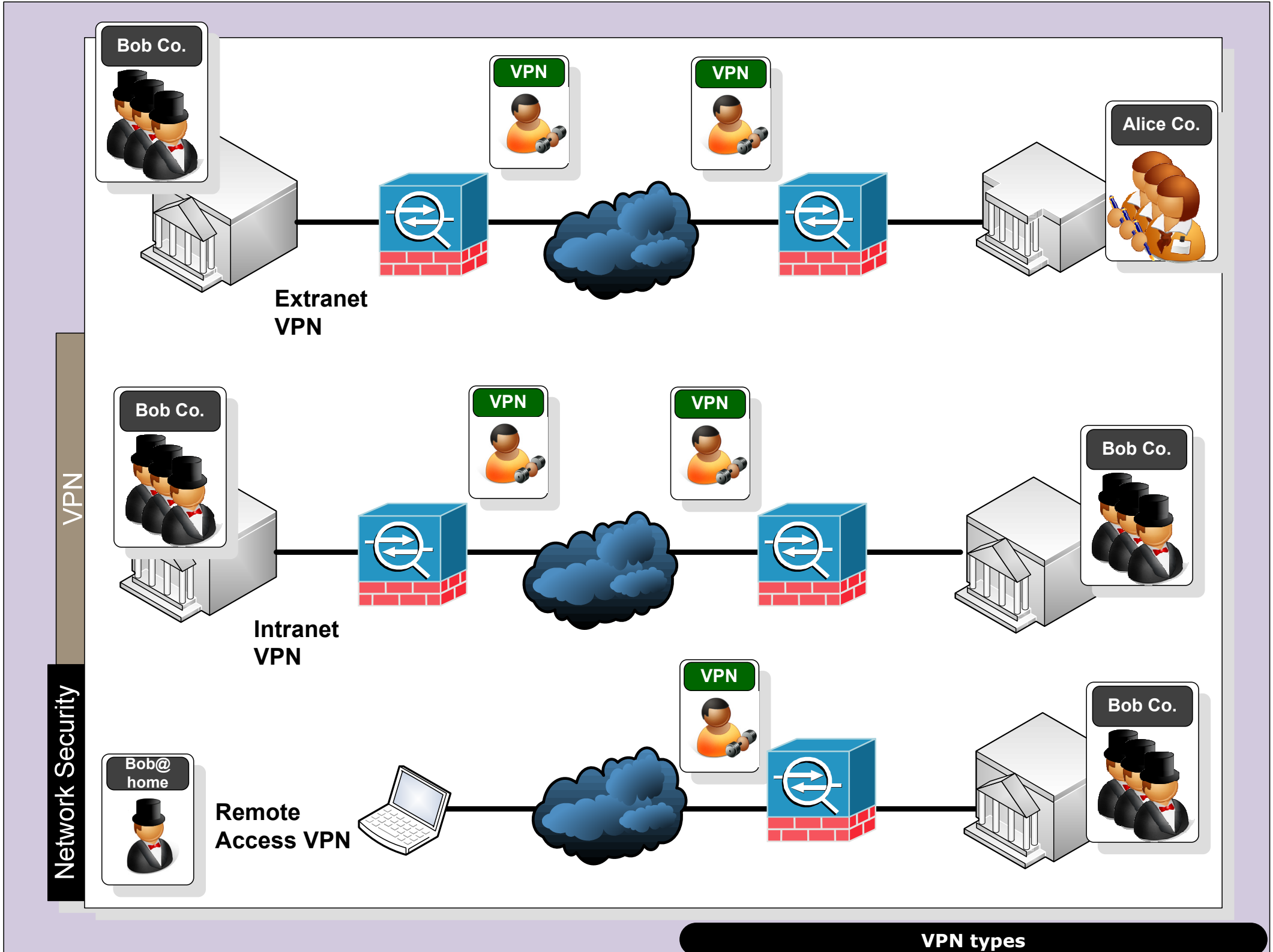
IPSec. An open standard. Includes both encryption and Authentication.

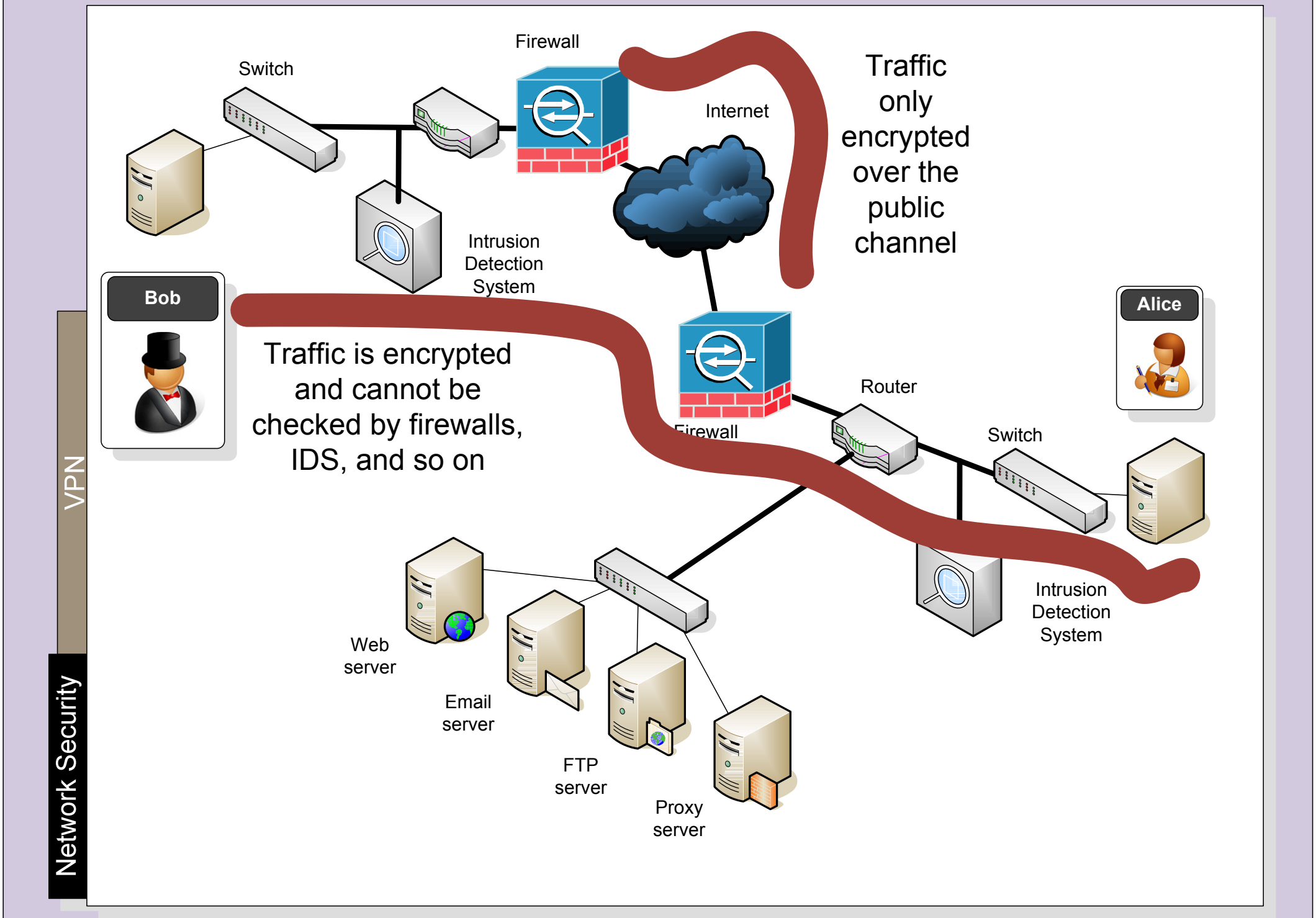
Traffic is encrypted over the untrusted network.

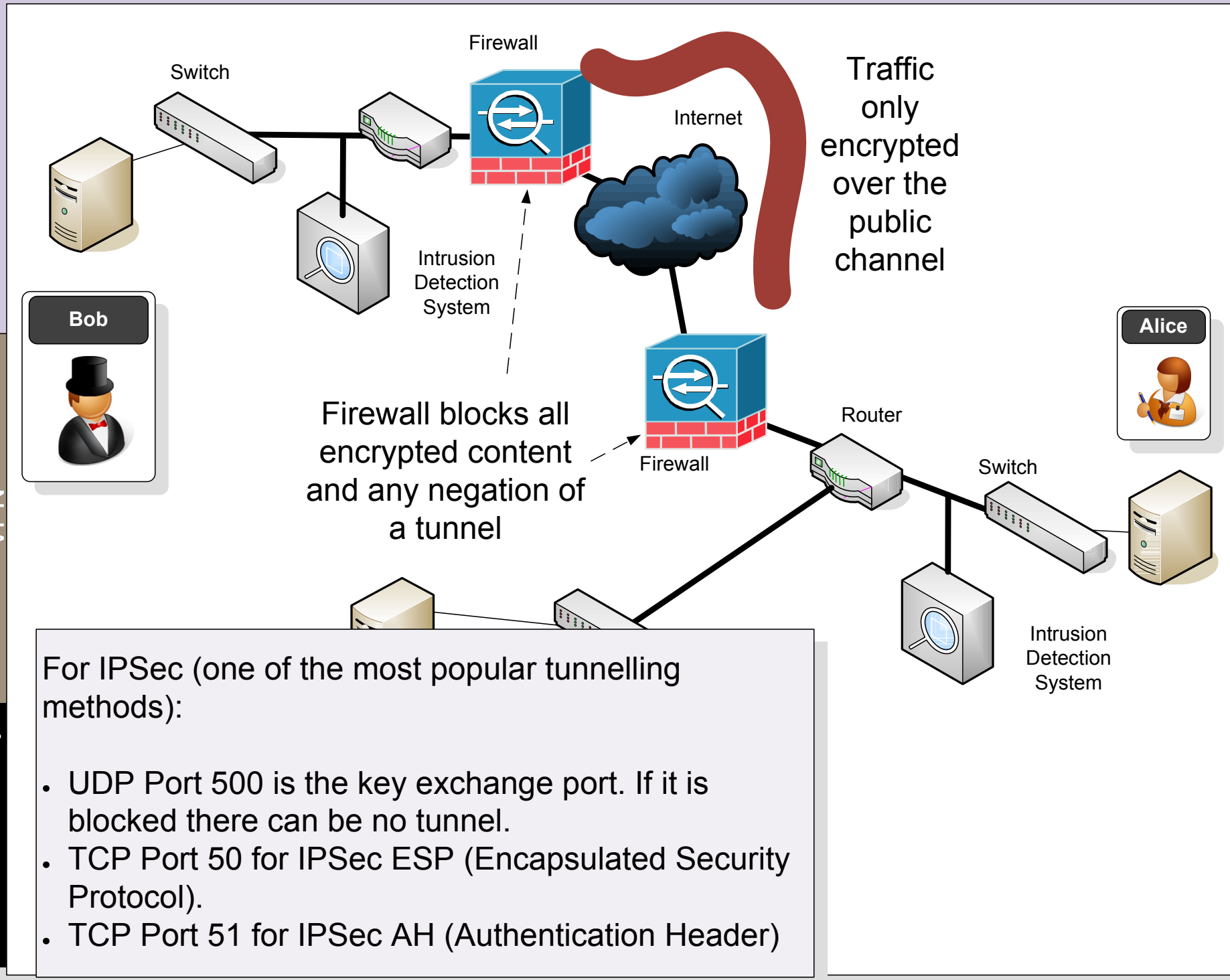




Tunnelling mode or transport mode


Bob Co.
VPN
VPN
Alice Co.
Extranet
VPN
Bob Co.
VPN
VPN
Bob Co.
Intranet
VPN
VPN
Bob@
home
Remote
Access VPN
Bob Co.
VPN
Network Security


Network Security
VPN
Switch
Firewall
Internet
Traffic only encrypted over the public channel
Intrusion Detection System
Bob
Traffic is encrypted and cannot be checked by firewalls, IDS, and so on
Alice
Router
Firewall
Switch
Intrusion Detection System
Web server
Email server
FTP server
Proxy server
Tunnelling mode or transport mode

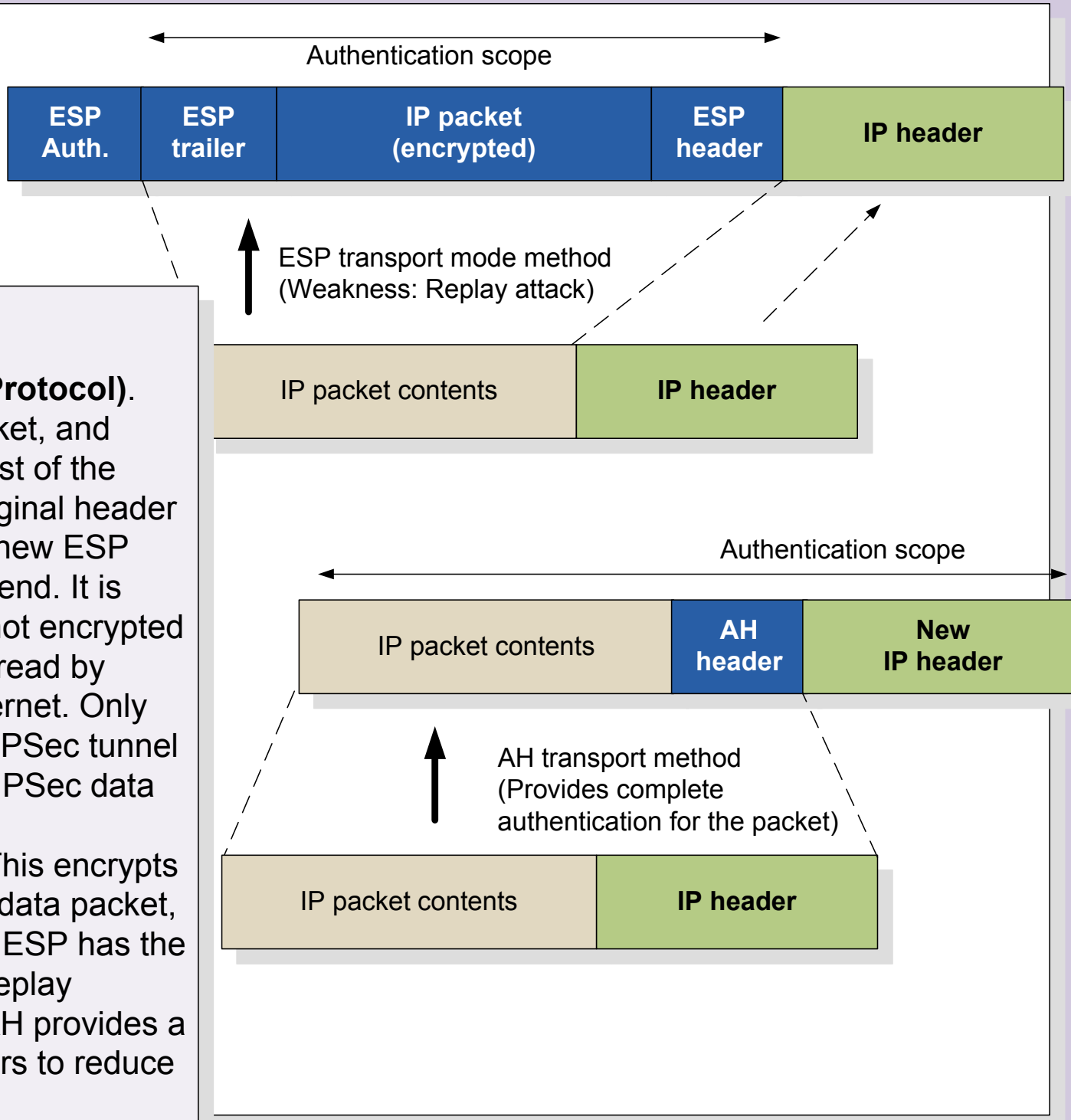


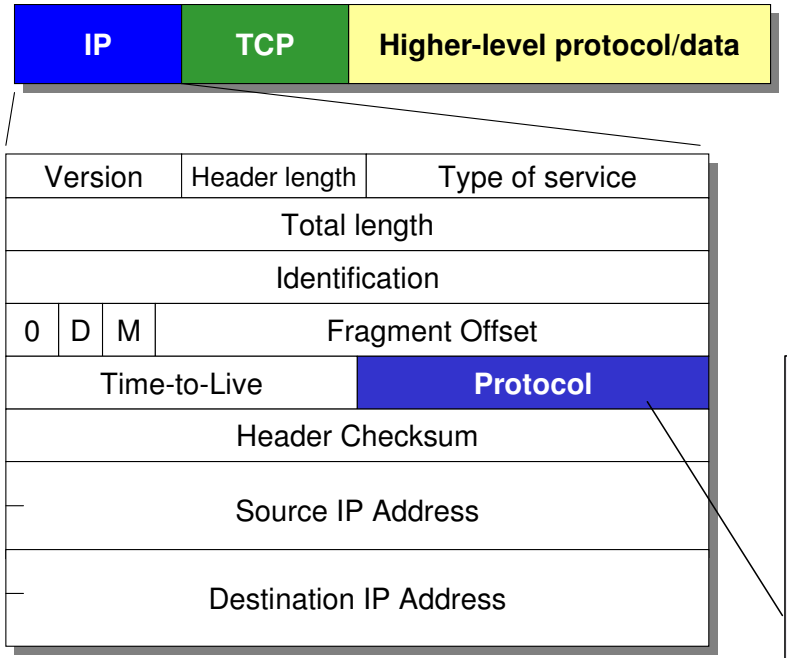
For IPSec (one of the most popular tunnelling methods):

- UDP Port 500 is the key exchange port. If it is blocked there can be no tunnel.
- TCP Port 50 for IPSec ESP (Encapsulated Security Protocol).
- TCP Port 51 for IPSec AH (Authentication Header)

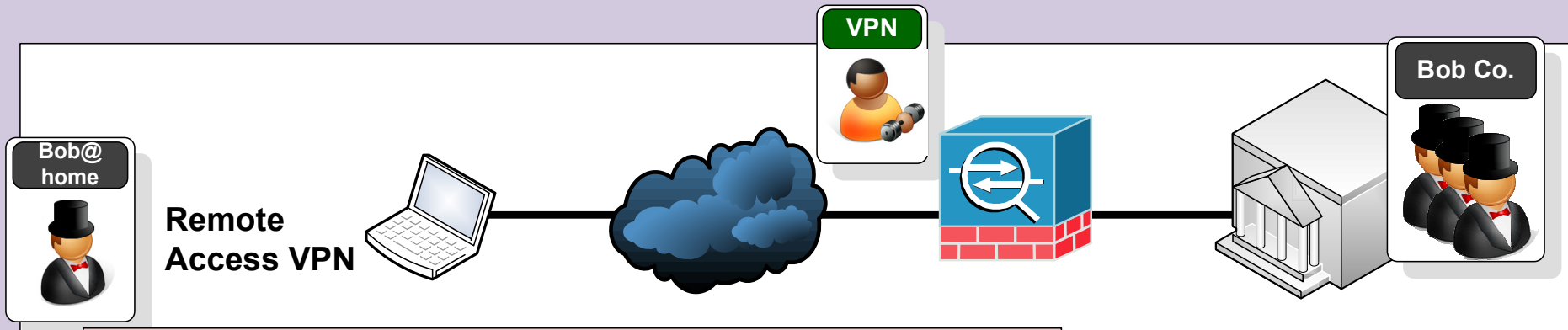
The IPSec protocol has:

- **ESP (Encapsulated Security Protocol)**. ESP takes the original data packet, and breaks off the IP header. The rest of the packet is encrypted, with the original header added at the start, along with a new ESP field at the start, and one at the end. It is important that the IP header is not encrypted as the data packet must still be read by routers as it travels over the Internet. Only the host at the other end of the IPSec tunnel can decrypt the contents of the IPSec data packet.
- **AH (Authentication Header)**. This encrypts the complete contents of the IP data packet, and adds a new packet header. ESP has the weakness that an intruder can replay previously sent data, whereas AH provides a mechanism of sequence numbers to reduce this problem.





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
```

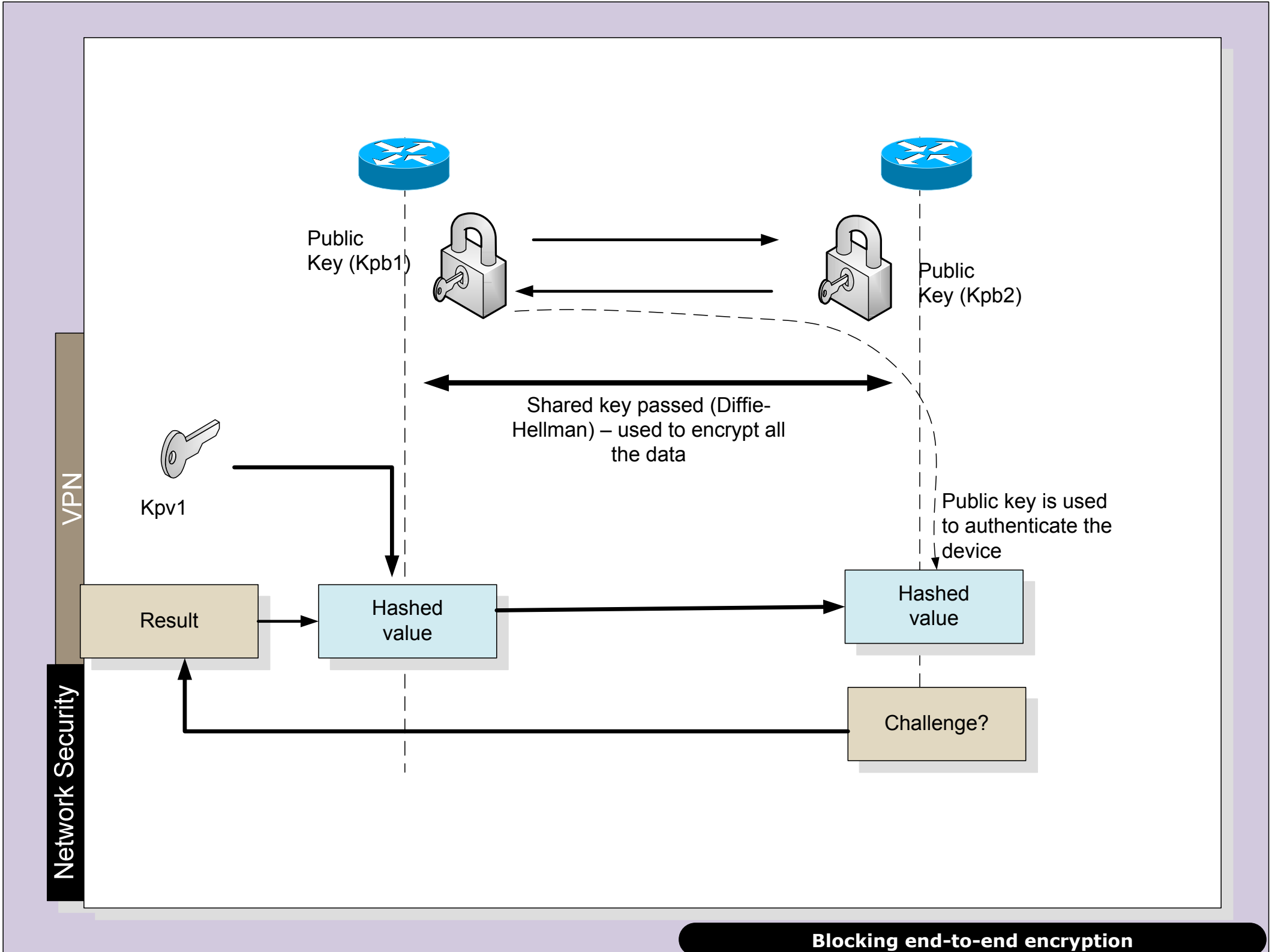
Phase 2

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

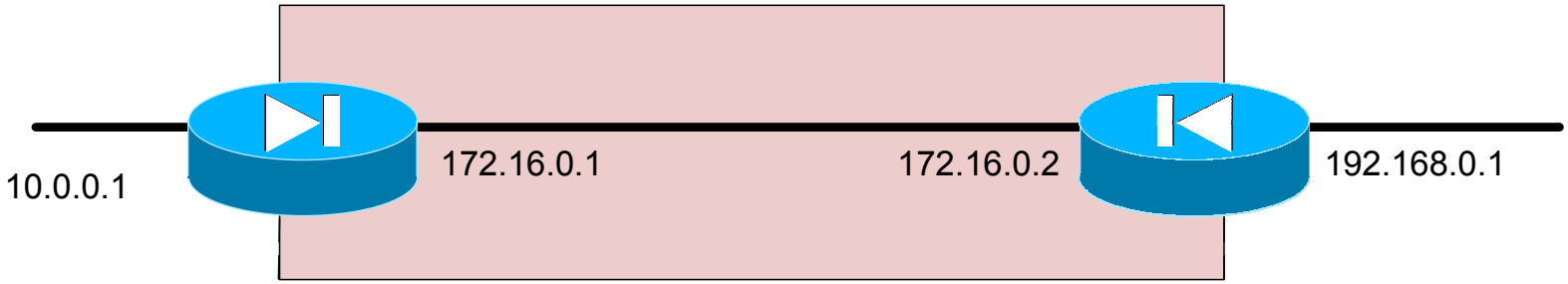
Crypto maps are exchanged

- 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
```

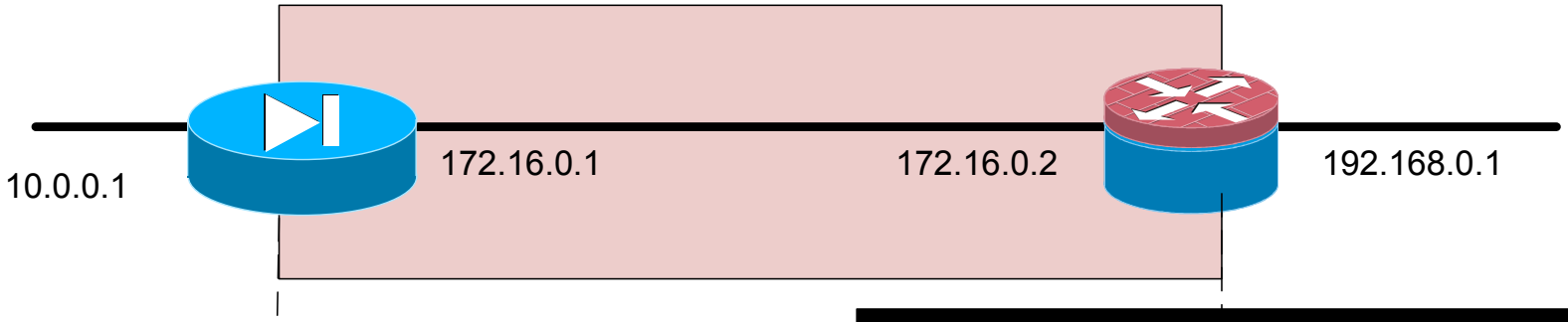


Blocking end-to-end encryption



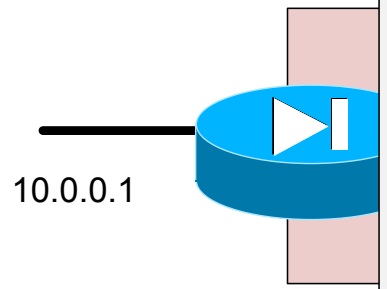

```
isakmp enable outside
isakmp key ABC&FDD address 176.16.0.2 netmask
255.255.255.255
isakmp identity address
isakmp policy 5 authen pre-share
isakmp policy 5 encrypt des
isakmp policy 5 hash sha
isakmp policy 5 group 1
isakmp policy 5 lifetime 86400
sysopt connection permit-ipsec

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
```

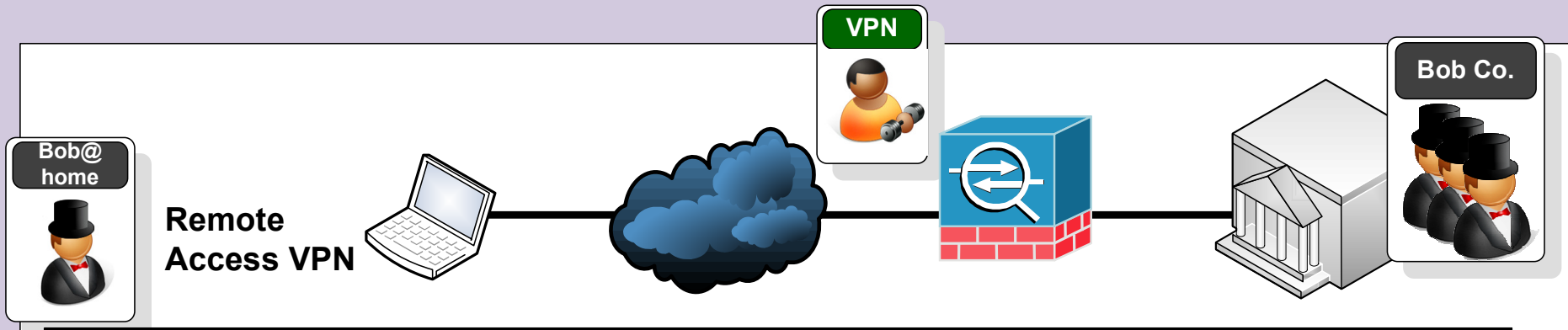



```
isakmp enable outside
isakmp key ABC&FDD address 176.16.0.2 netmask
255.255.255.255
isakmp identity address
isakmp policy 5 authen pre-share
isakmp policy 5 encrypt des
isakmp policy 5 hash sha
isakmp policy 5 group 1
isakmp policy 5 lifetime 86400
sysopt connection permit-ipsec

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
```

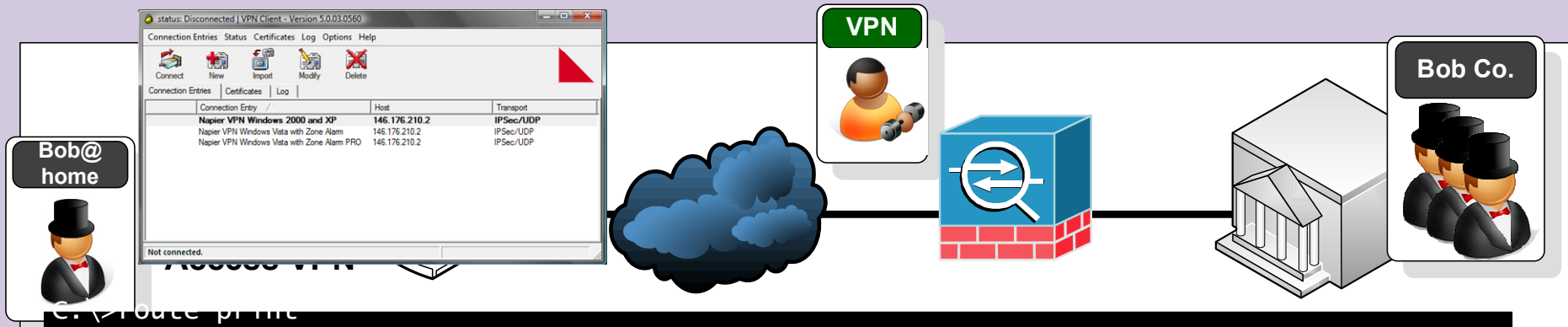



```
No.     Time        Source                Destination           Protocol Info
81 5.237402    192.168.0.3           146.176.210.2         ISAKMP   Aggressive

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)
```



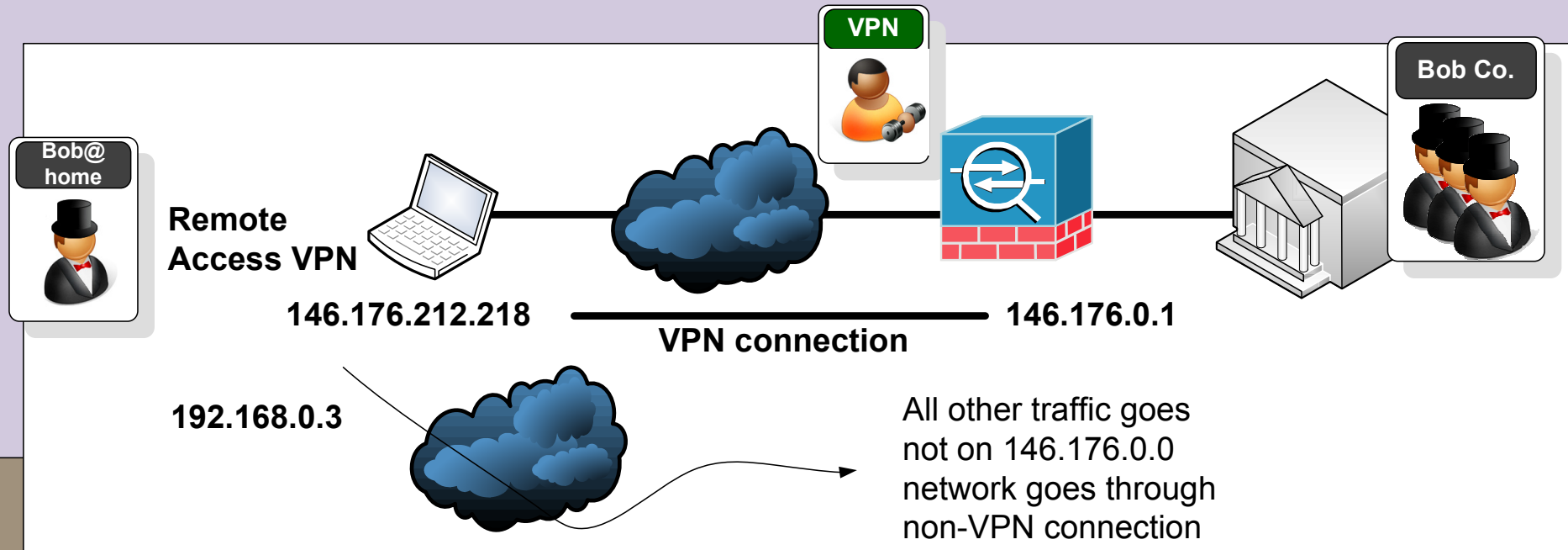

```
C:\>route print
===========================================================================
Interface List
 10 ...00 1d 09 3f 49 8d ...... Broadcom NetLink (TM) Fast Ethernet
  7 ...00 1f 3c 4f 30 1d ...... Intel(R) PRO/Wireless 3945ABG Network Connection

  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



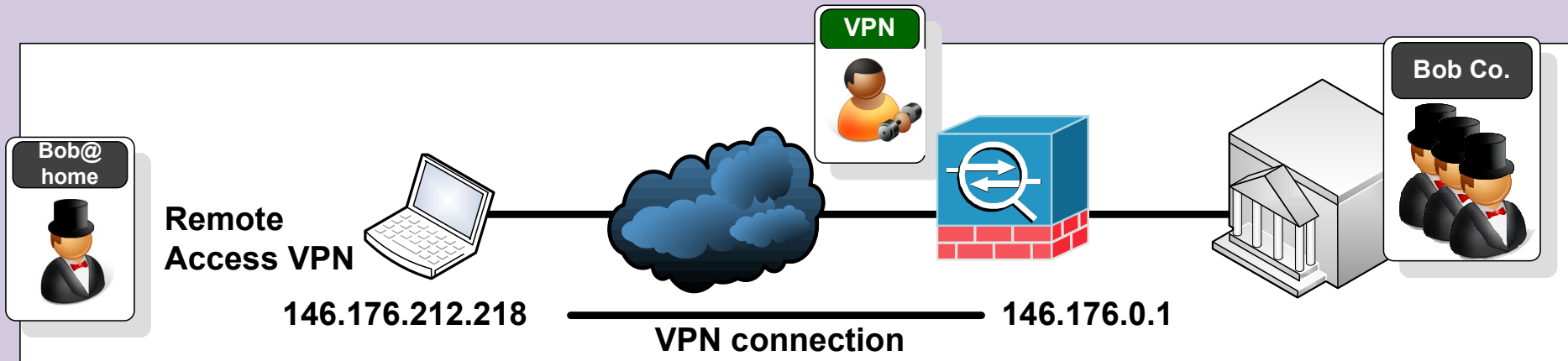

```
C:\>route print
===========================================================================
Interface List
 21 ...00 05 9a 3c 78 00 ...... Cisco Systems VPN Adapter
 10 ...00 1d 09 3f 49 8d ...... Broadcom NetLink (TM) Fast Ethernet
  7 ...00 1f 3c 4f 30 1d ...... Intel(R) PRO/Wireless 3945ABG Network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



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
  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
```

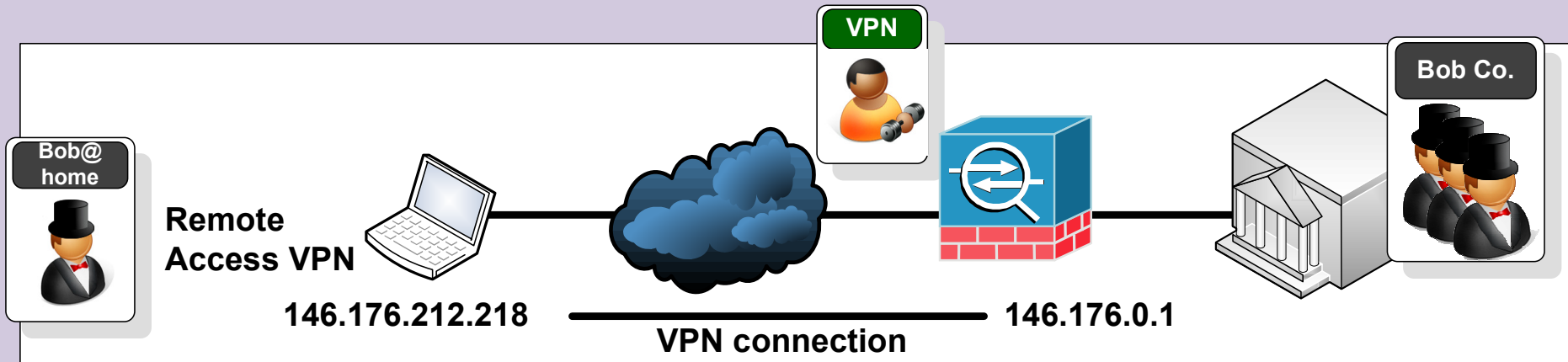
Before VPN connection

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    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

Traceroute for VPN




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

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

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

Before VPN connection

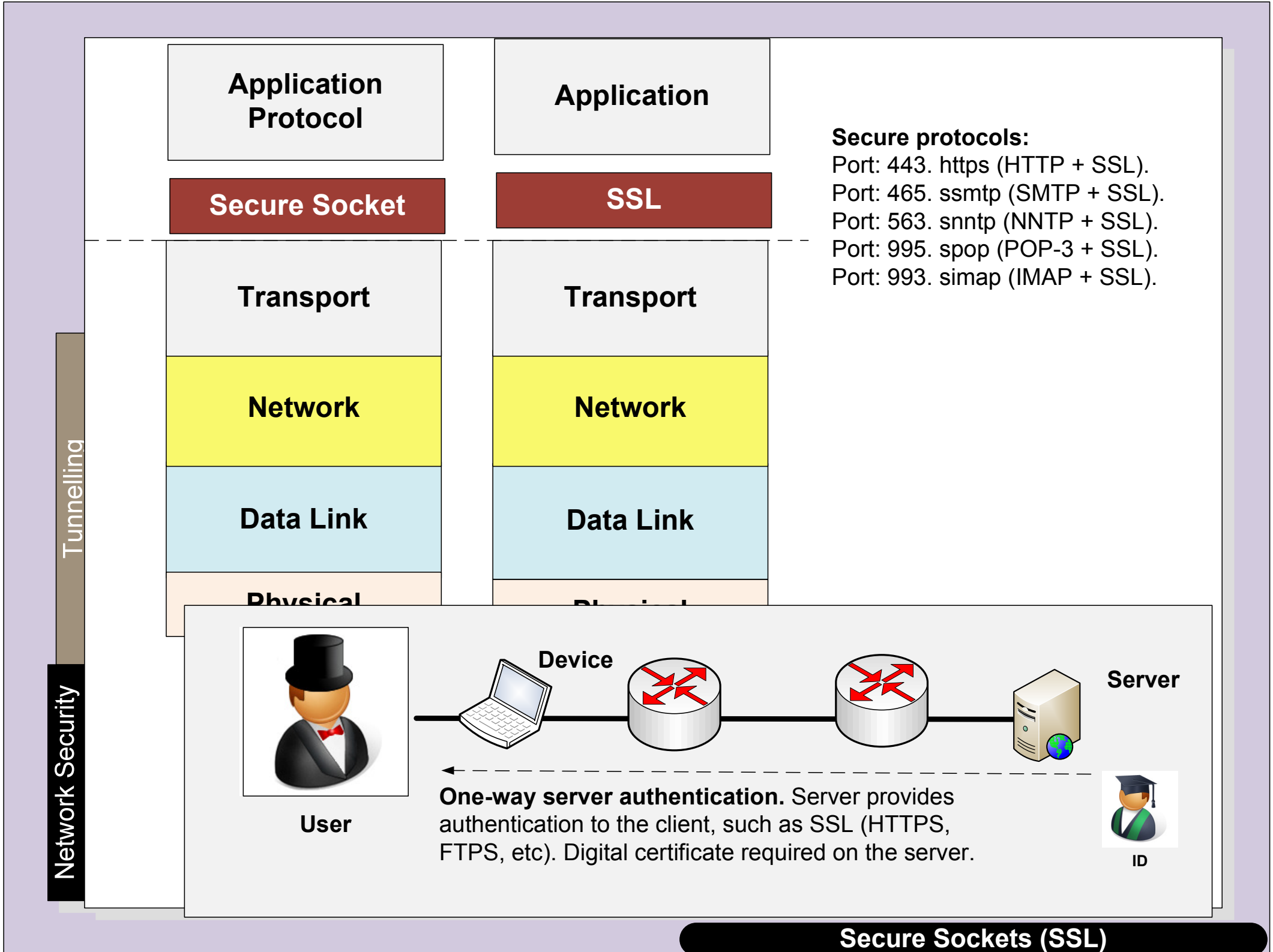
```
C:\>tracert www.intel.com

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]
```

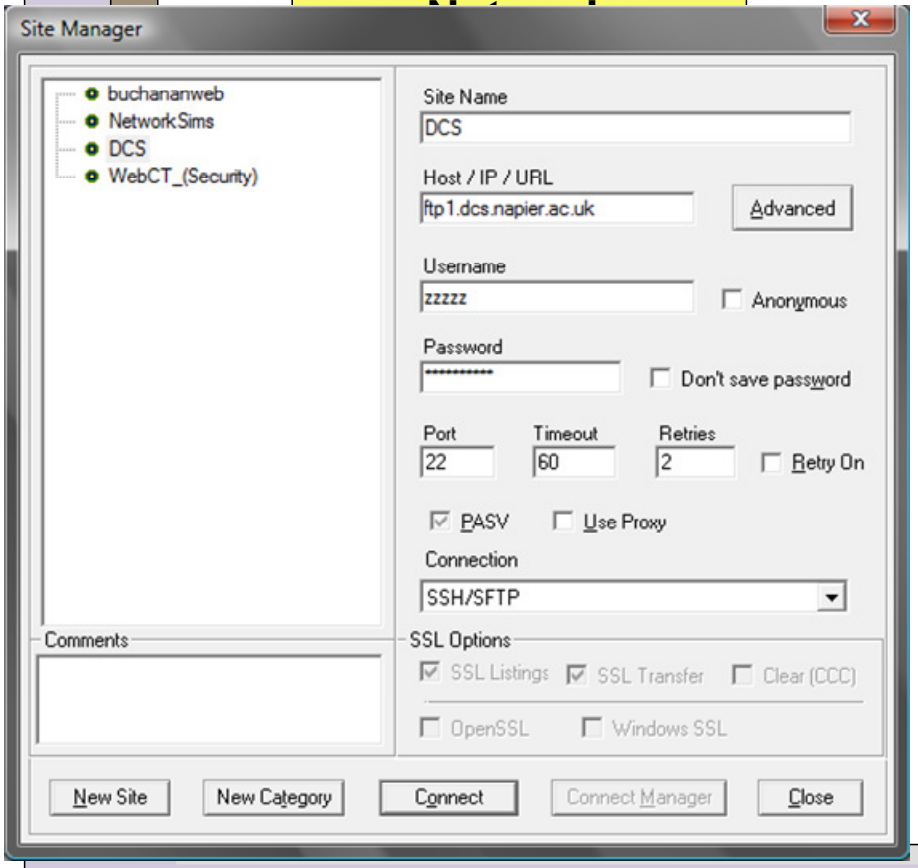
After VPN connection

Network Security

Tunnelling

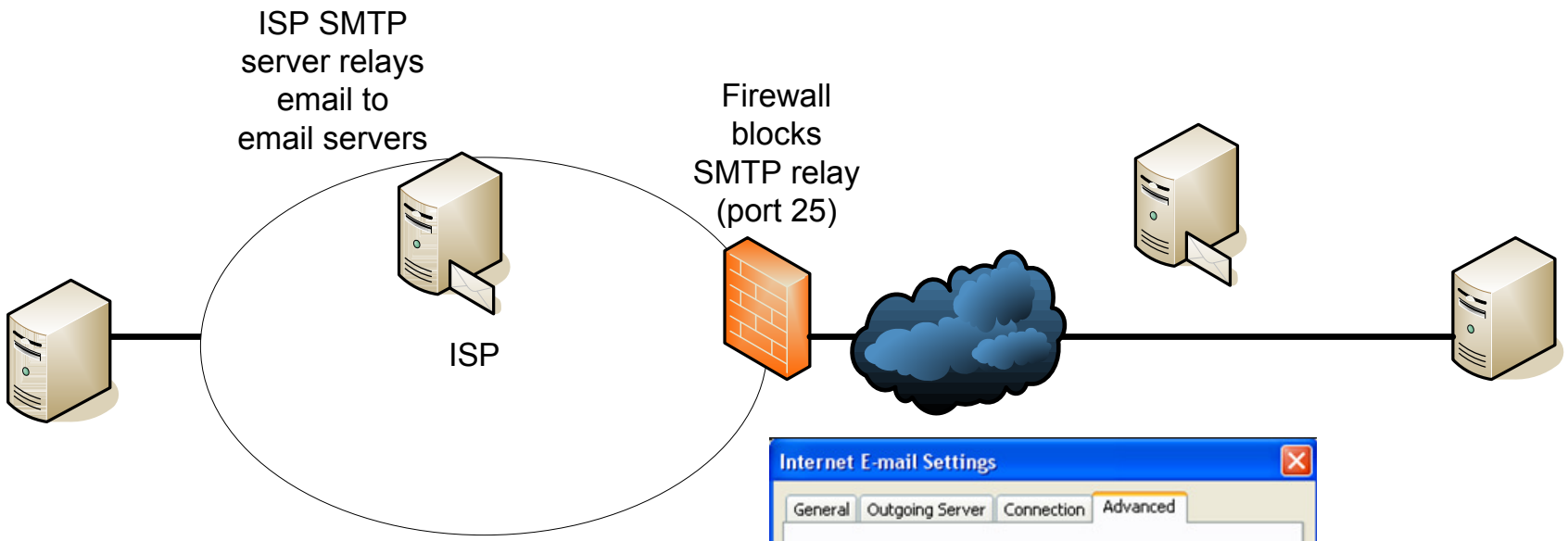
Author: Prof Bill Buchanan

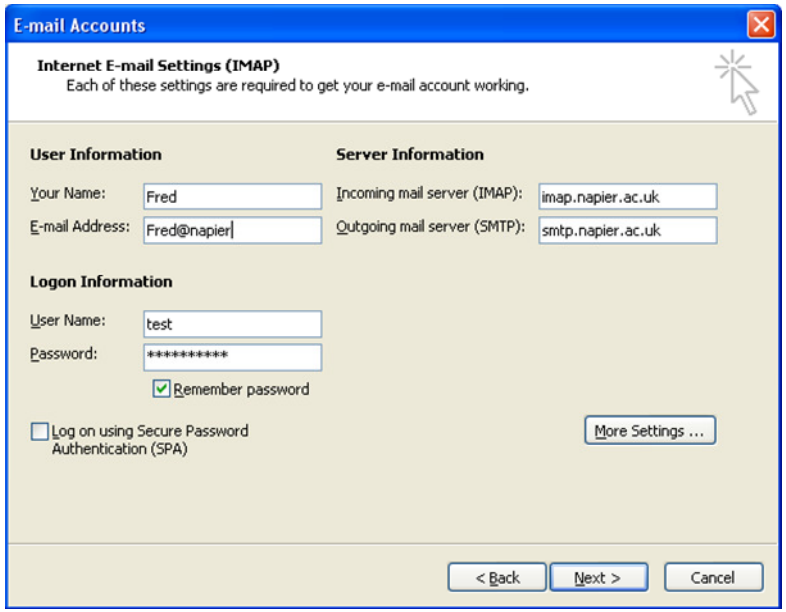

Application Protocol
Application
Secure Socket
SSL
Transport
Transport
Network
Network
Data Link
Data Link
Physical
Tunnelling
Network Security
Secure protocols:
Port: 443. https (HTTP + SSL).
Port: 465. ssmtp (SMTP + SSL).
Port: 563. snntp (NNTP + SSL).
Port: 995. spop (POP-3 + SSL).
Port: 993. simap (IMAP + SSL).
Device
Server
User
ID
One-way server authentication. Server provides authentication to the client, such as SSL (HTTPS, FTPS, etc). Digital certificate required on the server.
Secure Sockets (SSL)

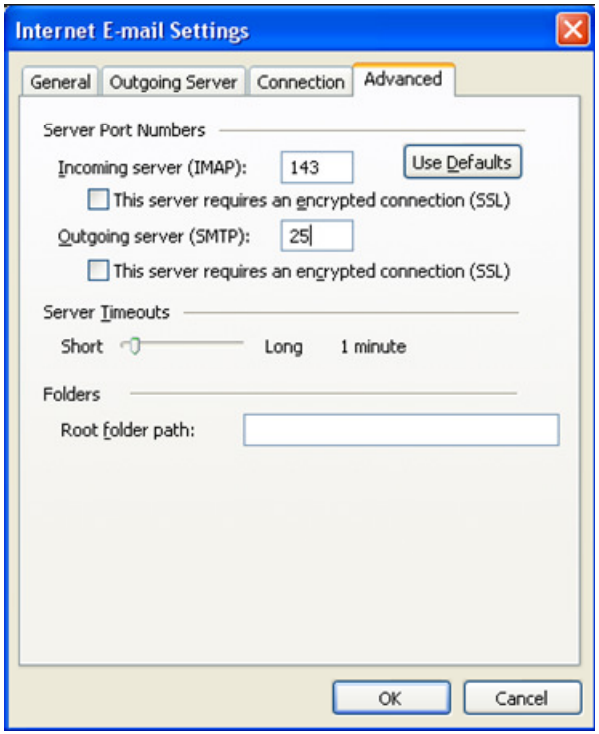


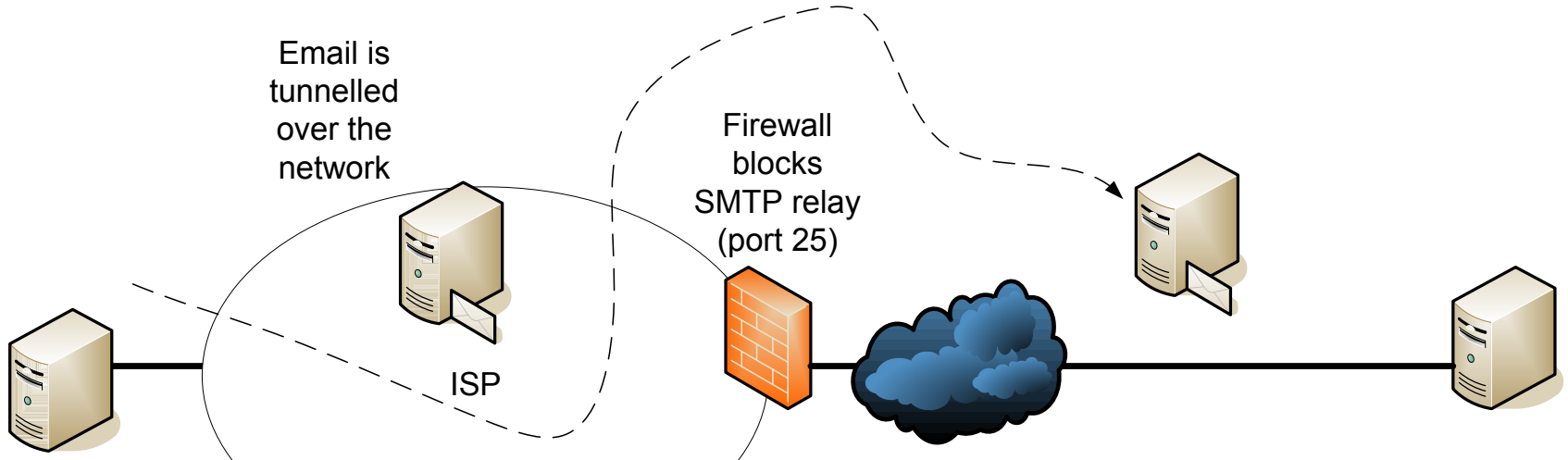

```
Enter Remote Host: ftp1.dcs.napier.ac.uk
Enter Username: zzAA
Enter Password: abcde

Connecting...Details:
MAC-hmac-md5
Port: 22
Cipher: 3des-cbc
Last login: Tue Jan 23 21:15:43 2007 from user-
514da235.l2.c1.dsl.pol.co.uk
Directory: /home/cs72
Tue Jan 23 21:19:30 GMT 2007
socweb1:~> ls
```

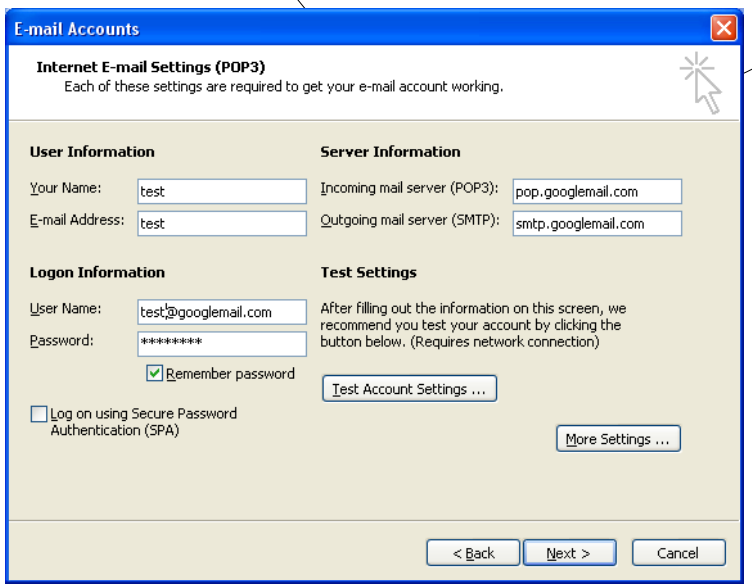
SFTP example

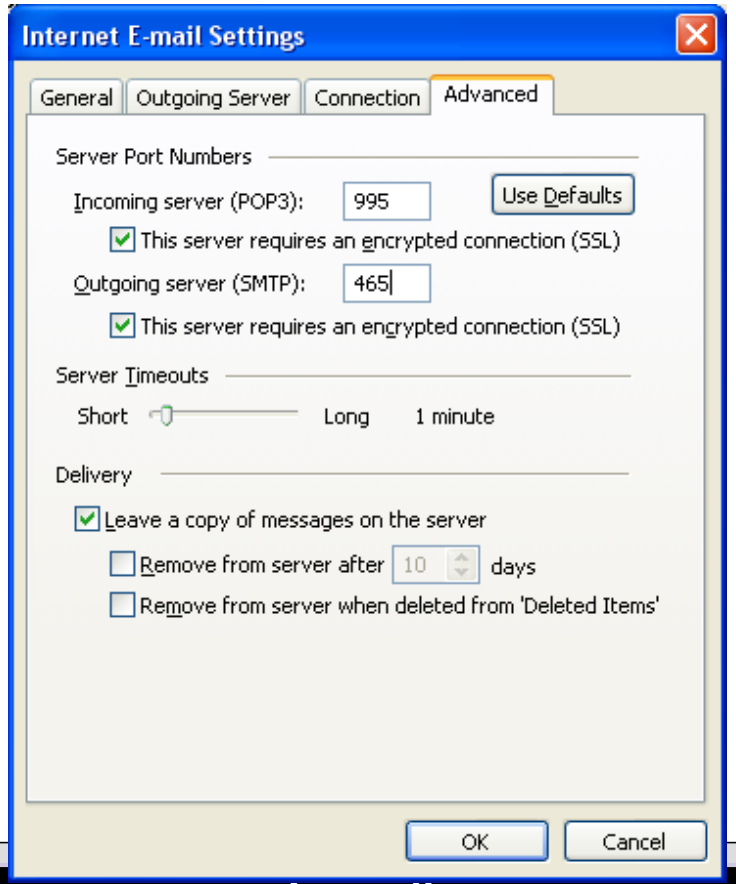

ISP SMTP server relays email to email servers
Firewall blocks SMTP relay (port 25)
ISP


E-mail Accounts
Internet E-mail Settings (IMAP)
Each of these settings are required to get your e-mail account working.
User Information
Your Name: Fred
E-mail Address: Fred@napier
Server Information
Incoming mail server (IMAP): imap.napier.ac.uk
Outgoing mail server (SMTP): smtp.napier.ac.uk
Logon Information
User Name: test
Password: **********
Remember password
Log on using Secure Password Authentication (SPA)
More Settings ...
< Back
Next >
Cancel


Internet E-mail Settings
General
Outgoing Server
Connection
Advanced
Server Port Numbers
Incoming server (IMAP): 143
Use Defaults
This server requires an encrypted connection (SSL)
Outgoing server (SMTP): 25
This server requires an encrypted connection (SSL)
Server Timeouts
Short
Long
1 minute
Folders
Root folder path:
OK
Cancel

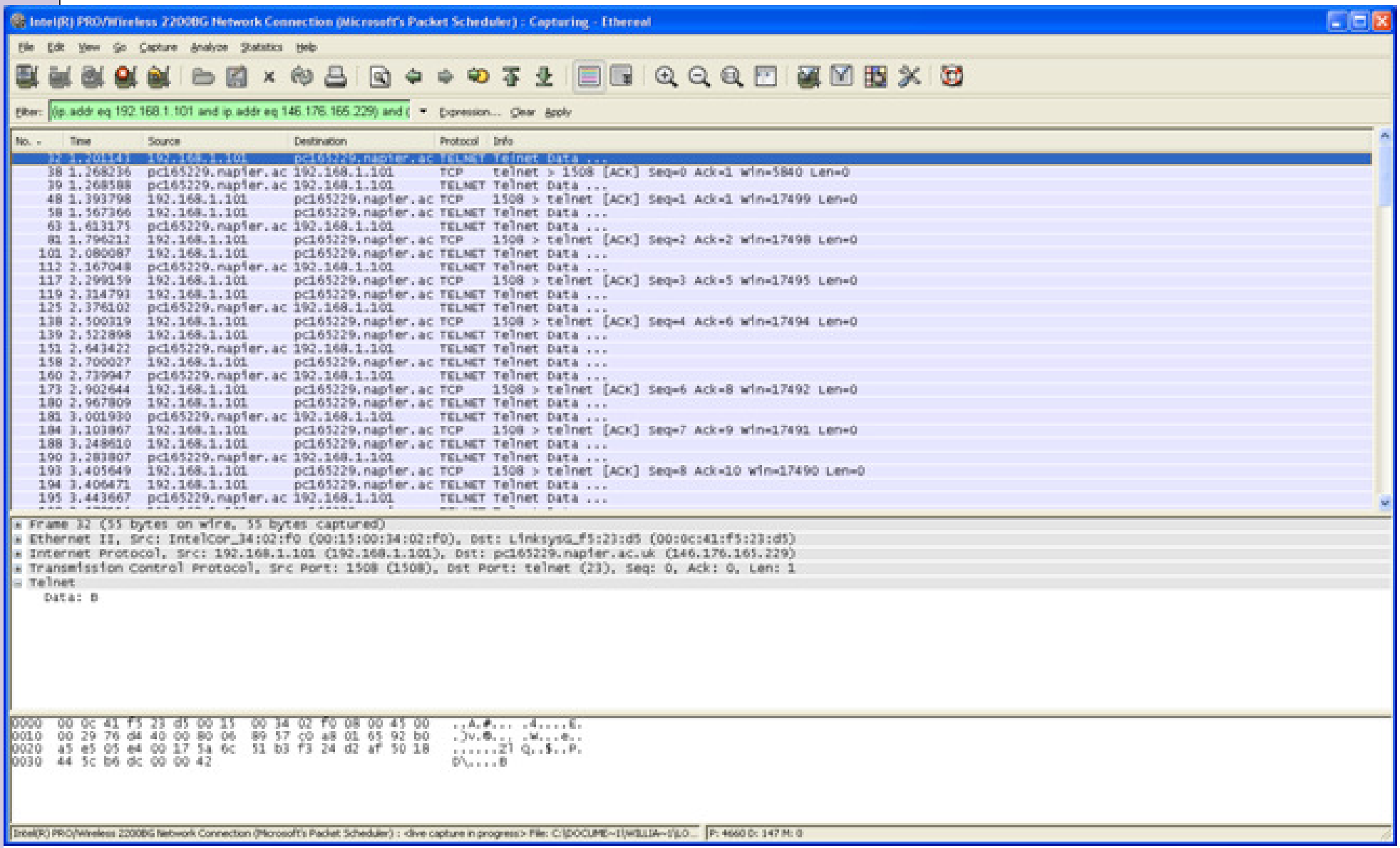






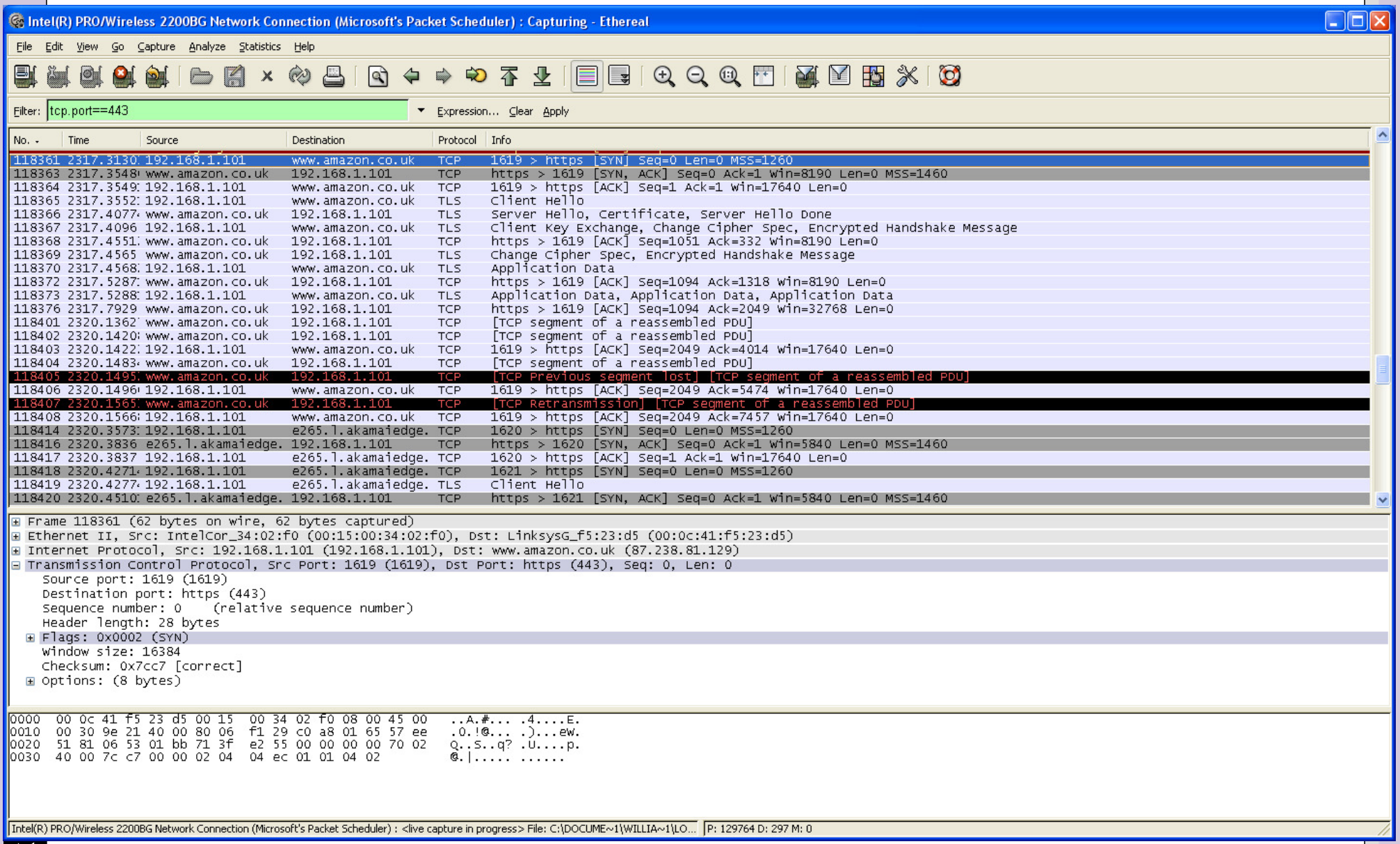
Secure protocols:

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).



Networ

Problem - TELNET



Network

HTTPS Example

Network Security

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

Author: Prof Bill Buchanan