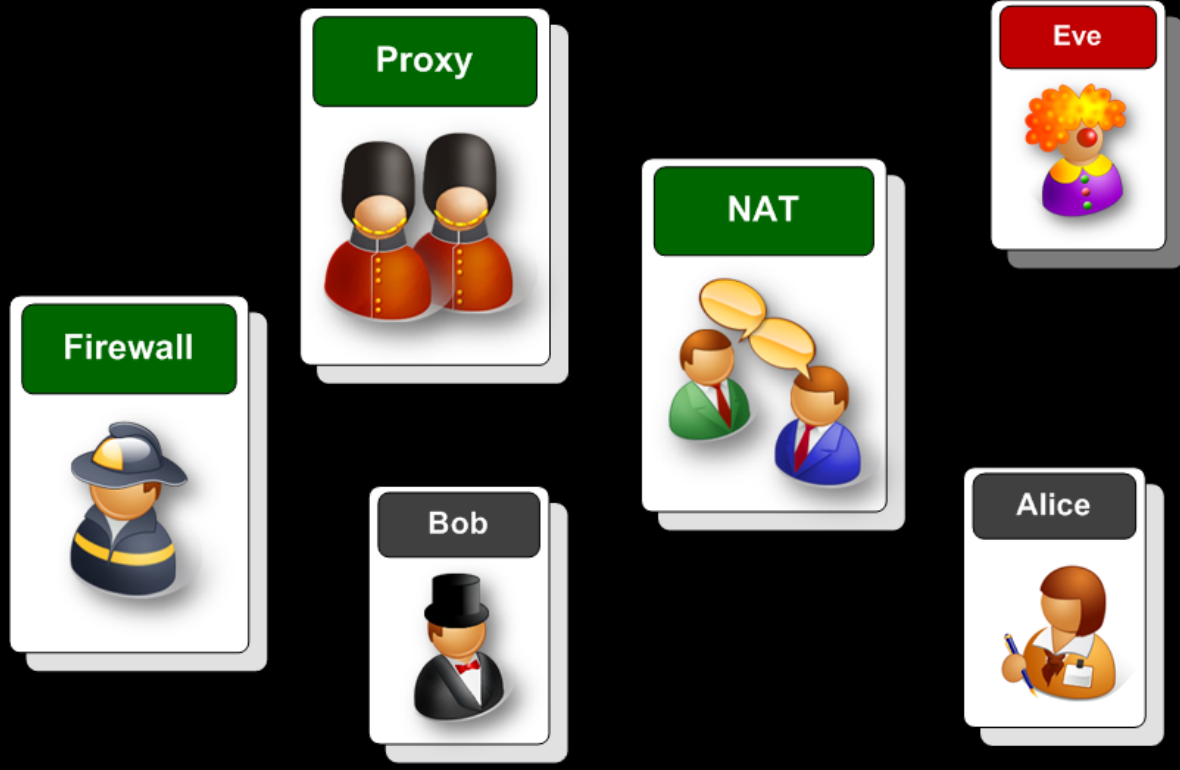
FIREWALLS

INTRODUCTION



Perimeter Security
Firewall Fundamentals
Types of Firewall Implementation

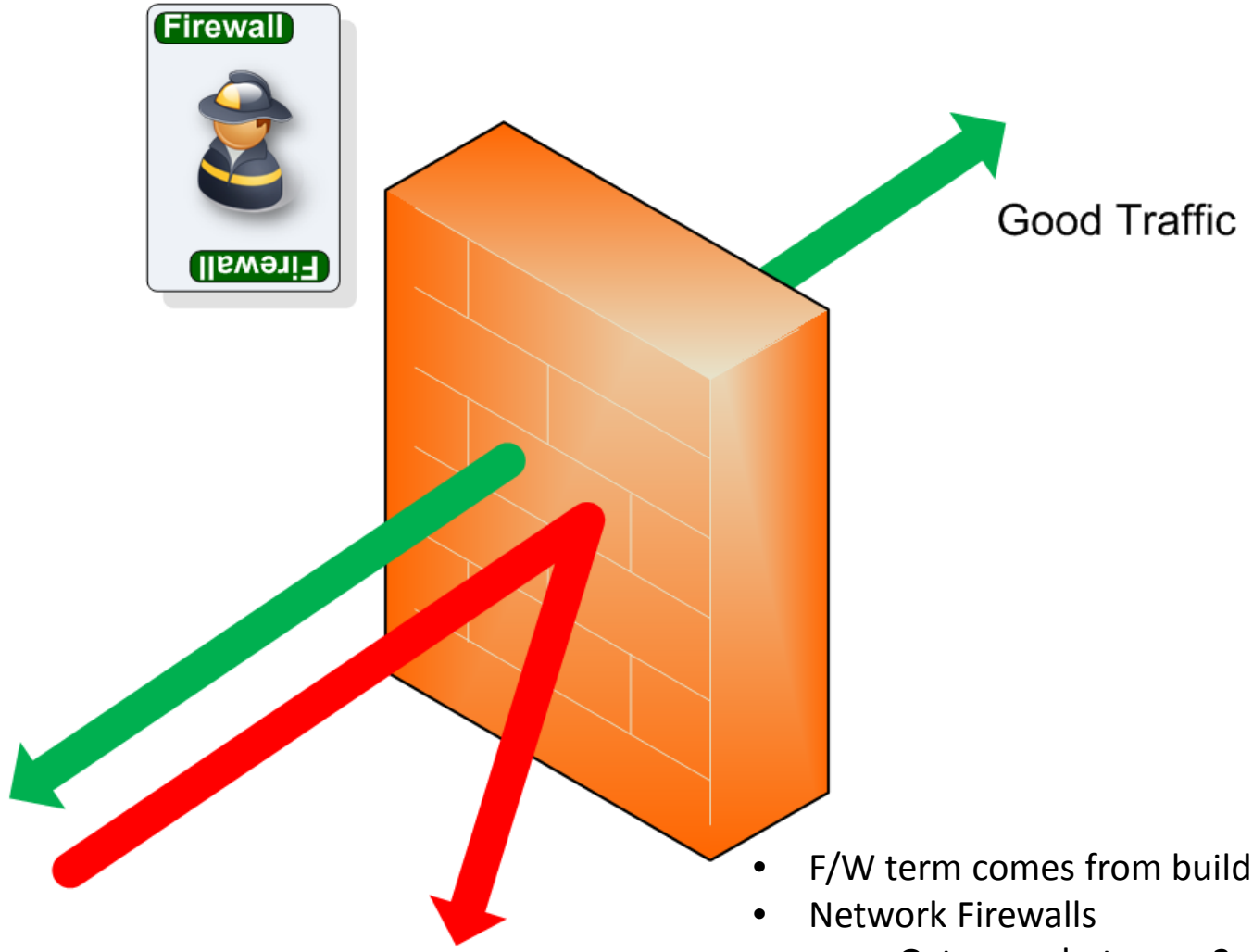
INTRODUCTION

Author: Rich Macfarlane

Perimeter Security

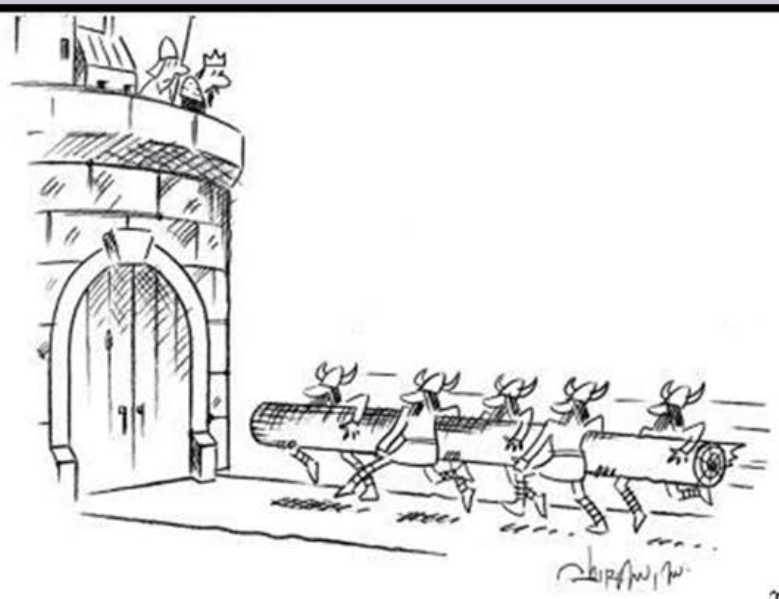
Why Firewalls?

- Mitigate Risks
  - Mitigate threats to assets from known vulnerabilities
  - Reduce services open to Internet
  - Mitigate trust attacks
- Segregation/Privacy
  - Segregate organisational traffic from Internet
  - Hide organisations assets, systems/services from attackers
    - Harder to perform reconnaissance
- Apply Organisation's Security Policy
  - Create choke points that traffic has to pass through – perimeter and internal – apply filtering
- Monitoring
  - Logging traffic passing through for analysing attacks



- F/W term comes from buildings
- Network Firewalls
  - Gateways between 2 networks
  - Allow **Good** traffic to pass
  - Reject **Bad** traffic

Author: Rich Macfarlane



"Is that the firewood we ordered or are we under siege?"

"I hate cold calls."

Author: Rich Macfarlane

Firewall is like a medieval castle gate

- Walls funnel people to the gate
- Guard on the gate - decides who passes through
- Choke point – all traffic should pass here

- Firewall built into most OS

- Routers with firewalling S/w running
- Proxy/Application Firewalls – firewalling specific applications

Personal S/W Firewall

Internet

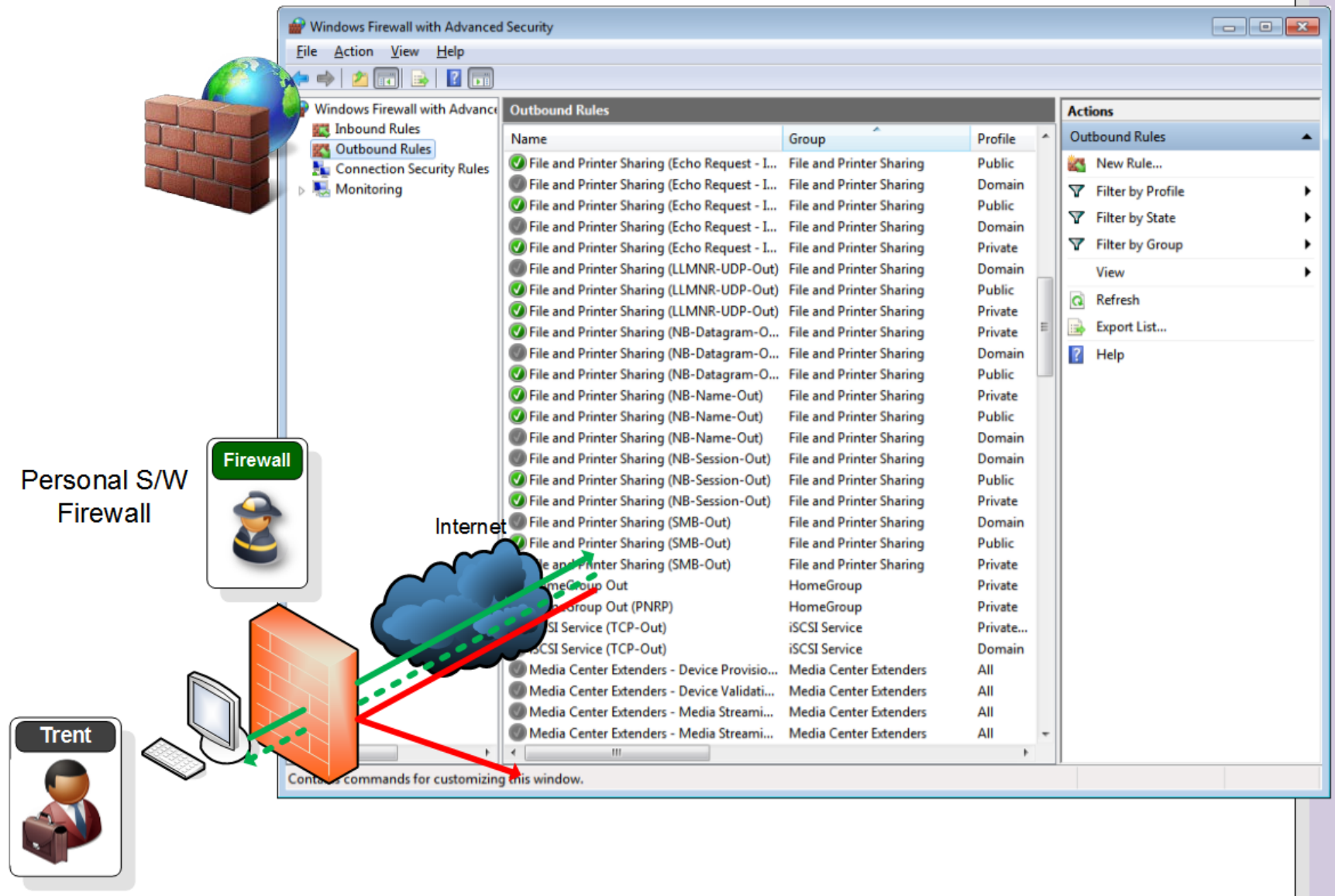
IPtables

Device-based H/W Firewall

Server-based S/W Firewall

- Hardware firewalling
- Custom OS/Hardware

Author: Rich Macfarlane

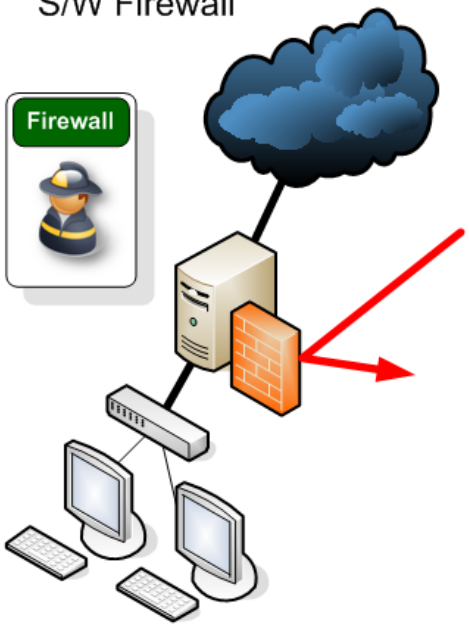


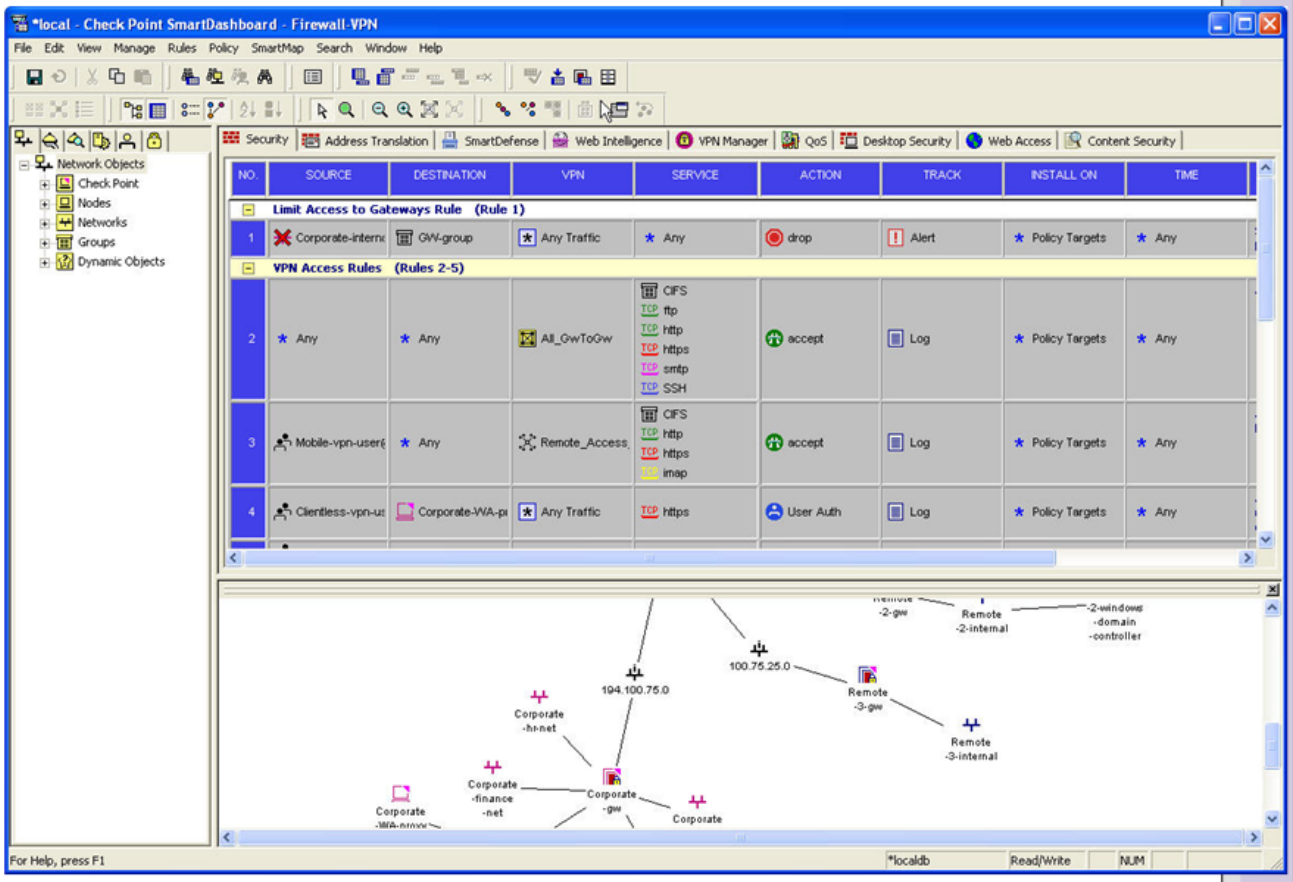
Q. Where is the perimeter f/w(s) implemented?

Author: Rich Macfarlane

Check Point®
SOFTWARE TECHNOLOGIES LTD.

Server-based
S/W Firewall

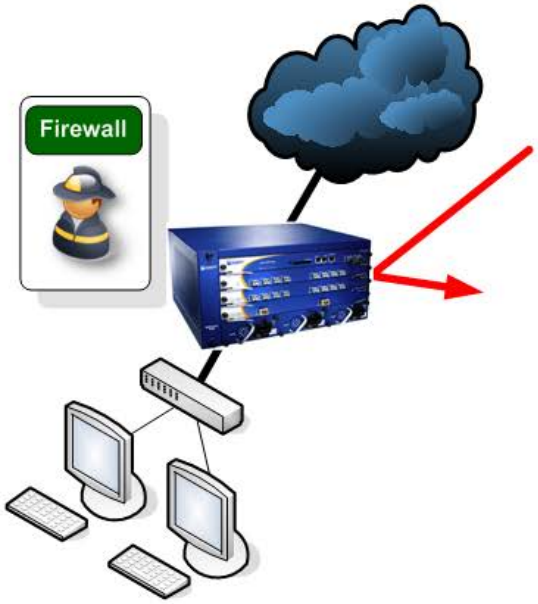


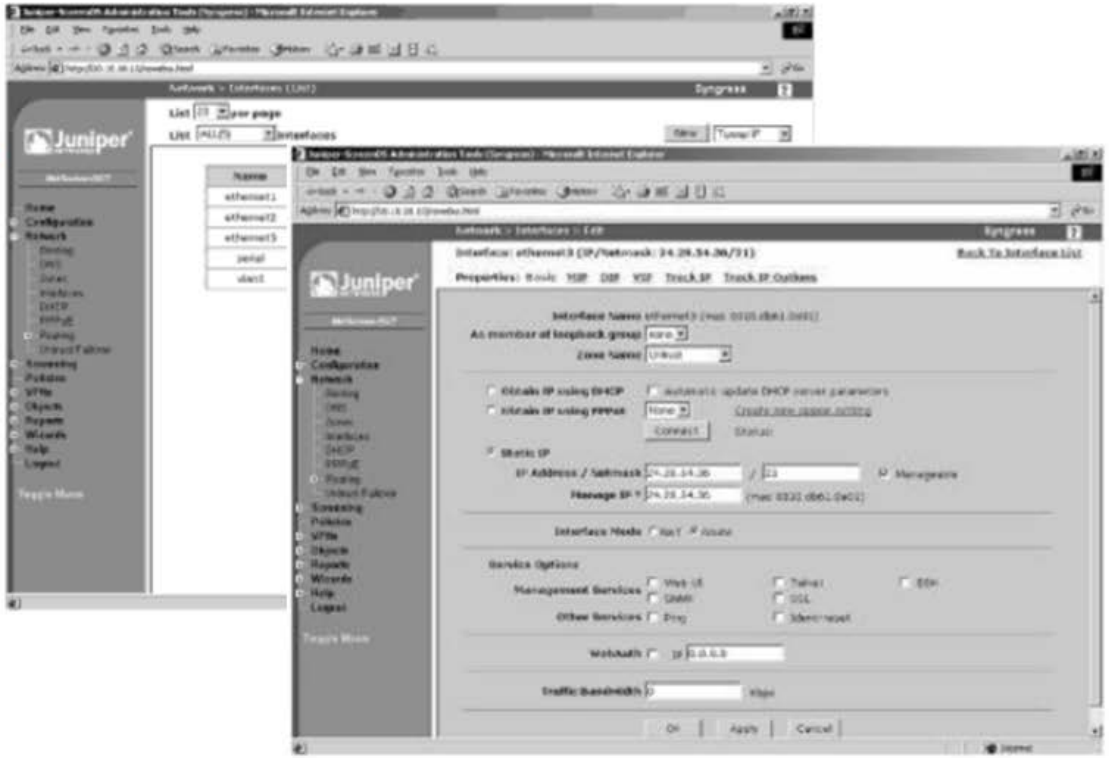


Author: Rich Macfarlane

```
-> unset interface untrust manage ping
-> unset interface untrust manage snmp
-> unset interface untrust manage telnet
-> set interface untrust manage ssh
-> set interface untrust manage web
-> set interface untrust manage ssl
```

Appliance-based
S/W Firewall





Author: Rich Macfarlane

Check Point
SOFTWARE TECHNOLOGIES LTD.

IPtables

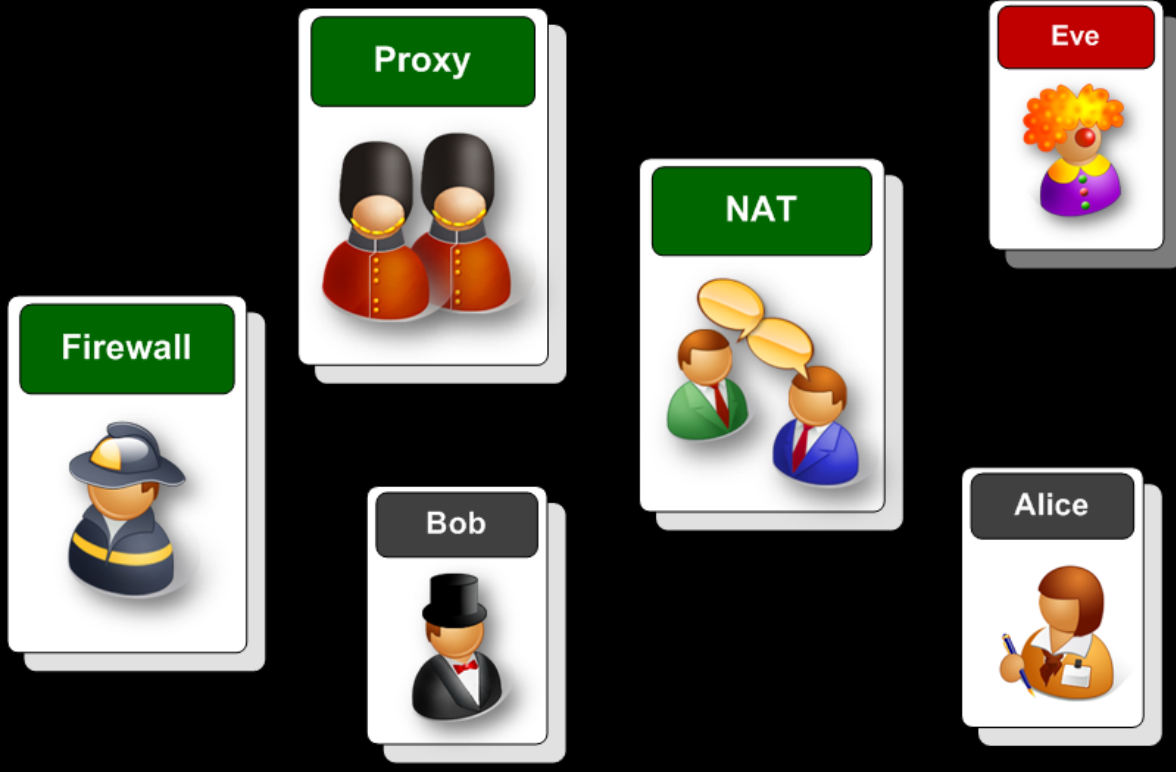
Internet Security & Acceleration Server 2004
Standard Edition

	 H/W Firewall	 S/W Firewall
Configuration	Complex	Easier
Performance	Faster – Optimised H/w	Generally Slower
Device Security	Good - Hardened OS	General OS – Needs Hardened
Cost	Higher	Lower

Author: Rich Macfarlane

Hardware vs Software Firewalls

FIREWALLS | CONCEPTS

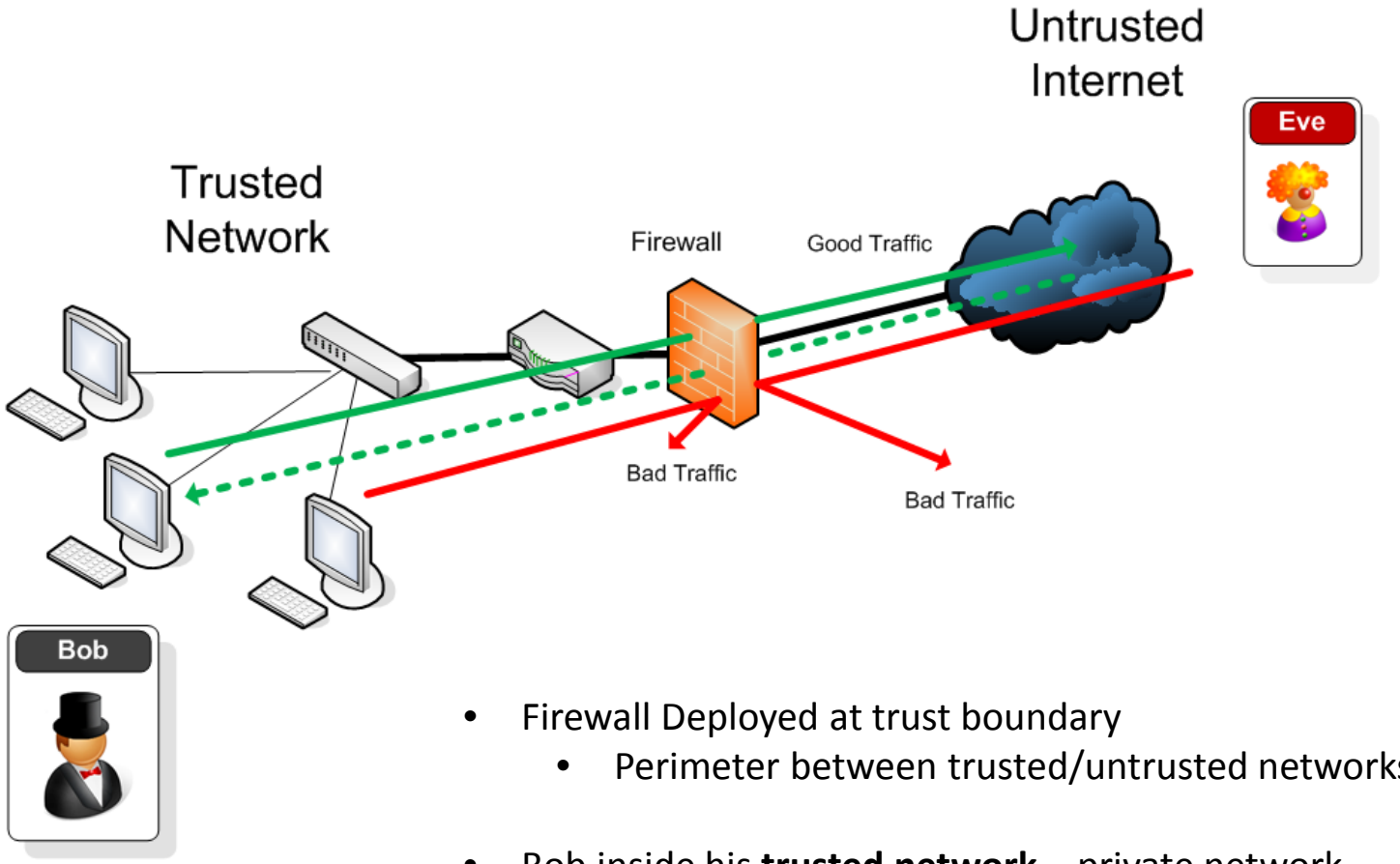


Trusted/Untrusted Networks
Perimeters
Firewall Capabilities

| CONCEPTS

Author: Rich Macfarlane

Trusted & Untrusted Network – Perimeter Between

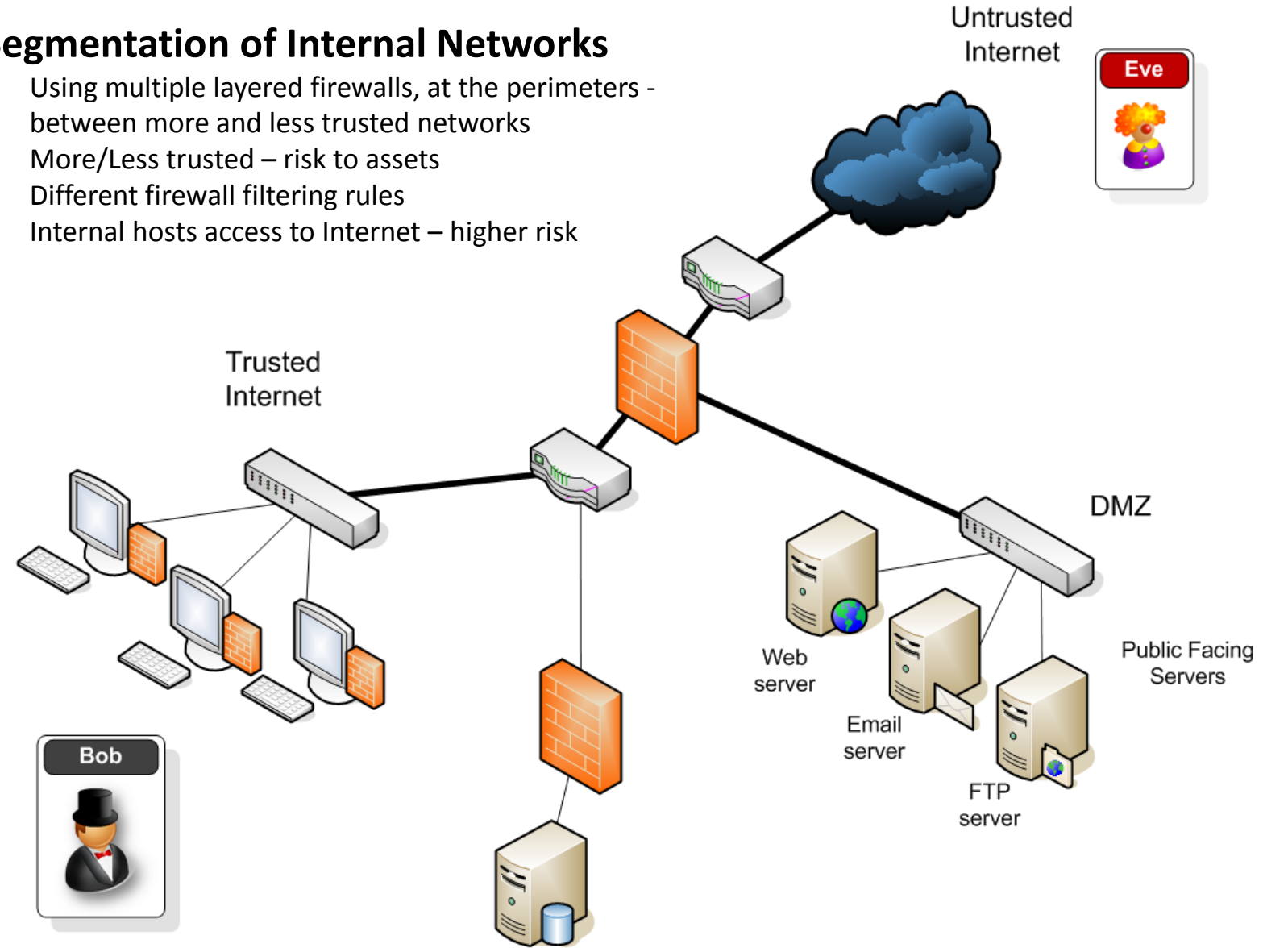


- Firewall Deployed at trust boundary
  - Perimeter between trusted/untrusted networks
- Bob inside his **trusted network –** private network connected to the Internet
  - Under Bobs organisations control
- Eve out on the Internet – the **untrusted network**

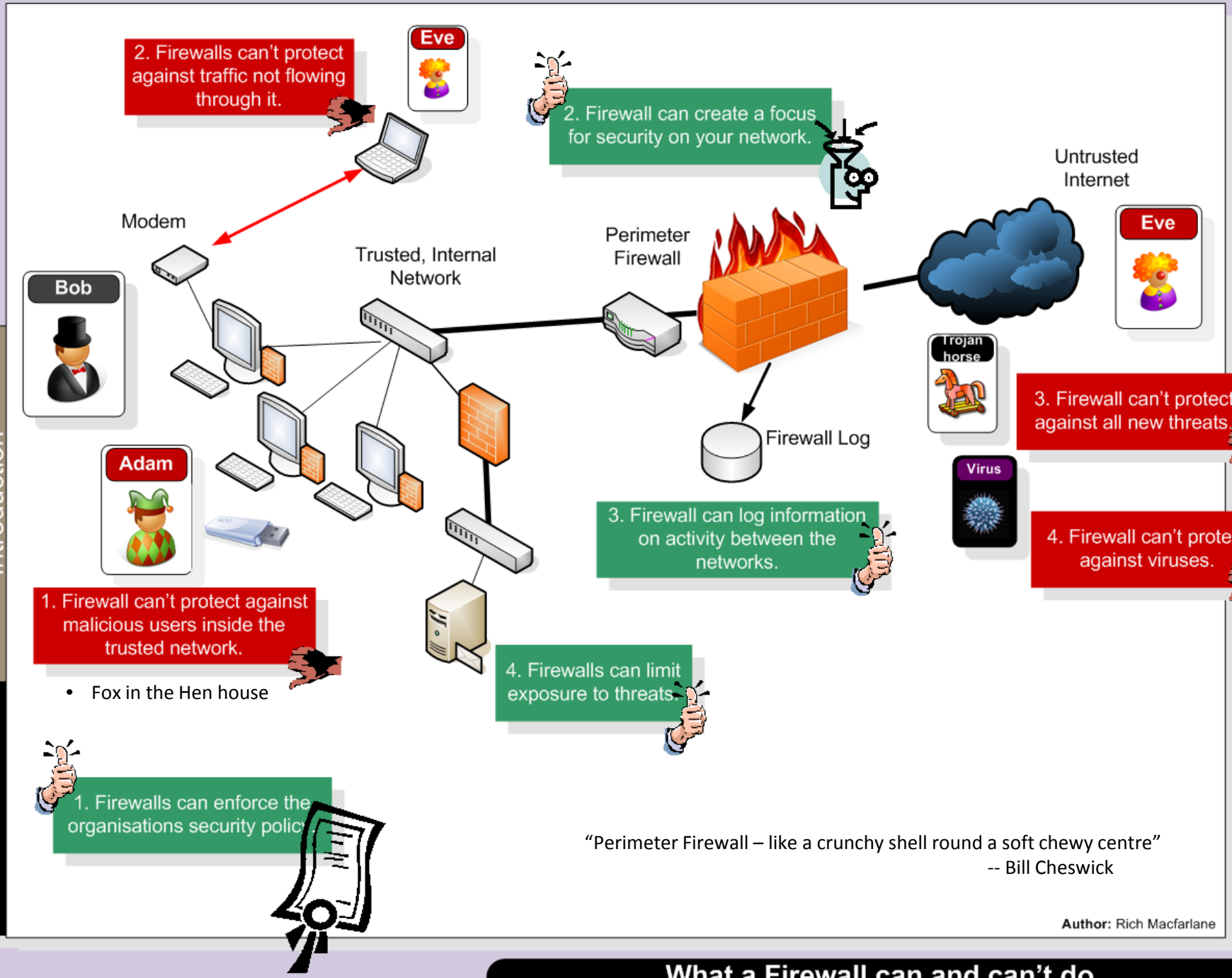
Author: Rich Macfarlane

Segmentation of Internal Networks

- Using multiple layered firewalls, at the perimeters - between more and less trusted networks
- More/Less trusted – risk to assets
- Different firewall filtering rules
- Internal hosts access to Internet – higher risk



Author: Rich Macfarlane



"Perimeter Firewall – like a crunchy shell round a soft chewy centre"
-- Bill Cheswick

Author: Rich Macfarlane

What a Firewall can and can't do

FIREWALLS | TOPOLOGIES

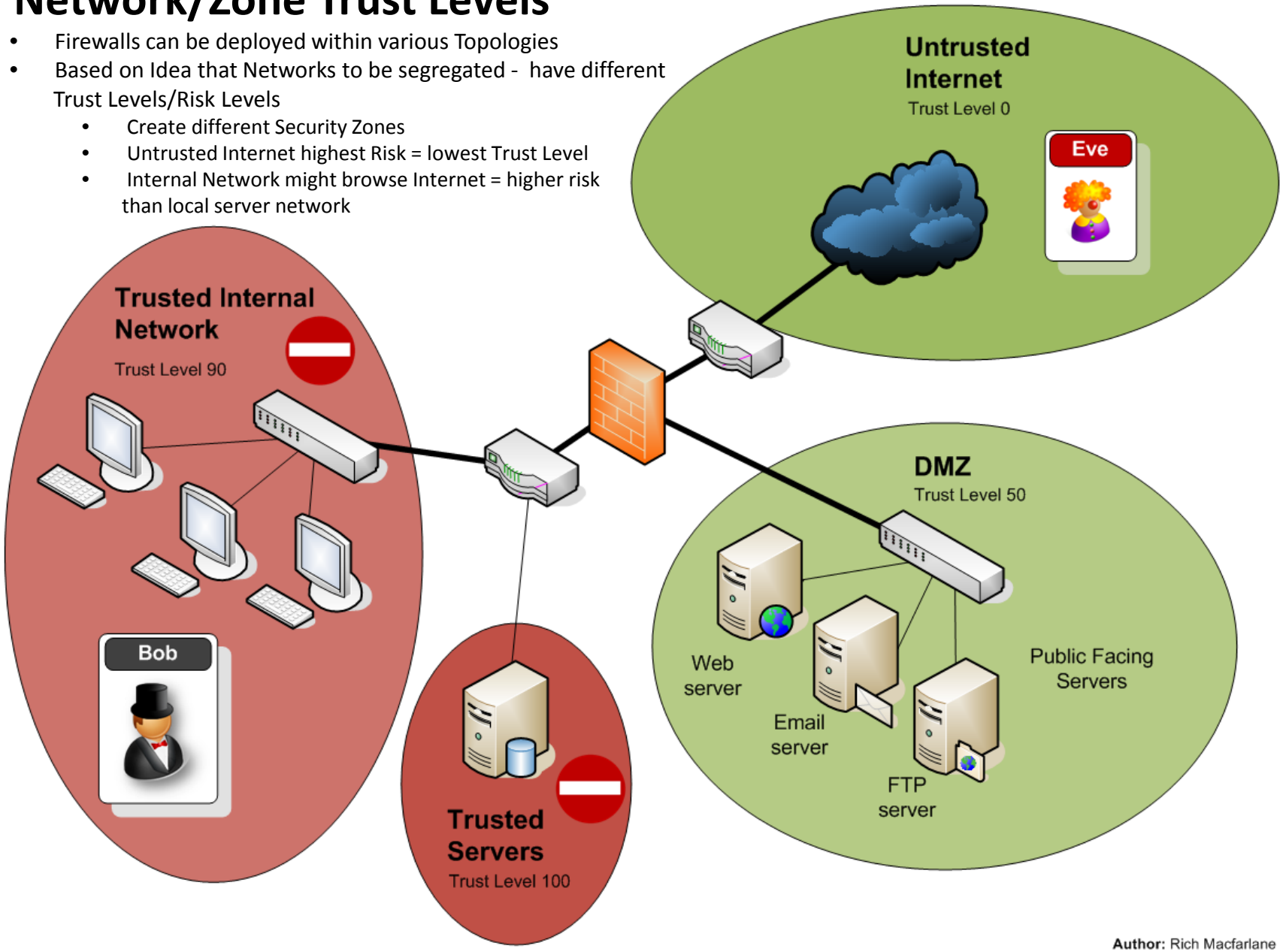
Security Zones
Firewall Topologies
Firewall Traffic Flows

| TOPOLOGIES

Author: Rich Macfarlane

Network/Zone Trust Levels

- Firewalls can be deployed within various Topologies
- Based on Idea that Networks to be segregated - have different Trust Levels/Risk Levels
  - Create different Security Zones
  - Untrusted Internet highest Risk = lowest Trust Level
  - Internal Network might browse Internet = higher risk than local server network



Author: Rich Macfarlane

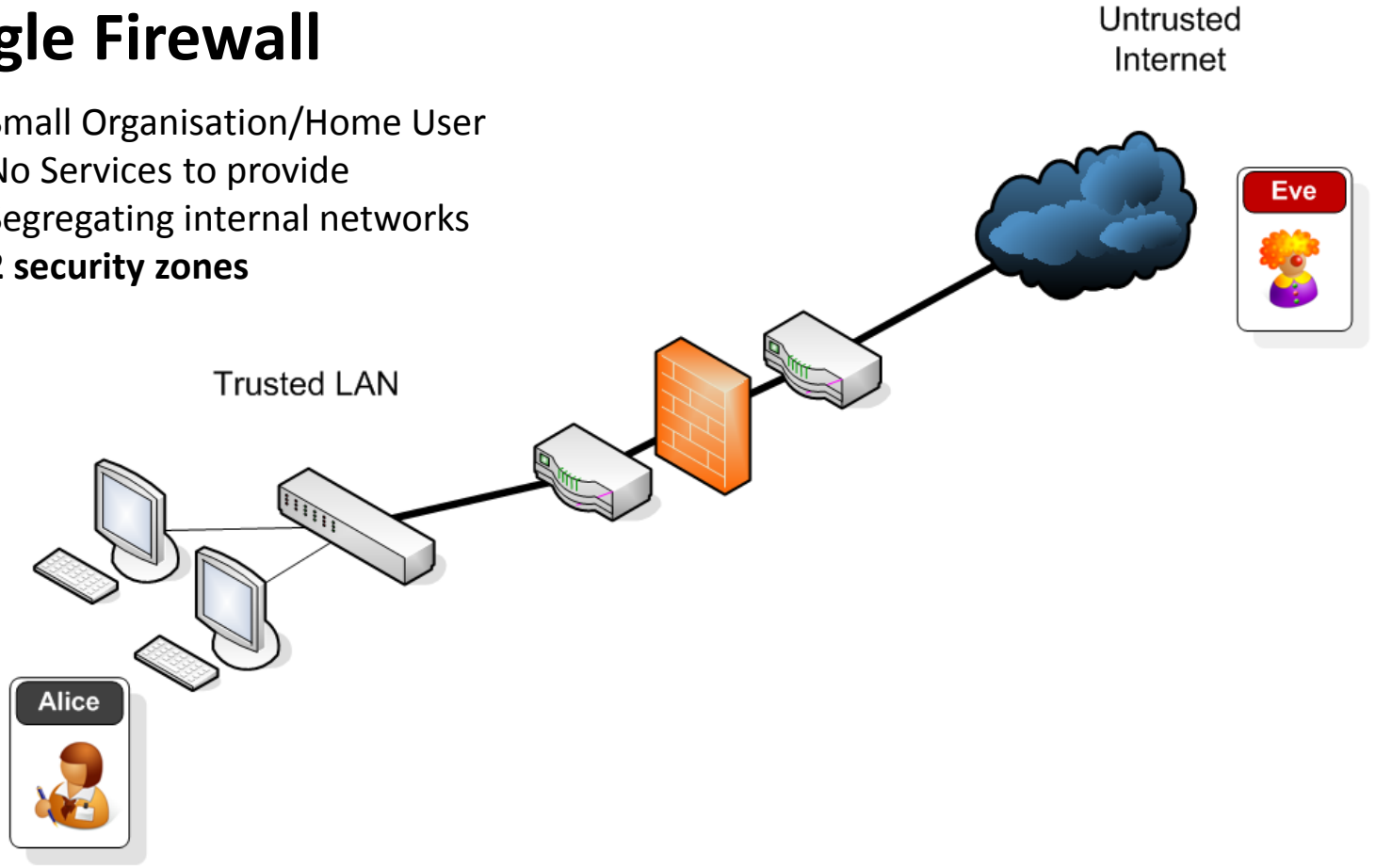
Firewall Topologies

Firewalls

Firewall Deployment Topologies

Single Firewall

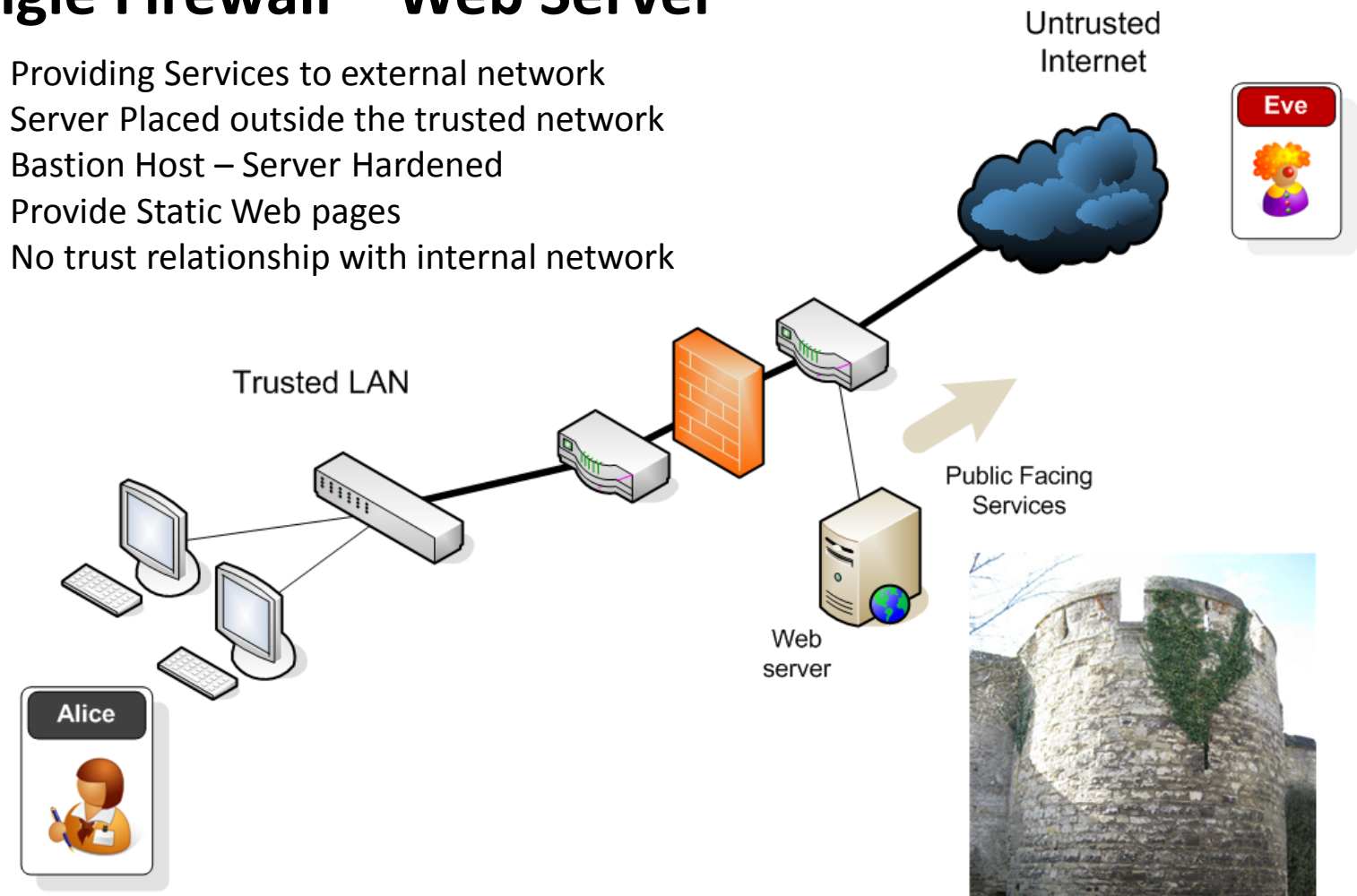
- Small Organisation/Home User
- No Services to provide
- Segregating internal networks
- **2 security zones**



Author: Rich Macfarlane

Single Firewall – Web Server

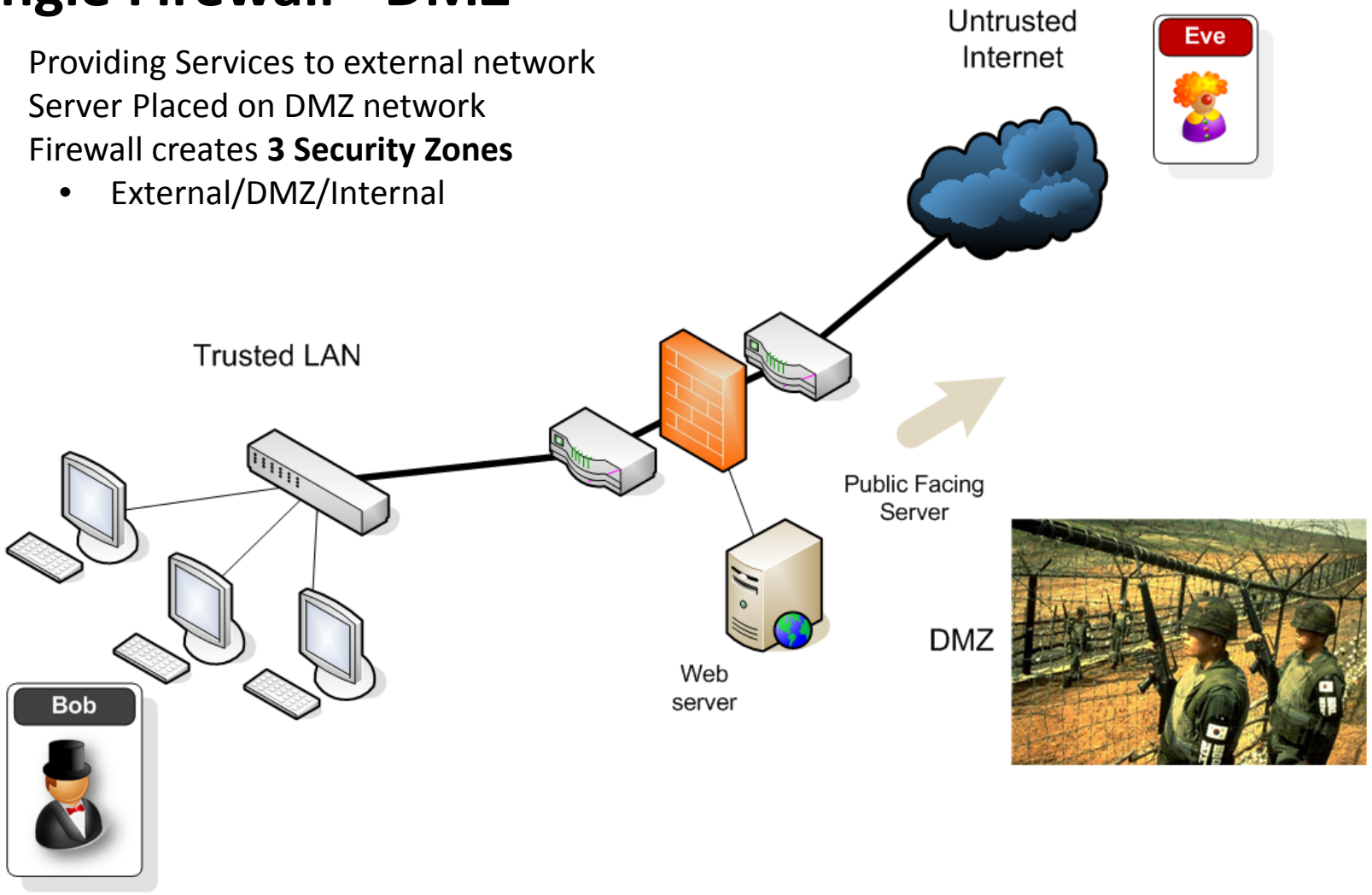
- Providing Services to external network
- Server Placed outside the trusted network
- Bastion Host – Server Hardened
- Provide Static Web pages
- No trust relationship with internal network



Author: Rich Macfarlane

Single Firewall - DMZ

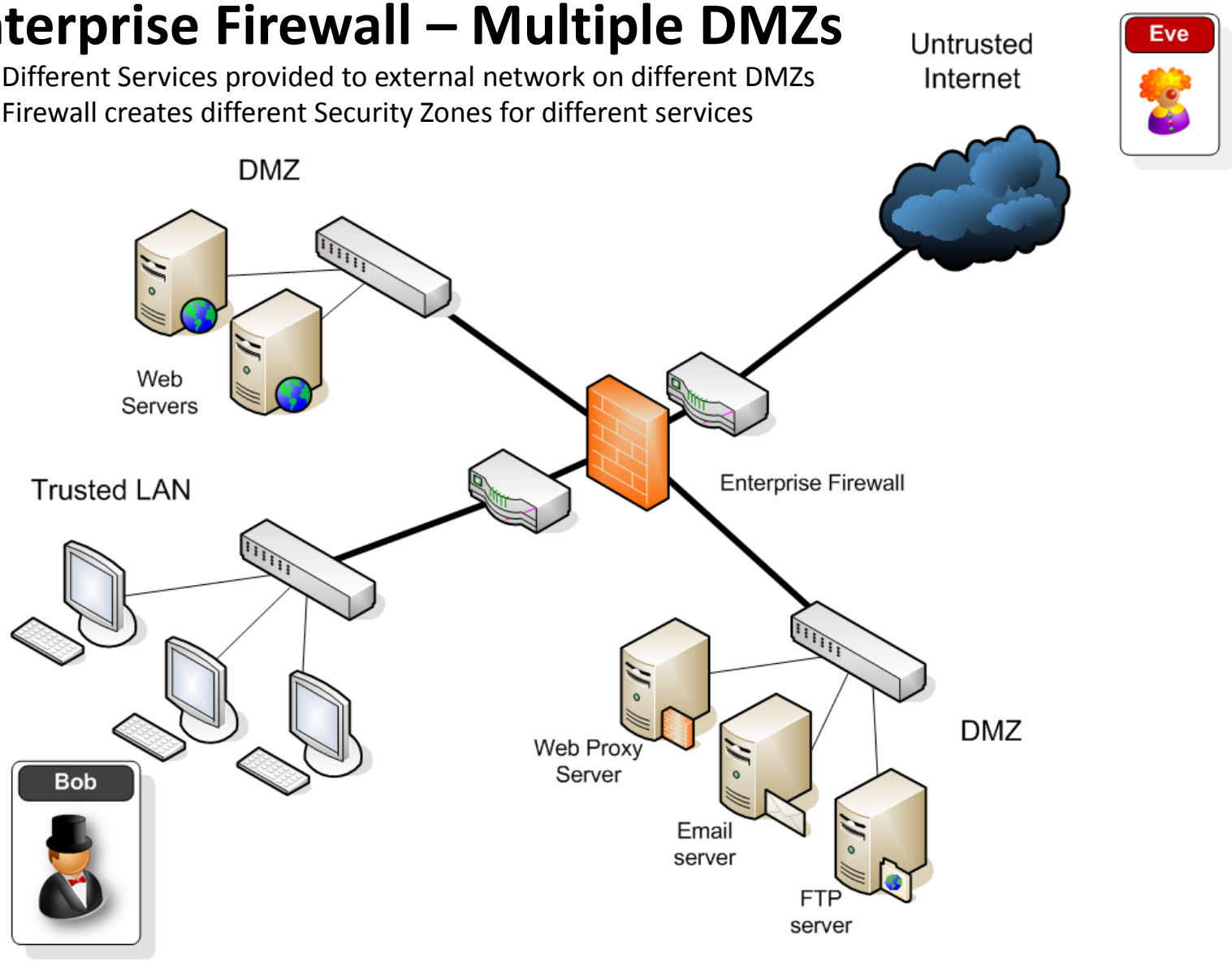
- Providing Services to external network
- Server Placed on DMZ network
- Firewall creates **3 Security Zones**
  - External/DMZ/Internal



Author: Rich Macfarlane

Enterprise Firewall – Multiple DMZs

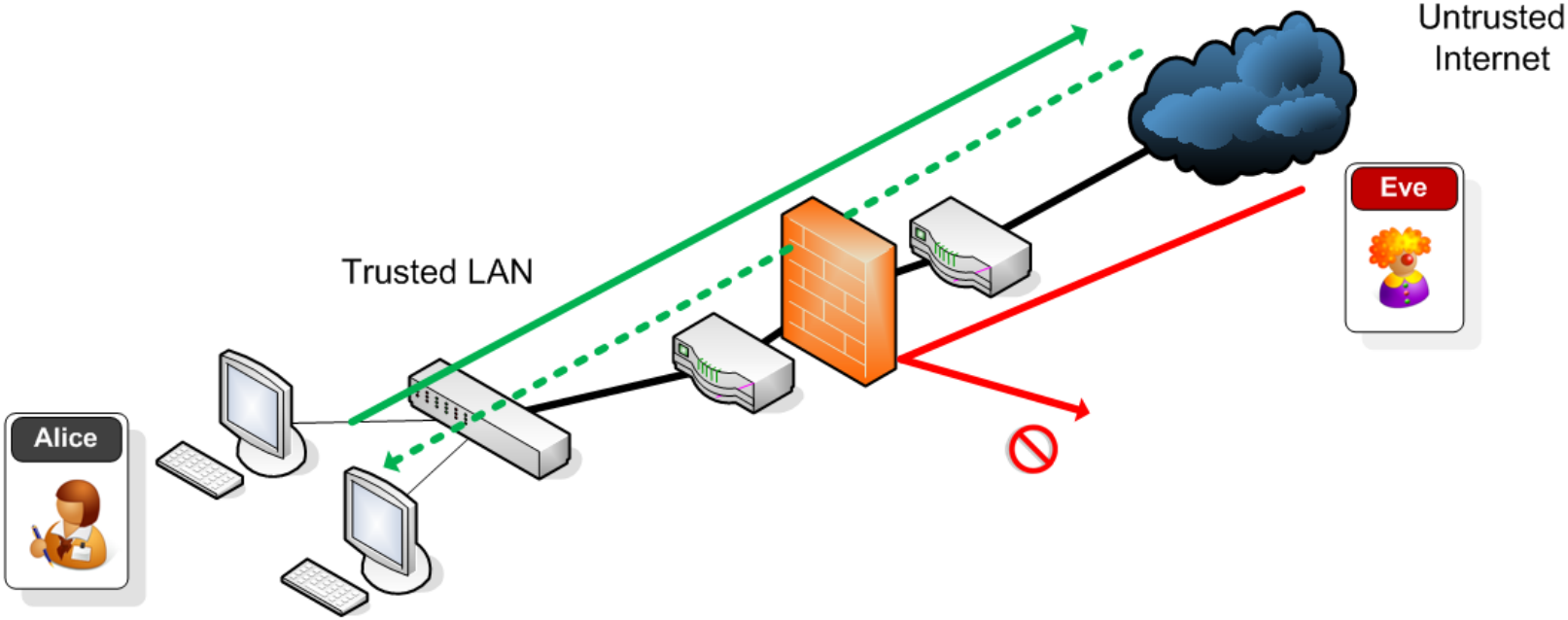
- Different Services provided to external network on different DMZs
- Firewall creates different Security Zones for different services



Author: Rich Macfaralne

Firewall Traffic Flows

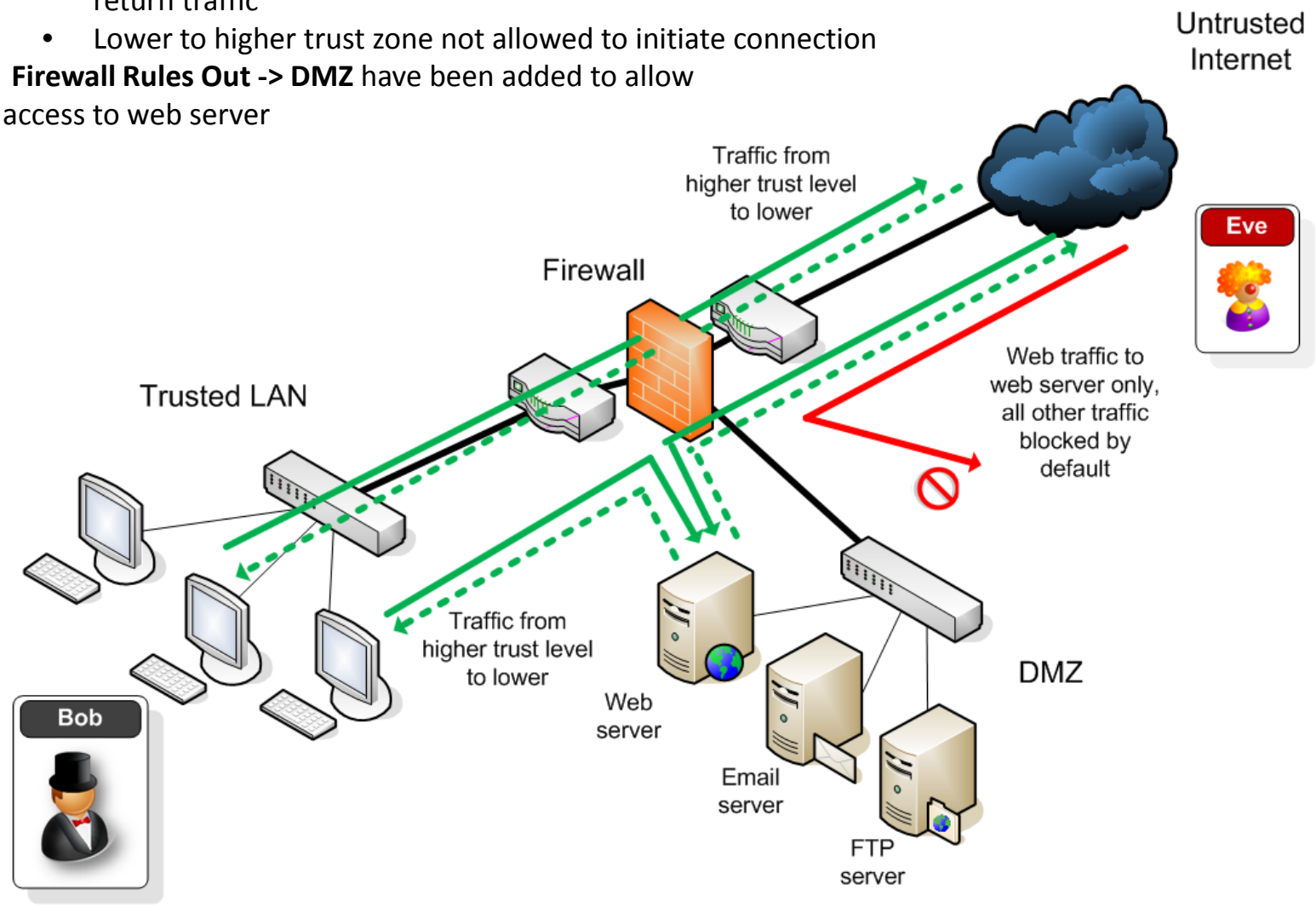
- Understand traffic flows through firewalls
- Based on security zones/firewall implementations



- Typically **default** is only Higher trust zone to lower allowed to initiate connection
  - Stateful also allows return traffic
- Lower to higher trust zone not allowed to initiate connection – packets dropped
  - Windows Firewall – lab problems – Ping from GNS3 Router to local host
    - Allows ICMP out + return traffic
    - Drops ICMP by default incoming

Author: Rich Macfaralne

- **Default Rules** the same:
  - Higher trust zone to lower allowed to initiate connection + allows return traffic
  - Lower to higher trust zone not allowed to initiate connection
- **Firewall Rules Out -> DMZ** have been added to allow access to web server



Author: Rich Macfaralne

Firewall DMZ Traffic Flow

FIREWALLS | ARCHITECTURES

Packet Filtering Firewalls

Stateful Firewalls
Application Inspection Firewalls
Application Proxy Firewalls
Hybrid Firewalls

Author: Rich Macfarlane

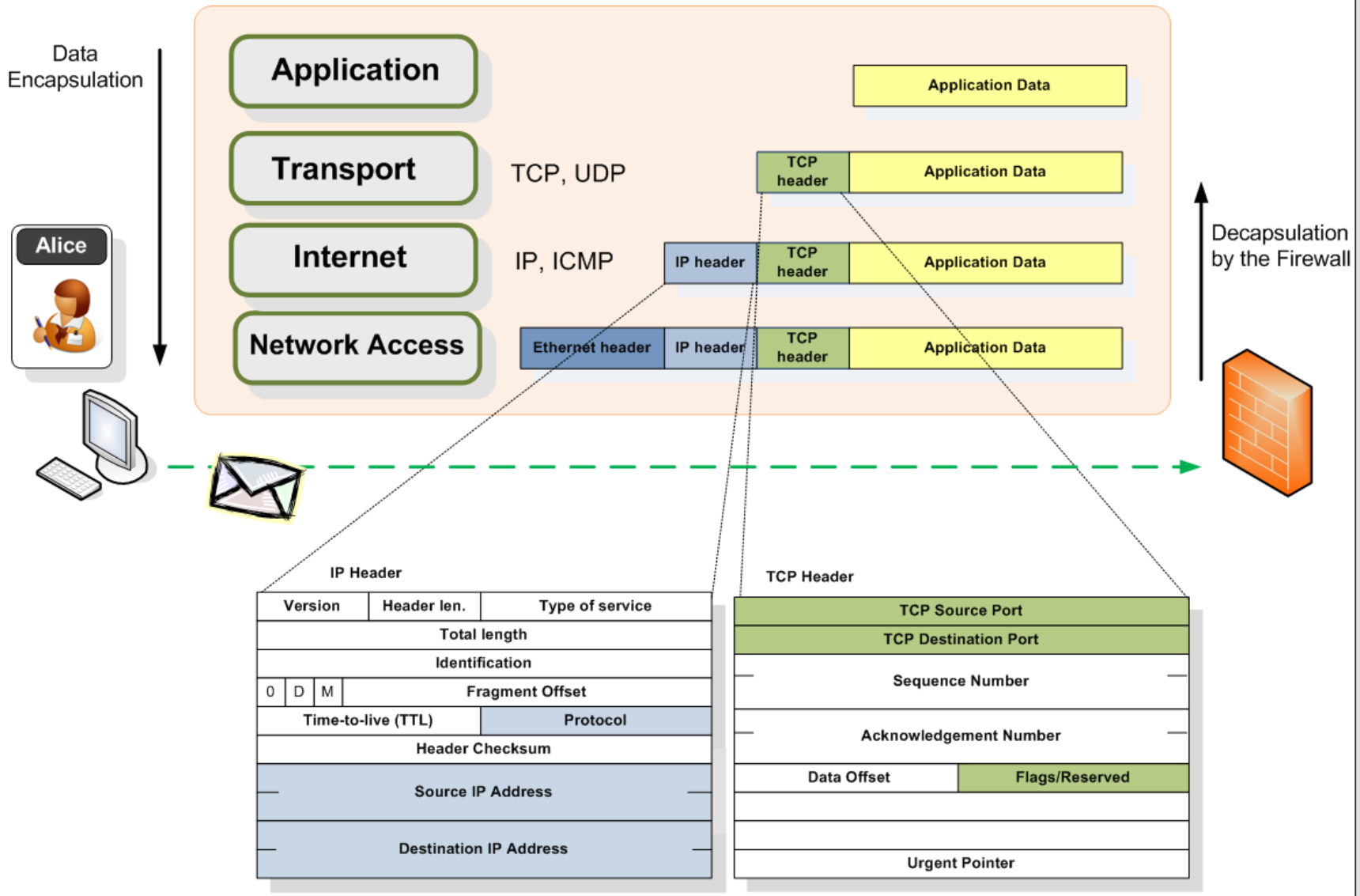
Packet Filtering

Stateless Packet Filtering

- Oldest/most basic filtering firewalls
  - Easily deployed on existing routers – Cisco in lab
  - Cheap
- Very fast
  - Only examine lower network layer headers IP/TCP
  - Can handle simplest filtering efficiently
- Each packet examined/filtered individually
  - No concept of connection state
  - Easy to bypass by attackers
    - Attacker can spoof connected state by crafting packet
- Data Content of Packet not examined

- Can be used in front of more advanced firewalls

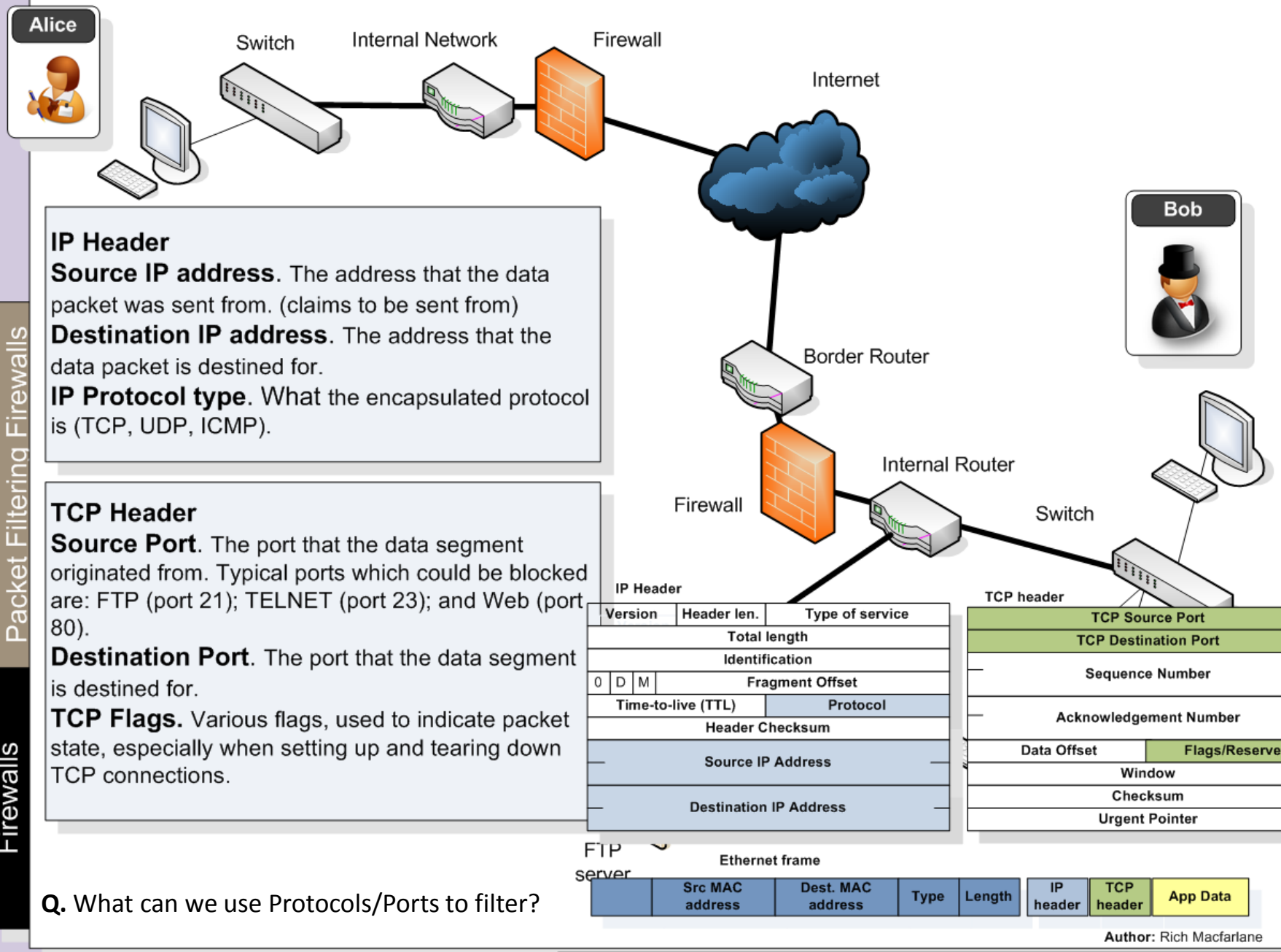
Firewalls are routers - de-capsulate packets + compare IP/TCP header values to rules



Packet Filtering Done on Layers 3 & 4

Q. What could **IP Addresses** be used to filter?

Author: Rich Macfarlane



IP Header

Source IP address. The address that the data packet was sent from. (claims to be sent from)

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

IP Protocol type. What the encapsulated protocol is (TCP, UDP, ICMP).

TCP Header

Source 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 Port. The port that the data segment is destined for.

TCP Flags. Various flags, used to indicate packet state, especially when setting up and tearing down TCP connections.

Q. What can we use Protocols/Ports to filter?

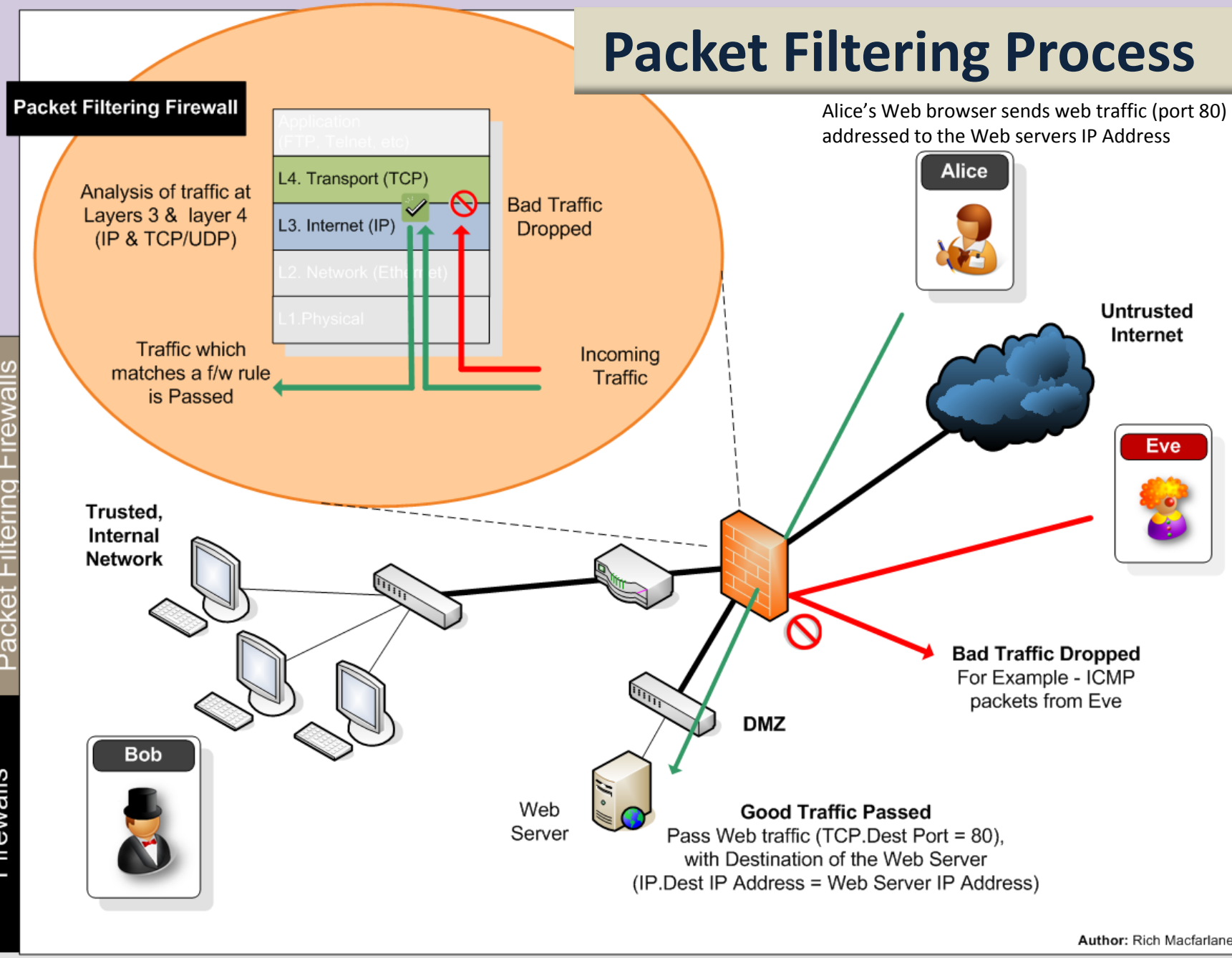
Author: Rich Macfarlane

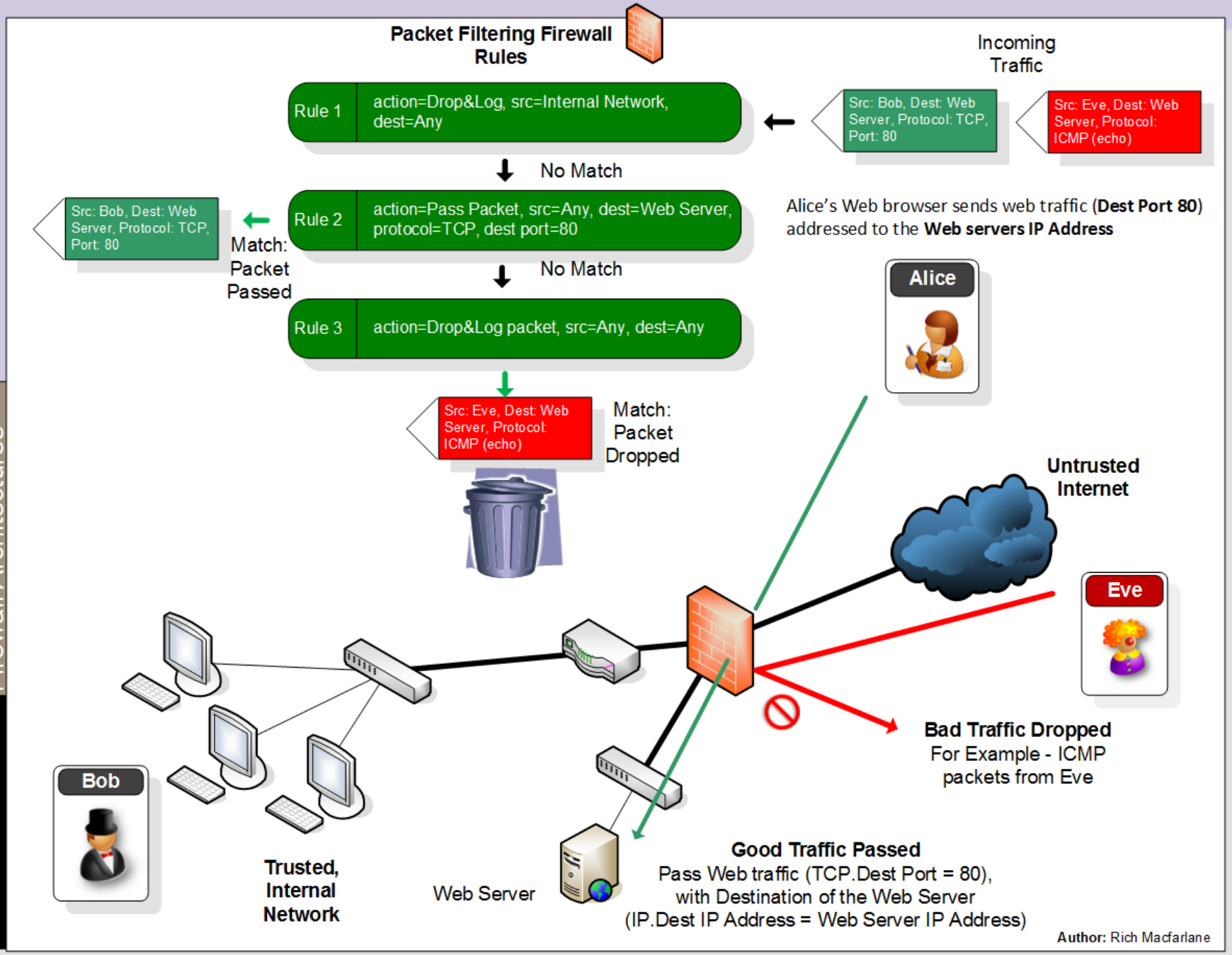
Packet Filtering Process

Stateless Packet Filtering

- Firewall de-capsulates each packet
  - Reads fields of IP/TCP packet header field values
  - Src/Dest IP Address
  - Src/Dest TCP/UDP Port
- Compare values against filtering rules in the firewall
  - Each rule checked against packet values
  - If values match rule – rule determines what to do with packet
  - Packet **passed** through firewall or **dropped** depending on rule action
- Each packet is filtered individually
  - No idea of Conversation – or TCP Session

Packet Filtering Process



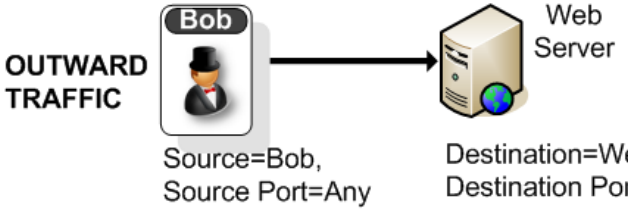


Open or closed firewall?

Static Packet Filtering Rules

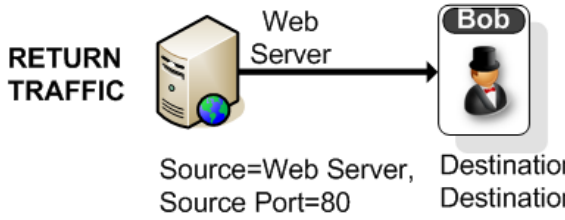
Packet Filtering Problems

- Each packet is filtered individually
  - No concept of ‘state’ or context of connection packet is part of
  - Most traffic uses TCP Session/Conversation
  - Have to open large range of ports for return traffic
  - Can use TCP Flags – Check if ACK flag for established connection
  - Easily Spoofed **`nmap -sA –p1-65000 IP_Address[range]`**
- Does not look into Payload
  - Application layer attacks
- Cannot deal with complex protocols
  - FTP uses fixed port number for command session
  - FTP uses dynamic port numbers for data sessions
  - Negotiated and passed in data payload of packet
  - Would have to open up large range of ports – security hole



OUTWARD TRAFFIC FIRWALL RULE

Rule 1	action=Pass Packet, src=Bob, dest=Web Server, protocol=TCP, dest port=80

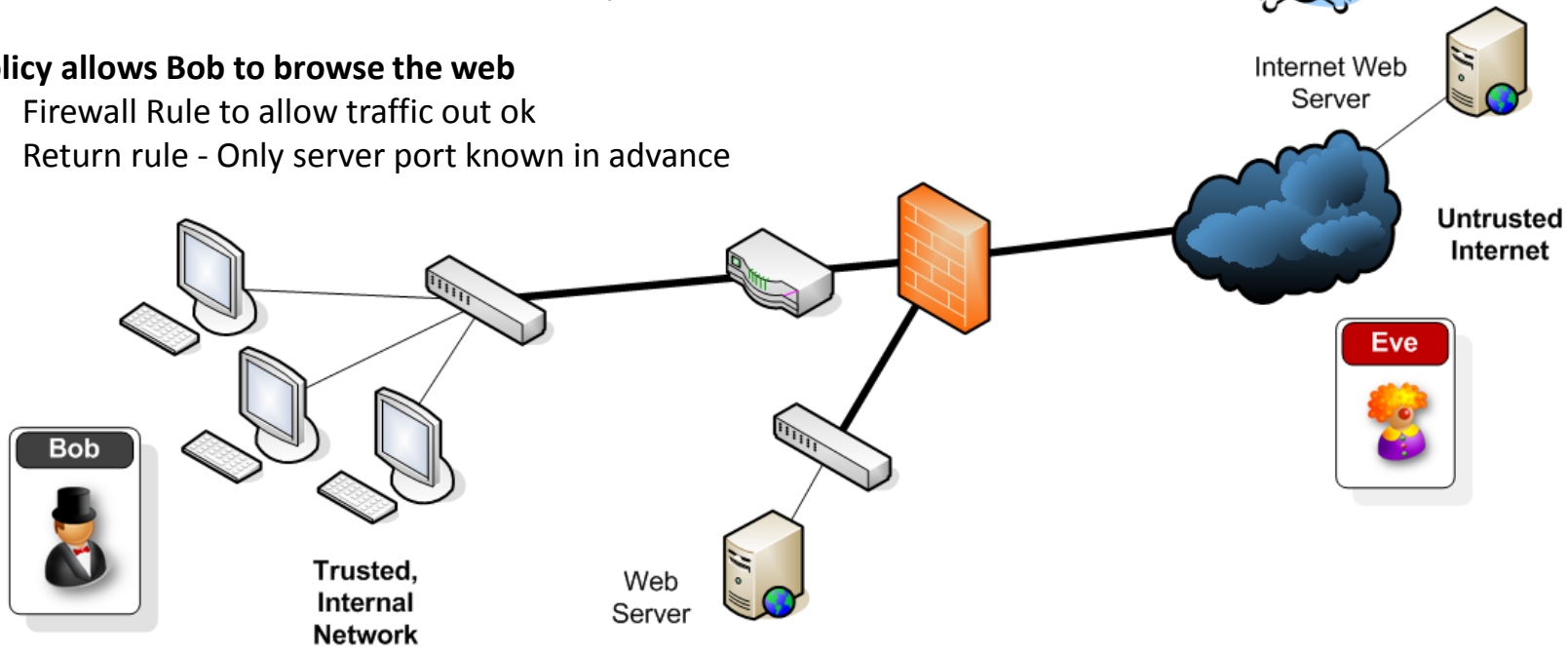


RETURN TRAFFIC FIRWALL RULE

Rule 2	action=Pass Packet, src=Web Server, dest=Bob, protocol=TCP, dest port=ANY

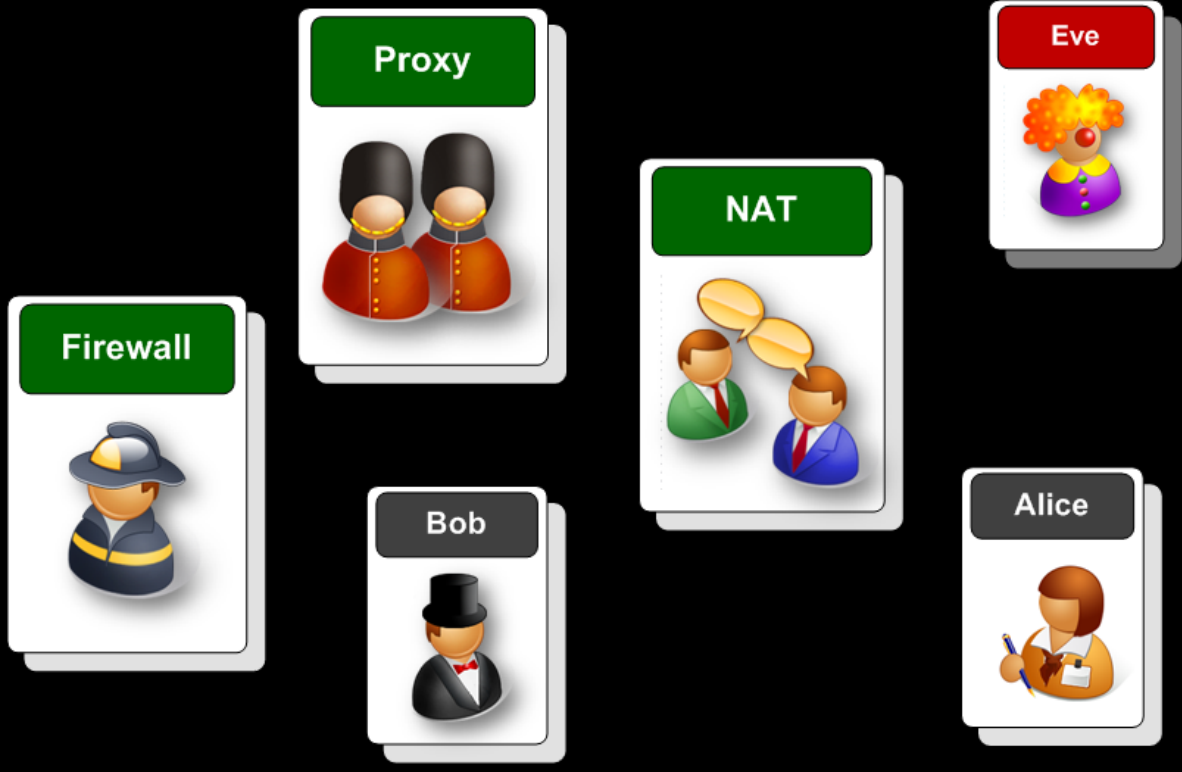
Policy allows Bob to browse the web

- Firewall Rule to allow traffic out ok
- Return rule - Only server port known in advance



Author: Rich Macfarlane

FIREWALLS | ARCHITECTURES



Packet Filtering Firewalls

Stateful Firewalls

Application Inspection Firewalls
Application Proxy Firewalls
Hybrid Firewalls

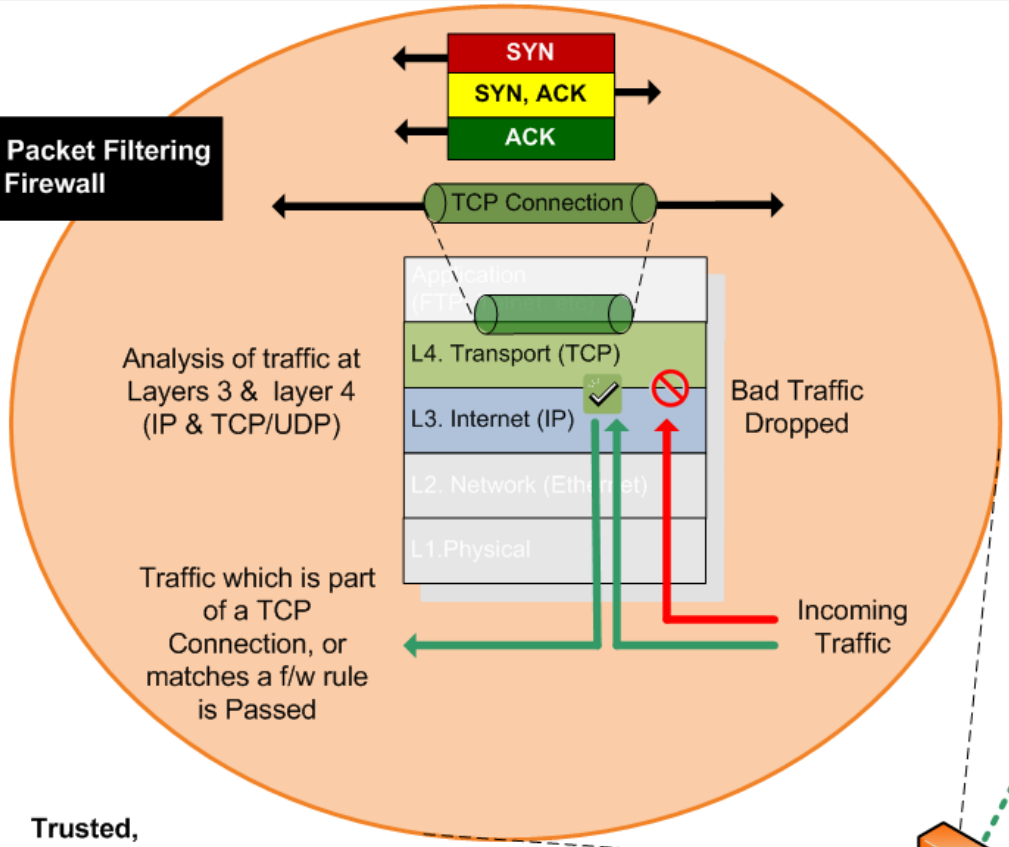
Author: Rich Macfarlane

Stateful Firewalls

Stateful Packet Filtering

- Packet Filtering firewall using rules same as stateless, but additionally track connection state
- Checks packet in context of connection
  - State of traffic flows tracked
- Maintains cache about current connections
  - State Table used to record initiated connections (once they have been passed by firewall rules)
  - State Table checked for return traffic matching stored connection
  - Match allowed through
  - No match – check packet against firewall rules
- Application Data Content of Packet still not examined

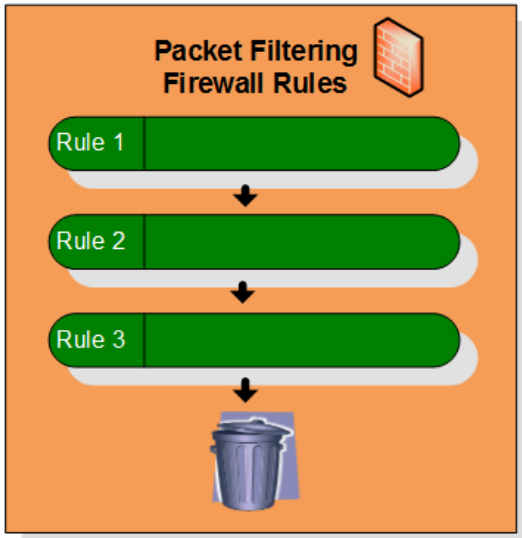
Stateful Packet Filtering Firewall

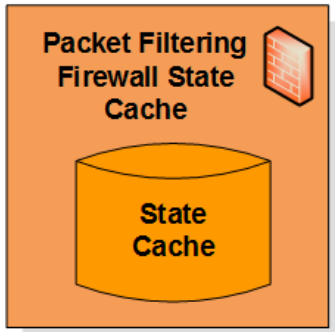


Alice's return data traffic automatically allowed through firewall, without specific return rule

Author: Rich Macfarlane

Stateful Filtering Process





SrcIP=AlicePC, DestIP=WebServer,
SrcPort=1777, DestPort=80

1. Packet sent to Web Server

Untrusted Internet

TCP SYN Flag set

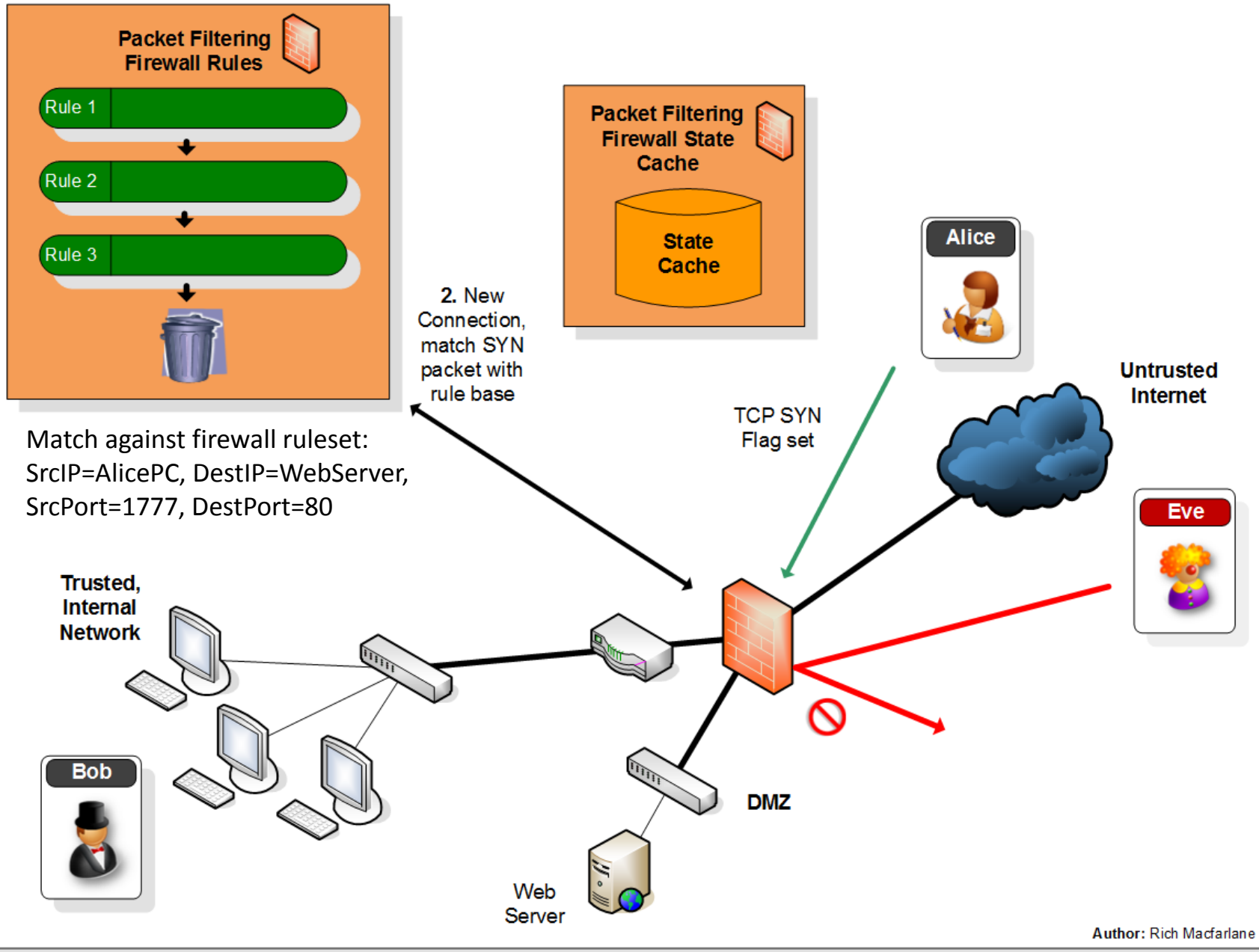
TCP flags checked to check if part of a current connection
Alice's packet has SYN flag set so NEW Connection

Trusted, Internal Network

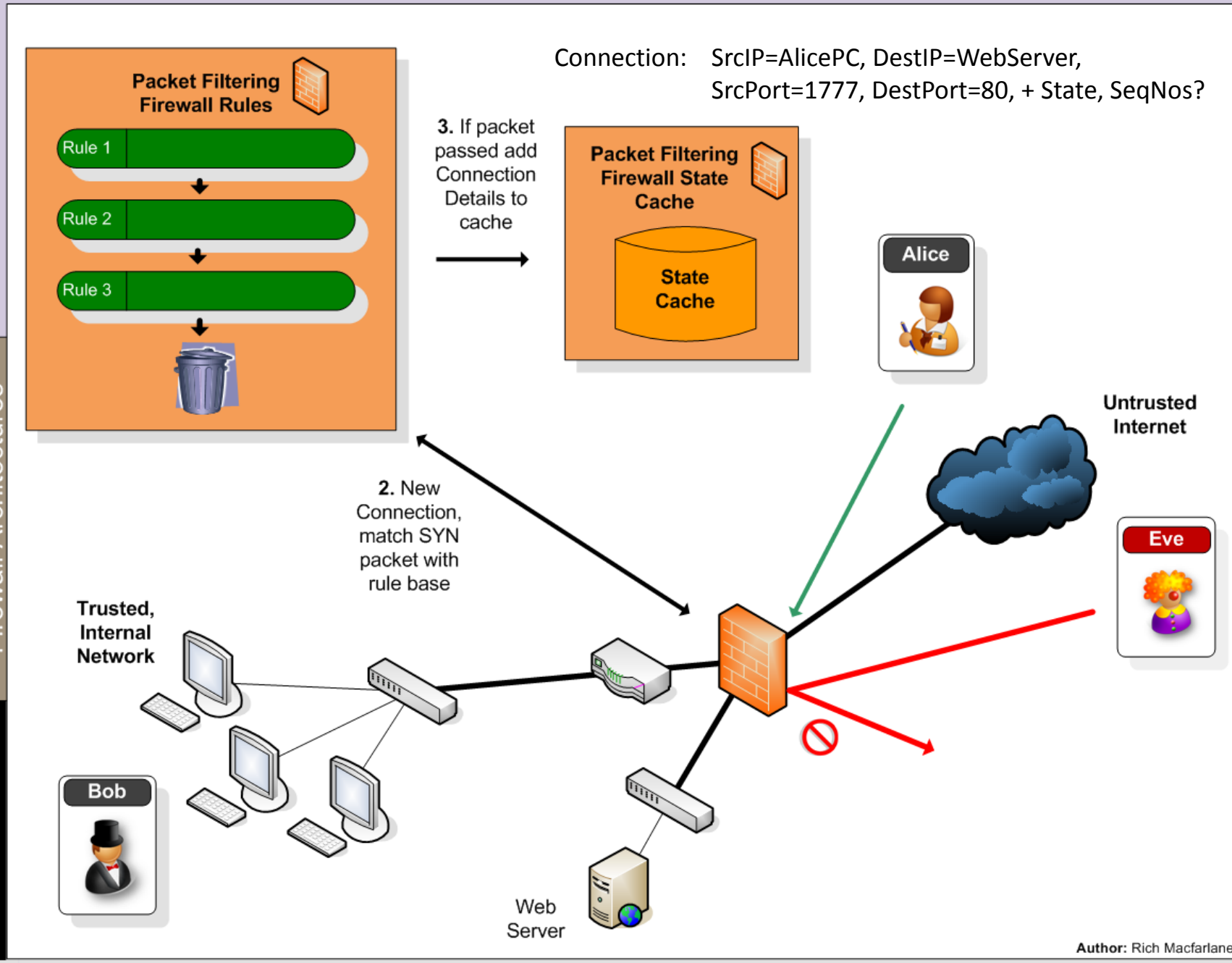
Web Server

Author: Rich Macfarlane

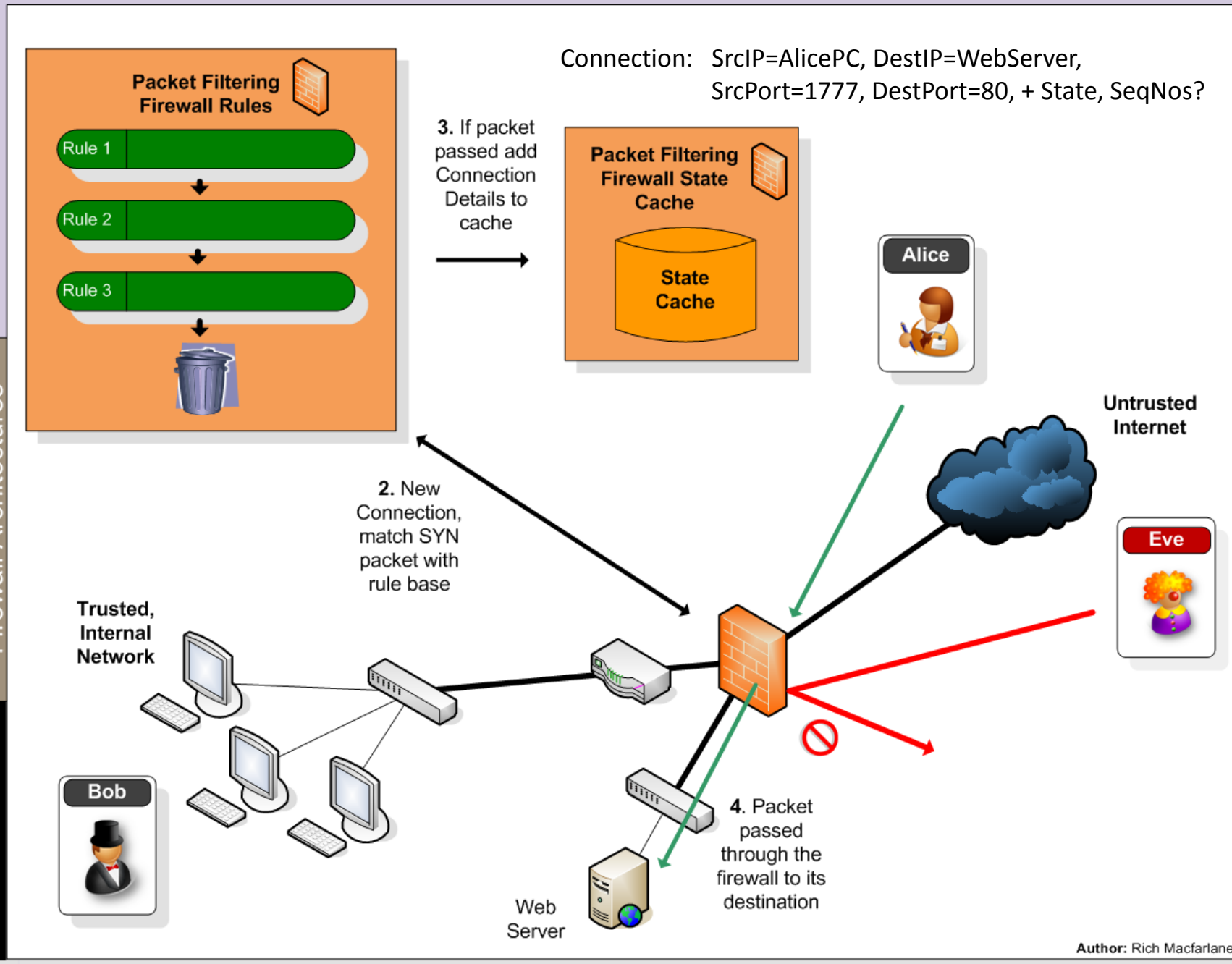
Stateful Packet Filtering Firewall



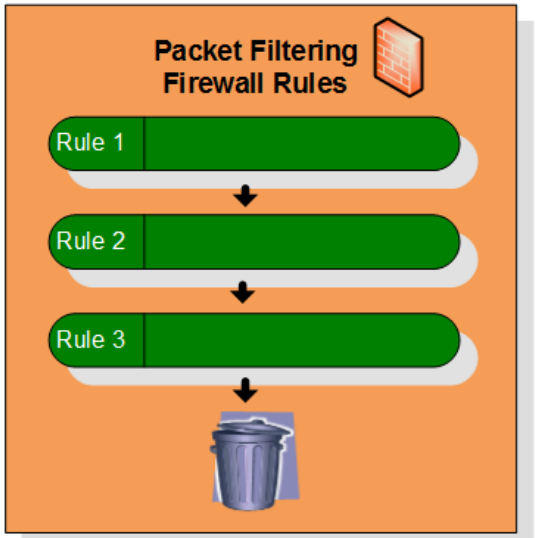
Stateful Packet Filtering Firewall



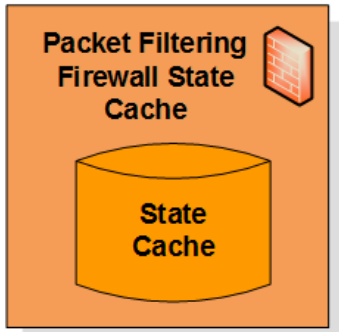
Stateful Packet Filtering Firewall



Stateful Packet Filtering Firewall



Connection: SrcIP=AlicePC, DestIP=WebServer, SrcPort=1777, DestPort=80, + State, SeqNos?

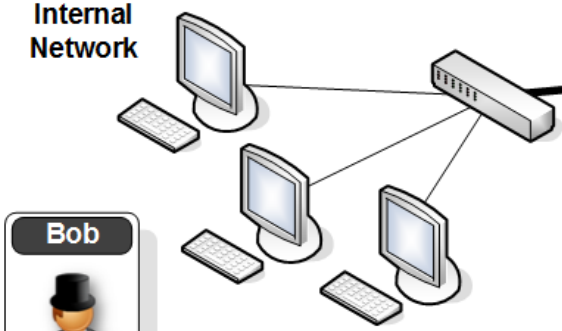


Firewall Ruleset not consulted!

5. Returning Packet checked against the cache details and passed

Untrusted Internet

Trusted, Internal Network



SYN/ACK

SrcIP=WebServer, DestIP=AlicePC, SrcPort=80, DestPort=1777

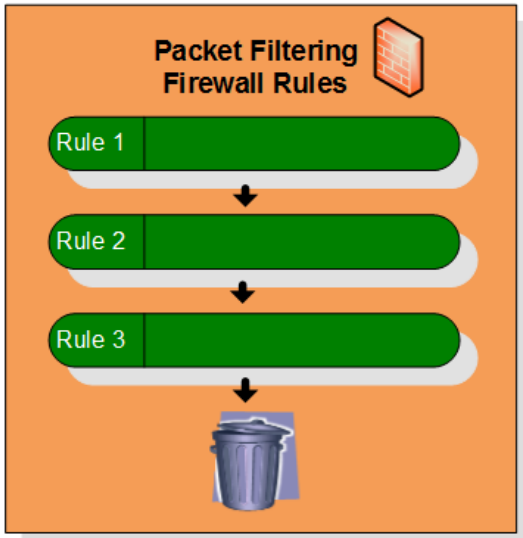
Web Server

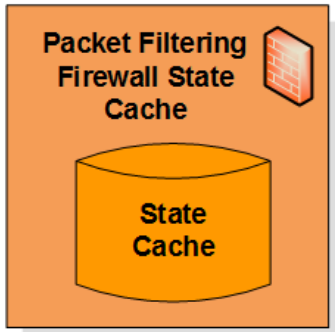
Author: Rich Macfarlane

Stateful Packet Filtering Firewall

Crafted ACK Packet

```
Alice# nmap -sA –p1-65000 Bob_IPAddress
```





Match against firewall ruleset and is dropped
SrcIP=EvePC, DestIP=BobPC,
SrcPort=80, DestPort=666

5. Returning Packet checked against the cache details and no match

Untrusted Internet

Eve

Trusted, Internal Network

ACK

1. Packet sent to Bob PC with spoofed connection state flag

Bob

Web Server

SrcIP=EvePC, DestIP=BobPC,
SrcPort=80, DestPort=666

Author: Rich Macfarlane

Stateful Firewalls

Removing Connections from Cache

- Standard connection teardown handshake
  - RST packet received
  - FIN/ACK packets exchanged correctly
- Timeouts
  - Typically configurable
  - Balancing act between availability and removing valid sessions
  - Seconds to days depending on Vendor/Firewall
  - Various Timeouts: Connection setup timer/Idle connection timer
- UDP
  - Connectionless – no state flags like TCP
  - Firewall may use its own state flags – created/replied
  - Timeout removes connection

FIREWALLS | ARCHITECTURES

Packet Filtering Firewalls
Stateful Firewalls

Application Inspection Firewalls

Application Proxy Firewalls
Hybrid Firewalls

| ARCHITECTURES

Author: Rich Macfarlane

Application Inspection Firewalls

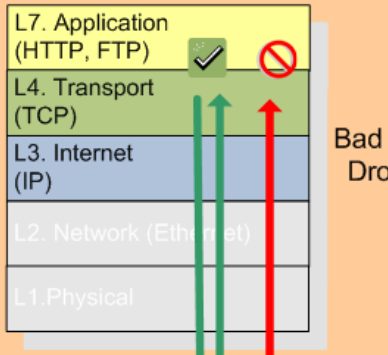
Application Inspection

- Typically Stateful Packet Filtering firewall, but additionally inspects the application payload
- Can analyse problematic protocols
  - Multi channel connections
- Can Validate Application protocol
  - Check commands
- Can Validate Application layer content
  - Match attacks in payload

Application Protocol Inspection Firewall

Analysis of traffic at Layers 3 & layer 4, and layer 7

Traffic which is part of a TCP Connection, or matches a f/w rule and is valid application protocol command is Passed



Bad Traffic Dropped

Incoming Traffic

Author: Rich Macfarlane

Application Inspection Firewalls

Application Inspection

- Deal with complex protocols
  - FTP, VoIP protocols
    - Multi channel protocol support
    - FTP outgoing control session packet payload contains negotiated data channel port number (PORT command)
    - Inspection Firewall can read this and allow traffic from the server to the data channel port number on the client system
  - ICMP
    - ICMP error packets returned from intermediate network devices, or which do not match outgoing packet
    - ICMP Time exceeded/host unreachable packets

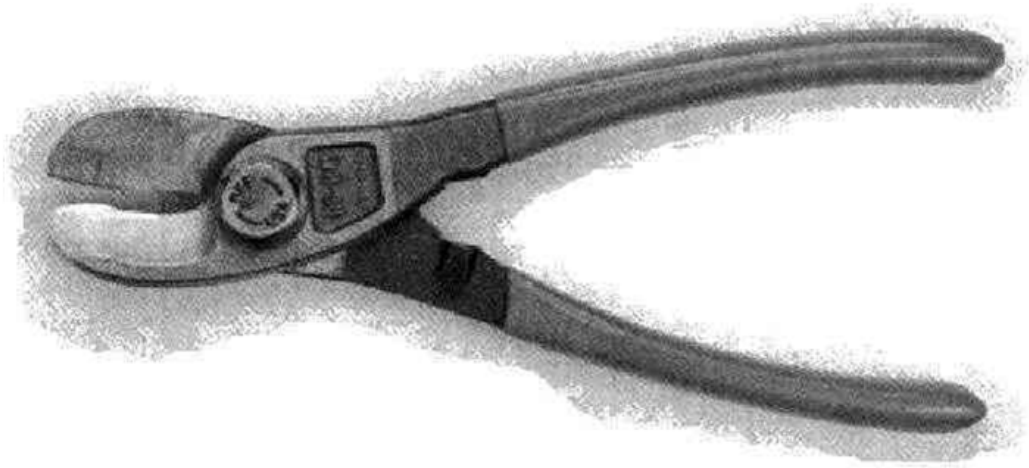
Application Inspection Firewalls

Application Inspection

- Can validate protocol content/commands
  - Check for valid commands for protocols
    - SMTP commands only in sessions on TCP/25
  - Enforce security policy
    - Certain protocol commands not permitted
    - Drop SMTP packets with VRFY command
- Typically pattern matching payload text
  - Entire pattern may have to be in single packet
  - Fragmented packets
  - Signature based – can be bypassed by altering commands slightly – add a space, or encode characters

Application Inspection Firewalls

- Stateful packet filtering + inspection of Application payload
- More Secure than Standard Packet Filtering
  - Validation of application protocols
  - Some content filtering
- Fast
  - Not as fast as Static Packet Filtering
  - Faster than a Proxy
    - Up to Gb range depending on vendor
    - Can be used as main perimeter connection on large pipe to Internet
- Support many protocols
  - More complex protocols which use payload to communicate
    - Video/Audio/Multi channel protocols



The ULTIMATELY Secure Firewall

For Internet use install the firewall between the demarc of the T1 to the Internet. Place the jaws of the firewall across the T1 line lead, and bear down firmly. When your Internet service provider's network operations center calls to inform you that they have lost connectivity to your site, the firewall is correctly installed.

The fact is, that if you're connecting your network to anything else, you're running a risk. Period. Usually, that risk can be reduced, often dramatically, by employing basic security precautions such as firewalls. But a firewall is a risk reduction system, it is not a risk mitigation system -- there is, always, some danger that something can go fatally wrong with anything built by humans.

The firewall above is the only 100% guaranteed secure solution.

Marcus J. Ranum

Author: Rich macfarlane