

Lecture#04

Cyber Security Essentials and Network Defenses

Muhammad Yousif

Department of Computer Science (CS)

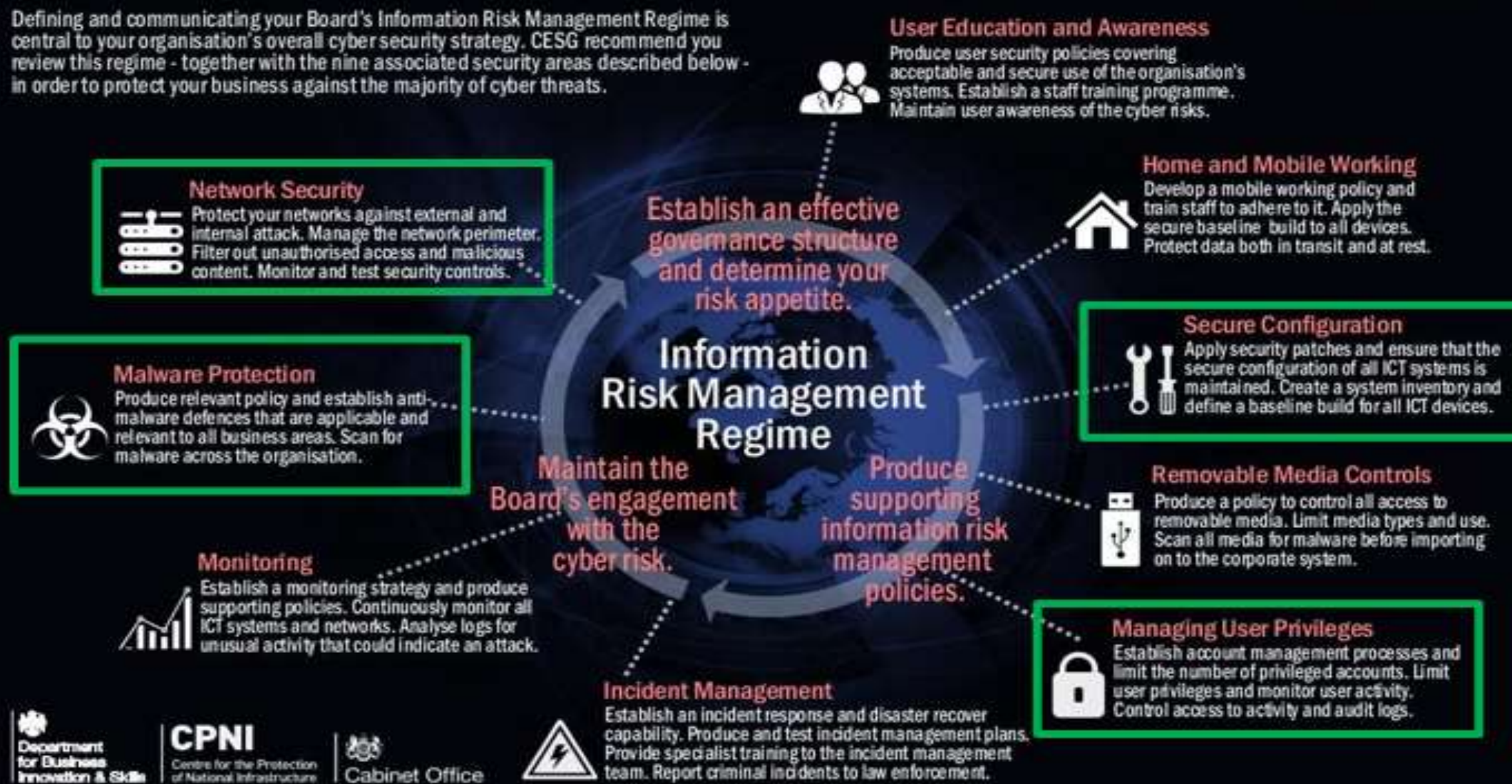
Minhaj University.

Myousif.cs@mul.edu.pk

10 Steps To Cyber Security



Defining and communicating your Board's Information Risk Management Regime is central to your organisation's overall cyber security strategy. CESG recommend you review this regime - together with the nine associated security areas described below - in order to protect your business against the majority of cyber threats.



Cyber Security Essentials

It requires...

FIVE MANDATORY CONTROLS:



Secure
configuration



Boundary
firewalls and
internet
gateways



Access control
and
administrative
privilege
management



Patch
management



Malware
protection

Cyber Security Essentials

It is a...



Clear statement of the basic controls that all organisations should implement to mitigate the risk from common internet-based threats.



Mechanism for organisations to demonstrate to customers, investors, insurers and others that they have taken essential precautions against cyber risks.



Requirement for suppliers bidding for certain UK Government and large business contracts that handle personal information:

- Professional services (commercial, financial, legal, HR and business services)
- ICT (IT managed or outsourced services and ICT services).

Cyber Essentials Certification

- Self-assessment
- External vulnerability scan by an approved tester
- Internal vulnerability scan by an approved tester

How it works...

Self-Assessment
Questionnaire



External vulnerability
scan*

- ✓ External full TCP port and top UDP service scan for stated IP range
- ✓ Vulnerability scan for stated IP range
- ✓ Basic web application scanning for common vulnerabilities

* According to CREST-accredited Certification Bodies.

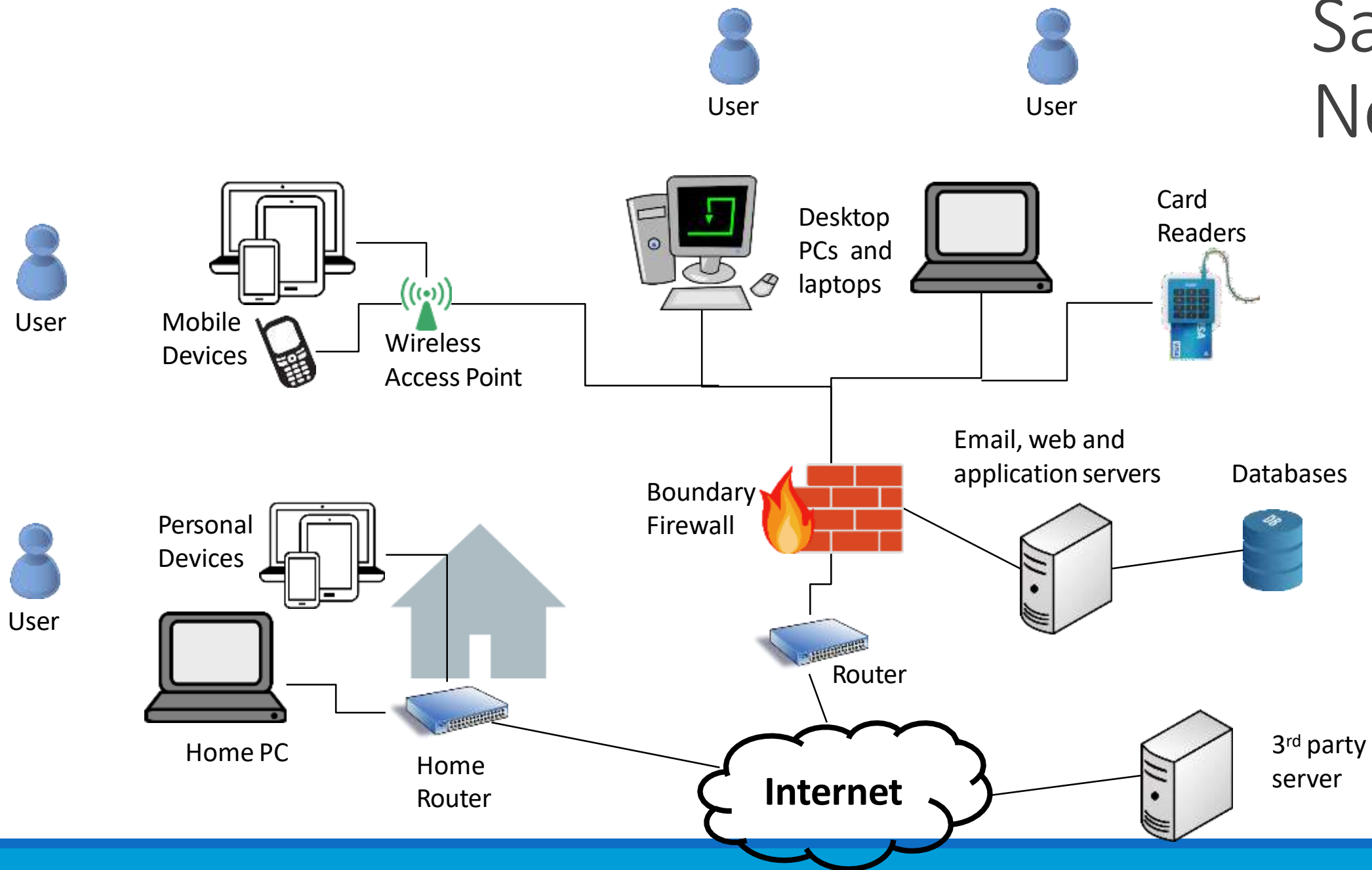


Internal vulnerability
scan and on-site
assessment

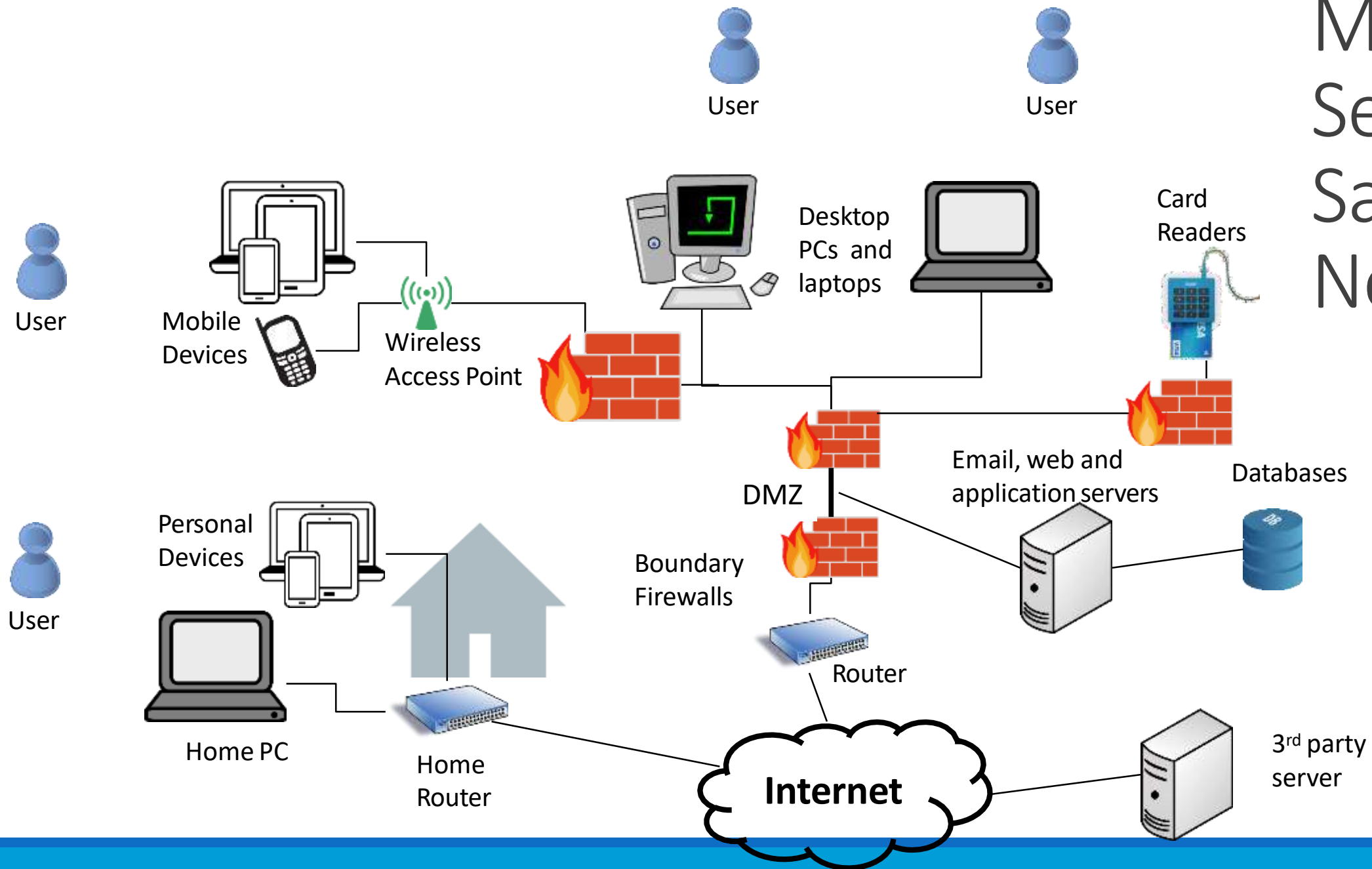
- ✓ Inbound email binaries and payloads
- ✓ Inbound emails containing URLs linking to binaries and browser exploitation payloads
- ✓ Authenticated vulnerability and patch verification scan



Sample Network



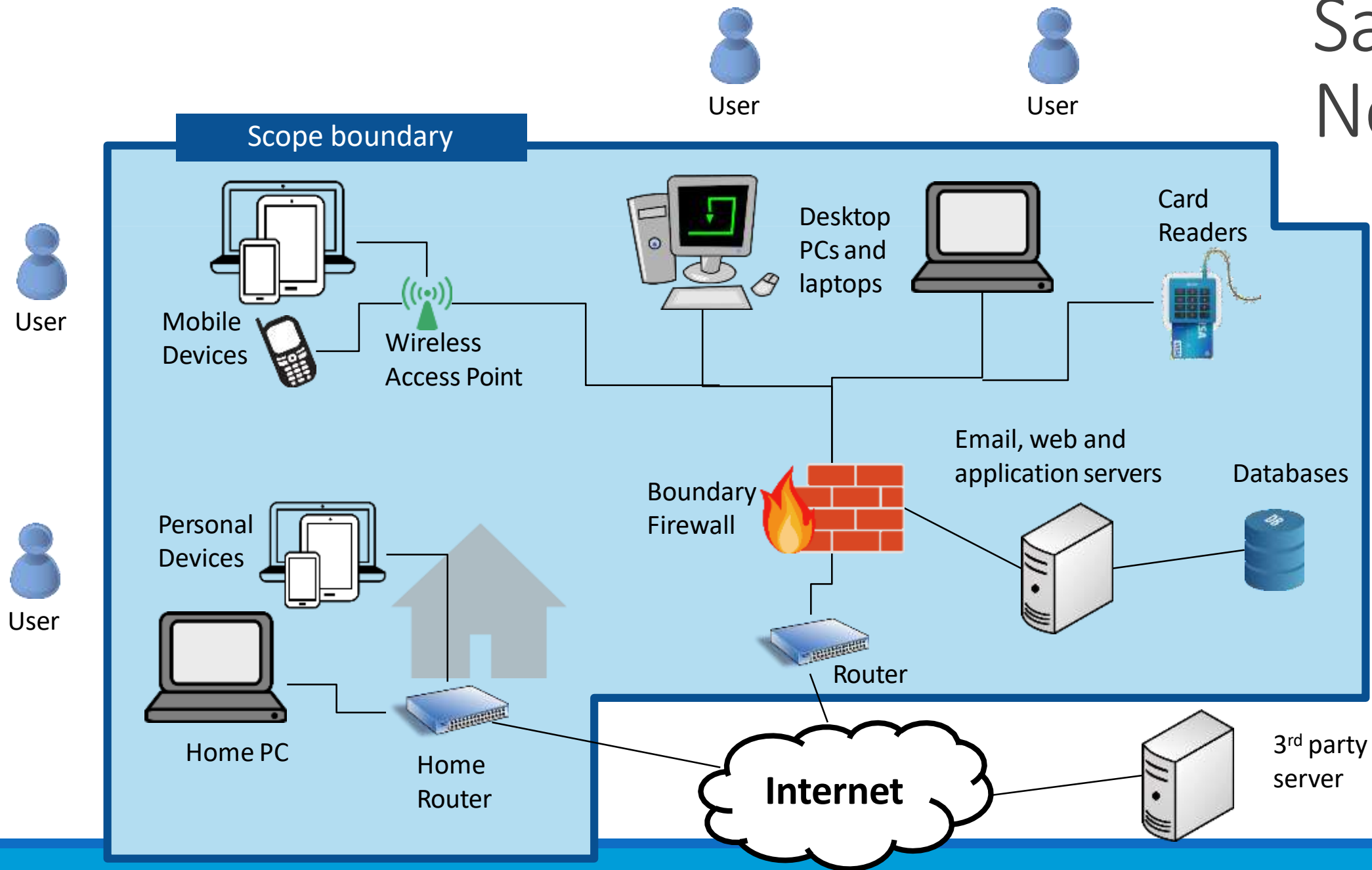
More Secure Sample Network



“A system which is unspecified can never be wrong, it can only be surprising.”

Step 1: Decide what you are going to protect and what is out of scope.

Sample Network



Cyber Security Essentials

It requires...

FIVE MANDATORY CONTROLS:



Boundary
firewalls and
internet
gateways



Access control
and
administrative
privilege
management



Patch
management



Malware
protection

1. Secure Configuration

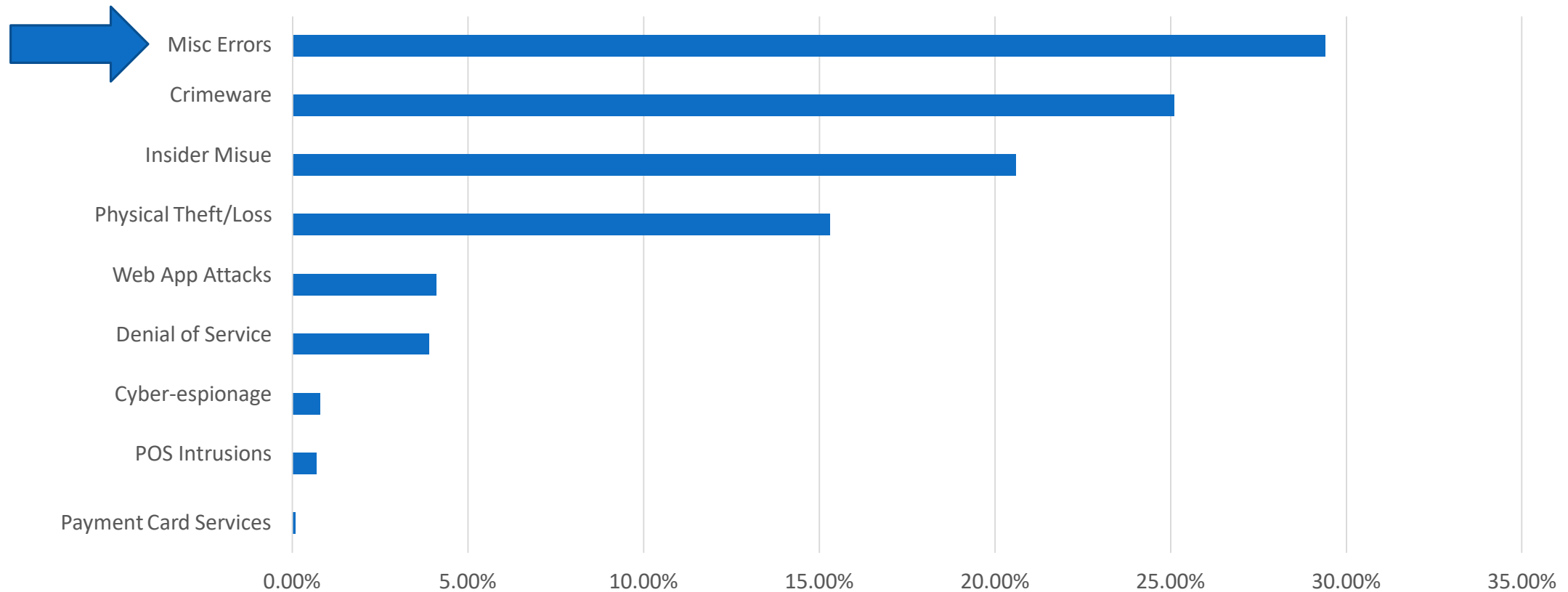
Objectives: Computers and network devices should be configured to reduce the level of basic vulnerabilities and provide only the services required to fulfill their role.

- Default settings are not necessarily secure.
- Predefined passwords can be widely known.

1. Secure Configuration

1. Unnecessary user accounts should be removed or disabled.
2. Any default password for a user account should be changed to an alternative, strong password.
3. Unnecessary software should be removed or disabled.
4. The auto-run feature should be disabled.
5. A personal firewall (or equivalent) should be enabled on desktop PCs and laptops, and configured to disable (block) unapproved connections by default.

Configuration is a real problem



Cyber Security Essentials

It requires...

FIVE MANDATORY CONTROLS:



Secure
configuration



Boundary
firewalls and
internet
gateways



Access control
and
administrative
privilege
management



Patch
management



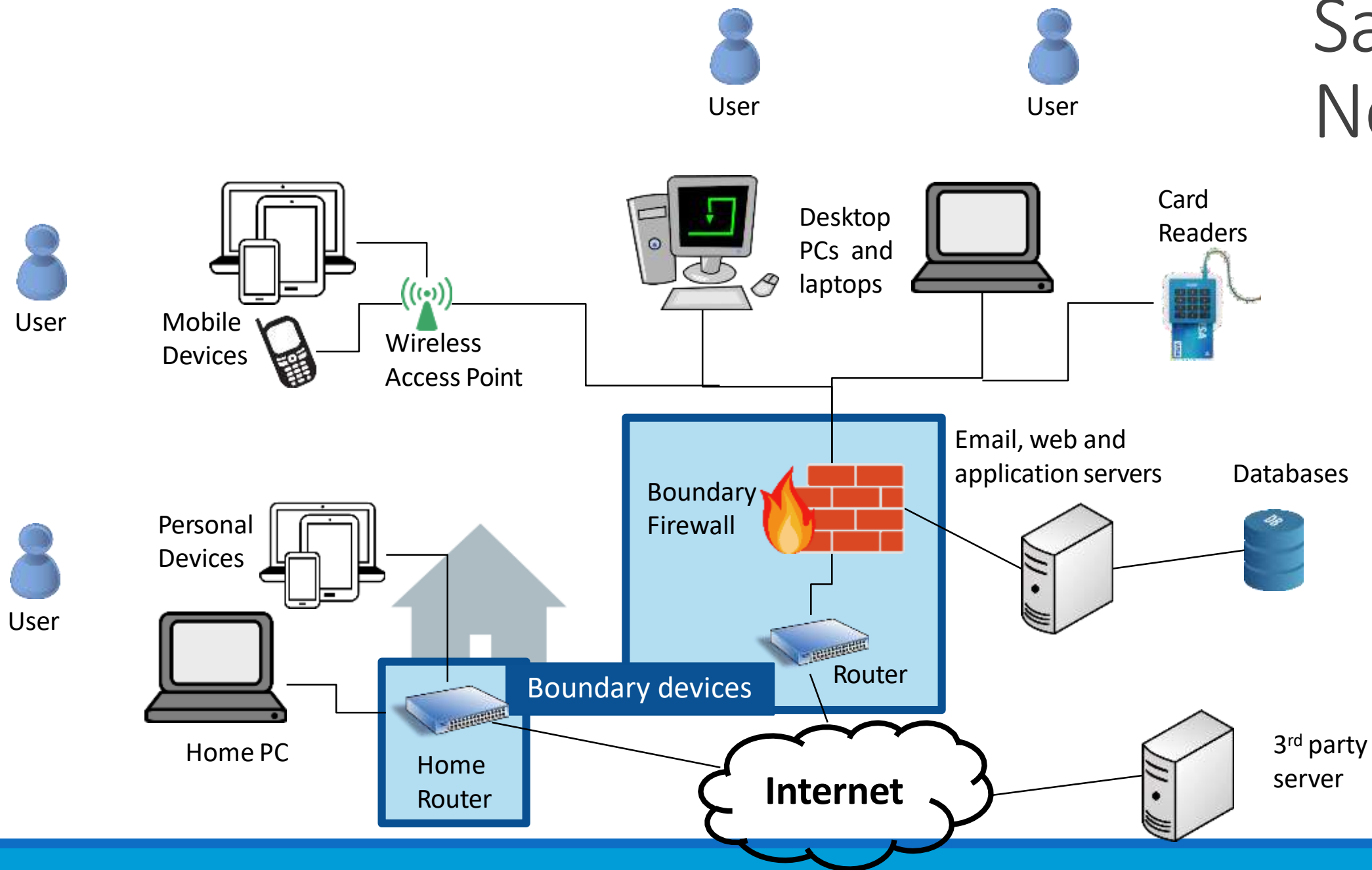
Malware
protection

2. Boundary firewalls and internet gateways

Objectives: Information, applications and computers within the organization's internal networks should be protected against unauthorized access and disclosure from the internet, using boundary firewalls, internet gateways or equivalent network devices.

- Boundary devices are the first line of defense.
- Firewall rules can be used to stop basic attacks before they even reach the internal network.

Sample Network



Boundary firewalls and internet gateways

1. Change default administrator passwords for all network devices and firewalls.
2. Each rule that allows network traffic to pass through the firewall should be subject to approval by an authorized individual and documented.
3. Unapproved services, or services that are typically vulnerable to attack, should be disabled (blocked) by the boundary firewall by default.
4. Firewall rules that are no longer required should be removed or disabled in a timely manner.
5. The administrative interface used to manage boundary firewall configuration should not be accessible from the internet.

File Action View Help

Windows Firewall with Advanced Security

- Inbound Rules
- Outbound Rules
- Connection Security Rules
- Monitoring

Name	Profile	Enabled	Action	Override
Bonjour Service	Private	Yes	Allow	No
Bonjour Service	Private	Yes	Allow	No
Bonjour Service	Private	Yes	Allow	No
Bonjour Service	Private	Yes	Allow	No
Dropbox	All	Yes	Allow	No
FiddlerProxy	All	Yes	Allow	No
Firefox (C:\Program Files (x86)\Mozilla Fir...	Private	Yes	Allow	No
Firefox (C:\Program Files (x86)\Mozilla Fir...	Private	Yes	Allow	No
'Firefox' (C:\Program Files (x86)\Mozilla F...	Private	Yes	Allow	No
'Firefox' (C:\Program Files (x86)\Mozilla F...	Private	Yes	Allow	No
HP Socket Service	All	Yes	Allow	No
IntelUSBoverIP:1	All	Yes	Allow	No
iTunes	All	Yes	Allow	No
Microsoft Office Outlook	Private	Yes	Allow	No
Microsoft SkyDrive	All	Yes	Allow	No
pluginhost.exe	Private	Yes	Allow	No
pluginhost.exe	Private	Yes	Allow	No
Skype	Private	Yes	Allow	No
Skype	Private	Yes	Allow	No
Skype	Public	Yes	Block	No

Actions

- Inbound Rules
- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help

Skype

- Disable Rule
- Cut
- Copy
- Delete
- Properties
- Help

Windows 8 Firewall rules

Cyber Security Essentials

It requires...

FIVE MANDATORY CONTROLS:



Secure
configuration



Boundary
firewalls and
internet
gateways



Access control
and
administrative
privilege
management



Patch
management



Malware
protection

3. Access control and administrative privilege management

Objectives: User accounts, particularly those with special access privileges should be assigned only to authorized individuals, managed effectively and provide the minimum level of access to applications, computers and networks.

- Principle of least privilege – only give users access they need.
- Admin accounts have the most access, if one get compromised it can lead to large scale loss of information.

3. Access control and administrative privilege management

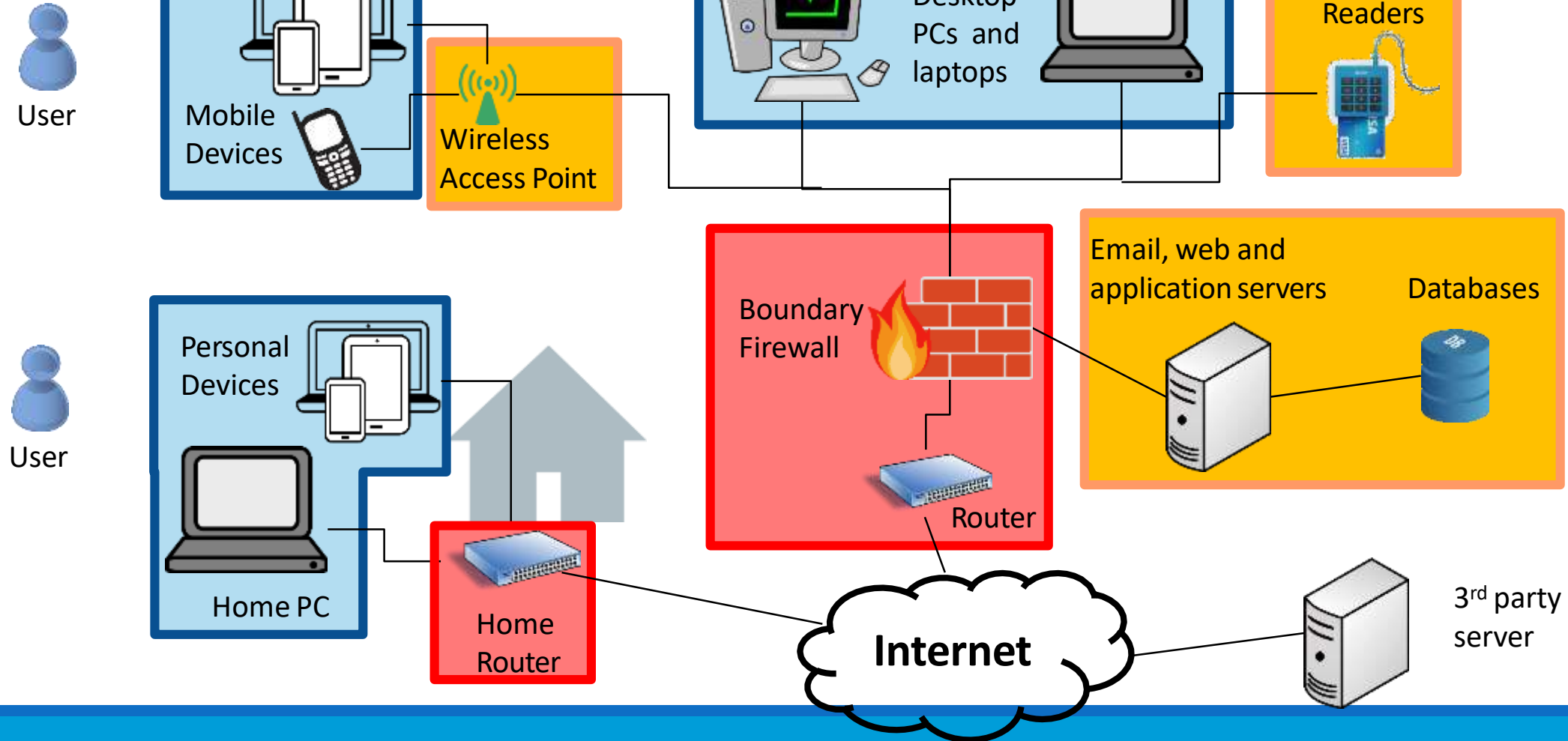
1. All user account creation should be subject to a provisioning and approval process.
2. Special access privileges should be restricted to a limited number of authorized individuals.
3. Details about special access privileges should be documented, kept in a secure location, and reviewed on a regular basis.
4. Admin accounts should only be used to perform legitimate admin activities and should not be granted access to email or the internet.
5. Admin accounts should be configured to require a password change on a regular basis.
6. Each user should authenticate using a unique username and strong password before being granted access to applications, computers and network devices.
7. User accounts and special access privileges should be removed or disabled when no longer required or after a pre-defined period of inactivity.

Low security devices

Critical device

Security device

Sample Network



Cyber Security Essentials

It requires...

FIVE MANDATORY CONTROLS:



Secure
configuration



Boundary
firewalls and
internet
gateways



Access control
and
administrative
privilege
management



Patch
management



Malware
protection

4. Patch management

Objectives: Software running on computers and network devices should be kept up-to-date and have the latest security patches installed.

- Vulnerabilities in software are patched through updates.
- If you don't install the update, the vulnerability is not patched.
- However, patching can cause compatibility problems. So you should always test the patches.

4. Patch management

1. Software running on computers and network devices on the internet should be licensed and supported to ensure security patches for known vulnerabilities are made available.
2. Updates to software running on computers and network devices should be installed in a timely manner.
3. Out-of-date software should be removed.
4. All security patches for software should be installed in a timely manner.

Cyber Security Essentials

It requires...

FIVE MANDATORY CONTROLS:



Secure
configuration



Boundary
firewalls and
internet
gateways



Access control
and
administrative
privilege
management



Patch
management



Malware
protection

5. Malware protection

Objectives: Computers exposed to the internet should be protected against malware infection through the use of malware protection software.

- Today's Firewalls are very good, most malicious software must be invited in by a user opening an email, browsing a compromised website, or connecting compromised media.
- Protection software continuously monitors the computer for known malicious programs.

5. Malware protection

- Install anti-malware software on all computers that are connected to or capable of connecting to the internet.
- Update anti-malware software on all computers.
- Configure anti-malware software to scan files automatically upon access and scan web pages when being accessed.
- Regularly scan all files.
- Anti-malware software should prevent connections to malicious websites on the internet.

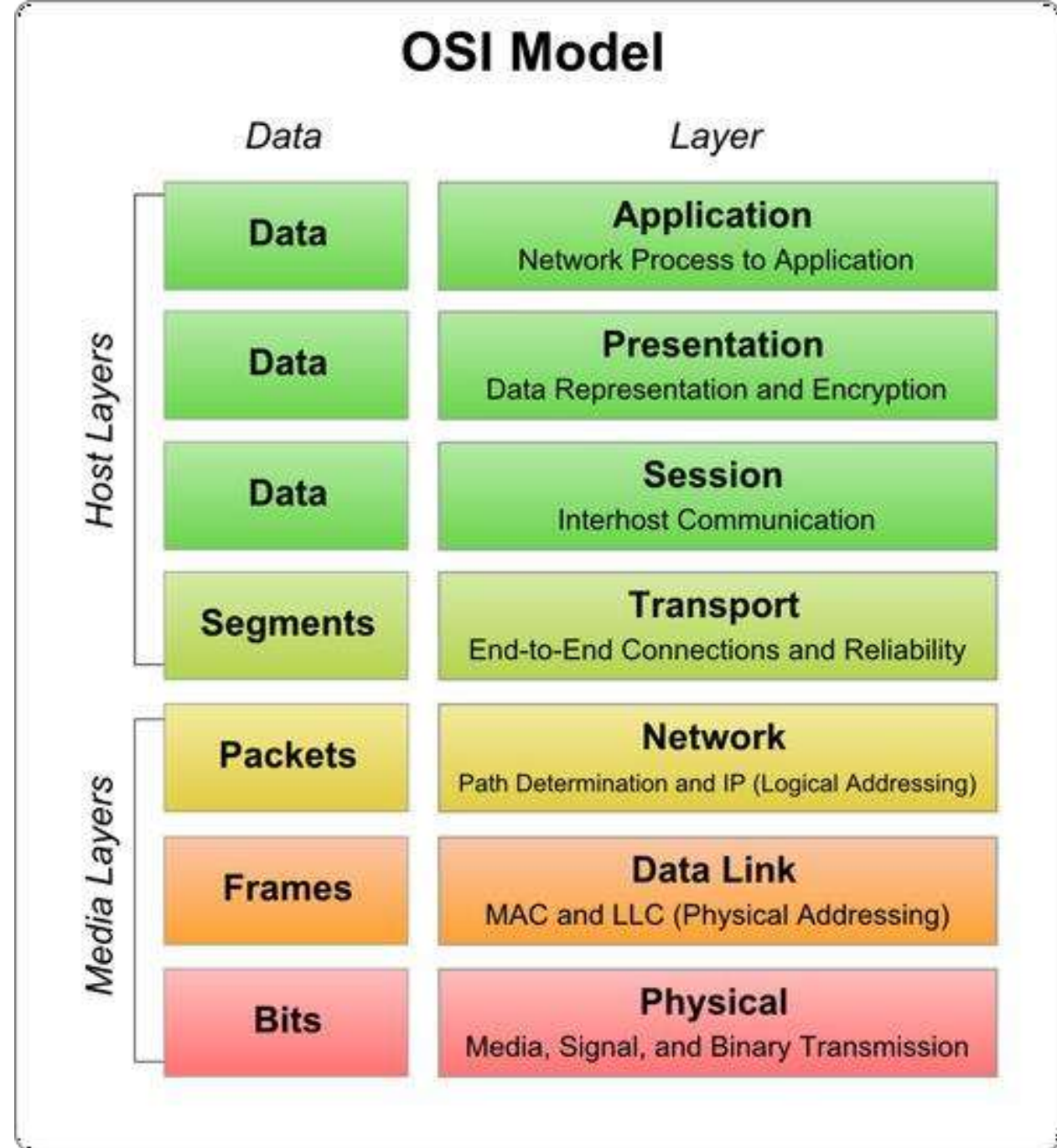
Break

Outline

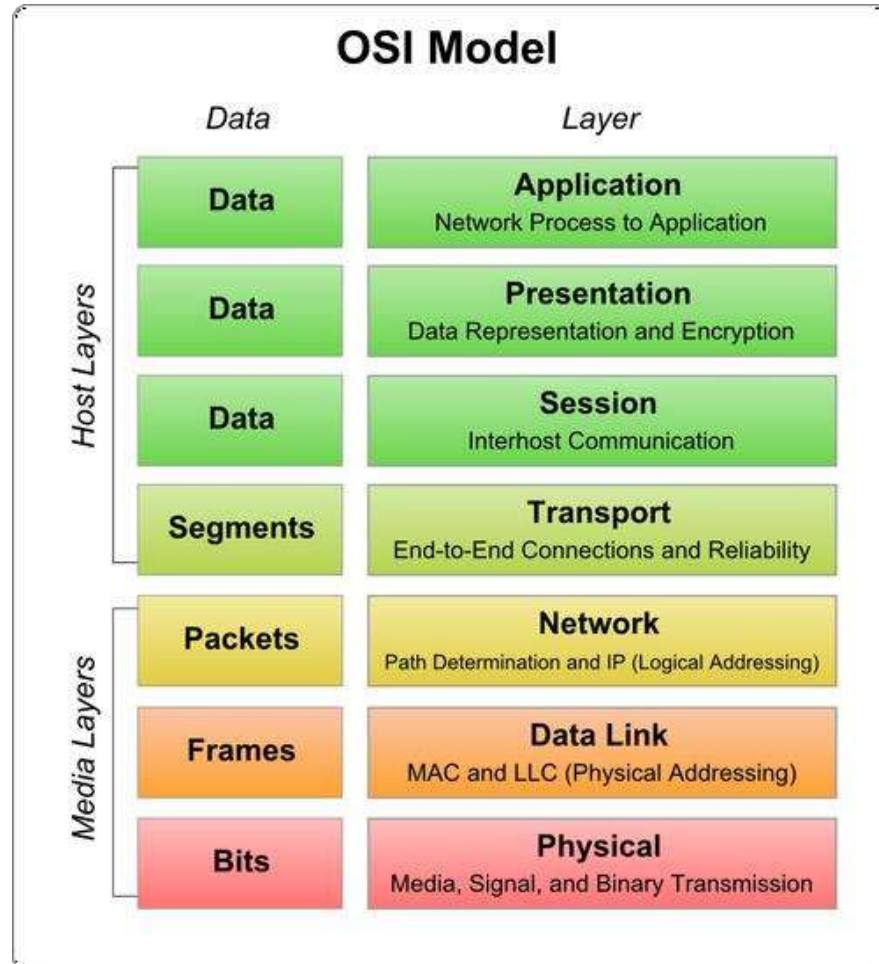
- Open System Interconnect (OSI) model
- Firewalls
- Intrusion detection systems (IDS)
- Time allowing:
 - Network Address Translation (NAT)

Open Systems Interconnect model

- A good way to think about networking steps logically
- Not how software is actually built



OSI in terms of debugging errors



Can your browser open another website?

Do you have a viewer that supports jpg (image format)?

Can you ping the webserver you are trying to reach?


Can you ping the gateway or DNS server?

Do you have an IP address?

Is the light on the modem on?

Is the network cable plugged in?

Sender:
Apache server

7	 Application Network process to application
6	Presentation Data representation and encryption
5	Session Interhost communication
4	Transport End-to-end connection and reliability
3	Network Path determination and IP (Logical Addressing)
2	Data Link MAC and LLC (Physical Addressing)
1	Physical Media, signal, and binary transmission


Data starts at the top of the OSI stack at level 7.

It progresses down the stack with each successive level adding or changing information.

At level 1 it travels across the physical layer to the recipient computer.

The recipient then processes the data up the stack. At level 7 an application processes the data.

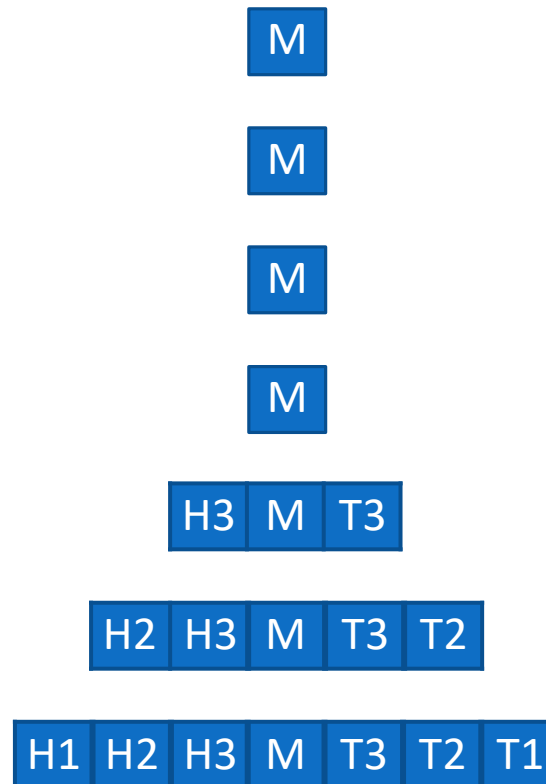
Recipient:
Firefox user

7	 Application Network process to application
6	Presentation Data representation and encryption
5	Session Interhost communication
4	Transport End-to-end connection and reliability
3	Network Path determination and IP (Logical Addressing)
2	Data Link MAC and LLC (Physical Addressing)
1	Physical Media, signal, and binary transmission

[illegible]

- Levels 7 and 6 involve the internal representation of the message
- Levels 5 and 4 involve setting up the connection
- Levels 3, 2, and 1 add header (H) and tail (T) information to each packet

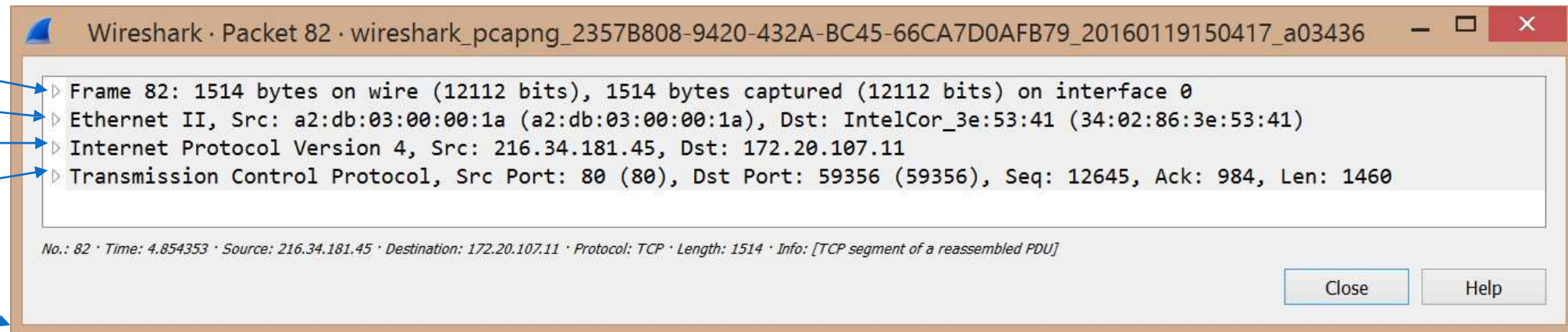
Information is added to the message as it travels down the OSI levels



7	Application Network process to application
6	Presentation Data representation and encryption
5	Session Interhost communication
4	Transport End-to-end connection and reliability
3	Network Path determination and IP (Logical Addressing)
2	Data Link MAC and LLC (Physical Addressing)
1	Physical Media, signal, and binary transmission

Header data on a packet

1. Physical
2. Data link
3. Network
4. Transport
- ...
7. Application



Frame header data on a packet

1. Physical
2. Data link
3. Network
4. Transport
- ...
7. Application

Wireshark · Packet 82 · wireshark_pcapng_2357B808-9420-432A-BC45-66CA7D0AFB79_20160119150417_a03436

Frame 82: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
Interface id: 0 (\Device\NPF_{2357B808-9420-432A-BC45-66CA7D0AFB79})
Encapsulation type: Ethernet (1)
Arrival Time: Jan 19, 2016 15:04:22.682715000 GMT Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1453215862.682715000 seconds
[Time delta from previous captured frame: 0.000002000 seconds]
[Time delta from previous displayed frame: 0.000002000 seconds]
[Time since reference or first frame: 4.854353000 seconds]
Frame Number: 82
Frame Length: 1514 bytes (12112 bits)
Capture Length: 1514 bytes (12112 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]

Ethernet II, Src: a2:db:03:00:00:1a (a2:db:03:00:00:1a), Dst: IntelCor_3e:53:41 (34:02:86:3e:53:41)
Internet Protocol Version 4, Src: 216.34.181.45, Dst: 172.20.107.11
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 59356 (59356), Seq: 12645, Ack: 984, Len: 1460

No.: 82 · Time: 4.854353 · Source: 216.34.181.45 · Destination: 172.20.107.11 · Protocol: TCP · Length: 1514 · Info: [TCP segment of a reassembled PDU]

Close Help

Information needed to physically transport the packet

IP header data on a packet

1. Physical
2. Data link
3. Network
4. Transport
- ...
7. Application

Wireshark · Packet 82 · wireshark_pcapng_2357B808-9420-432A-BC45-66CA7D0AFB79_20160119150417_a03436

Frame 82: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0

Ethernet II, Src: a2:db:03:00:00:1a (a2:db:03:00:00:1a), Dst: IntelCor_3e:53:41 (34:02:86:3e:53:41)

Internet Protocol Version 4, Src: 216.34.181.45, Dst: 172.20.107.11

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 1500
- Identification: 0xf76f (63343)
- Flags: 0x02 (Don't Fragment)
- Fragment offset: 0
- Time to live: 243
- Protocol: TCP (6)
- Header checksum: 0xe63b [validation disabled]
- Source: 216.34.181.45
- Destination: 172.20.107.11
- [Source GeoIP: Unknown]
- [Destination GeoIP: Unknown]

Transmission Control Protocol, Src Port: 80 (80), Dst Port: 59356 (59356), Seq: 12645, Ack: 984, Len: 1460

No.: 82 · Time: 4.854353 · Source: 216.34.181.45 · Destination: 172.20.107.11 · Protocol: TCP · Length: 1514 · Info: [TCP segment of a reassembled PDU]

Close Help

Annotations:

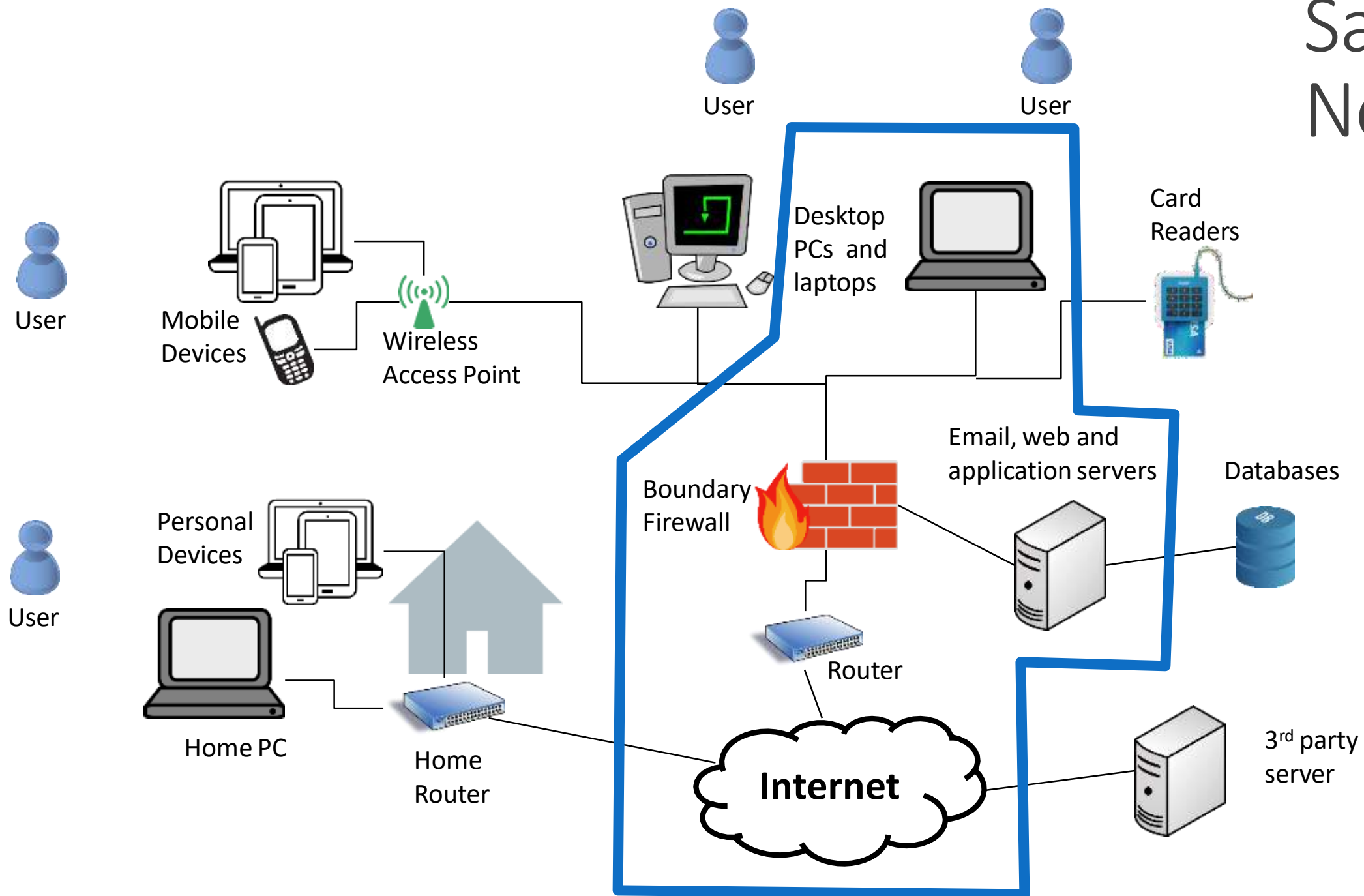
- Version 4
- Type of the next header
- Source and destination IP addresses
- Internet Protocol (IP) information

Firewalls

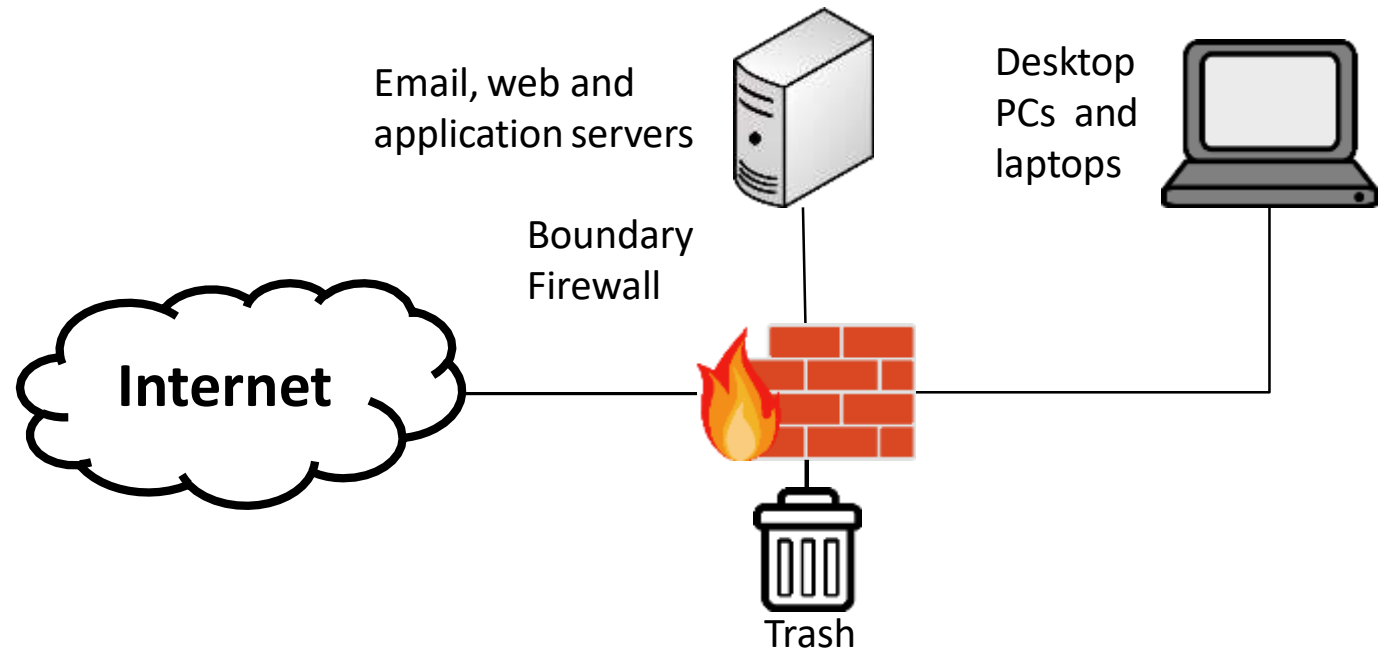
Firewalls

- Firewalls divide the untrusted outside of a network from the more trusted interior of a network
- Often they run on dedicated devices
 - Less possibilities for compromise – no compilers, linkers, loaders, debuggers, programming libraries, or other tools an attacker might use to increase their attack
 - Easier to maintain few accounts
 - Physically divide the inside from outside of a network

Sample Network



- Questionable things come from the internet AND from the local network
- Firewall applies a set of rules
- Based on rules, it allows or denies the traffic
- Firewalls can also act as routers deciding where to send traffic



Rule	Type	Source Address	Destination Address	Destination Port	Action
1	TCP	*	192.168.1.*	22	Permit
2	UDP	*	192.168.1.*	69	Permit
3	TCP	192.168.1.*	*	80	Permit
4	TCP	*	192.168.1.18	80	Permit
5	UDP	*	192.168.1.*	*	Deny

Sender:
Apache server



Recipient:
Firefox user





Sender:
Apache server

7	Application Network process to application
6	Presentation Data representation and encryption
5	Session Interhost communication
4	Transport End-to-end connection and reliability
3	Network Path determination and IP (Logical Addressing)
2	Data Link MAC and LLC (Physical Addressing)
1	Physical Media, signal, and binary transmission

A firewall takes in network traffic and compares it to a set of rules. In order to do so it must first process several OSI levels to reach the data it needs.

For example, to filter out all traffic from IP 216.34.181.45 the packet needs to be processed through level 3 where IP addresses can be read.

Firewall

3	Network Path determination and IP (Logical Addressing)
2	Data Link MAC and LLC (Physical Addressing)
1	Physical Media, signal, and binary transmission



Recipient:
Firefox user

7	Application Network process to application
6	Presentation Data representation and encryption
5	Session Interhost communication
4	Transport End-to-end connection and reliability
3	Network Path determination and IP (Logical Addressing)
2	Data Link MAC and LLC (Physical Addressing)
1	Physical Media, signal, and binary transmission

There are many types of Firewalls

Key differences include:

- How implemented
 - Software – slower, easier to deploy on personal computers
 - Hardware – faster, somewhat safer, harder to add in
- Number of OSI levels of processing required
 - Packet size (level 1)
 - MAC (level 2) and IP (level 3) filtering

Today we will talk about:

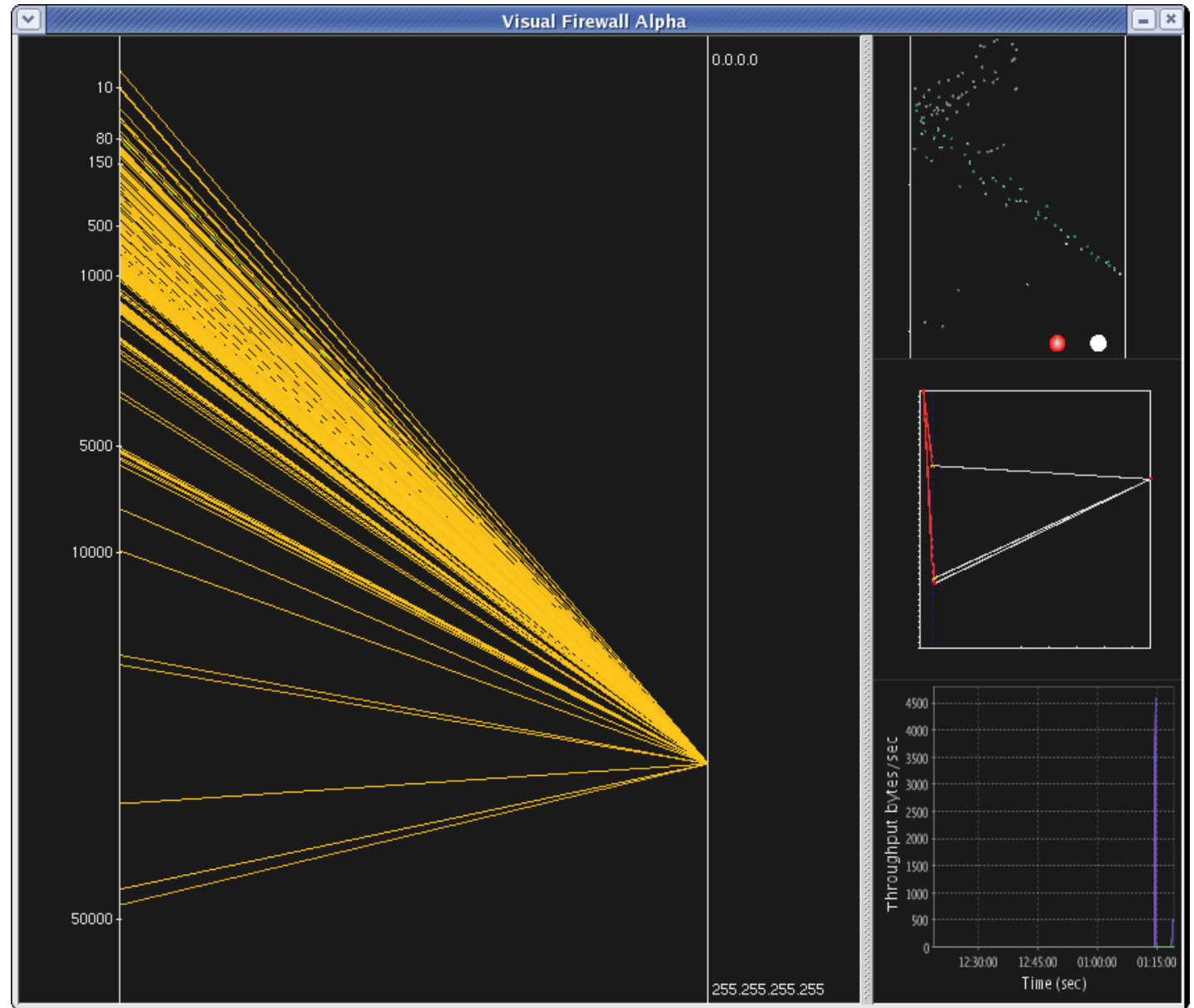
- Packet filtering gateway
- Stateful inspection firewall
- Application proxy
- Personal firewalls

Stateful inspection firewall

- Maintains state from one packet to another
- Similar to a packet filtering gateway, but can remember recent events
- For example, if a outside host starts sending packets to many internal destination ports (aka a port scan) a stateful firewall would record the number of ports probed and once it is over the threshold specified in the policy it would block all further traffic

Port scan

- An attacker is looking for applications listening on ports
- A single IP address (right) is contacting many ports (left) to see if any respond



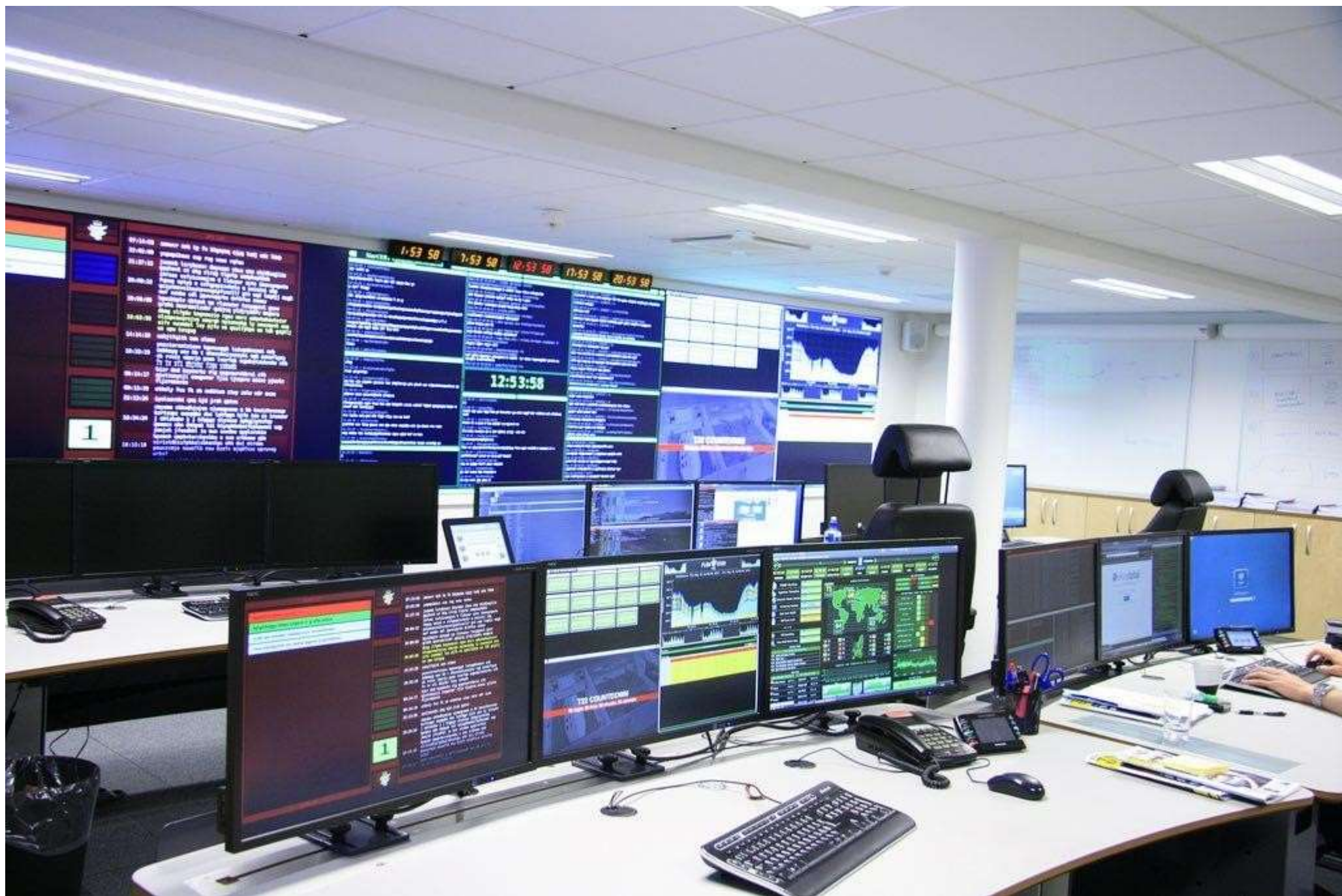
Application proxy

- Simulates the (proper) effects of an application at OSI level 7
- Effectively a protective **Man In The Middle** that screens information at an application layer (OSI 7)
- Allows an administrator to block certain application requests.
- For example:
 - Block all web traffic containing certain words
 - Remove all macros from Microsoft Word files in email
 - Prevent anything that looks like a credit card number from leaving a database

Personal firewalls

- Runs on the workstation that it protects (software)
- Provides basic protection, especially for home or mobile devices
- Malicious software can disable part or all of the firewall
- Any rootkit type software can disable the firewall

Intrusion Detection Systems (IDS)



Firewalls are preventative, IDS detects a potential incident in progress

- At some point you have to let some traffic into and out of your network (otherwise users get upset)
- Most security incidents are caused by a user letting something into the network that is malicious, or by being an insider threat themselves
- These cannot be prevented or anticipated in advance
- The next step is to identify that something bad is happening quickly so you can address it

Signature based

- Perform simple pattern matching and report situations that match the pattern
- Requires that admin anticipate attack patterns in advance
- Attacker may test attack on common signatures
- Impossible to detect a new type of attack
- High accuracy, low false positives

Heuristic based

- Dynamically build a model of acceptable or “normal” behavior and flag anything that does not match
- Admin does not need to anticipate potential attacks
- The system needs time to warm up to the new behavior
- Can detect new types of attacks
- Higher false positives, lower accuracy

Number of alarms is a big problem

- In the Target breach the IDS did correctly identify that there was an attack on the Target network
- There were too many alarms going off to investigate all of them in great depth
- Some cyberattack insurance policies state that if you know about an attack and do nothing they will not cover the attack.
- Having a noisy IDS can potentially be a negative.

Q&A