The University Of Queensland AUSTRALIA | CREATE CHANGE

Business Information Security

Week 09: Security Technology (Part 2)

- Proxies (continued)
- Virtual Private Networks (VPNs)
- Intrusion Detection Systems (IDSs)

Dr Alex Pudmenzky

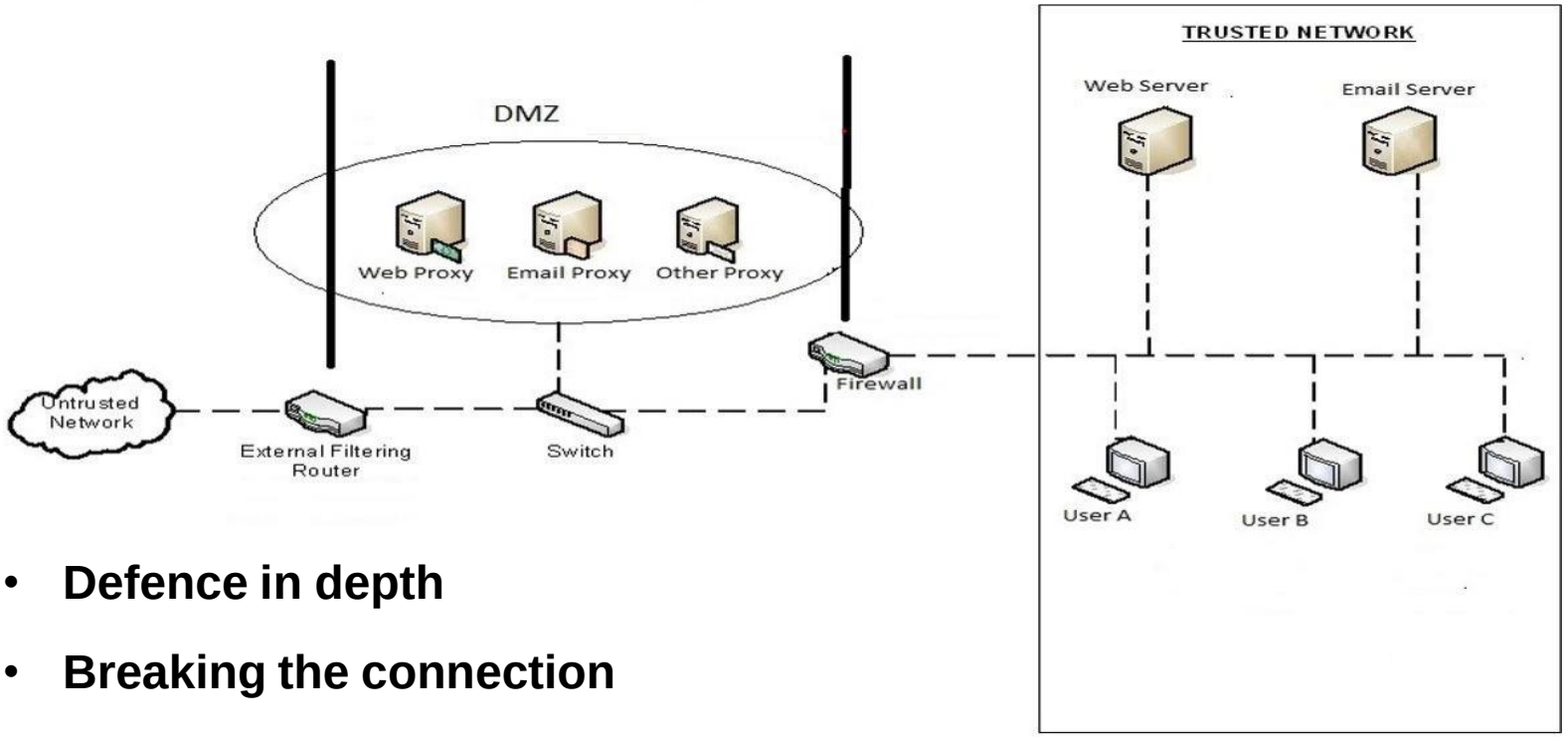
Semester 2, 2024

Overview - Network building blocks/Terminology

- HUB Layer 1 Physical
- Bridge Layer 2 Data Link
- Switch Layer 2 Data Link
- Router Layer 3 Network
- Firewall Layer 3/4 Network/Transport
- DMZ
- Server
- Proxy Layer 7/4 Application/Transport
- VPN
- IDS

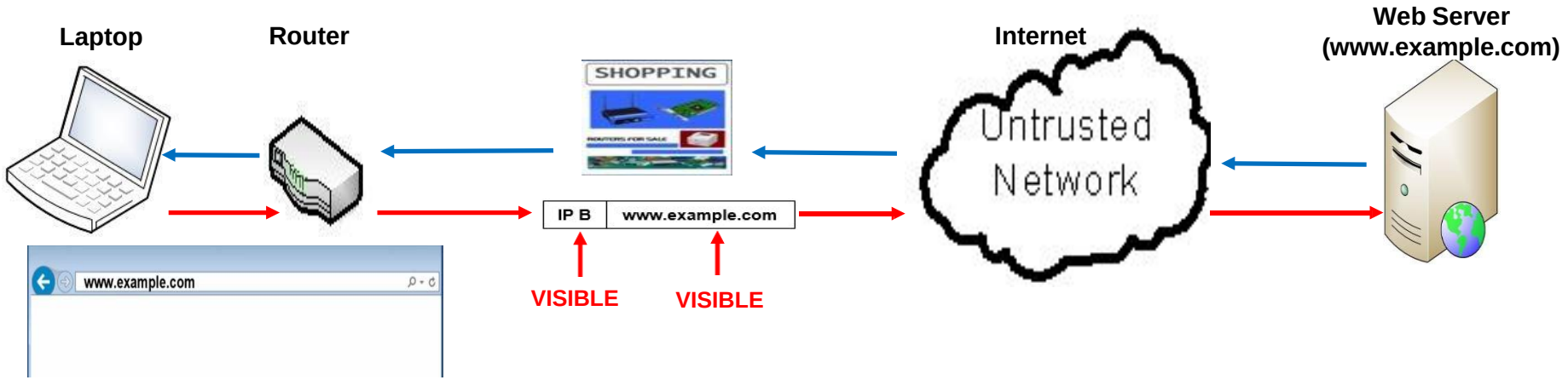
Security: the Demilitarized Zone (DMZ)

Let's talk more about the 'proxy' concept



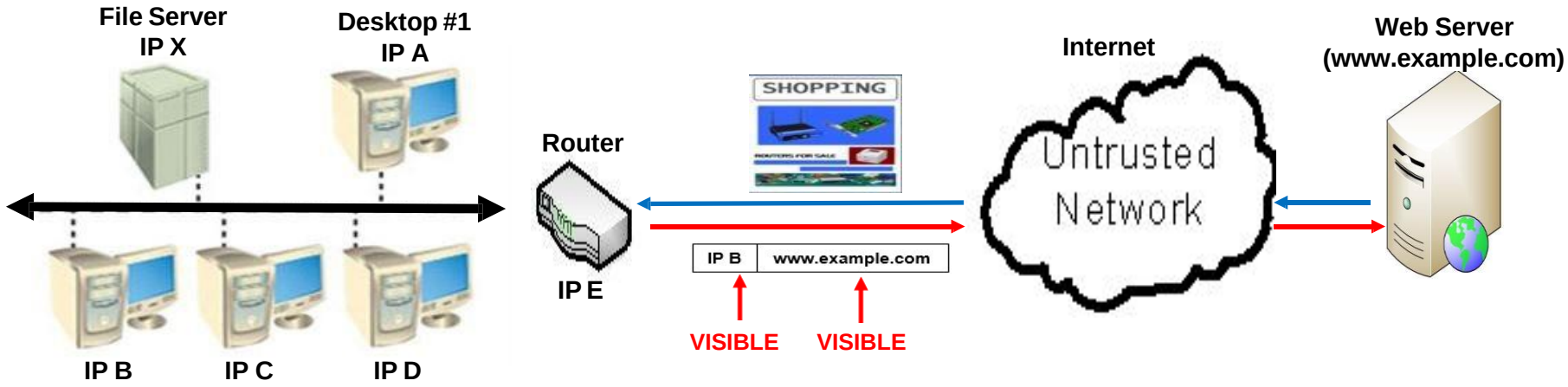
- **Defence in depth**
- **Breaking the connection**
- **Scope**

Home web surfing – what is happening?



- **Basis of online business – but no security unless we add it (refer back to TLS discussion)**
- **What information is available to the business Web Server?**
  WhatIsMyIPAddress.com (or worse, https://amiunique.org/fp)
- **<u>Now let's consider the same web request from a business network</u>**

Business web surfing – what is happening?

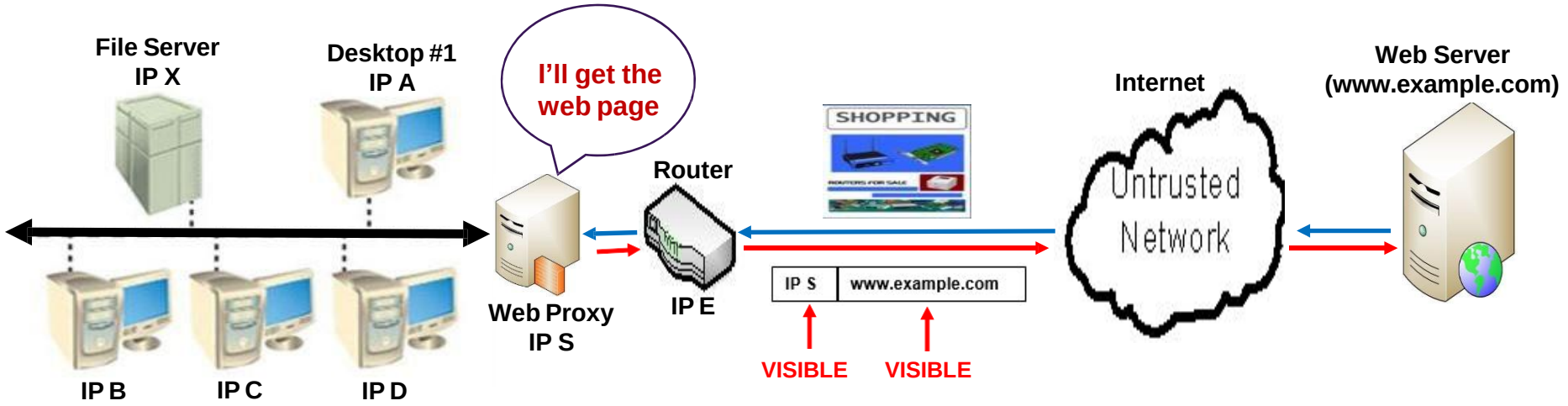


- It's easy to build up (***profile***) a business network which has **no controls in place to mitigate this risk!**
- **From a hacker/security analyst viewpoint – easier to attack what you know!**

BUSINESS NETWORK PROFILE (Externally Compiled)	
Desktop #1	IP A
Desktop #2	IP B
Desktop #3	IP C
Desktop #4	IP D
Router	IP E
File Server	Not known (as yet)

POOR SECURITY

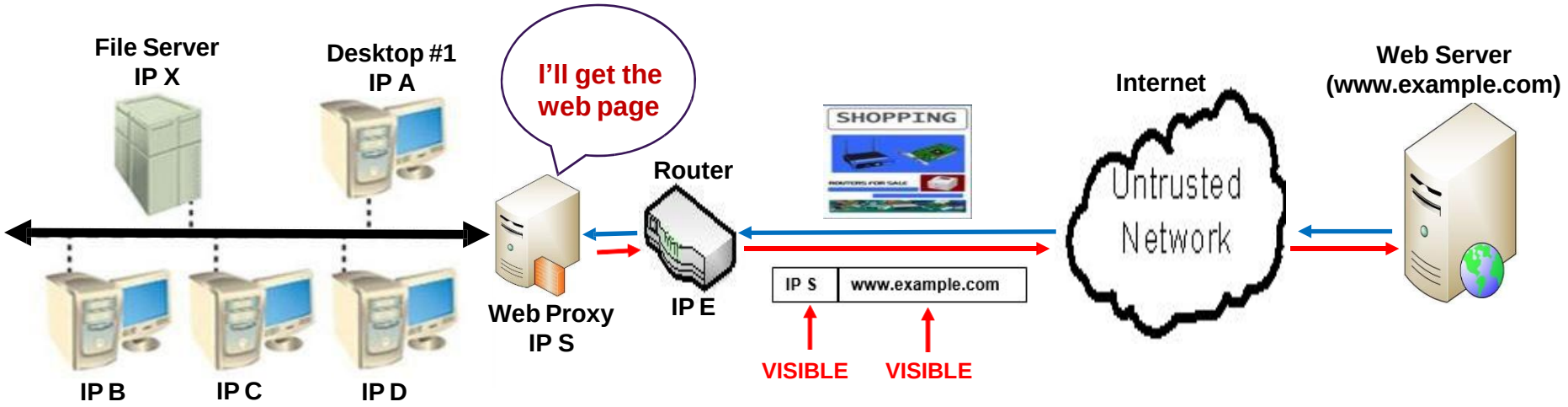
Business web surfing – with a **proxy** - what is happening?



BUSINESS NETWORK PROFILE (Externally Compiled)	
Desktop #1	Not known
Desktop #2	Not known
Desktop #3	Not known
Desktop #4	Not known
Web Proxy	IP S
Router	IP E
File Server	Not known

IMPROVED SECURITY

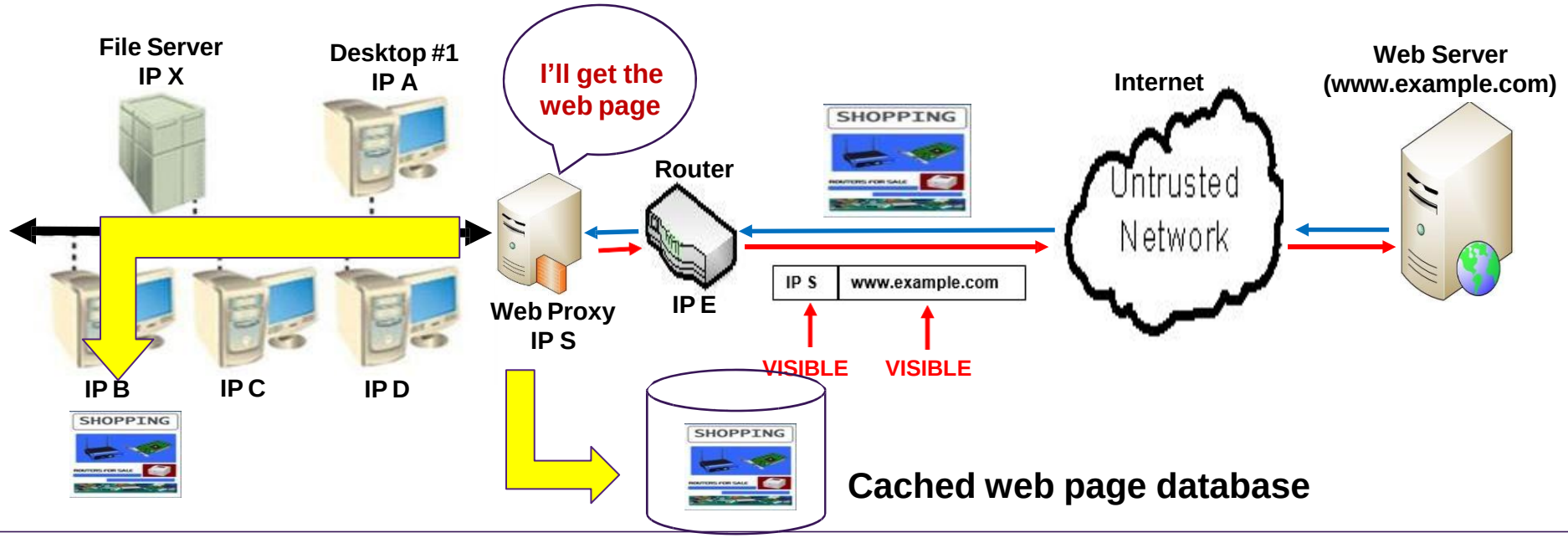
The benefits of a proxy (#1)



Benefit #1:

- **Privacy (for individual machines & the network overall)**
- **Privacy in terms of web surfing history – this is a large component of 'business intelligence' – the outside world knows the web sites we visit – how long we stay on these sites – what parts of these sites we access. Web sites we visit have a very good idea of our details – including (approximately) where we live.**

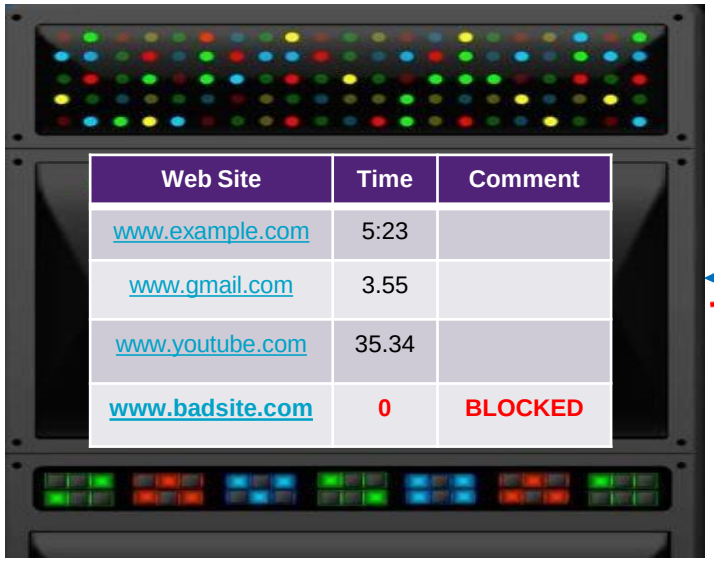
The benefits of a proxy (#2)



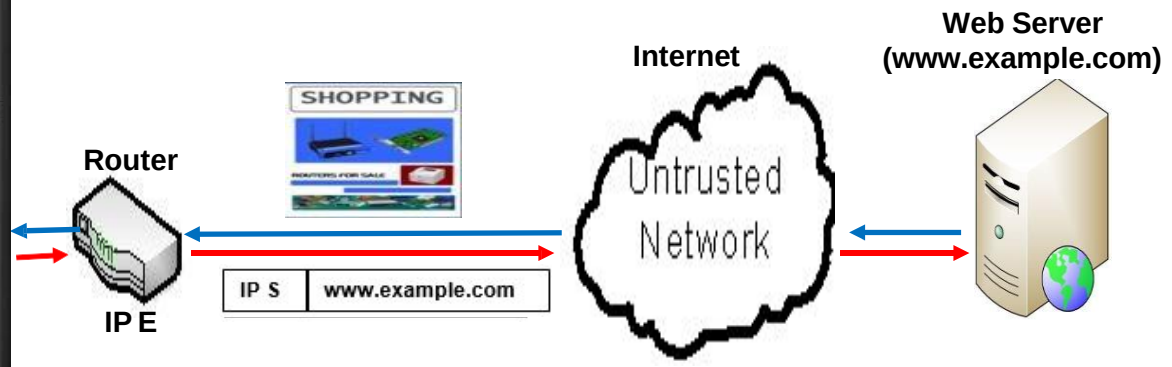
Benefit #2:

- **Speed – faster retrieval of web pages AND**
- **Bandwidth – reduces the need to go out onto the Internet – this is being responsible at a corporate level – it should be part of the Issue Specific Security policy ('Planning' in week 3)**

The benefits of a proxy (#3)



web proxy server



Benefit #3:

- **Management** – **web usage enforced as per Issue Specific Security**
- Activity logging – we see this in all entries – this is just an example
- 'Blacklisted Sites' – we see this in the 4th entry – the proxy stops the corporate network being used for 'undesirable' activities
- All these details are logged for a long term record and ongoing analysis
- We shall come back to this issue – **proxies assist in good management of corporate policy**

Proxy types

Transparent Proxy

•**Definition**: A transparent proxy, also known as an intercepting or inline proxy, intercepts the client's requests without modifying them.

•**Characteristics**:

- The client is unaware of the proxy's presence.
- The client's IP address is visible to the destination server.
- Often used for content filtering, caching, and monitoring.

Non-Transparent Proxy

•**Definition**: A non-transparent proxy, also known as an anonymous proxy, modifies the client's requests before forwarding them to the destination server.

•**Characteristics**:

- The client is aware of the proxy's presence.
- The client's IP address is hidden from the destination server.
- Often used for privacy, security, and bypassing geo-restrictions.

Explicit Proxy

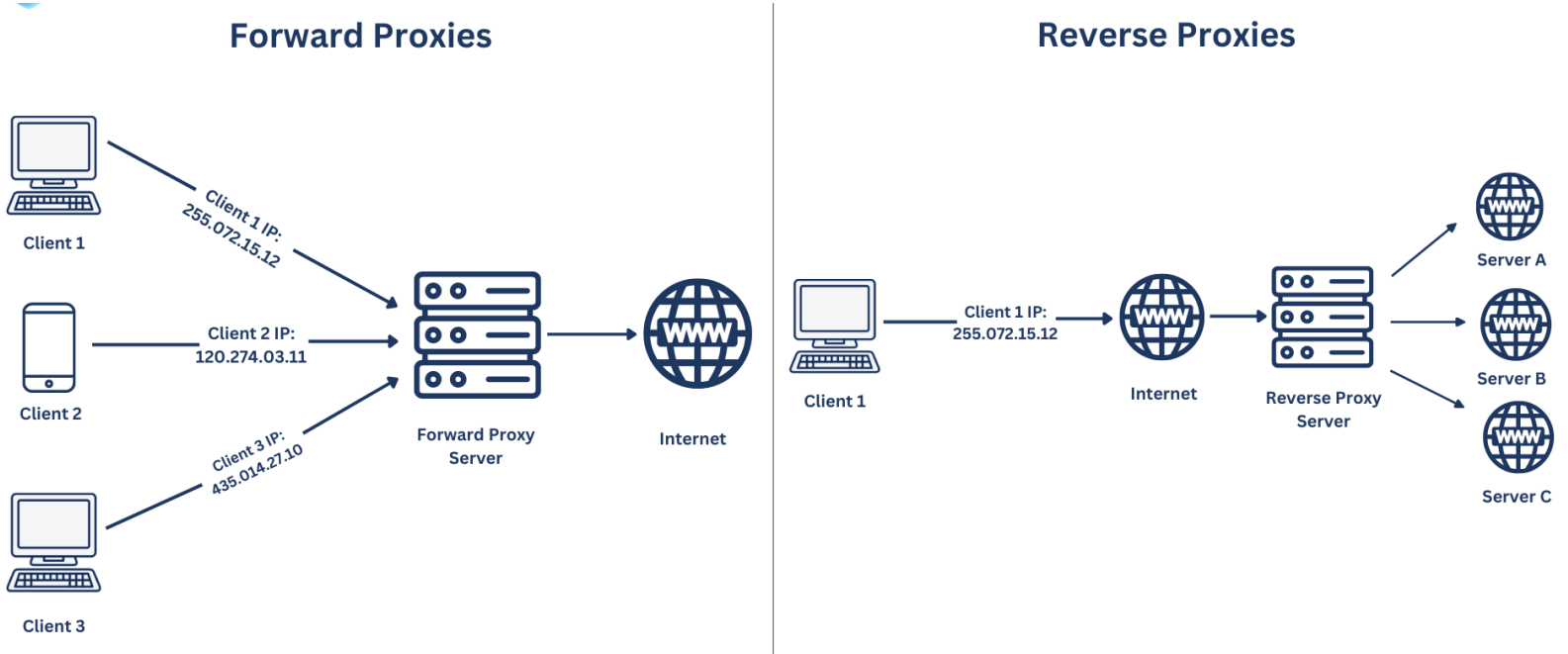
•**Definition**: An explicit proxy requires the client to configure their browser or application to use the proxy server.

•**Characteristics**:

- The client must be configured to use the proxy.
- Can be either transparent or non-transparent.
- Often used in corporate environments for access control and monitoring.

Proxies – in summary

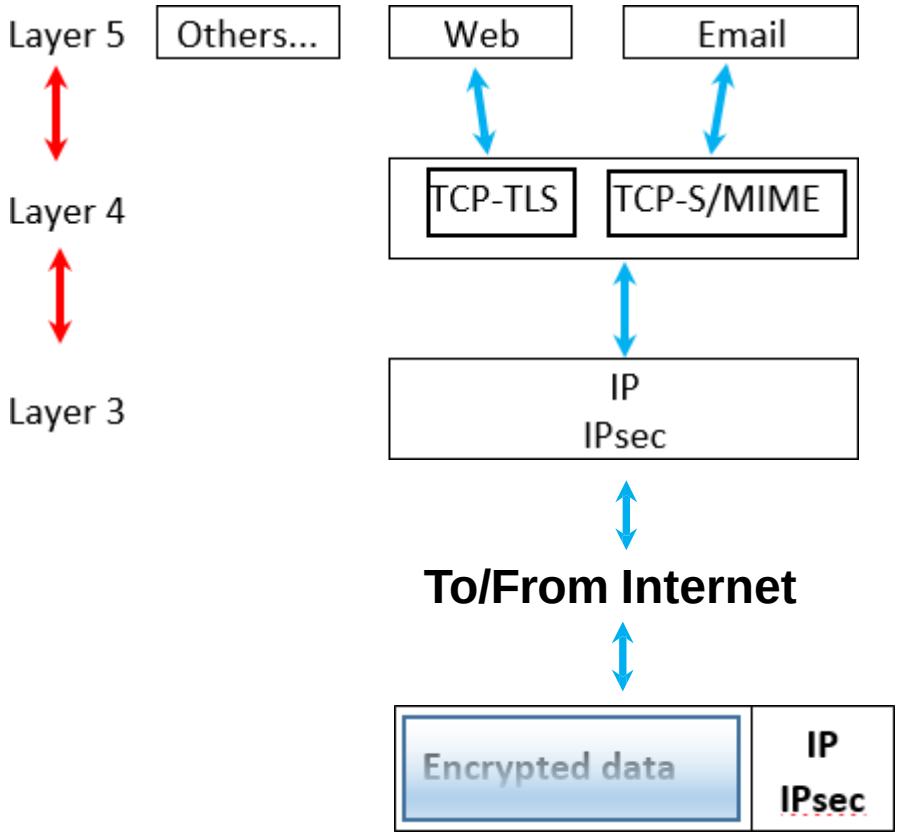
- **Proxies are firewalls – application 'layer' firewalls**
- Proxies are **specialized** – they only deal with 'their' protocol (e.g. web, email) – this is completely different to layer 3/4 firewalls that look at everything (all protocols)
- **Proxies can analyse the data in packets** – again this is different to layer 3/4 firewalls that only analyse the packet headers – proxies are therefore slower than packet filtering firewalls – **but the 'nasty stuff' is always in the data**!
- Proxies are very **efficient in implementing corporate web policy**
- We have talked about a proxy as a single role entity – actually there are '**forward**' and '**reverse**' proxies (diagram below) – we treat them as a single entity



Virtual private networks (VPNs)

- **Transparent proxies cannot encrypt data!**
- A significant **need for private**, **secure network connection** between **businesses** (e.g. professional practices, SMEs, even corporates); any entity using data communication capability of *unsecured*, *public* network
- The **need to maintain the business policies** when workers are remote from the business (but using the business network). This usually involves the **VPN working in cooperation with the corporate proxy server.**
- VPN must accomplish:
  - **Encryption of ALL incoming and outgoing data**
  - **Authentication**

VPN – encryption/decryption of ***ALL*** outgoing data



Many different communicating applications

Web applications use TCP-TLS and email applications uses TCP-S/MIME

ALL APPLICATIONS USE IP
Only one protocol (for unsecured & secured purposes

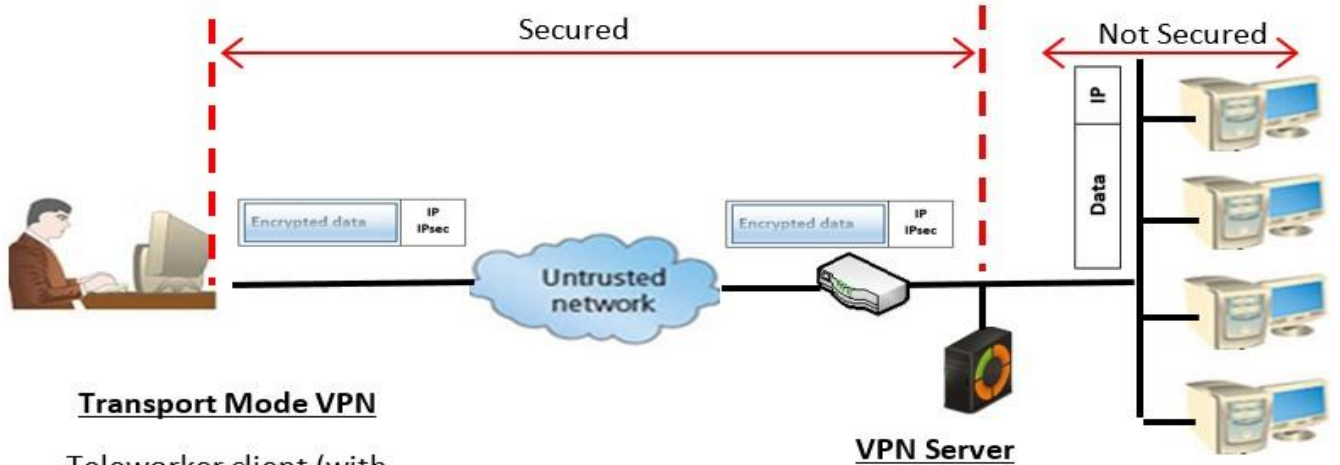
End result is that ALL COMMUNICATIONS are secured when we use a VPN based on IPsec

This is exactly the result that many situations need - *all communications secured* – regardless of the type of sending application! Let's consider two popular scenarios for VPN usage in business

Virtual private networks (VPNs) – Design #1

(1)Transport mode

- **Allows user to establish secure link directly with remote host, encrypting only data contents of packet**
- **Most popular use:**
  - Remote access worker connects to office network over Internet by connecting to a VPN server on the perimeter
  - We say that using the VPN puts the remote worker '*behind*' the firewall/router – '*inside*' their work network. The worker can use all her/his usual work resources from home.



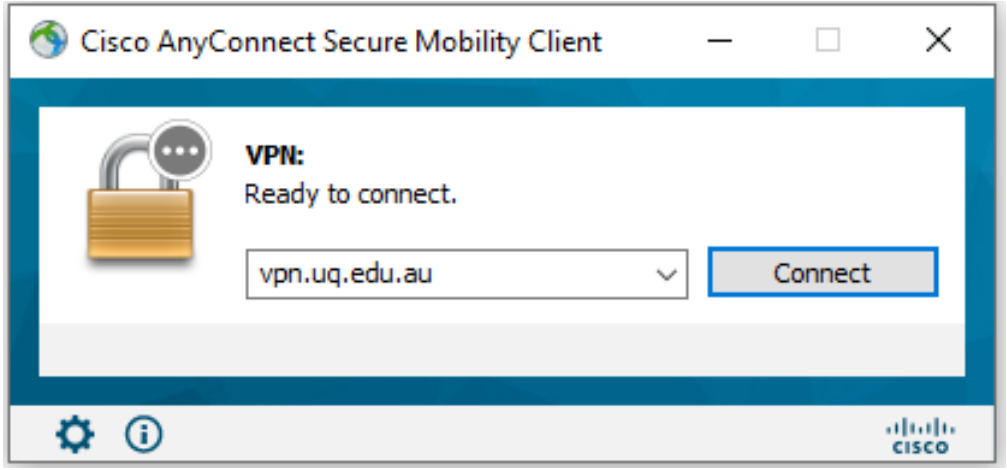
Transport Mode VPN

Teleworker client (with VPN agent) encrypts **ALL** outgoing traffic – decrypts **ALL** incoming traffic to VPN server

VPN Server

Acts as intermediate. Decrypts **ALL** incoming – encrypts **ALL** outgoing traffic to client VPN

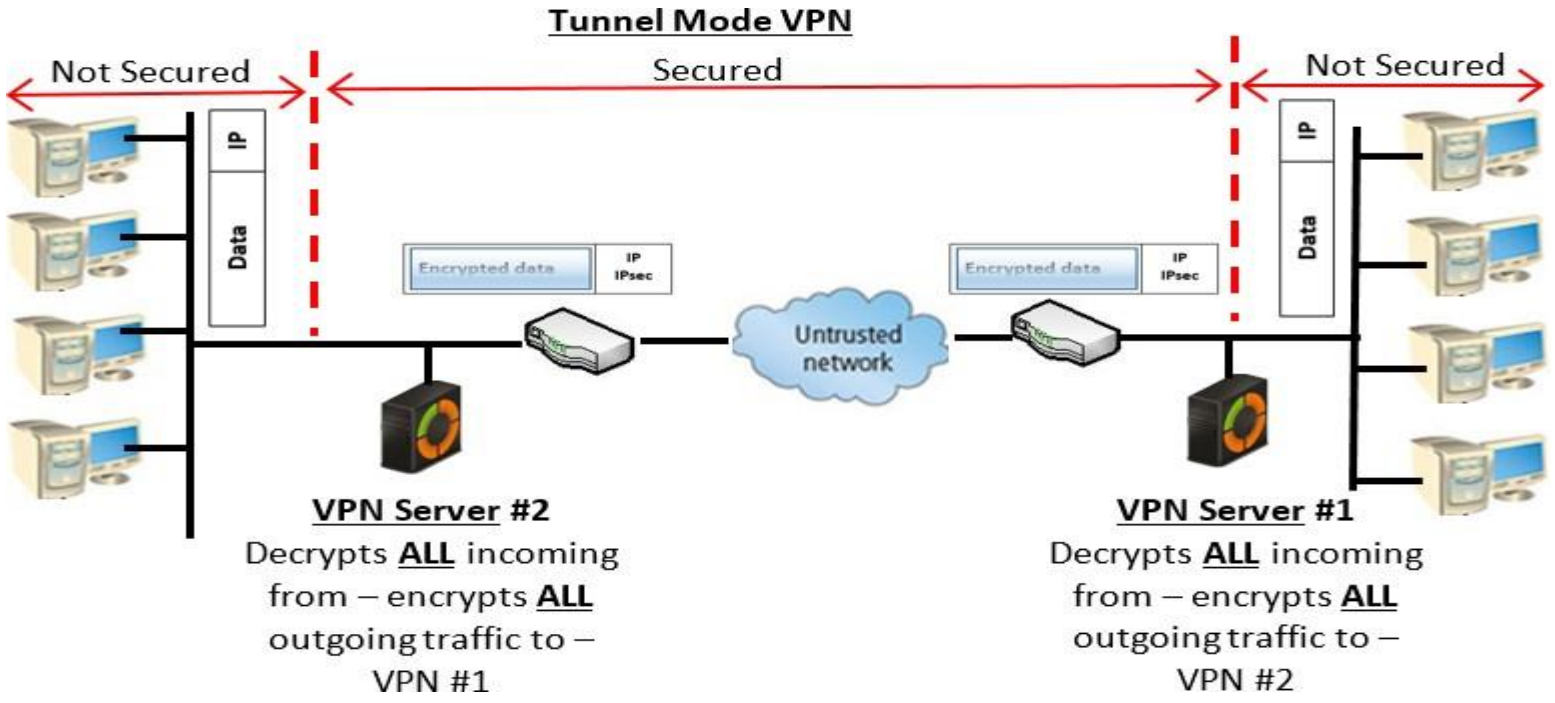
Example Transport Mode: Cisco AnyConnect for UQ



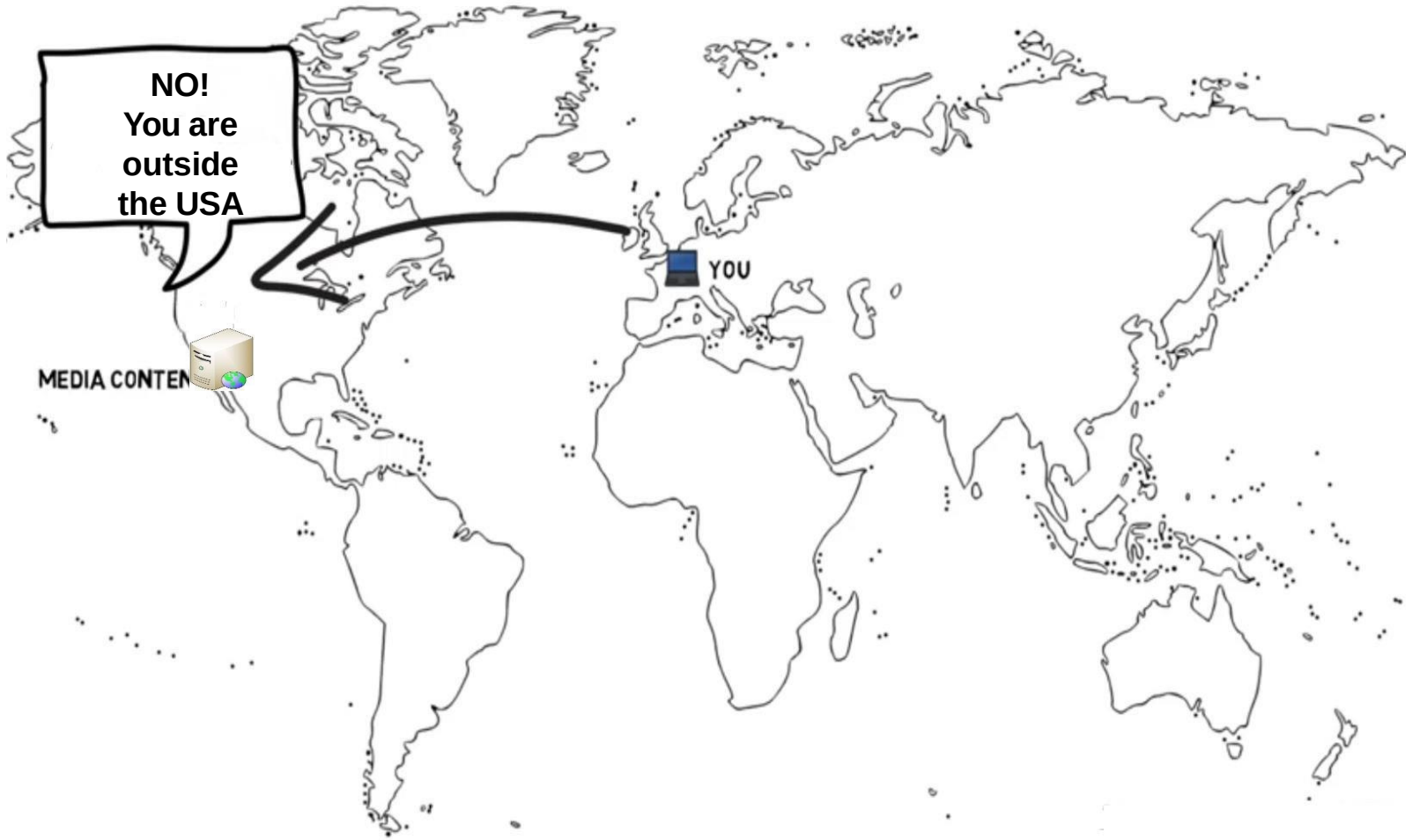
Virtual private networks (VPNs) – Design #2

(2) Tunnel mode

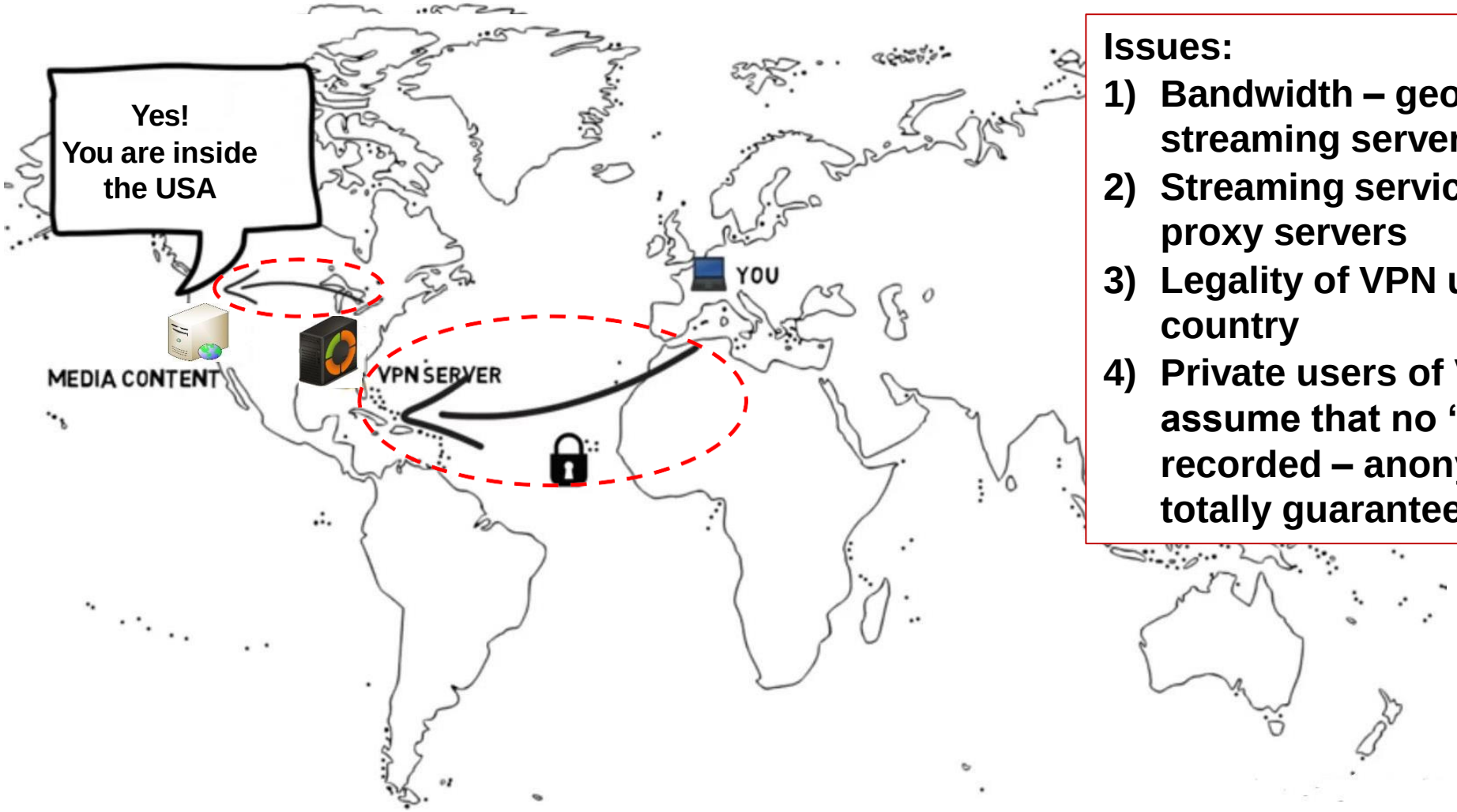
- **Organization establishes two perimeter tunnel servers**
- **These servers act as encryption points, encrypting all traffic that will traverse unsecured network**
- **Very popular secure solution for professional practices (e.g. medical, legal, dental)**



‘Geographical’ restrictions to certain services are problematical



VPN – '*geographical*' restrictions to certain services *may be* avoided!



Issues:

1) **Bandwidth – geography near your streaming server**
2) **Streaming service blocks VPNs / proxy servers**
3) **Legality of VPN use up to the country**
4) **Private users of VPNs should not assume that no 'activity logging' is recorded – anonymity may not be totally guaranteed**

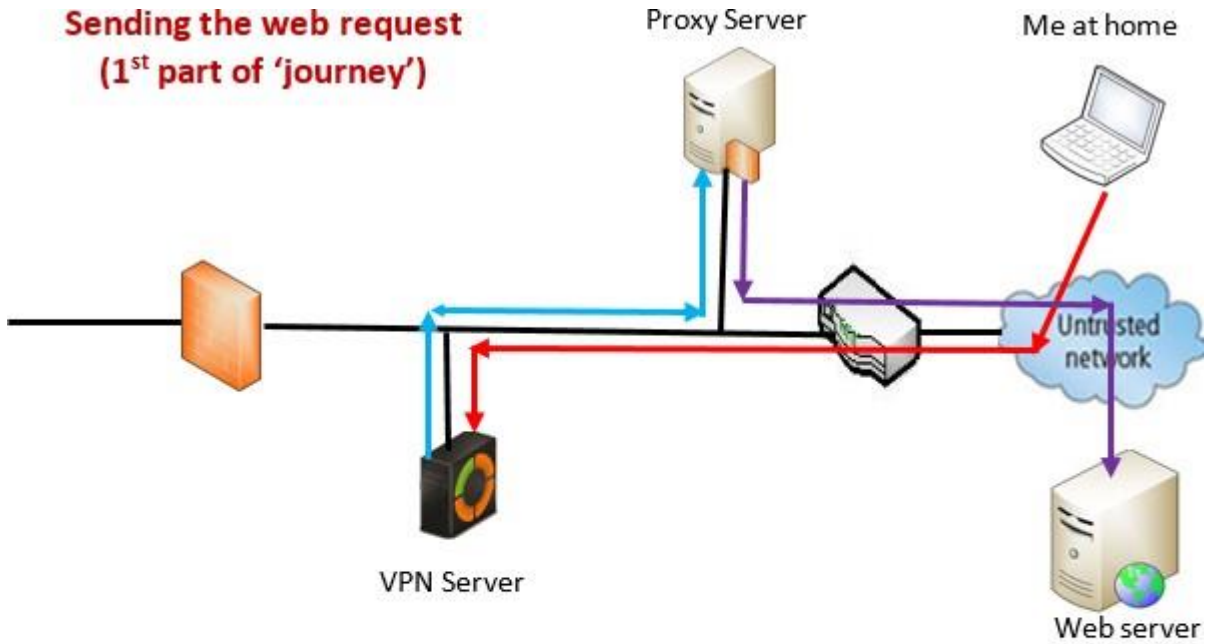
VPNs – the 'business case'

1. **VPNs provide a cheap, secure and flexible way to extend the 'boundaries' of the business network**
   - **The 'teleworker' – becoming more popular in many sectors**
   - **Business to business linkages – opening up (in a secure way) the necessary resources to business partners**

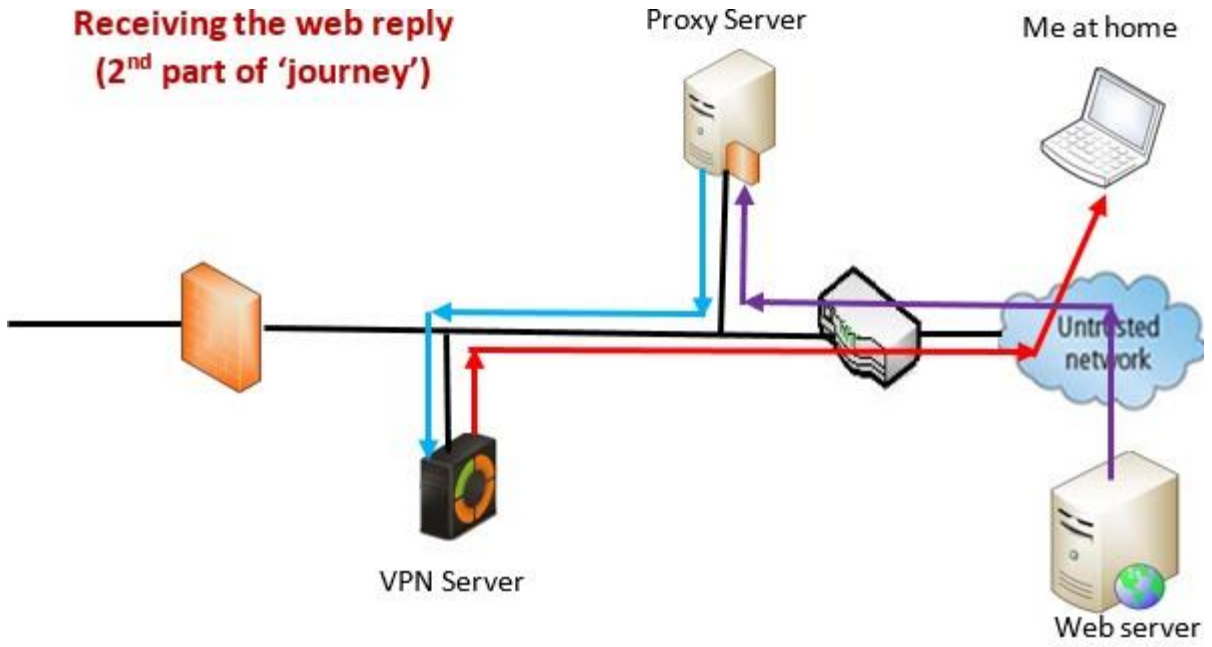
2. **In the 'teleworker' model, the VPN also means that the remote network users (i.e. the 'teleworkers') must follow the same corporate policies as workers 'within' the network must embrace. This is a good result for the organization.**

3. **Point 2 is further enhanced (for web usage) when we consider how a VPN server and a Web Proxy server interact – we now look to consider this!**

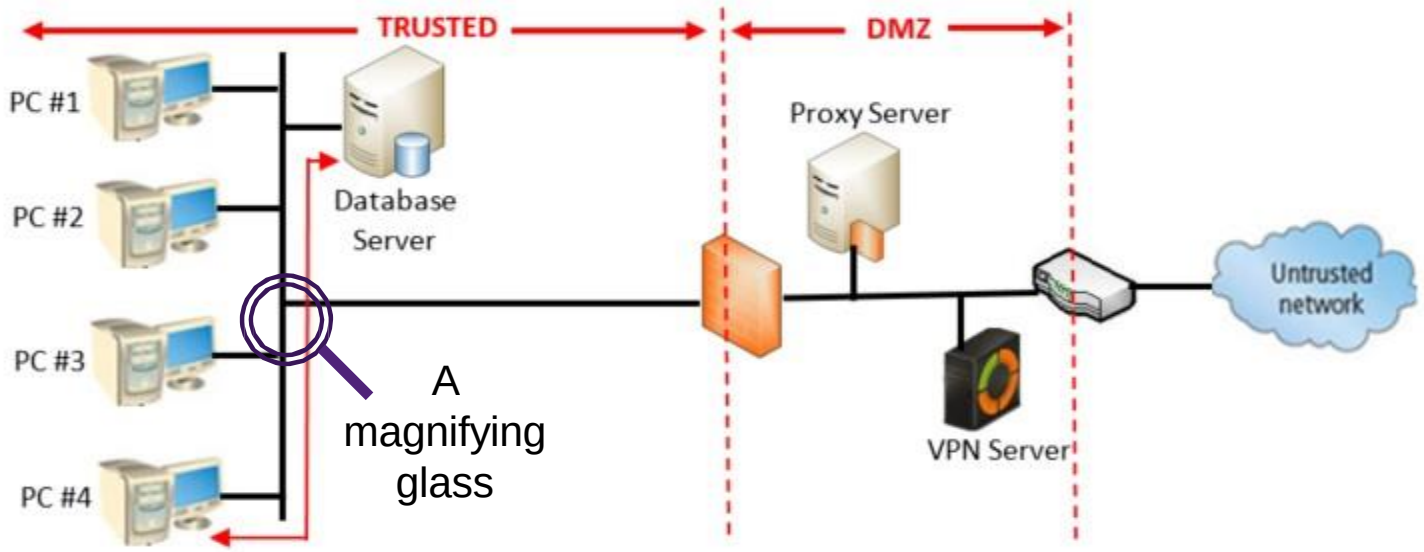
Proxies AND VPNs – working together #1



Proxies AND VPNs – working together #2



Intrusion Detection System (IDS) : Introduction – why needed?

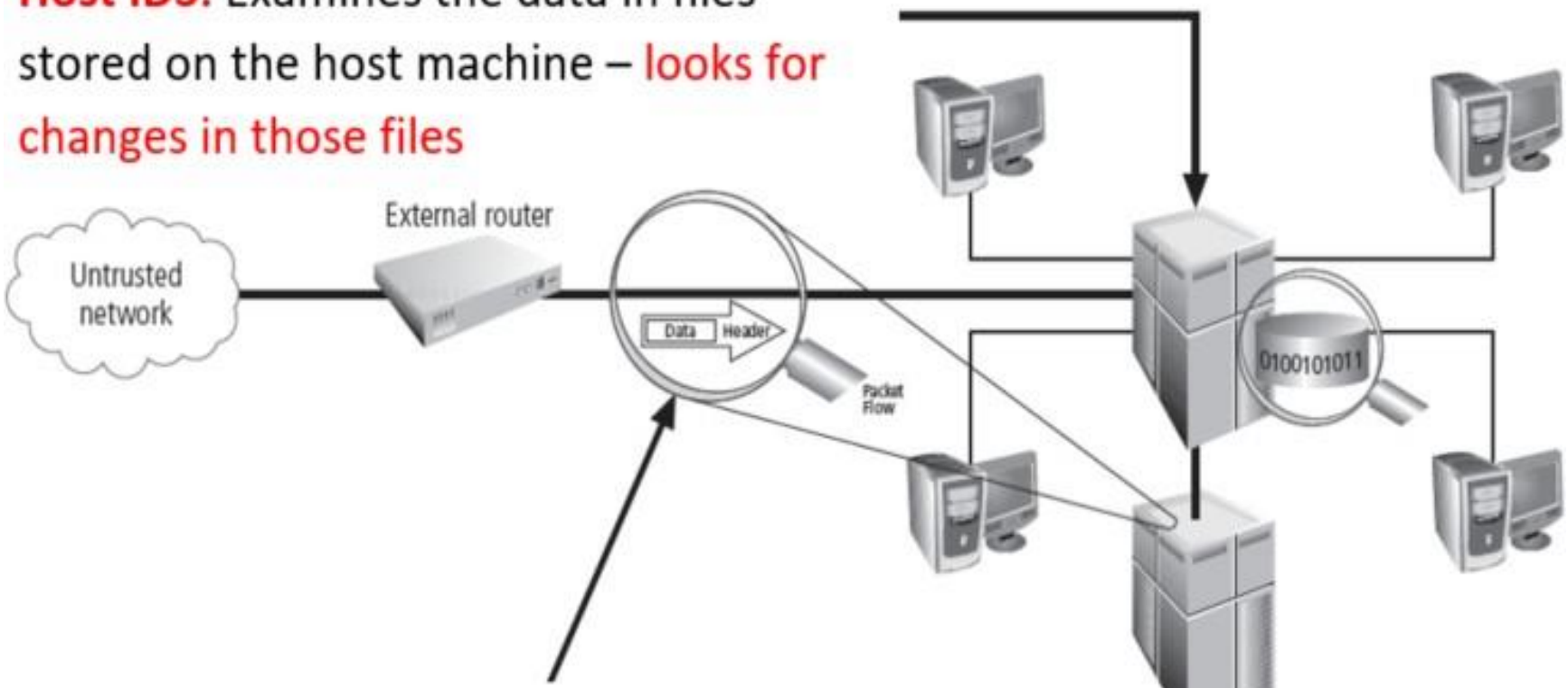


- We have a 'secure' network: firewalls, proxy, VPN server, 'defence in depth'
- At least 50% of security incidents originate INSIDE the organization
- At staff member (PC #4) is a disgruntled employee – plans to steal corporate data (stored on the database server)
  - The employee plans the incident – stays late to avoid other staff
  - What is in place to stop this – the employee is '**behind**' all the existing controls!

We need something like a '*magnifying glass*' over the internal network - IDS

IDS (intrusion detection systems) – strategy in overview

Host IDS: Examines the data in files stored on the host machine – looks for changes in those files



Network IDS: Examines the packets on network – looks for unusual patterns or suspicious contents

HIDS: L6 & 7
NIDS: L3 & 4

Intrusion Detection System (IDS) : Some Terminology

An intrusion detection system (IDS) – a software system - will:

- detect a violation of its configuration and activate alarm
- enable administrators to configure systems to notify them directly of trouble

Important terminology

- Intrusion: type of attack on information assets in which instigator attempts to gain entry into or disrupt system with harmful intent
- Incident response: identification of, classification of, response to, and recovery from an incident
- Intrusion prevention: consists of activities that seek to deter an intrusion from occurring
- Intrusion detection: consists of procedures and systems created and operated to detect system intrusions

IDS – More terminology

- Alert or alarm

- False attack stimulus – event causes alarm – but no attack - false alarm this is a nuisance – can be time consuming for IT staff

- **False negative** – does not respond to actual attack – this is very bad – must be avoided if possible (accuracy of IDS)

- False positive – alarm/alert – but no attack – **again, a nuisance**!

- Noise – 'normal' ongoing activity – usual operating situation

Why use an IDS

- **Prevent problem behaviors** by increasing the perceived risk of discovery and punishment
- To **manage insider risk** – to complement firewalls
- **Detect attacks** and other security violations
- **Detect preambles** to attacks
- **Provide useful information** about intrusions that take place (remember our discussion about '***risk actuals***' – the actual security incidents that the organization experiences)

IDS: 2 types of operating scope & 2 detection methods used

- IDS **operating scope**:
  - Network-based - NIDS
  - Host-based - HIDS
  - Application-based - AIDS (we do not treat this type)

- All IDSs use one of **two detection methods**:
  - Signature-based
  - Statistical anomaly-based

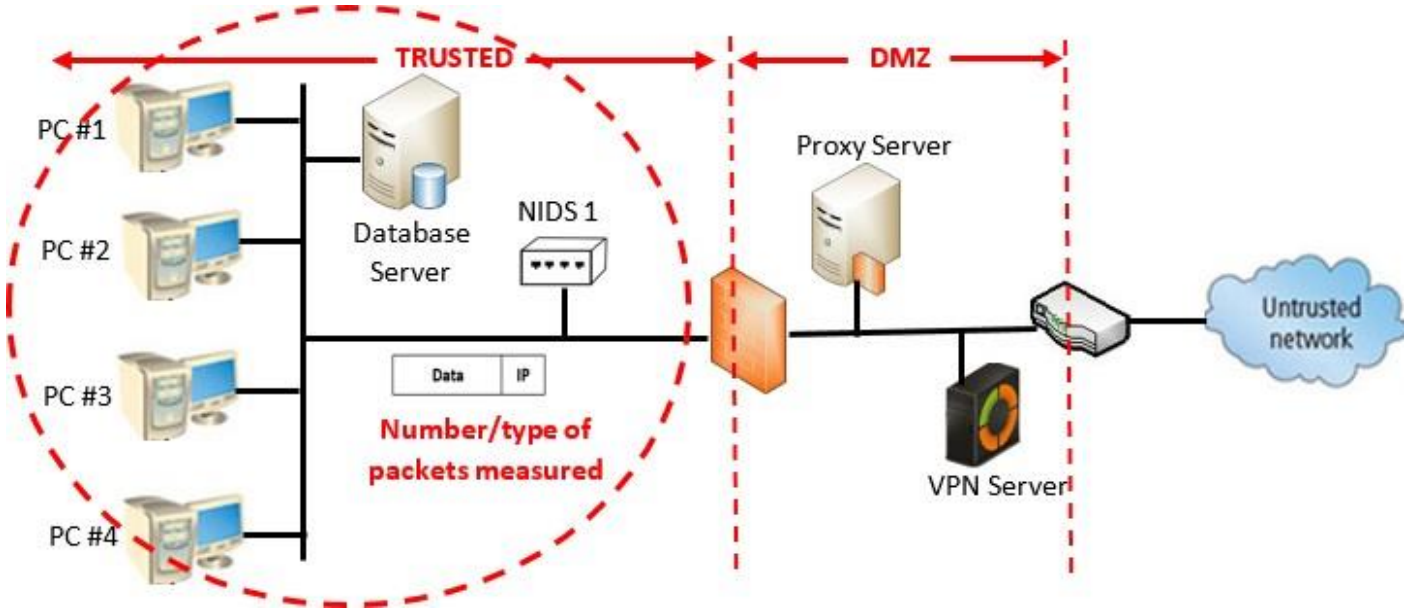
Detection method (1) : signature-based IDS

- Examine data traffic in **search of patterns that match known signatures**
- Widely used because many attacks have clear and distinct signatures (patterns)
- Problem with this approach: **as new attack strategies are identified, the IDS's database of signatures must be continually updated** (very similar to the virus 'pattern-matching approach)

Looking in each 'packet' for known signatures or patterns (of attacks)

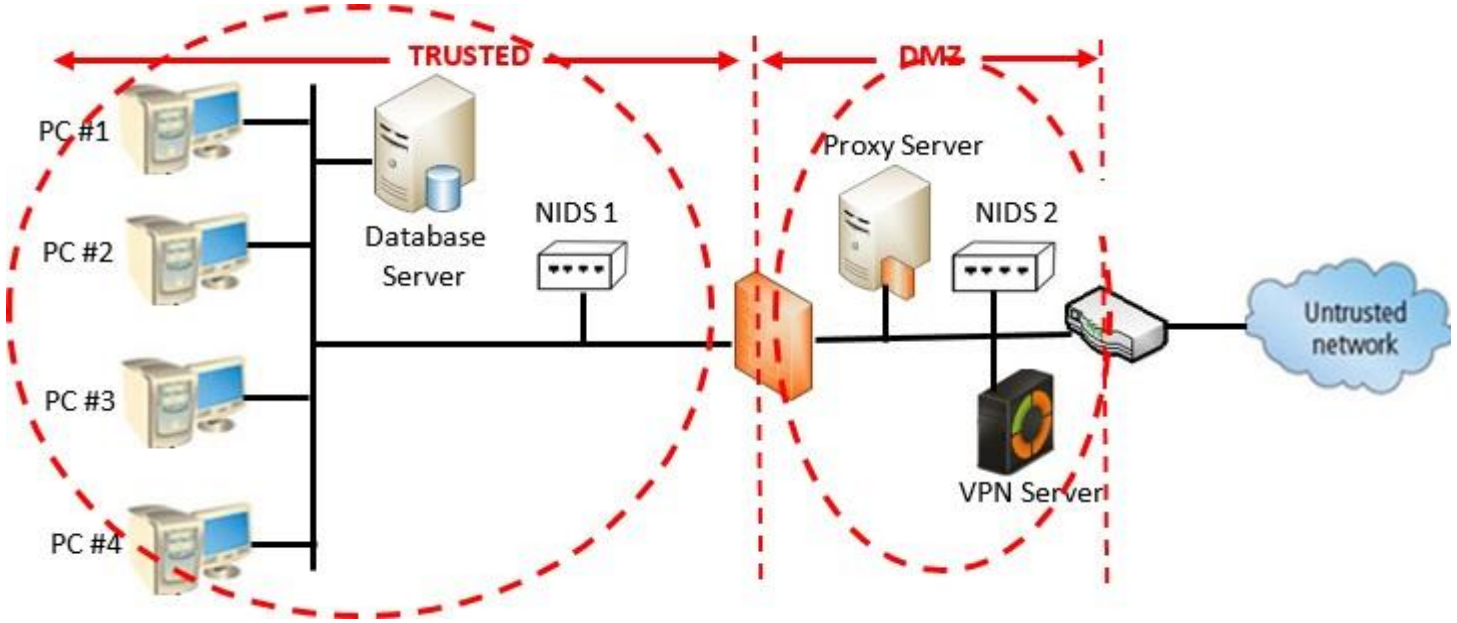
Detection method (2) : statistical anomaly-based IDS

- The statistical anomaly-based IDS (stat IDS) or behavior-based IDS **sample network activity to compare to traffic that is known to be normal**
- **When measured activity is outside baseline setting, IDS will trigger an alert**
- This type of IDS **can detect new types of attacks**, but requires much more overhead and processing capacity than signature-based - may generate many false positives



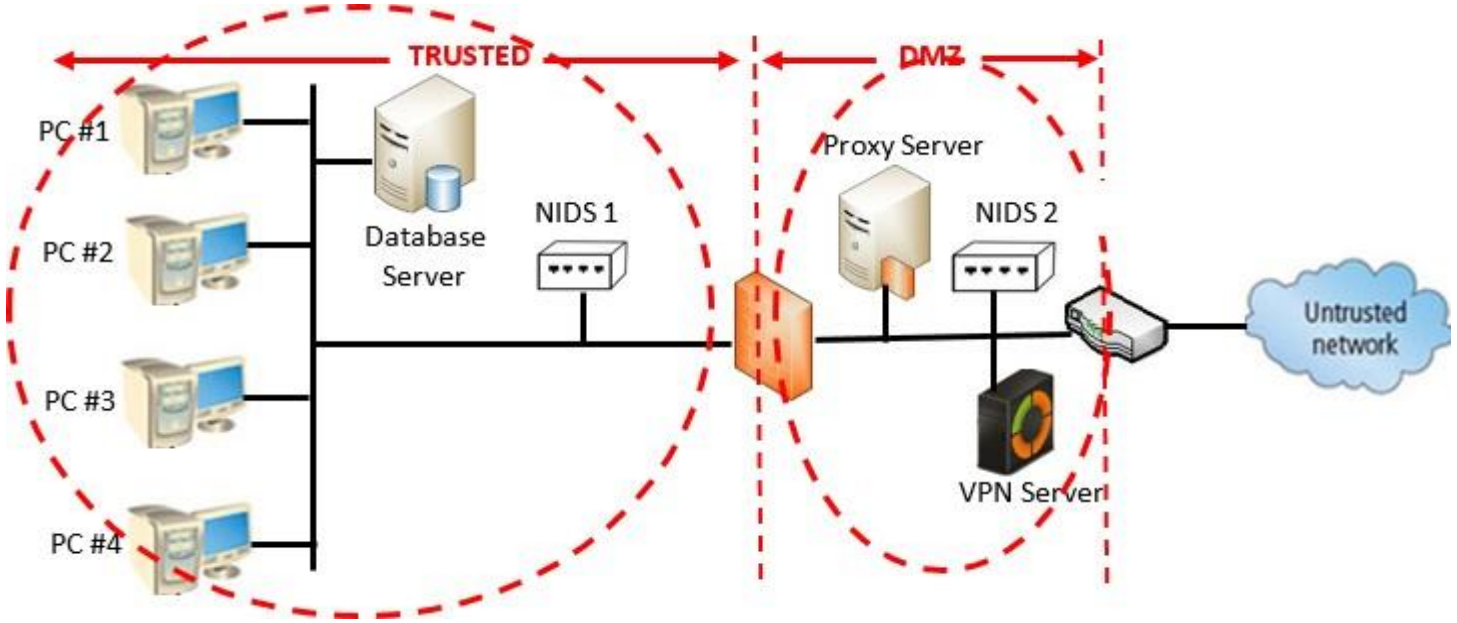
IDS Scope (1): Network-Based IDS (NIDS)

- **Scope** – where we place the IDS and the boundary set for the operation of the IDS
- Resides on computer or appliance connected to segment of an organization's network; looks for signs of attacks
- Installed at specific place in the network where it can watch traffic going into and out of particular network segment



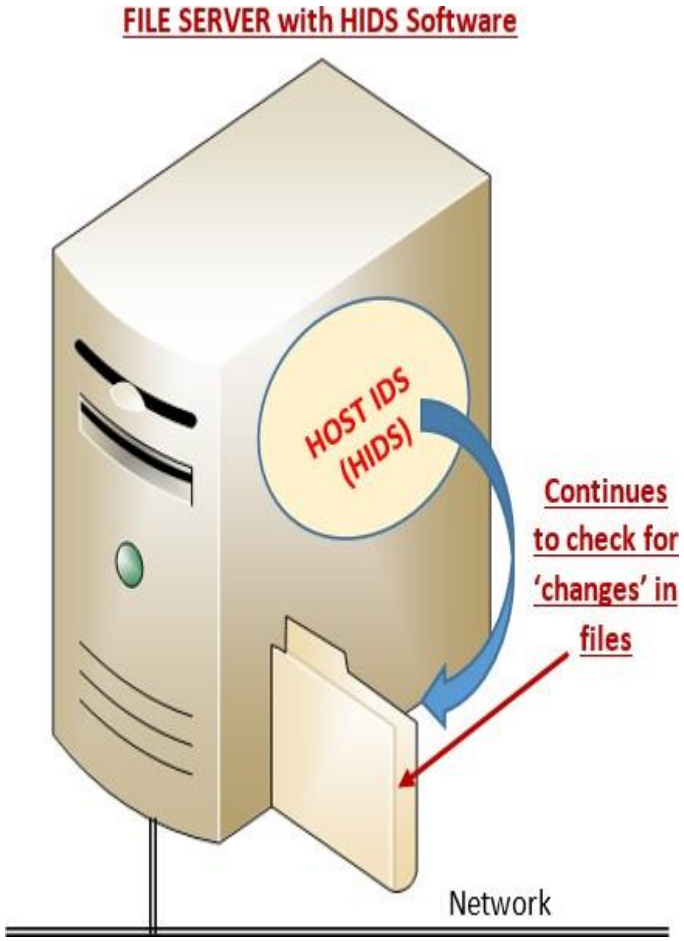
Advantages and Disadvantages of NIDSs

- Good network design and placement of NIDS can enable organization to use a few devices to monitor large network
- NIDSs **not usually susceptible to direct attack** and may not be detectable by attackers
- **Can become overwhelmed by network volume** and fail to recognize attacks
- **Cannot analyze encrypted packets** AND **cannot reliably ascertain if attack was successful or not**



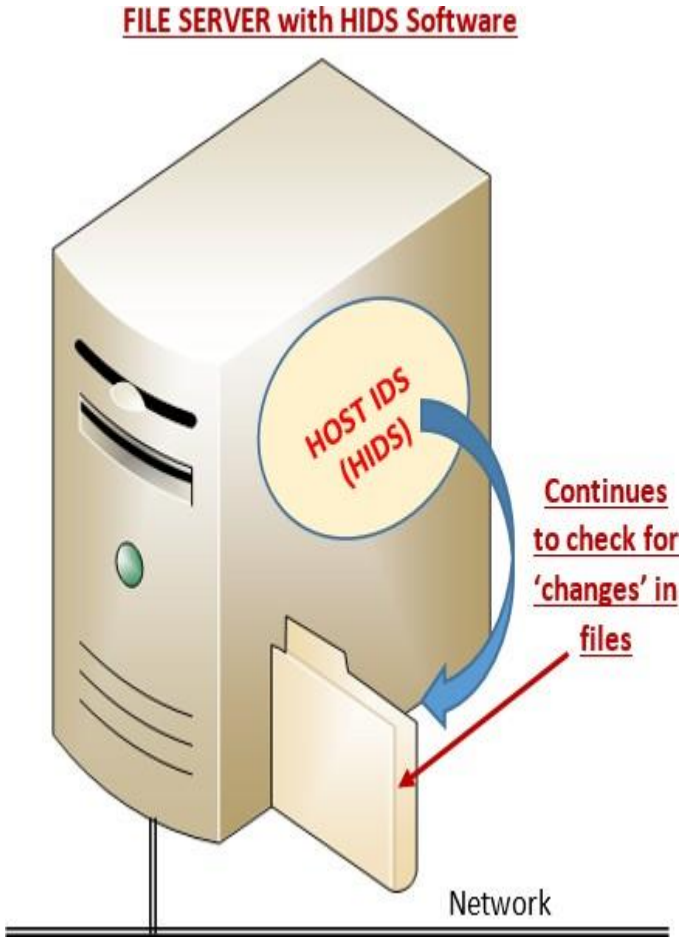
IDS Scope (2): Host-based IDS

- Host-based IDS (HIDS) resides on a particular computer or server and monitors activity only on that system
- Benchmark and monitor the status of key system files and detect when intruder creates, modifies, or deletes files
- Most HIDSs work on the principle of configuration or change management
- Advantage over NIDS: can usually be installed so that it can access information decrypted before/after traveling over network
- Can detect local events on host systems and detect attacks that may elude a network-based IDS



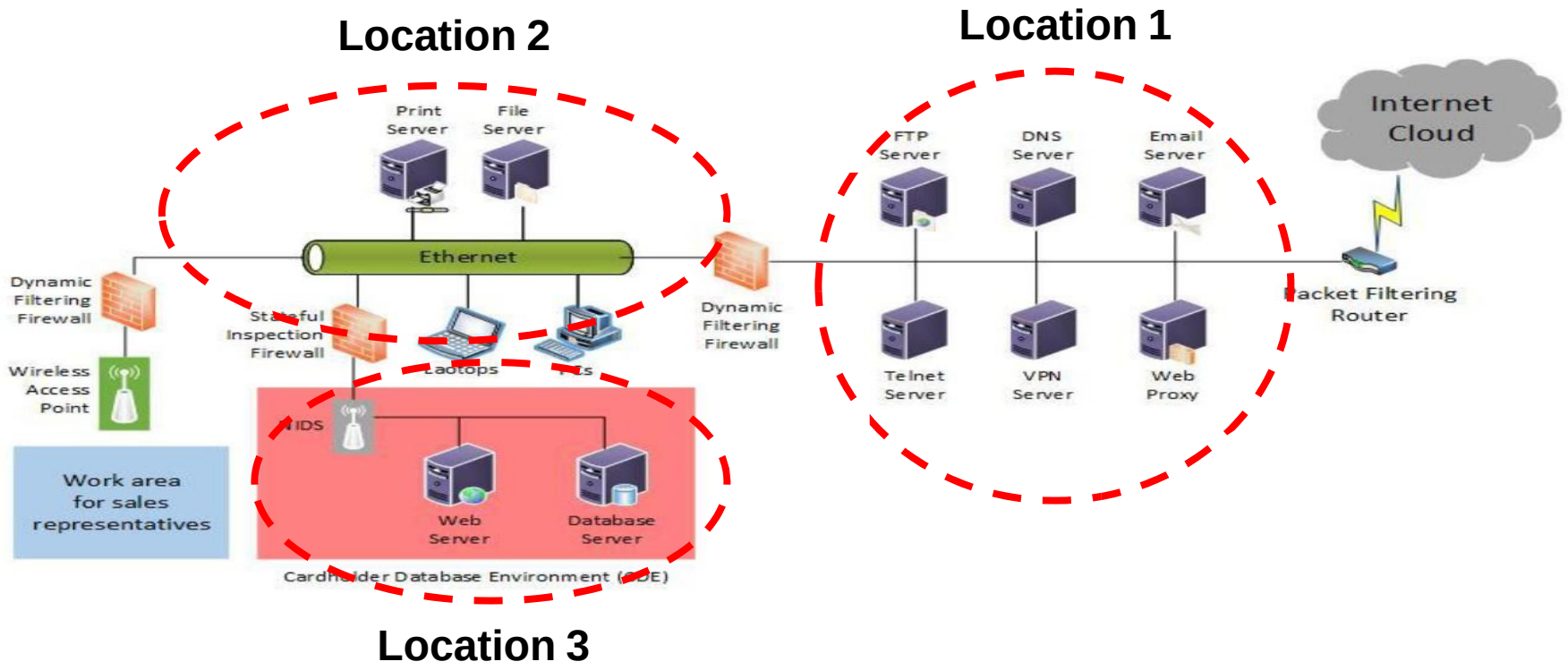
Advantages and Disadvantages of HIDSs

- Vulnerable both to direct attacks and attacks against host operating system
- Susceptible to some denial-of- service attacks
- Can use large amounts of disk space
- Can inflict a performance overhead on its host systems



Deploying Network-Based IDSs

- NIST recommends several locations for NIDS machines
  - **Location 1: behind external firewall, in the network DMZ**
  - **Location 2: On major network backbones**
  - **Location 3: On critical subnet(s)**



Summary

- ‘build a secure network’
- Proxy servers
- Virtual Private Networks (servers)
- Intrusion Detection Systems

- After the break – payment systems & payment standards

"Somebody broke into your computer, but it looks like the work of an inexperienced hacker."

```
        end;

    write(Endtext);
end.
CREATE TABLE product(
    class MultinomialNB(object):
    def __init__(self):
2})
        self.X = None
        self.y = None
    def __loading(self):
        self.list_labels = cl.Counter(
int acc(std::function<int(int, int)>
    auto it = operands.begin();
    int result = func(*it, *(++it));
    if (operands.size() > 2) {
        for (++it; it!=operands.end();
            result = func(result, *it);
        }
    }
    return result;
```

Thank you