Report Title: Synthesize a solution to a potential real-life scenario

Module: Internet Technology and Security

Candidate Name: Cieran Hughes

Candidate Number: 1800730

Course: Applied Computing

Abstract

In this report, it will include:

- Research on all areas of a network and security of that network. This research will be mainly surrounding the topic of BYOD and MDM software. Some of this research can include cloud servers, intranet and extranet.
- A scenario of a proposed network that Hyper-fort can use which has a BYOD scheme implemented in it and a proposal of suitable MDM software that can be used alongside the network.
- The research that was undertaken at the beginning of the report applied to the scenario of Hyper-fort and why the parts of the proposed scenario was chosen.
- An implantation strategy of how the proposed network will be installed.

Contents Page

1. Introduction 1

2. Related Work 1

2.1 Bring Your Own Device (BYOD) 1

2.1.1 Overview 1

2.1.2 Strategy for Different Branded Devices and Operating Platforms 1

2.1.3 Change of device Use 1

2.1.4 Reason for using BYOD 2

2.1.5 Advantages 2

2.1.6 Disadvantages 3

2.2 Mobile Device Management (MDM) Software 4

2.2.1 Overview 4

2.2.2 Data Leakage and Prevention 4

2.2.3 How MDM Software Works 4

2.2.4 MDM Features 4

2.2.4.1 Remote Wipe 5

2.3 Cloud Servers 5

2.3.1 Overview 5

2.3.2 Benefits 5

2.4 Intranet 5

2.4.1 Overview 5

2.4.2 Uses 6

2.5 Extranet 6

2.4.1 Overview 6

2.5.2 Advantages 6

2.5.2 Disadvantages 6

3. Problem Formulation 7

3.1 Wireless Security 7
3.1.1. Encryption 7
3.1.2 Access Levels 7
3.2 External Access 7
3.2.1 VPN 7
3.3 BYOD 8
3.3.1 Usage 8
3.3.2 DFD 9
3.4 MDM Software 9
3.4.1 Microsoft Intune 9
3.4.1.1 Overview 9
3.4.1.2 Reason 9
3.5 Internet security 10
3.5.1 Firewall 10
3.5.2 Online Presence 10
3.6 Physical Security 11
3.6.1 RDIF Card Use 11
3.6.2 CCTV 11
3.7 Servers 11
3.7.1 AAA (Authentication, authorization and Accounting) 11
3.7.3 Cloud 12
3.8 Redundancy 12
3.8.1 Routers and Switches 12
4. Implementation 12
4.1 How the System will be Implemented 12
5. Results and Findings 13
6. Conclusion 13

7. Appendix 14
7.1 Appendix 1 – BYOD Policy 14
1. Introduction and Scope 14
1.1 Introduction 14
1.2 Scope 14
2. Roles and Responsibilities 14
2.1 User Responsibilities 14
2.2 Designated Manager Responsibilities 14
2.3 Implementation Officer 15
3. Policy 15
3.1 Objectives 15
3.2 System, Device and Information Security 15
3.3 Monitoring of User-Owned Devices 16
3.4 Support 17
3.5 Use of Personal Cloud Services 17
3.6 Compliance Sanctions and Disciplinary Matters 17
7.1 Appendix 2 – Packet Tracer Simulation 18
8. Bibliography 19

1. Introduction

This report provides information from research through online web articles and posts. It will show the advised simulation for Hyper-fort to use for their network. It will pay most attention to introducing the BYOD and MDM systems to the network, outlining the security concerns with these areas and solutions for these concerns. There will be research on the areas talked about throughout the report first. Then following this the section will show analyse the simulation, explaining how the network functions and a recommended MDM to use. Finally, a section on how the network will be implemented and recommendations.

2. Related Work

2.1 Bring Your Own Device (BYOD)

2.1.1 Overview

Bring Your Own Device (BYOD) is being increasingly used by companies. It is the process of company employees using a device of their choice [1]. An example of this would be checking their corporate email on a personal smartphone.

A good way where a company will put this in too practise is if they have a hotdesking system. This is where the employees don't have a desk and come in day to day and use a free desk of their choice. To be able to do this. The BYOD system needs to be in place, so employees can come in and use their own device for work and play throughout the day [2].

2.1.2 Strategy for Different Branded Devices and Operating Platforms

The companies that support BYOD in their policies there will be rules on devices that can be used. Looking at the Appendix 1 – BYOD Policy Section 3.4 Support, it states that the company will support all devices, but the user has the responsibly to learn and install the relevant software to get the device in line with the whole policy. So, if the device can support all the policy then it won't be able to be used by the employee as a BYOD.

2.1.3 Change of device Use

When the device has a change of use there are procedures in place that can stop data from being leaked or obtained by personnel that are unauthorised to see it.

An example of this is an employee losing a device or getting stolen. Looking at the Appendix 1 – BYOD Policy Section 3.2 System, Device and Information Security, it says that the device is required to have tracking and wiping software configured on it. Therefore, if the device does get lost or stolen then the employee or the security director can wipe the lost device remotely so there is no company data on the device.

2.1.4 Reason for using BYOD

As seen in Appendix 1 – BYOD Policy Section 3.1 Objectives, there are many reasons for a company using BYOD. Some of these reasons are:

- Reducing the cost for the company as employees provide their own devices.
- Improve moral by giving the employees the freedom to choose their own devices that they can work on, this includes personal devices that they own.
- Improved productivity. With the employees using their own devices, usually they product higher quality work at a faster output rate as they are used to the system [3]
- Improved use with Cloud services. BYOD goes hand in hand with cloud services as the company's employees have the devise on them at all time. This makes them able to access they advanced work tool at any time on the device. As Hyper-fort uses cloud services to deliver IT services to the staff and clients, this work for them.

2.1.5 Advantages

There are advantages to the company when using BYOD. Some of these are listed below:

- It saves the company money as they don't need to provide all the employees with specific devices and equipment, the employees provide it for themselves [4]. Also, when people use their own equipment, they will take more care when looking after it as they paid for it themselves. This is an advantage for the company as it the BYOD scheme wasn't in place, they would need to replace all broken equipment [5].
- Another advantage of BYOD is the users will be familiar with the technology they are using. When employees bring their own device, they are already used to all the components of it like the OS, they will be familiar with the shortcuts and so on. This takes away the irritation of working on a company device that the employee isn't used too [5].

- It allows the company to have up to date technology. This is the case as the employees will be buying the latest technology to work on as they will get irritated with old, slow technology [4].
- Finally, an advantage of BYOD is improved productivity. As stated in the reasons for BYOD, when employees use their own devices, they product higher quality work at a faster output rate as they are used to the system [3]. This is because when they are used to a machine and have used it for a while it is configured how they like. This will make it quicker for the user to navigate the system, therefore producing work quicker. Also, after using a device for a long amount of time the user of the device will be more used to the keyboard and mouse, so they will be quicker typing and using the device, therefore also being more productive

2.1.6 Disadvantages

There are also many disadvantages to a company that use BYOD. Some of these can be:

- People leaving the company. There are procedures in place for this, but it is hard to get around as the employees will always have some sort of data retained on their device [4].
- Accessing the companies cloud services from an unsecure place. When employees are accessing the resources from the cloud services provided by the company, there is a chance that they could be accessing these resources from an unsecure WIFI point. These could be in airports, coffee shops, stores or at home. When they access the company's resources from these points, they provide hackers with easy access to a company's network or system.
- The cost for the employee [5]. As said above the company doesn't need to pay for the device, but the employee might not agree or want to pay this cost for a new device as these devices can be expensive. If starting a new job and the company expects the employee to buy a starting device as they don't have one it could put the employee off.
- Lost or stolen devices. There are procedures in place to stop this. These procedures are installing wiping and tracking software on the devices, but this software isn't always 100% effective [4].

2.2 Mobile Device Management (MDM) Software

2.2.1 Overview

Mobile device management software is security software that can monitor, manage and secure employees mobile devices that are connected to the company's network [6]. It allows IT administrators to control, secure devices and enforce the security policies on the smartphone, table or other endpoints [7]. The main intent of the software is to secure the devices in the company's network [7], as when the devices are secure, they can introduce other software like Mobile Information Management.

2.2.2 Data Leakage and Prevention

The way data leakage is kept in control is using Mobile Information Management (MIM). This is software can be put on the devices and it manages the security of the business sensitive data used for work purposes [8]. It works by focusing on the data itself, rather than the service or the applications using it. It will encrypt or strongly password protect the data, ensuring that only the authorised applications can access, transmit or store the sensitive data [8]. This is how data leakage is kept as a minimum when using BYOD.

2.2.3 How MDM Software Works

The MDM system relies on the end device having the MDM agent installed on it. This would be stated in the security policy that the company would provide. It also relies on the MDM server that lives in the server room or on the cloud [7].

The IT administrators would specify and configure the policy on the MDM server, these policies would then be pushed on the end devices using the MDM agent software on them. The MDM agent will apply the policies on the end device by using application programming interfaces (APIs) which are built in to the operating system [7].

2.2.4 MDM Features

There are many features on MDM. Some of these are listed below:

- Device Tracking [7]
- Remote Wipe [7]
- Password Enforcement [7]
- Data Encryption Enforcement [7]

2.2.4.1 Remote Wipe

Remote wiping of a device is the process of the IT administrator or device owner to send a command to an end device and delete data on the device [9].

A remote wipe can wipe curtain data specified, from selected data in folders, return the device to factory settings or remove all the programming on the device making it unusable [9]. A remove wipe is useful for a company using BYOD, as theft of a device can not to a problem as all the data can be deleted with a command to the device.

2.3 Cloud Servers

2.3.1 Overview

A cloud server is a virtual server that is rented from an external company. The cloud server is built, hosted and delivered through a cloud computing environment over the internet which can be accessed remotely [10].

2.3.2 Benefits

There are many benefits of a company using cloud servers. Some of these benefits are listed below:

- When using cloud server, it is easily scalable. The company can add memory or disk space with ease at just an extra cost [10].
- Avoidance from hardware problems. As the server is virtual it is reliable for a company that want to be up all the time with no downtime [10].
- Speed. Cloud servers are quicker than physical server. When hosting a website, a cloud server hosted website will be accessed quicker than a physical server hosted website [10].

2.4 Intranet

2.4.1 Overview

An intranet is a private enterprise network designed to give support to the employees in the company network [11]. An intranet tool can be anything that is only usable from being inside the network. This can be, the device being in the building of the server the intranet is running from or using a VPN to access the resources on the server. These can be an internal website, internal communication platform, internal collaboration tool or an internal social network.

2.4.2 Uses

There are many uses for an intranet. One of these can be an internal website hosted with in company showing progress of implementations in the software and the stages the work is in. Another use for an intranet is hosting a communication tool. As this will be the best way for big companies to connect their staff that can be located worldwide. Another use for an intranet is to centrally host important documents like the Employee Handbook or Security Policies documents.

2.5 Extranet

2.4.1 Overview

An extranet is a part of a company's intranet that has been extended outside of the company [12]. This then can be accessed by the supplier, venders, partners, customer or other businesses [12]. The extranets can be accessed using firewall server management, digital certificates, username and passwords or similar authentication [12].

An example of a use of an extranet is sharing data with another company. This can be progressions of a task that is needed to be done or shared resources between them [12].

2.5.2 Advantages

There are many advantages of using an extranet. Some of these are listed below:

- Collaborate with other companies [13].
- Exchange large amounts of data [13].
- Share exclusive product catalogues with specific trade partners [13].

2.5.2 Disadvantages

There are a few disadvantages of using an extranet. Some of these are listed below:

- Extranets can be expensive to implement [13].
- Security can be a concern when hosing valuable information [13].

3. Problem Formulation

3.1 Wireless Security

The wireless access points in the building in the Hyper-fort offices all use WPA2-PSK security. Connecting to these access points means having the SSID and the Pass Phrase.

3.1.1. Encryption

The encryption on the wireless access points is AES. This security is the highest security that can be added to these wireless access points making it impossible to brute force attack to get the encryption key [14]. This is important 95% of the Hyper-fort network is wireless, so if there was a vulnerability in wireless data transfer then this would mean 95% of the transferred data could be read.

3.1.2 Access Levels

The Hyper-fort network will need to have access levels as the company allows their large staff and customer base access resources on their network. On the network there is information that can't be shared with users that are unauthorised to see the data, as there is personal data of employees and customers. Another worry for the company is protecting their intellectual properties as it is worth billions.

To protect this data, it is assumed that when the user signs in to the network there is a login portal hosted by the intranet. Each person that can access the network had a unique login for this portal, and this will push them on to a specific VLAN giving them access to data that is only relevant to what they are doing. This will all be done by using an AAA sever on the network. An example would be a customer on the network using the resources, not being able to see the company's financial data.

3.2 External Access

3.2.1 VPN

This VPN is a site-to-site VPN. It is assumed that this VPN is configures securely. This type of VPN allows the user to connect to the company's LAN network securely over the internet, allowing them to access the company's resources from outside the LAN [15]. There will be two type of VPNs used, the first one would be for one user connecting from home. The other

VPN would be connecting a close working company, such as a partner, supplier or customer. The VPN client would be installed on a local server in the network and the remote accessing computers would connect to that.

The first VPN is an intranet VPN. This VPN would allow access to employees using the BYOD scheme and working from home or anywhere outside of the office. This VPN would work by the employee of Hyper-fort connecting to the VPN client in the Hyper-fort network, then this will allow them to use the LAN as if they were in the building. This is an advantage for the company as the BYOD will allow the employees to work from wherever securely.

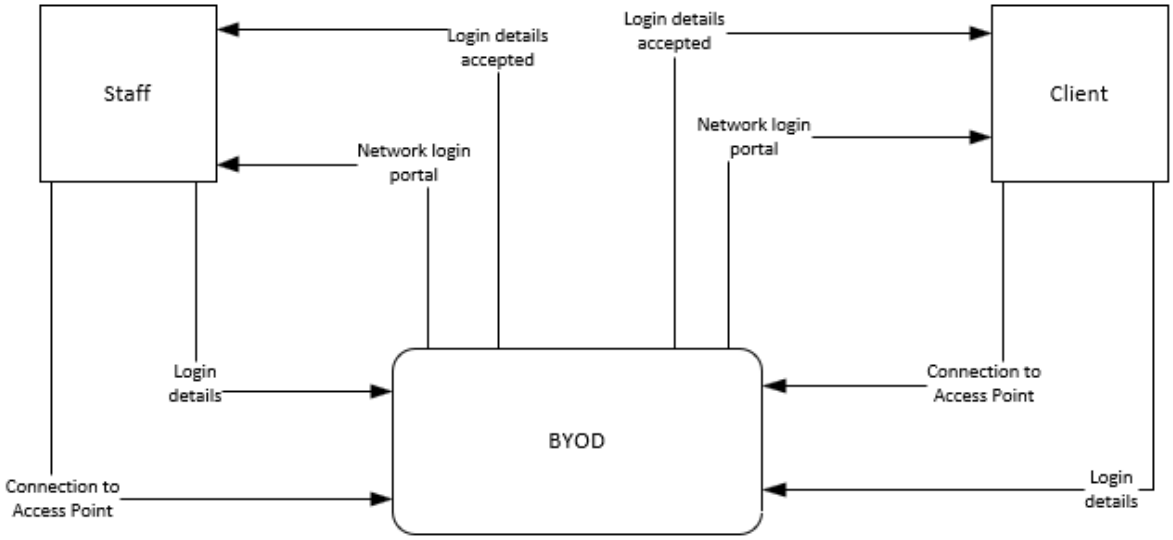
The second VPN is an extranet VPN. This VPN will allow access to parts of the intranet that the close working company would need to have access too. Hyper-fort would use this to connect the clients to the intranet, giving them access to the company's resources on the cloud servers that they offer the clients.

3.3 BYOD

3.3.1 Usage

The use of BYOD in the Hyper-fort network will improve all parts of the employees work life. This gives them the opportunity to work from wherever they are if they have an internet connection. It also allows them to work on their preferred operating system and device, boosting productivity. There are security risks involved with Hype-fort using BYOD but using a correct MDM will decrease the risks.

3.3.2 DFD



3.4 MDM Software

3.4.1 Microsoft Intune

The MDM that is advised for Hyper-fort to use is Microsoft Intune. An overview of the system with reason is below.

3.4.1.1 Overview

Microsoft Intune is an MDM that is cloud based. It keeps the users productive and the data shared to their devices safe [16]. Using the software, many device management settings can be added making the devices secure. The software will work well with the network shown in Appendix 2 – Packet Tracer Simulation as it can work locally in a network and on cloud resources.

3.4.1.2 Reason

Device Support [16]. Microsoft Intune can support a diverse company with many different devices on it. It supports iOS, Android, Windows, and macOS devices [16] giving Hyper-fort the ability to offer the staff and clients a wide range of devices that are supported.

Remote Wipe [16]. Microsoft Intune also supports remote wiping of devices from an administrative app in a very clever way. If a device is lost or stolen then the whole device can be wiped, protecting the user and the company as all the data is gone. But when an employee

leaves the company, Microsoft Intune can selectively wipe apps and app data [17]. This is done by the administrator selecting the device and then selecting the app on the device that the company data will be wiped from, so next time the app is run the company data is wiped.

VPN and WiFi certificate support [16]. Microsoft Intune can make WiFi Profiles for the users. So, when they log in to the intranet they can be identified and audited so if something happens on the network it can be seen what user has done it. Also, Microsoft Intune can support VPNs [18]. So, staff or clients that want to use the Hyper-fort resources on the network or file share on the network can have their own personal VPN. This VPN can be configured giving them specific access rights meaning they can only access data that is required for them to use. Also, these VPNs can be used with many connection types, including Cisco AnyConnect [18].

Security [16]. Microsoft Intune uses certificates that are used so only the intended recipient can decrypt the data. An example of this is if a company email is sent over the network using the email server, it is encrypted using the public key from the recipient's certificate. Then the email is decrypted using the private on their device [19]. This is the same for the data that is encrypted meaning Hyper-forts intellectual property is protected.

3.5 Internet security

3.5.1 Firewall

The firewall in the network will monitor incoming and outgoing traffic [20]. A stateful inspection firewall will be used in the Hyper-fort network. This type of firewall looks at the state, the port number and the protocol of traffic [20]. Filtering decision are made using the admirative rules that can be set, the information on the previous connections and the packets belonging to the same connection [20]. An example would be the network security director in Hyper-fort blocking social media sights from being used in the work network, as it was found that 20% of the links on Facebook users' newsfeeds will open viruses [21].

3.5.2 Online Presence

Hyper-fort has a massive online presence. This online presence will be from the website it hosts and the social media presence it uses to promote it activities. This website is a major part of the promotion and needs to be up and working for maximum use. This website can be

hosted from one of the servers the company owns. This website can be created and developed by internal or external sources as the external sources can use a VPN to edit the website.

3.6 Physical Security

3.6.1 RDIF Card Use

It is assumed that there is a RFID reader on the front door of the office building where the two offices are and the server room, all located on different floors. This will add to the security as the only way that the employees can get in to the building is by using their personal RFID cards.

There is a RFID reader on the door of the server room. This RFID reader will let in the relevant people in so that the there is no unauthorised access to the server room. All the conditions for opening the door from the card ID in is on a central IOT server in the server room. This can be added to easily, so if an admin wanted to give an employee access then the card ID can be added to the condition list to give them the access needed.

This system also notes down the time of entry by each card ID. Meaning the unique card IDs can be traced to the names of employees, giving time and date of when they unlocked the front door of the building, or the server door.

3.6.2 CCTV

It is assumed that all over the building there is CCTV cameras. These cameras will add to security as they use by PoE. This means all footage is recorded and stored on the servers in the server room. The cameras themselves will be in all places where the is IT kit deterring the employees or visitors from stealing, or anyone breaking in.

3.7 Servers

3.7.1 AAA (Authentication, authorization and Accounting)

An AAA server is a server that handles requests from users to access computers, resources, files or anything else on the network, then allow them access depending on their log in credentials [22].

The AAA server that is places in the Hyper-fort network will work by looking at the login requests from the BYOD's and the PC in the network and cross referencing the login details with the internal database. This database will have access writes and security information on the user. The AAA server will determine what files the user can read, write and not access, then according to this information show them the files and resources they are authorised to look at in the network. This will protect all data that Hyper-fort wants to keep safe, such as staff and client personal data and their intellectual property data.

3.7.3 Cloud

As Hyper-fort use cloud services to deliver IT services to the staff and clients. As seen in Appendix 2 – Packet Tracer Simulation the clients and staff connected to the network from within the network or through remote access, can use the internal intranet or extranet to access the cloud server that is connected to the network.

3.8 Redundancy

3.8.1 Routers and Switches

It is assumed that all the connections have a fault tolerant configuration through the Hyper-fort network. This will make the network more secure and there is a less of a chance of the network being down.

4. Implementation

4.1 How the System will be Implemented

The implementation of the system discussed will be done by firstly simulating all the equipment. Then once all the equipment is in place, adding the necessary security in the simulation and testing it. After this is will be shown to the top level of the Hyper-fort business, if there are any improvements then these will be added to the simulation. If the top level of the company are happy with the simulation, then it will be implemented.

The physical side of the implementation will be done by obtaining all the new equipment and setting it all up. Once this is done over one night the equipment will be set up as shown in the simulation and tested. This will be done to make sure the new system is secure. Finally, when

the new equipment is working properly, the old equipment that is being replaced or used for a different purpose will be changed to do its new job.

5. Results and Findings

The results and findings from this report mean that the simulation that is shown is secure when using BYOD with staff and clients. These findings were obtained by the writer researching around the scenario given on Hyper-fort and making the simulation for them specifically. As the simulation and findings are specific for Hyper-fort it gives them maximum security and a unique network supporting how they function.

6. Conclusion

To conclude, the simulation for Hyper-fort is secure as the top encryption is used on Access Points and the MDM that has been selected focuses on security. This MDM also support the working of the company as it supports the cloud resources and remote access. The findings from the scenario make the simulation advised unique and secure as all the findings were specific for Hyper-fort giving them the ability to used BYOD securely.

7. Appendix

7.1 Appendix 1 – BYOD Policy

1. Introduction and Scope

1.1 Introduction

This policy defines acceptable use by Hyper-fort users whilst using their own devices for accessing, viewing, modifying and deleting of Hyper-fort held data and accessing its systems.

Hyper-fort is a data controller, for the purposes of the Data Protection Act (1998). It is assumed that all staff have an awareness of the Data Protection Act (1998) and that they understand the consequences of the loss of Hyper-fort owned personal data.

IT management is regulated by the Computer Use Regulations for Hyper-fort available under the Policies and Regulations section on the internal intranet website.

The policy will be subject to review, in line with Hyper-fort guidelines, for effectiveness.

1.2 Scope

This policy applies to all mobile devices (e.g. laptops, tablets, smartphones), portable storage media (e.g. memory sticks or CDs), remote computers, and other devices used to access corporate systems and store Hyper-fort information.

2. Roles and Responsibilities

2.1 User Responsibilities

Hyper-fort, as the Data Controller, remains in control of the data regardless of the ownership of the device. As a User you are required to keep Hyper-fort information and data securely. This applies to information held on your own device, as well as on Hyper-fort systems. You are required to assist and support Hyper-fort in carrying out its legal and operational obligations, including co-operating with Information Systems should it be necessary to access or inspect Hyper-fort data stored on your personal device.

2.2 Designated Manager Responsibilities

The Security Director is responsible for the development, compliance monitoring and review of this policy and any related procedures.

2.3 Implementation Officer

The Security Director is responsible for the dissemination and implementation of this policy throughout Hyper-fort.

3. Policy

3.1 Objectives

A BYOD scheme has the potential to reduce costs and improve morale by giving staff the freedom to choose their own devices for their work, including devices they might be using in their personal lives. It is Hyper-fort's intention to place as few technical and policy restrictions as possible on BYOD subject to Hyper-fort meeting its legal and duty of care obligations.

3.2 System, Device and Information Security

The use of your own device MUST adhere to the Hyper-fort's Computer Use Regulations. When you use your own device as a work tool, you MUST maintain the security of the Hyper-fort's information you handle (which includes but is not limited to viewing, accessing, storing or otherwise processing).

From time to time, Hyper-fort may require that you install or update Hyper-fort-approved device management software on your own device.

It is your responsibility to familiarise yourself with the device sufficiently to keep data secure. In practice this means:

- Preventing theft and loss of data (using PIN/Password/Passphrase lock)
- Keeping information confidential, where appropriate.
- Maintaining the integrity of data and information.

You must never retain personal data from Hyper-fort systems on your own device. If you are in any doubt as to whether particular data can be stored on your device, you are required to err on the side of caution and consult with your manager or seek advice from The Security Director.

You must:

- Use the device security features, such as a PIN, Password/Passphrase and automatic lock to help protect the device when not in use.
- Keep the device software up to date, for example using Windows Update or Software Update services.
- Activate and use encryption services and anti-virus protection if your device features such services.

- Install and configure tracking and/or wiping services, such as Apple's 'Find My iPhone', Android's 'Where's My Droid?', or Windows' 'Find My Phone', where the device has this feature.
- Remove any Hyper-fort information stored on your device once you have finished with it including deleting copies of attachments to emails, such as documents, spreadsheets and data sets, as soon as you have finished using them.
- Limit the number of emails and other information that you are syncing to your device to the minimum required.
- Remove all Hyper-fort information from your device and return it to the manufacturers' settings before you sell, exchange or dispose of your device.

In the event that your device is lost or stolen or its security is compromised, you MUST promptly report this to the Security Director, in order that they can assist you to change the password to all Hyper-fort services (it is also recommended that you do this for any other services that have accessed via that device, e.g. social networking sites, online banks, online shops). You must also cooperate with Hyper-fort in wiping the device remotely, even if such a wipe results in the loss of your own data, such as photos, contacts and music.

You must not attempt to circumvent the device manufacturer's security mechanisms in any way, for example 'jailbreak' the device.

Hyper-fort reserves the right to refuse, prevent or withdraw access to Users and/or particular devices or software where it considers that there is unacceptable security, or other, risks to its staff, business, reputation, systems or infrastructure.

3.3 Monitoring of User-Owned Devices

Hyper-fort will not monitor the content of your personal devices, however Hyper-fort reserves the right to monitor and log data traffic transferred between your device and Hyper-fort systems, both over internal networks and entering Hyper-fort via the Internet.

In exceptional circumstances, for instance where the only copy of a Hyper-fort document resides on a personal device, or where Hyper-fort requires access in order to comply with its legal obligations (e.g. under the Data Protection Act 1998, the Freedom of Information Act 2000, or where obliged to do so by a Court of law or other law enforcement authority) Hyper-fort will require access to Hyper-fort data and information stored on your personal device. Under these circumstances all reasonable efforts will be made to ensure that Hyper-fort does not access your private information.

Under some circumstances, for example where you legitimately need to access or store certain types of information, such as financial records, on your own device, you must seek authority from your Line Manager. Hyper-fort may then need to monitor the device at a level which may impact your privacy by logging all activity on the machine. This is in order to ensure the privacy, integrity and confidentiality of that data.

3.4 Support

Where possible Hyper-fort supports all devices, but you have a responsibility to learn how to use and manage your device effectively in the context of this policy.

Help and advice is available on a reasonable endeavour's basis, via the Security Director including help installing and configuring apps and other software.

Hyper-fort takes no responsibility for supporting, maintaining, repairing, insuring or otherwise funding employee-owned devices, or for any loss or damage resulting from support and advice provided.

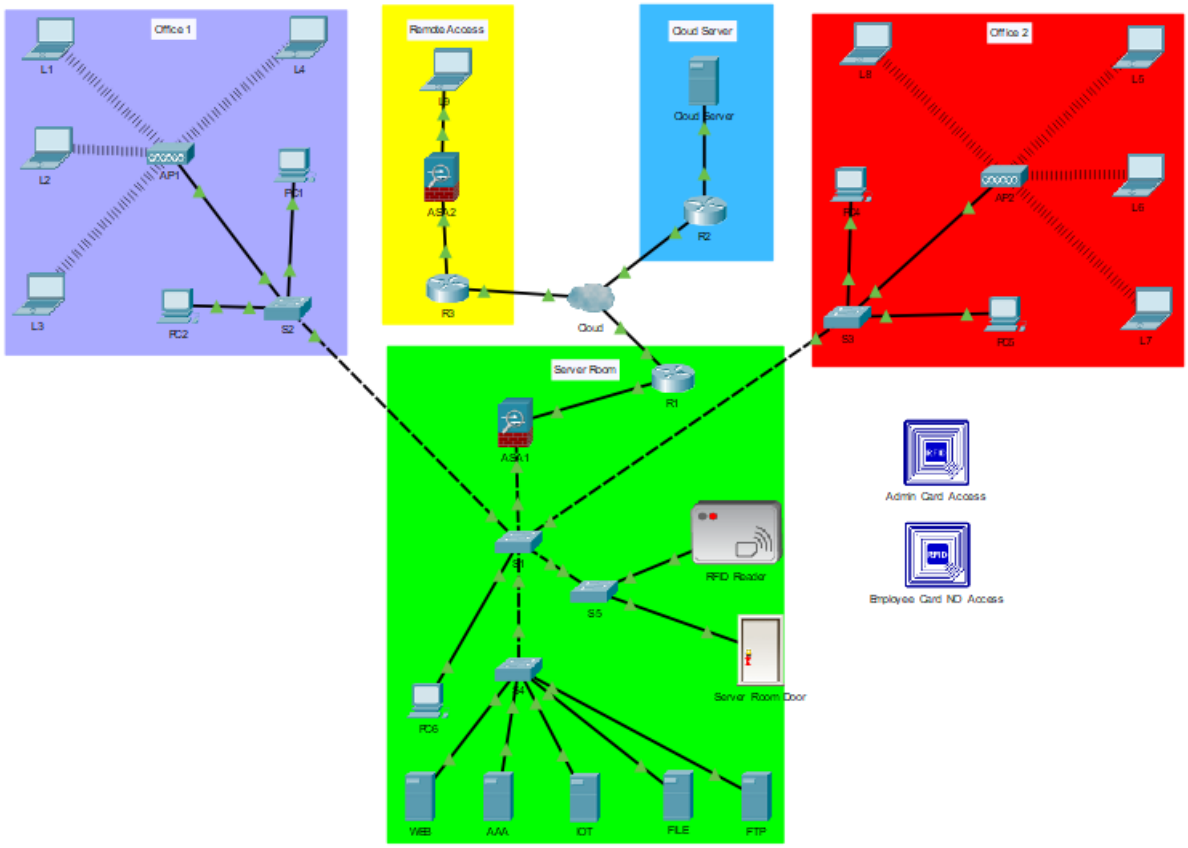
3.5 Use of Personal Cloud Services

Personal data as defined by the Data Protection Act (1998) and Hyper-fort confidential information may not be stored on personal cloud services.

3.6 Compliance Sanctions and Disciplinary Matters

Compliance with this policy forms part of the employee's contract of employment and failure to comply may constitute grounds for action, under the Hyper-fort's disciplinary policy.

7.1 Appendix 2 – Packet Tracer Simulation



8. Bibliography

[1] D. Evans, “What is BYOD and why is it important?,” techradar, 07 October 2015. [Online]. Available: https://www.techradar.com/uk/news/computing/what-is-byod-and-why-is-it-important-1175088. [Accessed 29 12 2018].

[2] C. Hopping, “We explain what Bring Your Own Device means and how to implement a successful company strategy,” ITPRO, 28 February 2017. [Online]. Available: https://www.itpro.co.uk/strategy/28072/what-is-byod. [Accessed 29 December 2018].

[3] DMS Technology, “The 7 Best Reasons to Implement BYOD for Enterprises,” DMS Technology, 11 May 2018. [Online]. Available: https://www.dmstechnology.com/7-best-reasons-implement-byod-enterprises/. [Accessed 02 January 2019].

[4] P. Beauchamp, “BYOD in the Workplace: Benefits, Risks and Insurance Implications,” HUFFPOST, 07 July 2016. [Online]. Available: https://www.huffingtonpost.com/parker-beauchamp/byod-in-the-workplace-ben_b_10973342.html?guccounter=1. [Accessed 02 January 2019].

[5] optimusLEARNING, “The Advantages and Disadvantages of BYOD,” optimusLEARNING, 04 September 2013. [Online]. Available: https://www.optimuslearningservices.com/practical-ld/advantages-disadvantages-byod-in-learning/. [Accessed 08 01 2019].

[6] V. Beal, “MDM - mobile device management,” Webopedia, [Online]. Available: https://www.webopedia.com/TERM/M/mobile_device_management.html. [Accessed 01 January 2019].

[7] M. Rouse, “Mobile Device Management (MDM),” TechTarget, [Online]. Available: https://searchmobilecomputing.techtarget.com/definition/mobile-device-management. [Accessed 01 January 2019].

[8] F. Stroud, “Mobile Information Management (MIM),” Webopedia, [Online]. Available: https://www.webopedia.com/TERM/M/mim-mobile-information-management.html. [Accessed 01 January 2019].

[9] M. Rouse, “Remote Wipe,” TechTarget, [Online]. Available: https://searchmobilecomputing.techtarget.com/definition/remote-wipe. [Accessed 01 January 2019].

[10] PROBRAND, “Cloud Server,” PROBRAND, [Online]. Available: https://www.probrand.co.uk/it-services/cloud-server. [Accessed 01 January 2019].

[11] B. Hall, “What is an Intranet?,” interact, 20 June 2017. [Online]. Available: https://www.interact-intranet.com/blog/what-is-an-intranet/. [Accessed 01 January 2019].

[12] M. Rouse, “Extranet,” TechTarget, [Online]. Available: https://searchnetworking.techtarget.com/definition/extranet. [Accessed 01 January 2019].

[13] wikipedia, “Extranet,” wikipedia, 30 December 2018. [Online]. Available: https://en.wikipedia.org/wiki/Extranet. [Accessed 01 January 2019].

[14] Mohit Arora, “How secure is AES against brute force attacks?,” EE Times, 05 July 2012. [Online]. Available: https://www.eetimes.com/document.asp?doc_id=1279619. [Accessed 02 January 2019].

[15] J. Tyson and S. Crawford, “How VPNs Work,” How Stuff Works, [Online]. Available: https://computer.howstuffworks.com/vpn4.htm. [Accessed 04 01 2019].

[16] Microsoft, “What is Microsoft Intune?,” Microsoft, 30 December 2018. [Online]. Available: https://docs.microsoft.com/en-gb/intune/what-is-intune. [Accessed 08 01 2019].

[17] Microsoft, “How to wipe only corporate data from Intune-managed apps,” Microsoft, 09 October 2018. [Online]. Available: https://docs.microsoft.com/en-gb/intune/apps-selective-wipe. [Accessed 08 January 2018].

[18] Microsoft, “Create VPN profiles in Intune,” Microsoft, 25 08 2018. [Online]. Available: https://docs.microsoft.com/en-us/intune/vpn-settings-configure. [Accessed 08 January 2019].

[19] Microsoft, “S/MIME email signing and encryption in Intune,” Microsoft, 21 08 2018. [Online]. Available: https://docs.microsoft.com/en-us/intune/certificates-s-mime-encryption-sign. [Accessed 08 01 2019].

[20] Cisco, “What Is a Firewall?,” Cisco, [Online]. Available: https://www.cisco.com/c/en_uk/products/security/firewalls/what-is-a-firewall.html. [Accessed 04 01 2019].

[21] Gemalto, “Can I get a virus from social media sites?,” Gemalto, [Online]. Available: https://www.justaskgemalto.com/us/can-i-get-virus-social-media-sites/. [Accessed 04 01 2019].

[22] M. Rouse, “AAA server (authentication, authorization, and accounting),” TechTarget, [Online]. Available: https://searchsecurity.techtarget.com/definition/AAA-server. [Accessed 04 01 2019].