

Synthesize a Solution to a Potential Real-Life Scenario

Internet Technology and Security

Kieran Perrin

Contents

Introduction	2
Policies	2
Acceptable Use	2
Device Management	3
Restitution.....	3
Security	3
Risks	4
Implementation Data Flow Diagram.....	4
Packet Tracer Solution	4
Mobile Device Management Software	5
Advantages and Disadvantages of BYOT	6
Advantages.....	6
Disadvantages	6

Introduction

Hyper-Fort Ltd want to move toward using bring your own device (BYOD) framework in their office. In this document I will go over the pros and cons of a BYOD framework and provide an implementation solution that includes a secure and productive system for all users. For this to happen necessary policies will be written up such as a user policy and a device management policy. For implementation purposes a data flow diagram should be made and an example of a working network in packet tracer should be created. Once the physical implementation is dealt with, then software choices should be made, discussing the pros and cons of the choices available. Once everything is discussed a conclusion on my recommendation and future improvements will be made.

Policies

Setting up policies for standard practice is important for a company, this is so expectations of use are set. Policies allow companies to track liability for problems whether it was employees or management. They also ensure that there is compliance with the law and can be used to defend employees or the company when claims are made. For Hyper-Fort specifically moving toward a BYOD environment; user, device management and security policies need to be updated. Below are my proposed policies.

Hyper-Fort Ltd grants employees the privilege of bringing personal devices such as smart-phone, tablets and laptops to work for convenience. Hyper-Fort Ltd reserves the right to remove this privilege if any policies or guidelines are not followed. This policy is in place to ensure the security of Hyper-Fort Ltd and its client's data and infrastructure.

Acceptable Use

There are two main factors for acceptable use:

1. Acceptable business use can be defined as actions that may affect Hyper-Fort Ltd and a direct or indirect way.
2. Acceptable personal use during office hours can be defined as acceptable use of social media or other forms of communication.

During office hours certain websites will be blocked from access, this is up to the discretion of Hyper-Fort Ltd but may include sites including:

- Pornography
- Gambling
- Games

Employees must not use devices at any time to store and transmit any illicit or proprietary information owned by or regarding the company. Also employees must not engage in any harassment/bullying to other employees or members of the public.

Acceptable applications include only those obtained through a secure vendor such as the Google Play Store or the Apple App Store. News, weather and productivity apps are allowed and limited use of some social media applications such as Facebook are acceptable during down time i.e. breaks. Under no circumstances are applications that are downloaded from un-secure sources allowed on devices.

Devices may be used to access company resources such as email, calendars, documents or contacts.

Devices cameras and microphones will be disabled whilst on-site.

Device Management

Smartphones including iPhone, Android and Windows phones are permitted, so long as they are on a supported software version such as android 4.1 or higher and IOS 10 and higher.

Tablets are also permitted Including Android tablets, iPad's and Windows devices, again only if they are on a supported software version.

Laptop computers are permitted including those running Windows or Mac OS. Those that are using Linux based operating systems are not permitted.

All devices must be brought to the I.T department for inspection and proper configuration such as installation of a device management software before accessing the company network.

No devices that are "Jailbroken" (IOS) or "Rooted" (Android), will be permitted access to the network.

Restitution

Hyper-Fort Ltd will not reimburse employees for any amount toward the costs of their personal devices.

Hyper-Fort Ltd may reimburse employees a percentage of the phone/data plan if the employee has requested it through the proper channels. No reimbursements will be given for any over charges or data roaming.

Security

All devices must be password protected using the devices features and using a strong password before accessing the company's network.

A strong password consists of:

- At least 6 characters long
- Upper and lower case letters
- Numbers
- Symbols

All passwords should be changed every 90-day period and new passwords should not be the same as the previous 10 passwords used.

If left unused, the device should password lock itself after 5 minutes.

After failing to enter the password correctly 5 times the device should lock and require the I.T department to unlock.

All applications that are not permitted will automatically be prevented from being downloaded.

All devices that are not on the list of supported devices by the company policy will not be permitted access to the network. Devices used for personal use only are also not permitted access to the network.

Employee's level of access to the company data will be restricted based on user profiles that are defined by the I.T department and are automatically enforced by the system.

Hyper-Fort Ltd reserved the right to wipe the data on employee's devices in the circumstance that:

- The device has been reported stolen

- The employee has left the job or been terminated
- The employee is in breach of the user policies
- The device poses a threat to the system such as being infected with a virus or malware etc.

Risks

Employee's personal data may be at risk of being lost at any point therefore it is the employee's responsibility to take precautions such as backing up messages, photos and contacts to another device or a cloud service.

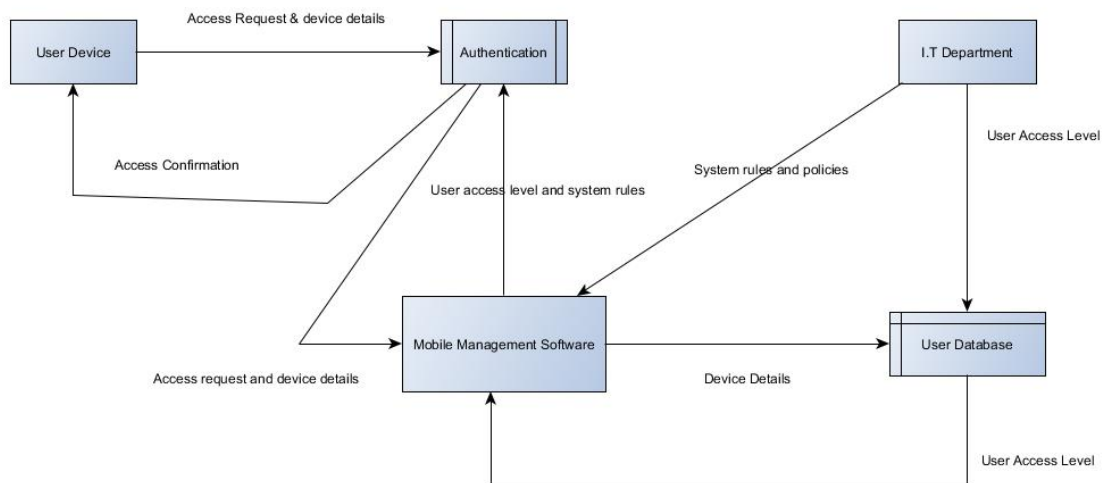
Lost or stolen devices must be reported to the company within 24 hours so the necessary precautions can take place.

Employees are completely liable for the safety and wellbeing of their devices, Hyper-Fort Ltd will not assume any responsibility if a device is lost, stolen or broken in any way.

Hyper-Fort Ltd reserve the right to discipline employees including termination if they do not comply with the policies stated on this document.

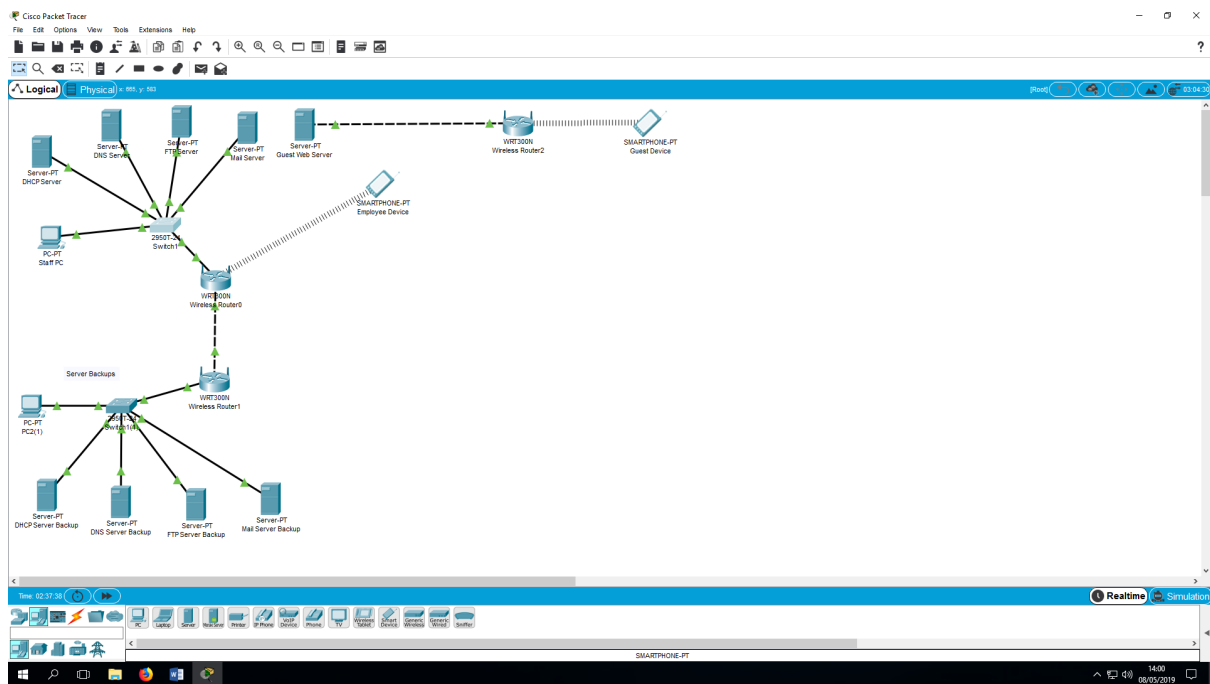
Implementation Data Flow Diagram

To get a better picture of the kind of system that needs to be implemented a data flow diagram should be drafted. This way we can see if the system works on a theoretical level before trying to implement any physical or software changes to the system already in place. If the data flow diagram proves to work theoretically it can then be used as a basis for implementing the physical and software solutions. Below is my data flow diagram suggestion.

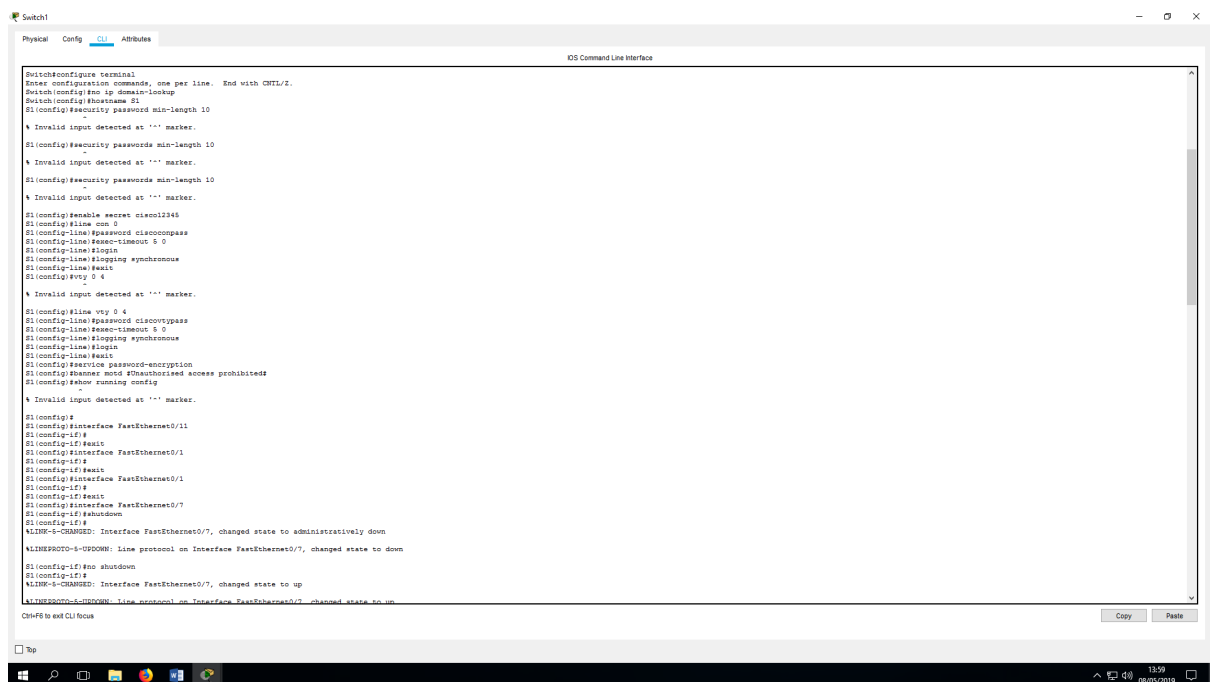


Packet Tracer Solution

Below is a network topology of Hyper-Fort Ltd drawn in Cisco Packet Tracer. The network layout consists of separate servers for different functions such as mail, FTP, DHCP and DNS. The reason for this is there is a layer of redundancy if something were to go wrong. On top of that, there is a backup of each server at a separate location. Employee access and guest access is separate for security purposes.



Below is a screenshot of the command line instructions input into the switch to make it more secure. The switch now has password protection so only admins can access and change network settings and has an auto lock feature if left for 5 minutes. All the ports that are unused on the switches and the routers are turned off for better security.



Mobile Device Management Software

For security purposes a mobile device management software should be used for all employees' devices so the I.T department can monitor and implement rules on the devices. There are multiple different software solutions for mobile device management. After researching the possible different services available to me I have decided on using the Microsoft Intune Enterprise Mobility + Security

software. The reason I decided upon using the Microsoft solution because it has all the features you would want from an MDM software including:

- Mobile device & app management
- Multiple compatible OS options
- Advanced Microsoft Office 365 data protection
- Integrated PC management
- Integrated on-premises management
- Identity & access management
- Information protection
- Identity-driven security

Also, the Intune software is compatible to use with the Microsoft Azure security and has cloud services so on-site aren't necessary.

Advantages and Disadvantages of BYOT

There are multiple advantages and disadvantages of having employees bring their own devices to the work place.

Advantages

Some of the advantages include:

- The cost to the company is reduced as supplying employees with devices is not necessary.
- Employees using their own device allows for more flexibility in the work place. It allows them to choose the tools they work with and provides a better work-life balance as a result.
- There are lower training costs and time spent because employees are already familiar with their own devices.
- Employees who work away from the office have access to the same resources and data as those in the office.

Disadvantages

Some of the disadvantages include:

- The disadvantage of BYOT is having to change the current system in the office environment to allow for the devices to be used.
- Although there are precautions that can be put in place to increase the security of employee's devices, there will always be the higher risk of a breach of some kind if the devices.
- Everyone has different choices in devices, and some are better than others. Some employees might be at a disadvantage because they don't have access to certain applications and such because their device isn't of a high enough standard.