



INTERNET TECHNOLOGY AND SECURITY

Sean Andrew



Table of Contents:

Abstract	1
Introduction.....	2
Research.....	3
Problem Formulation	5
Implementation	6
Results/ Findings.....	11
Conclusion	12
Bibliography	13

Abstract

In this report I am going to look into creating a framework for a BYOT (Bring Your Own Technology) network for the Ruckus Company. To do this I will create a framework of what the network should look like and data flow diagrams showing how the network will operate and accept devices that are up to date and secure onto the network. To design the network I will use Cisco Packet Tracer to help me demonstrate how the network will look and how it will work with devices that will connect to the network and yEd to design the data flow diagrams showing how the network will work and accept devices onto the network.

I will also select a Mobile Device Management Software that will work well with the BYOD policy that I have created using rules that will help keep the network safe and secure from potentially compromised devices.

Introduction

For this report I am going to be designing a framework for the network which will set out the list of devices that will be allowed to connect to the network and what sort of things are required from the device to be able to use the network. I will also be making data flow diagrams which will be designed in yEd for Ruckus which will show how the data will flow with the BYOT network and how the network will handle new devices connecting to the network and what happens if a blacklisted or devices without the correct permissions tries to gain access to the network. After I have designed the framework for the network, I will then design what the network will be set up like in Cisco Packet Tracer and show the configuration and how the devices will be able to connect to the network. I will also pick an MDM software that would work well with the network and explain why I picked the certain software.

I will also assess issues that come along with BYOT like data leakage as this can be a big problem for businesses, what type of data is retained by the mobile devices as this can lead to problems later on.

I will also be using Cisco Packet Tracer to help me design the network for the Ruckus Company, I will be using this to show how the network will be set up and how it will allow outside devices to gain access to network resources such as internet access, secure documents etc...

Research

I have done some research into MD software which will be useful for the network and that covers a large range of devices and the one I have looked into using is Microsoft Intune. This software looks like it can work for this network as it allows connections for all different kinds of devices as seen here [3] which says that a whole different range of devices can connect to it from Iphones to Andriod devices and Microsoft devices. And because it is all done on the cloud, it can be managed from any devices that can connect to the internet from anywhere as long as they have internet access.

This software also has a built in “Microsoft Advanced Threat Analytics” [3] which is said to monitor the network and all devices to make sure that they are all working correctly and there are no threats on any of them as well as they are not doing anything malicious on the network.

For Andriod devices it also allows you to remote control the screens of the devices which is what the technicians would have needed if they need to install certain software onto the devices for the Users or wipe them if they are lost which can help to keep data secure on the devices and not lose any from the company.

I have done some research into how I should set out my policies for letting devices connect to the network and have started to design my own policy based off some policies I have seen online. [2] My policy will look like this.

This document provides policies and standards that devices that will connect to the network will need to follow. This applies to the following devices: Smart phones, tablets, laptops, smart watches or anything that has wireless capabilities and is able to utilise the networks Ruckus Company's network.

For devices to gain access to the network they will need to have meet all the conditions listed below to ensure that their devices are up to date and secure, this will allow the network to remain safe and secure to minimize the risk of a security breach on the network.

The current devices which are allowed to connect to the network are:

Andriod Smartphones and tablets
Apple Smartphones and tablets
Microsoft Smartphones, tablets and laptops.

When connecting your devices to the network you are agreeing to let Ruckus Company to monitor your device to make sure that it is safe and secure while on the network and see what you are doing on the network. This will allow us to ensure your network usage isn't inappropriate. Ruckus Company respects the privacy of your devices and will not access any of your personal data stored on there, the only time Ruckus might need to access the device is when the technicians will need access to the device to install the required applications into it to give them access if the device is lost

or stolen with data from the company. Ruckus will not access or delete any data on the device unless it is deemed necessary if the device is not recoverable, before any action is taken Ruckus will inform the owner of the actions that will need to be taken.

Requirements of all BYOD accessing Ruckus's network-

- Certain apps are not allowed to be installed on devices that are connecting to the network, one example of a type of application that can bring risks to the network is VPN's. This is not allowed due to the potential security risks the app brings to the network.
- All devices that connect to the network must be protected and have at least a password or a pin set on the devices to help prevent unauthorised access on your devices. This helps prevent any malicious activity from taking place on any unaccompanied devices.
- All devices data must be encrypted if taking data outside of the company. This can help protect against the loss of data as if the data was lost or misuse of the data. Another rule that can be enforced is that all devices that are carrying sensitive data needs to be encrypted to help protect against any unauthorised user getting the data. This helps if someone was to get access to this data then they will not be able to make any sense of it as they won't have the encryption key to read it.
- All devices must "auto-lock" after a certain amount of time of not being used (2-5 minutes) This can help prevent unattended devices from being left unprotected and misused by someone else and locking themselves, requiring the password or pin to regain access to them.
- All devices must be using their official Operating Systems and be running up to date security measures. This means that no "jail broken" or "rooted" devices are allowed to connect as they are potentially a risk to the network as and any data on there.
- The User will not share any of the company's data outside of the organisation with any or person or devices, this excludes emails that are secure and sent to other employers inside the same organisation.
- The User agrees to delete any data that they have from the organisation that is no longer deemed necessary as it is still sensitive data to the organisation and could be a potential security risk if it was lost.
- If the device is lost or stolen the technicians

User Acknowledgment and Agreement

It is Ruckus Company's right to restrict or decline computing privileges/ network access or take legal actions with users who have failed to comply with the following policy and rules. These rules above should be followed and upheld for as long as you are a part of the company.

Problem Formulation

One of the things that I need to find is a MDMS (Mobile device management software which will be able to do what I need to do and that can do what I have, some of the things that this Mobile Device Management software will have to do is only allow certain version of operating systems onto the network as If it allows a potentially out of date operating system onto the network then it leaves a security risk as they could have loop holes in their security.

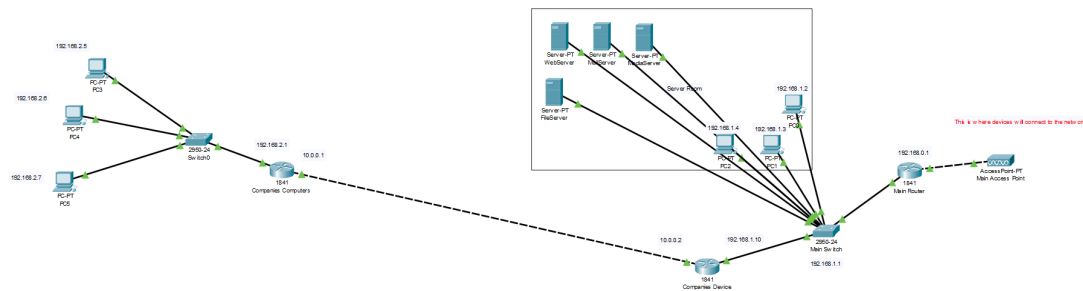
Another thing the Mobile Device Management software will have to do it allow a range of devices to connect to the network and be able to manage them all easily as this can range from devices from brands like Samsung, iPhone, Huawei etc... This has a risk as if a device which isnt supported and can't be monitored connects to the network then there is a potential security risk as the company can't see what that device is up to and monitor it.

Another thing that the Mobile Device Management software will have to do is be able to access the device if its lost or stolen and be able to remote control it, allowing for data to be removed or erased if it contains any sensitive information from the company. The company will also need to be able to lock the device or encrypt the data remotely if they are unable to delete the data for any means.

Another thing that the Mobile Device Management software will have to do is be able to not allow any "jail-broken", "cracked" or "rooted" devices to connect to the network as they are using unofficial software and are a potential security risk when connecting to the network.

Another thing that the Mobile Device Management software will have to do is it will have to encrypt any data that is taken from the company on any device to help prevent them from sharing this outside of the organisation. So, if anyone was to gain access to this data outside of the organisation then they will not be able to do anything with it as they won't have the encryption key.

Implementation



This is a simulation of what the network that I have designed will look like for Ruckus Company. All the routers on the network have been secured and protected with a password which has been encrypted as shown:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#service password-encryption
Router(config)#
```

Ctrl+F6 to exit CLI focus

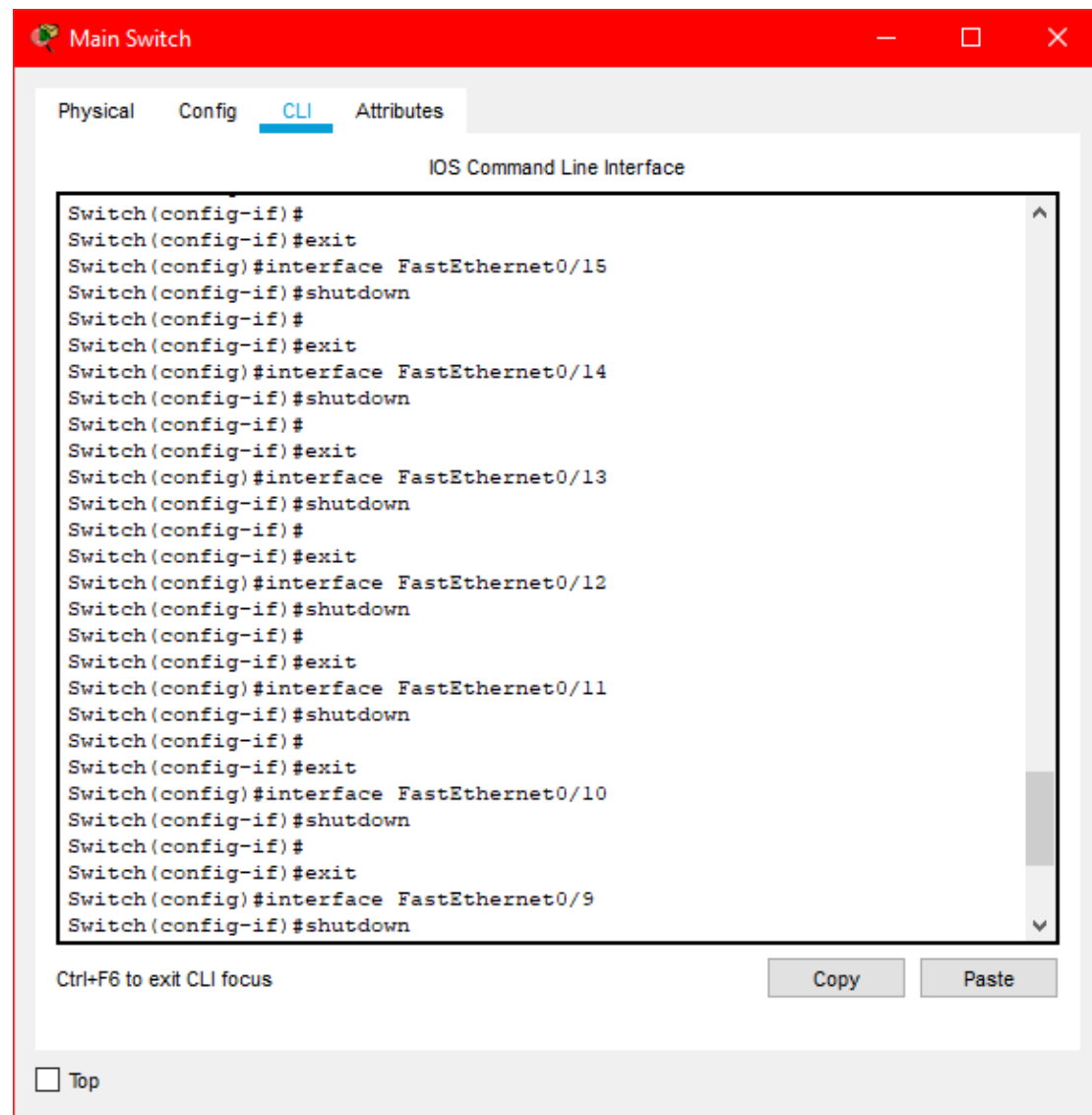
Copy

Paste

All line consoles have also been given password to help prevent unauthorised access to the network:

```
Router(config)#lin con 0
Router(config-line)#password XXXXXXXXXX
Router(config-line)#secret password
```

This has been done on all hubs and devices on the network so users are unable to do unauthorised things on the network.



I have also closed down all unused ports to help protect the network from any unauthired devices trying to connect directly into the network.

I also have firewalls on each of the routers to help prevent hackers or any unauthorised access to be made onto the network.

I have also put a banner on to the routers on the network so when anyone goes onto it it will display a message as well as when someone logs in it will display a message.

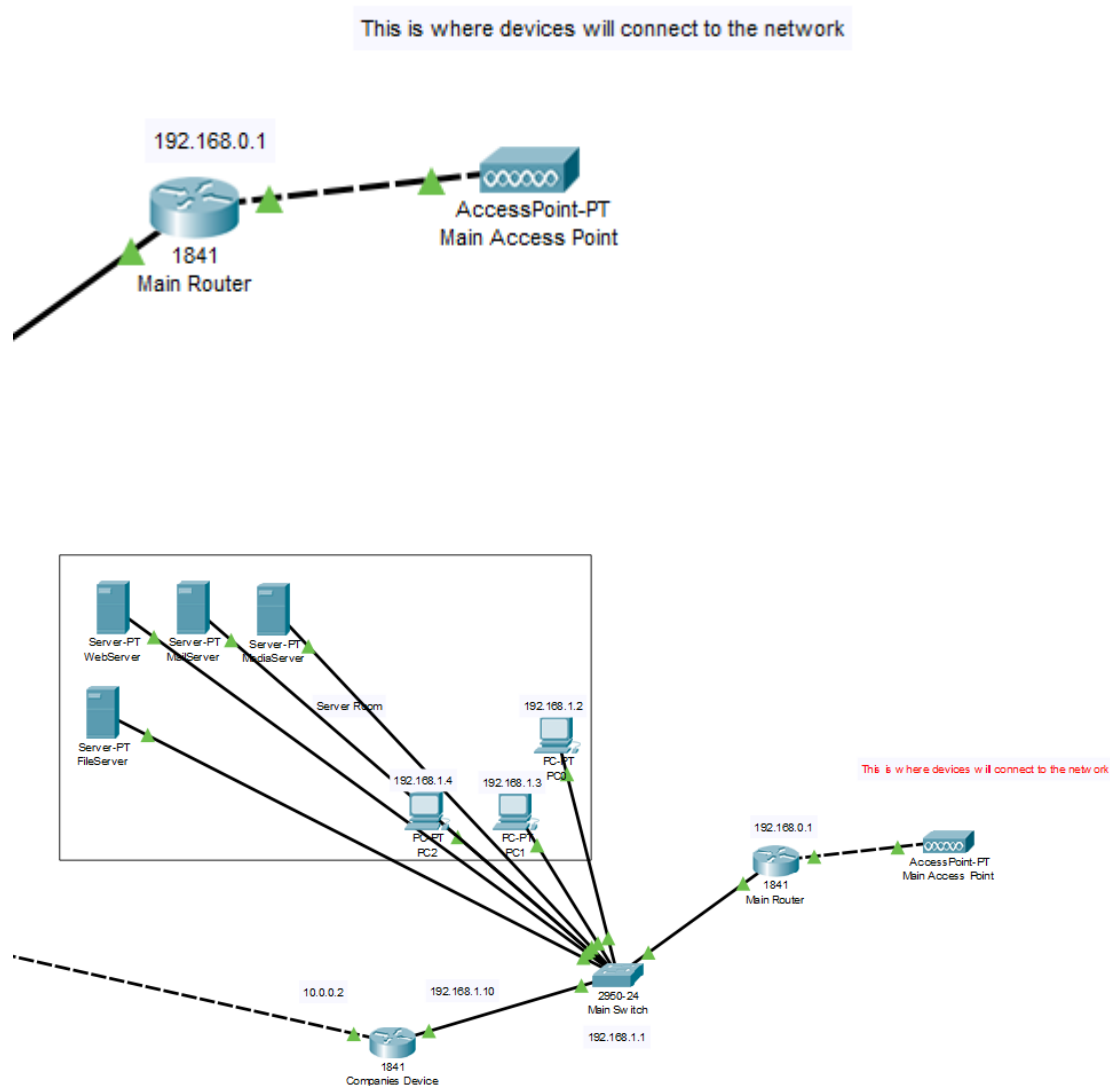
```
no unauthorised access
```

```
Router>enable
```

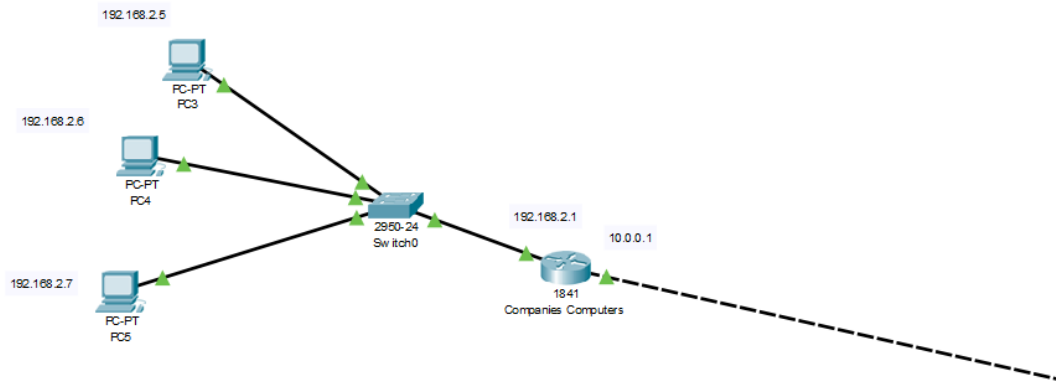
```
Password:
```

```
Router#
```

There are access points on the network to allow devices that don't have the ability to be connected wired into the network, for example phones, tablets etc...



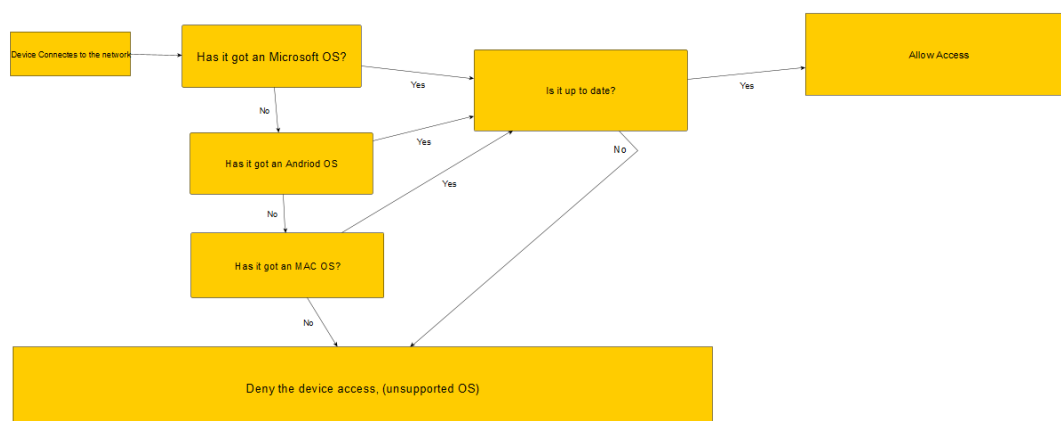
This is the point of the network which mobile devices will be able to connect to it through the access point. The room on the top left is the server room which will contain all of the documents and information for the company which can be accessed by the machines in the company and devices connecting to the access point.



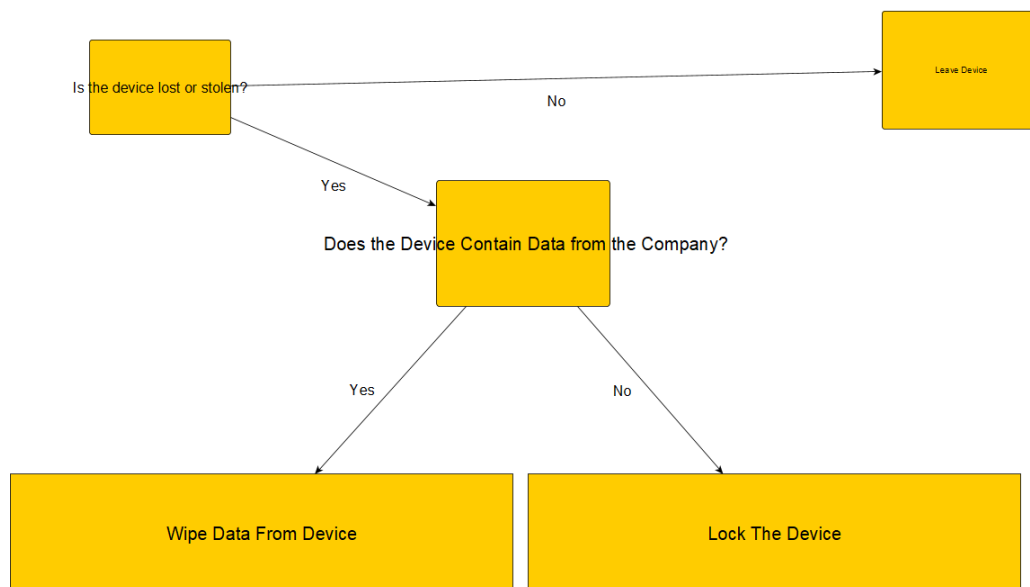
This is the part of the network which is inside the company and will be the machines that will need to access the network and get access to the servers from inside the company.

When the Devices connect to the network the Mobile Device Management softwill run checks on the devices to see if they are eligible to connect. The data flows will and decisions will look something like this:

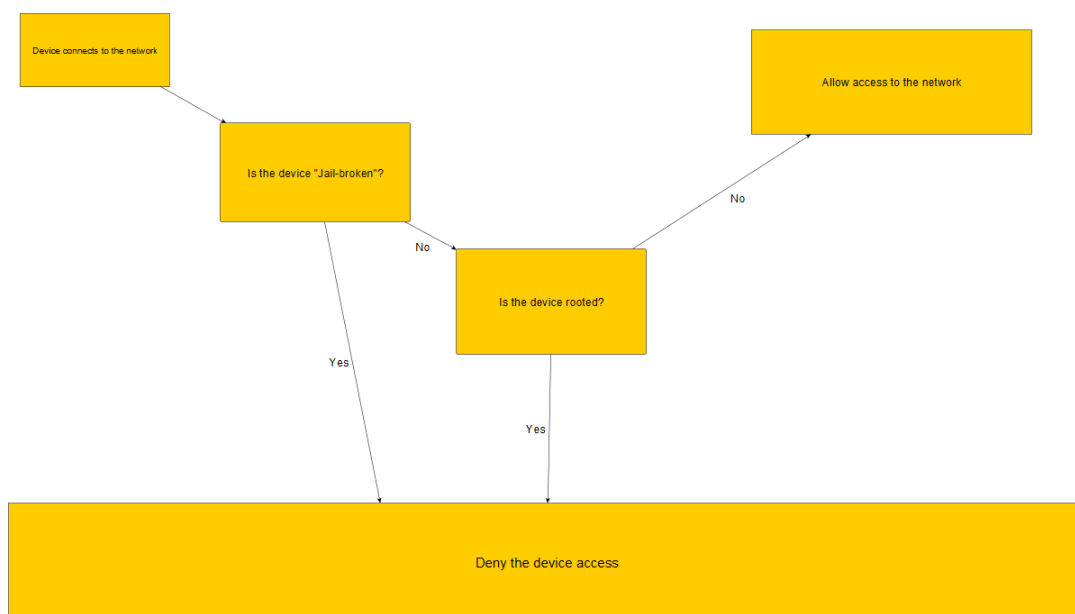
This is the flowchart of the decisions that will be made to check the OS of the devices conncting.



This is the dataflow of the decisions made to check if the lost/stolen device has data on it and if it should be wiped or locked.



This is the dataflow that will check to make sure that the device is running its official OS and not “Jail-borken” or “cracked”



Results/ Findings

When looking for a Mobile Device Management software that will be fit for the purpose of the organisation, I found a couple which could be used.

One example of a suitable Mobile Device Management software that could be used is Baramundi. Baramundi is a Mobile Device Management software which comes with all the software needed to manage devices connected to the network and carry out routine tasks on the network with things such as scanning new devices that connect to the network and making sure they follow the policy set in place. This software also provides protecting to any devices connected to it with a built-in firewall to help keep any threats out of the network. It supports all devices from Android to iOS but the only thing that it lacks is the ability to locate lost phones and secure data that is on it. Baramundi also has support available online 24/7 so if anyone was to have trouble setting up the software or ran into problems running it then they would be able to get support to resolve it.

Another example of a suitable Mobile Device Management Software that could be used is Microsoft Intune. Microsoft Intune is capable of supporting any of mobile devices no matter mobile, tablet or laptop. Microsoft Intune utilises the use of the cloud to manage its devices, allowing it to manage devices on any device and anywhere the network admin can get access to. Intune also allows remote control and access of devices from anywhere the admin is as long as they have access to a computer or tablet. This software also offers protection for all devices that are connected to it with Windows Defender ATP integrated into the software which can help protect any malicious activity on the network and any unwanted devices connecting to the network. The Windows Defender ATP also allows the admin to set up so specific software is not allowed to be installed on the network and certain apps or programs are not allowed to run on the network as they can cause security problems, for example VPN's as they open a connection to a external source to mask your IP. Intune also includes programs for all of the devices to use that connect to the network such as Office 365 which includes all of the office package (Word, Excel, PowerPoint etc...) and Outlook. Microsoft Intune also has 24/7 support available for people who require it when installing or using Intune or any of its other components.

On this review website by PCMAG [4] it contains a couple of different Mobile Device Management software's and what each of them is capable of doing. As you can see on this review website Baramundi software isnt capable of locating mobile devices so it lacks some of the functionality that the network will need. Microsoft Intune on the other hand offers the functionality that the network needs and supports a wide range of different devices.

Conclusion

To conclude I recommend that Ruckus Company uses Microsoft's Mobile Device Management software Intune to help manage the network as it provides all the tools needed to help keep the network secure and also set up rules on the network to not allow certain devices to connect unless they meet a certain criteria. The Windows Defender will help keep any potential threats or unsecure devices away from sensitive data on the network and keep any sensitive data safe.

Intune also offers a way to access devices anywhere and lock or wipe them as they are connected to the cloud. Because it uses the cloud it also allows Network Administrators to access and manage the network from anywhere as long as they have access to the internet and a device that can use the software. Intune also monitors the network automatically and helps keep the network running by its self.

In the future I can try to broaden my search while looking for Mobile Device Management software by looking into more examples and more reviews about them to give me a better idea if they are any good from people that have actually used them.

Bibliography

- [1] Comtact, "The Cyber Source Blog," Comtact, 5 December 2017. [Online]. Available: <https://www.comtact.co.uk/blog/creating-a-byod-policy-8-points-every-policy-must-contain>. [Accessed 20 March 2019].
- [2] P. Domain, "Docracy," 02 2013. [Online]. Available: <https://www.docracy.com/0to97btx120/bring-your-own-device-policy-sample>. [Accessed 27 03 2019].
- [3] <https://uk.pcmag.com/cloud-services/76023/microsoft-intune>, "Microsoft Intune," pcmag, 10 Oct 2017. [Online]. Available: <https://uk.pcmag.com/cloud-services/76023/microsoft-intune>. [Accessed 01 05 2019].
- [4] "PC MAG," [Online]. Available: <https://www.pcmag.com/article/342695/the-best-mobile-device-management-mdm-software>. [Accessed 05 05 2019].