

MSC Project Report Liam Blunt

Final

by Liam Joseph Blunt

FILE	4166_LIAM_JOSEPH_BLUNT_MSC_PROJECT_REPORT_LIAM_BLUNT_FINAL_2 60366_1263765513.DOCX (2.74M)		
TIME SUBMITTED	20-NOV-2020 10:00AM (UTC+0000)	WORD COUNT	24161
SUBMISSION ID	136873139	CHARACTER COUNT	123195



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Development of Network Security in a Small Enterprise Environment

by

Liam Blunt

Supervisor: Nitheesh Kaliyamurthy

Second Marker:

Project submitted as part of the requirements for the
award of MSc Computer Networks & Cybersecurity

November 2020

DECLARATION

I, Liam Blunt, declare that I am the sole author of this Project; that all references cited have been consulted; that I have conducted all work of which this is a record, and that the finished work lies within the prescribed word limits.

This work has not previously been accepted as part of any other degree submission.

Signed : Liam Blunt

Date : 20/11/20

FORM OF CONSENT

I Liam Blunt hereby consent that my Project, submitted in candidature for the M.Sc. Computer Networks & Cybersecurity, if successful, may be made available for inter-library loan or photocopying (subject to the law of copyright), and that the title and abstract may be made available to outside organisations.

Signed Liam Blunt

Date 20/11/20

ABSTRACT- Recently, in the ever-evolving landscape that is cybersecurity, small businesses are slowly falling behind the curve, trusting in their supposed lesser-value target status to protect them from threats. Research shows that this is no longer the case, and too many small businesses simply ignore or are ignorant to this threat. Therefore, this project aims to determine and improve towards a suitable network security strategy in order for small businesses to start taking this threat more seriously. Based on research performed using multitudes of different methods and tools to better protect their network, this project will use a test network to act as a means of experimentation to substantiate our claims that the implemented practices do indeed improve network security. To do so, this project will first delve into this encroaching problem to discover what ails these smaller businesses and why they are at such risk, using these factors in the later development, implementation and experimentation stages should they be deemed relevant. These experiments will allow us to both test against the previous configuration, as well as make improvements based on the results.

Contents

1. Introduction.....	5
1. Aims and Objectives.....	6
2. Literature Review.....	7
1. Financial Implications of Cyber Attacks	10
2. Implications of COVID.....	13
3. Threats.....	16
4. Defence	18
5. Peer Review	20
3. Research Methodology	22
1. Philosophy.....	24
2. Strategy	25
3. Contingency Planning	25
4. Risk Assessment	26
5. Timing	26
4. Development Methodology	27
1. Problem Identification	27
2. Network Design	28
3. Network Implementation	30
A. VPN Client Configuration.....	33
B. DNS Web Filtering.....	40
C. Wireless Networks.....	44
D. Guest Network	45
E. Radius Authentication	47
F. Switch configuration.....	50
G. Network Maintenance.....	51
5. Network Testing.....	52
1. Wi-fi Attacking.....	52
2. DNS Filtering.....	57
3. Evaluation	59
6. Conclusion	60
1. Recommendations.....	61
7. Reflection.....	62
8. Bibliography	63
9. Appendix.....	67

1. Security Tools Evaluation	67
2. OpenVPN Server Configuration	68
3. Wi-Fi EAP-TLS Authentication	73
4. Snort IDS Configuration	78
5. Interface Firewall Rules	80

1. Introduction

In recent years, following the standard trends of cybersecurity, the number and complexity of attacks is ever-increasing, therefore the need for adequate cyber security implementations is becoming only more apparent. That being said, it is not as if all businesses are aware of this looming threat, or at the very least they are aware of it, but believe they are not the type of business to be attacked as they have little to vary, such as small to medium businesses. This is true, in the past the high value businesses were the primary targets, but in recent years this trend has changed direction, why risk getting nothing or caught attacking well-prepared businesses when you could instead attack multiple low-risk-low-reward businesses who are emboldened by a false sense of security? It is this change in direction that has many smaller businesses scrambling to catch up to form a proper means of cybersecurity defence. According to the UK government, as of 2019 31% of small to medium businesses have had some type of data breach[1], whilst this may seem quite low, as they make up ~99% of UK businesses, that means that ~1.7 million businesses have had at least a single *reported* data breach[2]. In addition, separate insurance business estimate the actual figure to be more akin to ~50-60%[1], [3]. As you can imagine, the growing number of cybersecurity threats, the uncertainty of its scale and the business world's relatively unprepared-ness all factor together to form a significant threat to both businesses across the UK and a significant impact to future prospects. Therefore, should this project assist even a small percentage of small business, it would be beneficial.

So, the aim of this project is to both establish the common network threats many small businesses face, and address how they can be defended against in a reasonable manner permissible by the restrictions of small businesses. Whilst this type of research has been done before in a similar manner, too many focus on the human factor, which while a large risk in any sort of network, they are not the be all to end all; it does not matter how secure the computers and their users are, if the network by which they communicate is insecure, then the latter will be all for naught. In addition, from many of the guides whilst they give a vague guideline, that is often all it is, a nudge in the right direction. Whilst it could be said that that could be sufficient, from the point of view of someone looking up such a guide, they are very unlikely to know the means by which you 'secure your wireless access' or the installation of more advanced features and routing.

1. Aims and Objectives.

As indicated in the latter section of the introduction and the title, the aim of this project is;

‘Enhancing of network security within a small enterprise environment.’

To achieve this aim, there must be a set of objectives to follow, and they are as such;

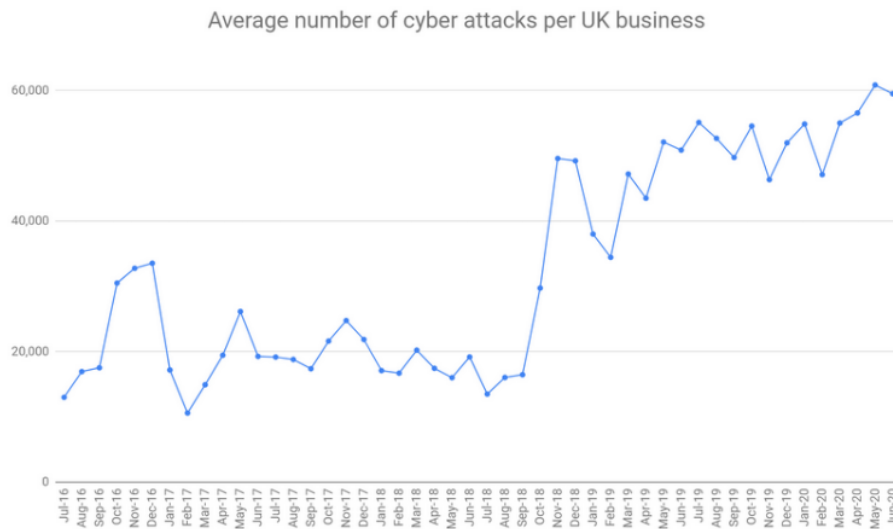
- Research into common and/or average network configuration in target environment
- Research into security concepts and tools to be used.
- Investigation of most common/effective threats to the target environment
- Research into defence against most common threats.
- Using information gathered, development of a ‘test bench’ network environment.
- Using penetration tools, simulate common threats against the test bench network.
- Evaluation of experimentation
- Improving of test bench network security using results of penetration testing as a guide

For the purpose of the test bench network, this writer will take some liberties in the network design. As it is a test network, redundancy, while absolutely necessary for a production network, can be disregarded in this scenario as it would needlessly complicate the design, cost more and for very little return in regard to security.

2. Literature Review

As mentioned previously in the introduction, nowadays businesses are becoming more and more reliant, or rather, integrated within the internet as it is subsequent technologies due to the advantages it provides, such as larger customer base, improvements in business operation efficiency and so on. However, as with anything, these advantages do not come without their disadvantages and whilst there are many, the main focus of this documentation will be that of security, as such threats from both the internet and threats against a business's local network.

Although as mentioned before, the internet and networking has become a central pillar the large majority of businesses whether they rely on it directly or indirectly, despite this, too many businesses see security not so much *essential*, but *optional*. Whilst this might have been true in



the very beginning of computing, it is *far* from the case today, especially so in a business setting.

Figure 1 - Beaming Cyber Attack Report[4]

In figure 1, we can see a good example of how many 'attacks' are attempted against UK businesses from 2016-2020[4], collected by the UK ISP Beaming's 2020 security report. It is worth noting that these attacks are not entirely malicious, but a small percentage are scrapers, scanners or other tools used to *find* targets, but none the less shows the sheer *scale* of possible attackers, as well as unsuccessful attacks. It is also worth noting that according to the same source, 50-70% of the attacks on UK businesses originate from IP addresses from China, USA,

Brazil, Taiwan, or Vietnam, so it is not as if UK businesses only have nationally located attackers to worry about. It is also worth noting that the recent COVID-19 lockdown has caused an increase in cyber-attacks as more people are at home, on their personal devices for work, so rather than a single strong target at a workplace, their personal devices can be targeted instead and/or as well, this point will be expanded upon later in this document. According to Beaming's 2019 cyber-report, the sudden spike in attacks is due to the adoption of IoT devices in UK businesses, which are often targeted due to their relatively weak security, their ability to be used in botnets, making them a lucrative target and their ability to collect data on the targeted business.[5]

As a whole, businesses have taken a rather reactive approach to cyber security, small businesses even more so than their larger counterparts. Whilst this is to be expected from a resources perspective, even now, ten years after cybersecurity was deemed a "Tier 1 threat in the 2010 National Security Strategy, alongside Terrorism, War and Natural Disasters"[6]. As you can imagine, since then, the government has put forth multiple schemes and guides in order to help businesses across the UK defend against the growing threat, in addition to the introduction of multiple laws citing the greater need for protection of personal data held by businesses such as the EU's GDPR, and the UK's Data Protection Act of 2018.

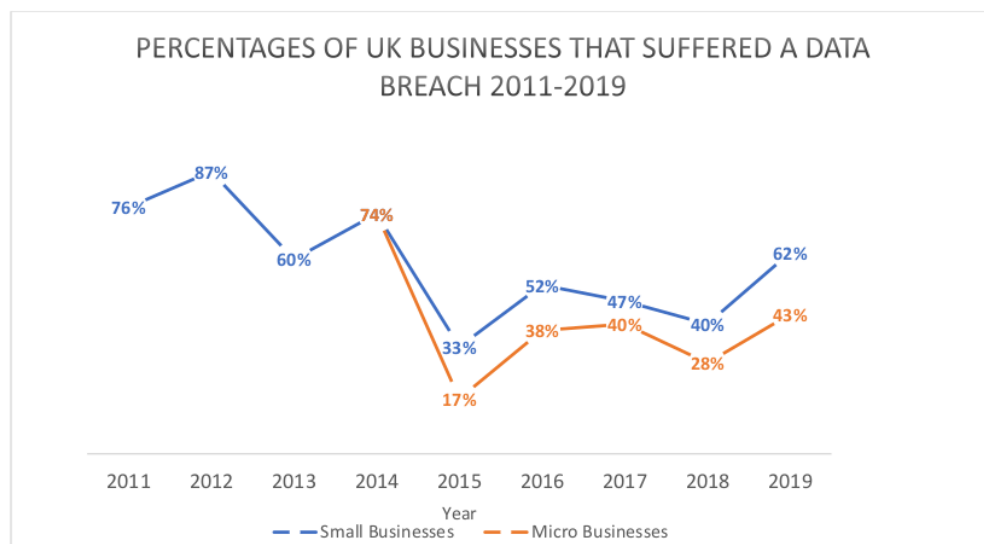


Figure 2- UK Business Data Breach statistics[7]–[13]

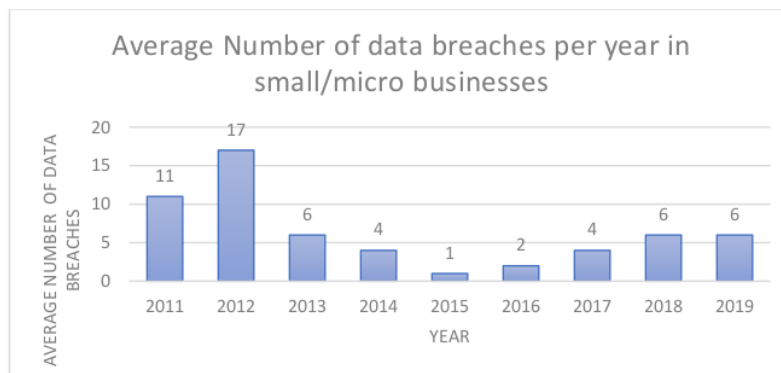


Figure 3- Average Number of UK small business data breaches per year

Above, in figure 2 we can see the percentage of UK businesses that had suffered at least one data breach on a yearly basis from 2012-2020, derived from the UK governments and affiliates 'Cyber Security Breaches Survey'. Worth noting that until 2016, there was no distinction between small and micro businesses and is the reason for the split in figure 2. The data is drawn from each year's respective report, whilst there is conflicting data in later years' reference to the latter years, by keeping the data to the respective years' report we can keep some semblance of conformity in the statistics. As you can see, micro and small businesses follow the same trend, most likely due in part to the fact that they share the same restrictions and challenges when it comes to resources, both personnel-wise and financially. Another conclusion that we can draw is not only are there more *attempted* attacks, but there are also more *successful* attacks, against a wider range of businesses, whilst this may seem obvious due to the increasing number of attacks, it is not a statistic shown by figure 1 alone. Now, as we can see there was a significant dip in 2013-2015[14], likely due to a number of factors; it could be the UK government push for cybersecurity of which included a £650 million investment between 2010 and 2016, it could be a reactive approach from businesses due to the high number of data breaches in earlier years, and so on. Essentially there are numerous factors related to this decrease, but as we can see, that is no longer the case, with an upwards trend up to 2019 in the number of breaches, and whilst 2020 is not included, it can be stipulated that this trend has continued.

When it comes to malware, the UK as a whole is the most targeted of the EMEA area encompassing Europe, the Middle East and Africa, the EMEA zone itself receiving 26% of the world's malware detections according to Malwarebytes' 2020 report[15]. Whilst the amount of malware has increased, the type of malware has shifted, depending on the target, with consumers' top malware being adware, and UK businesses being targeted by hijacking

software and trojans. Technically speaking, a trojan is a deployment type holding a malware, but seeing as anti-malware software cannot detect the payload, they instead detect the carrier.

1. Financial Implications of Cyber Attacks

Now, focusing on the economic damages, to put it into perspective how damaging cyber-attacks are; the UK government estimates an annual cost of £27 Billion, with Intellectual Property (IP) theft and espionage being the most damaging results of attacks[14]. Now, focusing on small businesses, according to SecureTeam, a UK-based cybersecurity consultancy, “nearly 2/3rds of small businesses fell victim to cybercrime in 2018”[16], and whilst this is a shockingly high number of businesses, it is difficult to assign a value to these cybercrimes as a whole, as depending on who you ask, you get a different answer, Secureteam puts the average cyberattack targeting UK businesses cost at £6100, Hiscox proposes ~£10,000[17] and the UK government’s 2020 ‘Cyber Security Breaches Survey’ suggests £3100[7]. As you can see, the value per attack is very difficult to ascertain, and can vary greatly, depending on the extent. In the case of small businesses, the UK government puts the financial cost at an average of £0[8], as, for the most part, small business suffer no material damage, and therefore have no outcome. In this case, the government suggests on average, of those attacks *with* an outcome, an attack will cost £3,110[7]. Whilst not as high as the previous assumptions, considering the amount and the possibility of multiple attacks in a single year, it is still *very* costly. Additionally, a cyber-attack isn’t simple ‘clean up’, it could disrupt company operations for weeks or months depending on the type of attack and how well prepared they were for such an occasion. A good example of this scenario would be a ransomware attack, whereby data is locked/encrypted and ransomed back to the owner; the reason they work so well is because some businesses would rather pay the ransom cost as it would be cheaper to do so than the potential loss of revenue enabled by the ransom, reports suggesting as high as 53% of UK businesses affected simply pay the ransom[18]. There is the option of hiring professionals to retrieve the data, but this is often an expense far from the time and budget constraints of a small business and is often more costly than the ransom, although it does come with better odds of retrieving the data back successfully, seeing as the global average for data retrieval on ransom payment is ~30%[19, p. 9]. Rather ironically, should a company have an insurance policy, more often than not it covers ransomware, and , looking at it at a cost-benefit scenario, insurance companies are more likely

to just pay the ransom rather than seek remediation. As such it can be said insurance companies are 'fuelling' the ransomware industry.

While discussing the economic consequences, it is important to remember that they are not limited to the targeted business, more often than not, businesses rely on one another be it a partnership, customers, or supplier. Therefore should something happen to one business, it is often felt by those said company interacts with. This can be disruptions in product flow, breach of information pertaining to other businesses or disruption of supply chain (such as in the case of a distributor/supplier), amongst others. Then of course, there is possible disruption to customers resulting in reputational loss, resulting in further financial costs due to lost business.

Moving on from the economic *damages*, there are also the economic implications/limitations of a small business, of which you can imagine is a significant factor in their decision-making process, and therefore the running of the business. For example, due to financing constraints it is very unlikely for a small business to have any sort of 'IT department', and if they do it is more than likely to be a single person in charge of the entire business's IT direction. It is also likely that this one-man IT team does not have specialist training as it costs significantly more to hire a specialist than an IT-inclined person, so to speak. Therefore it is more likely for small businesses to hire someone that learns as they go along or, at the very least, someone who is not fully trained, if they have IT personnel, that is. Now, why is this? According to Market-Insight analysts, of those that made a profit, the average total *profit* for a small business ranges from ~£6000-£10,000[20] per year, as of the 4th quarter of 2019. Therefore paying a significant amount for an adequate IT strategy can take a significant chunk out of possible profit margins, restricting their room for growth. IT is very much a continuous short-term cost for long term benefit. Factor together the previous cost of the average cyberattack being between £3,000-£10,000, meaning that a single cyberattack could possibly wipe out the yearly profits for select businesses. Bear in mind, this is only of those that made a profit, according to the same report, roughly 10% of businesses broke even, with 5% making a loss, therefore for 15% of businesses, investing in further IT infrastructure is the least of their concerns.

It is worth noting that most businesses do not actually look at the financial cost of a breach, as it is not financially viable, with only 5% of businesses doing so[10], only in larger companies is it worth the time and manpower to create such a study. In smaller companies, whilst the average cost is much lower, it is in part due to the fact that as such a study has not been done, often only including direct costs such as data lost/remediation, material damage and possible

disruption costs in the calculation. A larger company on the other hand is more likely to include indirect costs such as reputational damage, legal costs ,retraining/updating staff ,updating of policy ,the cost breach aftermath/response, and the investigational costs of finding the source of the breach[21].

Whilst staff costs are an significant cost of cybersecurity, there is a commonly used alternative to hiring full-time specialists; hiring a consultant. More often than not, from a small business perspective, it is much more beneficial to hire a consultant as whilst they generally cost more to hire compared to a salaried specialist, they are usually only hired for a short time to complete a single goal, are quicker to hire than completing a recruitment process and arguably most importantly, they definitely have the skillset necessary for the job. This is especially important as according to Dell's 2018 survey, 88% of Small-Medium businesses had no *qualified* applicants after opening positions for a set amount of time[22]. As a result, as of 2019, ~27% of UK businesses have acquired the services of a consultant or other external managed service provider[7].

Lastly, there is a legal financial incentive to secure your network and beyond, as should the wrong data be compromised, those affected by the breach can take legal action, in addition to the fines the government will levy against the business. As of 2019, of those surveyed only, from multiple countries across the EU, 53% said they were 'mostly' GDPR compliant, with 10% saying they were somewhat compliant[23]. As this was a survey on a businesses' opinion of their GDPR compliance it can be imagined that the actual compliance is even worse. According to another survey surveying small businesses, although many boast their compliance with GDPR standards, they then faltered under more detailed questions, bring scepticism to their bravado. 44% of those surveyed said they were "not confident that they always obtain consent or determine a lawful basis before using personal data"[24], and seeing as this obtaining of consent or reason is one of the main tenants of GDPR, it can be safe to say that not all businesses are as compliant with this law as they would like us to believe. Now, whilst fines can vary greatly depending on cooperation, severity and amount of compromised data, fines to small businesses are relatively low, but large enough to warrant the prior investment to avoid them, for example the Dutch framework's default fines range from €100 for category 1 violations to €725, with a maximum of €1000 for category 4 violation, per violation up to €10,000,000 or 2% of annual turnover of the previous financial year[25]. This statistic is for business at the least, enterprises can have a maximum of €20,000,000 or 4% of previous

financial turnover. As you can imagine, these fines can certainly cripple a business' potential growth.

2. Implications of COVID

Whilst on the discussion of the cyber threats, the effects of the recent Covid-19 pandemic and subsequent lockdown cannot be overstated. Whilst it has been an all-round disaster for many industries, focussing on cybersecurity, it has only exasperated nearly all the problems previously mentioned. Take for example, the fear and panic resulting from the pandemic, according to INTERPOL there has been a sharp rise in Covid-related phishing, spam, malware, and malicious domain registration, using the fear of the pandemic to their advantage[26]. Additionally, the rush towards remote computing, with staff members being unable to work onsite, working from home over a remote connection became their only recourse. Most businesses did not have either the infrastructure in place to facilitate this, or at the very least the infrastructure to do so under maximum load with so many sudden concurrent users. Therefore in the rush to rapidly deploy remote systems, oversites are found to appear, which attackers make use of. Then there are the dangers that come with using personal devices for said remote connections[27], such as those that also come with Bring Your Own Device (BYOD) policies. To allow remote working, you must allow connection to the subsequent resources, but by doing so, you must allow for some degree of risk that comes with remote access. If an employee's laptop has been infected with malware or ransomware, it could use the remote connection to propagate over the VPN connection, in the same sense as if it were connected locally. There is then the problem with remote connections themselves, depending on how it is set up, due to the scale and speed of which these systems are set up, they leave themselves open to misuse, from VPN, firewall and cloud misconfiguration, internet connection and/or improper access control, amongst many others[28]. Essentially speaking, the added layers of complexity bring with them chances to make mistakes, this is why misconfiguration of systems are one of the biggest/most common threats to cloud security environments and the like, where ~66% of cloud attacks were done so via exploiting a misconfiguration in firewall and/or cloud resource[29, p. 8].

In addition, 52% of UK businesses saw a decrease in turnover, outside of their expected range, with the education, entertainment and food industries being hit the hardest[30, p. 5]. As of August 2020, of those businesses still open, ~11% of them are at moderate to severe risk of

insolvency[30, p. 18]. According to a report by Simply Business, the average loss by coronavirus for small businesses in the is £12,000[31], and looking at the estimated profits mentioned in the previous section being £6,000-£10,000, this is more than enough to wipe out savings and/or risk insolvency for many small businesses across the UK.

Whilst it would be great to say this is the only extent of damages, as the virus has not been eradicated, it will continue to damage businesses and people alike, an example of this being the second spike we are seeing as of the 8th of September. Should it the situation become bad enough, and a second lockdown is introduced, which is increasingly likely, it is estimated that ~17% of businesses will not survive[32]. Next, there is the fact that as of writing, furlough is set to end on in the UK on October 31st, this scheme meant that people could stave off unemployment in the meantime, but when this ends and businesses have to start paying these previously furloughed employees again, it will either, force businesses to continue operation under significant financial strain or fire employees leading to increased unemployment. Now, whilst there is a replacement 'Job Support Scheme', this shifts some of the costs of furlough back to the businesses, with employees receiving different amounts depending on hours worked[33]. For example, should the employee work for one third the hours they are scheduled, they receive 77% of their total scheduled pay, 22% paid by the treasury and 55% paid by the employer[34]. As you can imagine, with the previously mentioned financial straits, many businesses are not going to be able to shoulder this expense, even with the support, leading to the aforementioned mass unemployment, just less so than if no support were in place.

Then, to top it all off, there is the ever-looming Brexit situation, bringing with it even greater economic uncertainty, to put it as nicely as possible; small businesses are currently in a *very* precarious economic state as of late, and the future is not exactly looking great either.

Now, having stated the economic downsides of this, let us move onto the reverse. As mentioned before, the move towards remote working and social distancing has massively altered the business landscape, with many businesses opting to remain in a state of remote working, as since they now have the infrastructure needed, why move back to the office? Sure the cost of cloud environments can accrue large costs, but odds are they are much cheaper when compared to office rent, building maintenance, dedicated systems, etc. Now, obviously not all jobs can be done remotely, but it will none the less be a massive shift in on-site personnel, which will have effects on high streets and other areas that rely on commuting customers for the majority of their business. In addition, it has even affected rent prices in cities; why pay extra for a place

close to work if you are going to be working remotely anyway?[35]. This may result in large reaching effects to cities throughout the country. In addition, the ‘talent pool’, so to speak is now greater and easier to reach than ever, no longer must businesses get employees locally, they can now do so across the country or beyond, and whilst they could’ve done so before, with the systems now in place to do so, it is *much* easier and may become the social norm[36].

Now, remote working does have one glaring concern from an employee perspective; outsourcing. If an employee is going to be completely remote, why limit yourself to the country the business is in? According to Goldman Sachs, we can “expect a third wave of outsourcing and an increasing number of technology roles globally finding their way to India”[37]. This is not an unexpected result; it has happened before in the 2008, as businesses look to cut costs due to the financial impact of the financial crash, outsourcing becomes an increasingly viable strategy[38]. Now, with the rise of remote working, this is only going to further facilitate this push towards outsourcing. Worth noting, outsourcing does not necessarily have to be to foreign countries, more often than not it is simply sections of a business that are outsourced to specialised businesses.

3. Threats

This section will look into the ‘threats’ facing small businesses mentioned earlier in this document, but not expanded upon, and their feasibility in both being defended against and inclusion in this project. In doing so we can better understand the threats against businesses, and therefore what means of defence they can use and/or deploy, the defence discussion will be left to another section, as this will focus on threat analysis. While we could go on for ages with this topic, this topic will be restricted to the five most common threats from a businesses’ perspective, derived from the Malwarebytes’ and Bitdefender’s 2020 reports.

The most common and arguably most damaging are trojans. Trojans are an umbrella term for a malware delivery method, similar to the horse by which they got their namesake, this makes them what some would call; the swiss army knife of hacking, as due to their versatility, they can be *very* effective. According to both reports, of the top ten most common threats, at least three are trojans such as Dridex, Emotet and Trickbot. All of these trojans are advanced banking trojans, made for financial gain by infiltrating and collecting information from banks and e-commerce. The danger behind trojans is that, like the trojan horse, it can contain nearly any form of malware, and can be spread by email, advertisements, networks, messaging applications, pop-ups, mobile devices, etc.[39]

The second most common threat, according to Malwarebytes, is adware, not to be confused with malvertising, adware is a type of virus that shows the user unwanted advertisements, either as a distraction for other attacks or more commonly for the collection of advertising revenue. Having said that, due to the presence of advertising resulting from adware, it can often result in malvertising, which is one of the reasons they are often confused for one another. Most adware can be classified as a browser hijacker, such as changing shortcuts and homepages, adding additional advertisements to existing pages, or redirecting the user to an infected page allowing for a drive-by-download, all without their knowhow or consent from the user to do so.

The third most common threat business-wise is ransomware, a malware that encrypts a user’s files, locking them out and extorting ransom, usually in the form of untraceable cryptocurrency. The danger in ransomware is how numerous the ways of spreading it is, as the macro scripts that run the ransomware can often be hidden in documents such as word or pdfs. Then there is the possibility of infected webpages downloading and running the ransomware on a computer without the user knowing, and even more so worrying is that it is an increasing trend, with both

the number of ransom attacks and cost of the ransom rising. Although mentioned beforehand, the danger in ransomware is that not only does it encrypt all your files, getting them back is not guaranteed, as should you pay, it is not guaranteed that the attackers will give you the decryption key, having said that not doing so is technically bad business sense, as it would put off other potential 'customers' from paying, so logically speaking, it would be in everyone's best interest. On the other hand, paying allows for revenue, making attackers others financially profitable, further propagating its popularity as a means of attacking targets and gaining revenue.

The fourth most common threat is phishing, technically speaking phishing is not a singular threat but a designation of a group of threats, which as mentioned beforehand, has seen a sudden increase of growth due to the coronavirus and subsequent lack and/or muddling of information surrounding it. Phishing is a deceptive attempt to trick a victim into divulging information, the most common example is an email or text with a hyperlink which leads the victim to a form where they enter their details or to a download link that launches a virus or malware onto the target computer[40, p. 50]. Due to the sheer scale and variation of phishing, as well as the fact that it takes advantage of the human aspect of a computer network, makes phishing one of the more long-lasting and effective forms of threat, seeing as it has been around since the start of the century, and yet is *still* one of the most common attack methods. Another term for this type of attack is spam, largely in part due to the 'buckshot' approach attackers often use, sending out thousands, and hoping some of them are going to 'hit'. An important distinction, phishing emails are often spam, but spam is not phishing, as spam technically is just any unwanted messages.

The last most common threat is not technically an attack in and of itself but a worryingly common threat none-the-less; unpatched vulnerabilities. This threat is possibly one of the most damaging, as it is a threat that invites other threats, case in point; the WannaCry attack that crippled NHS computer systems in 2017, while the core of the attack was ransomware, the reason it worked was an unpatched copy of windows 7 accessed via what is deemed the EternalBlue vulnerability, the computer system in question had not been updated in years, and so the attackers took advantage of a *known* vulnerability, and ended up costing the UK £92 million[41], amongst the £6 billion worldwide, not to mention the non-financial impact. Now, the reason for this is usually either complacency as it 'just works', or systems rely on other systems, and an update breaks something, and as such it is left just as is. Just because it is

common, does not mean its correct, ideally businesses would have a dedicated personnel to keep track of system and software updates, but as you can imagine, that is not always the case.

4. Defence

This next section will deal with the aforementioned threats section by means of defending against them, while we could discuss on how to deal with them on a one-to-one basis, many means of defence deal with multiple or all of the aforementioned common threats.

Arguably the most effective defence against many forms of attack are knowledge, informing your users on common types of attack and how they work, not in too much detail, but enough for them to defend themselves. If for example, when connecting to a webpage, their web browser flags the connection, while many would simply skip the error and carry on, if your users can understand that something is likely wrong, they can take steps to avoid said error or report it should it be relevant.

The next means of defence is *avoidance*, while quite self-explanatory, there different means by which it can be achieved. Many businesses simply block access to websites that may pose a threat in one way or another, be the websites be malicious, ‘unsavoury’ or insecure. By doing so, you can simply block access to the source of the probable threat before the threat is introduced. There are many levels of blocking such as application, IP, DNS, Domain, browser-level and so on, as you can imagine, this means that there are a plethora of ways of blocking certain websites and/or clients/servers.

The next most popular means of defence is ‘antivirus’ software, but not specifically an *antivirus*, as most ‘antivirus’ software packages have branched out into covering larger defence areas such as anti-malware, ransomware remediation, file encryption, advanced threat control, web filtering, amongst many more features[42]. While some antivirus may perform better than others, for anyone using computers, they are an absolute essential in this day and age. The main differences between enterprise and home-grade antivirus is their means of deployment, for example Bitdefender Gravityzone used a node and client setup by which certain devices act as nodes for the deployment, update, and control of the other clients on the network, as well as support for servers, where most clients will connect to. In more recent years, the use of cloud-based control of these client antivirus systems has become more and more popular as the antivirus controls can be done remotely as well as offloading the scanning procedure of suspect files to cloud servers instead of clients doing so themselves as well as the real-time updating

of said antivirus based off of other users of the cloud. Arguably, the reason this is one of the better defence methods is that the figures given by Bitdefender and Malwarebytes are from antiviruses from client-installed-sources and as such, the attacks against networks are very unlikely to show up in these figures as they would be stopped elsewhere before reaching the client itself.

It is worth noting that these threats are sourced from antivirus business reports and is very likely why they are limited to the types of attacks that antivirus software can target, as network-based attacks are very likely outside their scope.

5. Peer Review

Looking at the report titled “The invisible hole of information on SMB's cybersecurity”, it gives an alternative perspective to the problems that small businesses face, not only are they under greater risk than ever, but they are also very often overlooked by the academic community[43]. The report suggests that when it comes to cybersecurity issues specific to small businesses, <5% of reports from both technological websites and media we so, and for the most part, these are where laymen would get their information on the risks they could face. Even in the academic world, where it may be taken more seriously, they discovered that between 2014 and 2018, across 35 academic peer review journals, only 58 total articles were written specifically about SME's, averaging 0-8 per journal. Whilst it can be said that not all of these journals were the type to publish these types of articles, only having done so at least once in the past 10 years, it shows that there is none the less a significant blind spot when it comes to the reporting of the problems that small businesses face and how they can defend or rectify it. There is an uptick in the number of articles and reports, but still an insignificant amount compared to the size of the problem and economic severity that small businesses face, not to mention the economic domino effect should enough of them fail.

The second document to compare to is ‘Overview of the Importance of Corporate Security in business’ by Sourav Mukherjee[44]. This document does something similar to what this writers’ document aims to do, show the problems facing businesses in terms of cybersecurity, and highlight it is increasing importance in recent years. The main differences lie in the topic area and scope, whereas this writers’ document focuses on small businesses and network security, the document in question takes a larger scope approach in exchange for depth of the topics in question, which depending on your viewpoint, can be either strength or weakness. By this it is meant that the document, whilst expansive in scope, restricts the solutions to the problems to quick bullet points. As there is no expansion on said points, save for a few, the reader must seemingly accept them without any referencing or explanation backing them up, even if they make logical sense, it would best to at least have some sort of academic reinforcement to your statements or line of thinking. The next main difference is the aim of the document, the document being reviewed answers as more of a checklist for businesses to follow and improve their computing operations, this document on the other hand will take a more detailed but smaller-in-scope approach and suggest security features, explaining why they work and testing how well said features work.

Therefore, those using this document as a guide can have a better understanding of *what* they are doing rather than doing so because the document said so, it is debatable whether or not the weight of a PhD student is enough solely. Additionally, the scope of the project, here it is looking at a corporate business, seemingly with an already established business elsewhere or that the business is large enough to have established IT departments and security department for crisis management. While not *completely* out of the question, the likelihood of them existing in small businesses is quite unlikely, at least in a professional manner, some employees may be given responsibility of these departments, without an official department present, but none the less.

The next article to review is “Securing small and medium-size businesses” by Steve Mansfield-Devine[45], as you can see by the title, there is *significant* overlap in the topic areas of both this article and this writer’s project, but the objective seems to deviate, the article does a very good job of illustrating the problem facing SME’s back in 2016, as well as what is being and can be done to help alleviate the problem. The fact that this project is necessary in the first place is evidence that this was, is and will likely continue to be a continuous problem for decades to come, realistically the best goal is to, rather than hope to completely *stop* the problem; minimise the damage.

Now, this next review will be of PFSense, rather than the overall topic, seeing as it is going to be playing an integral part of the proposed test network, it would be best to have at least a summary understanding beforehand. The book is titled “The PFSense Documentation”[46], and while not an official published book, it is the official Netgate documentation for PFSense as of 2020 and is more easily attainable seeing as it is both free and available on the Netgate website. While this writer would like to say PFSense is easy to use and ‘get used to’, seeing as this document *alone* is one thousand three hundred and eighty-one pages long, and does not cover any of the additional packages that can be installed, that would be tough point to argue. Now, while this writer would love to point out problems with it, seeing as this extensive documentation is written by the developers behind the project and has gone through multiple iterations, it is more than likely they know more about the concepts than this writer. All in all, it is as good of a guidebook to the concepts and their associated implementation for PFSense as you are going to get, relatively speaking as it is essentially a PDF copy of the PFSense wiki in a more pdf-friendly format.

3. Research Methodology

Now that we have a good idea of the problem facing smaller businesses, what can be done about it? This is where the development comes in. Admittedly the sheer *scale* of this problem is too much for a singular project, as within a business's network there are multiple aspects such as endpoint security, cloud security, human interference, and so on. Therefore, rather than give a shallow insight into the larger problem, this project will instead focus on giving a deeper insight to a particular *section* of said problem, in this case, as the title suggests; network security. Important to note the distinction of computer *network*, whilst it can be said that all computers that are connected together are part of the same *network*, technically speaking the item we are aiming for here is the network that connects said devices together, usually made up of routers, switches, access points, firewalls, etc.

Now, the scope of this project will focus on small businesses, a term that is quite vague seeing as there are differing definitions depending on who defines it. For this project, we will be using the definition given by the UK government; 10-49 paid employees[3], anything less is classed as a micro business, anything more is a medium-sized business. Technically speaking it is not the number of employees that matter but rather the capital and resources they have available to put towards security, in this case, and seeing as medium and large businesses tend to have *much* greater resources in general to put towards security, they are too large in scope to include, as a student's resources could not possibly hope to create a test scenario capable of what is required. It is worth noting that this project is also adaptable to micro businesses, as they often share the same problems in terms of cybersecurity, and by focusing on the bigger of the two, it is thereby adaptable to both, but would not be if the focus were on a micro-business. There is also the classification of non-employer business, where employees are not paid or are self-employed, such as family run businesses, charities and self-employment[47]. In this project's prospects, this classification of business ranges too wildly in their resource availability, more so than employee-classified businesses and as such have been left outside the scope as they are too much of a wildcard. When it comes to medium-sized businesses, they tend to have the resources to put directly towards an IT 'department', or at the very least have IT specialists whose sole job is navigating the business's cybersecurity, and as such they are outside the scope of this project because at that point the business should have more than enough resources to expend on their dedicated cybersecurity. So, while this project's results *could* be used by a medium-

sized business, it is very unlikely that they do not have a better alternate available. In regard to the focus on small businesses, barring the aforementioned reasons, it being that while it would be *technically* possible to test against a larger business, it is not something that can be simulated in this writer's home environment. Something of that scale would require the assistance of an actual larger business rather than the simulation of such, which due to the ongoing pandemic, lockdowns, and the fact that a businesses' network security would be highly suspect if they told anyone outside their admin teams' the details, the infeasibility is as such, too high. A small business on the other hand can be simulated to a more representative degree, in a home environment, which is much preferable seeing as unnecessary interaction with others is not exactly preferred at these times.

As the testbed network's point of interest is to test security, there will be concessions made in other aspects that are normally a part of business networking such as redundancy, availability and so on. Therefore the network will be a router-on-a-stick, flat-styled network, as it would be sufficient for testing, not so much an active in-use network, but sufficient none the less. Now, one glaring aspect that we cannot test is cloud-based networks. The hosting of websites and services is a good example of this, while performing attacks against them would allow potential attackers to damage or gain information on the business in question, doing so from a testing standpoint is a legal, moral, and technical nightmare. For obvious reasons, there are fine restrictions on what types of tests you can perform depending on what cloud provider and package you have, most of which, if breached, can lead to legal action and/or termination of services. All in all, as it is evidently not worth the risk, the cloud aspect of the network will be remembered, but excluded of any testing scenarios.

1. Philosophy

This section will use the guidelines of the Saunders Research Onion, to present the proposed technique/direction the project will take in its attempts to ‘solve’ the problem proposed earlier in this document. A diagram of said ‘onion’ model can be seen below.

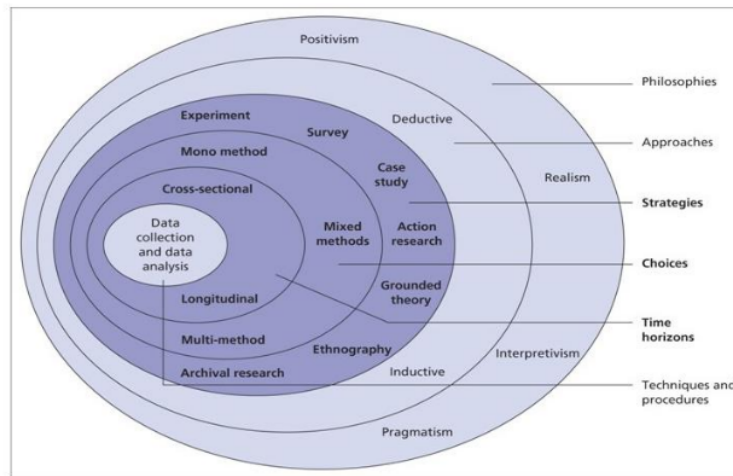


Figure 4- Saunders Research Onion[48]

The philosophy trait in this project will that of a positivist, with near-all forms of data being used and analysed being as a result of configuration and subsequent experimentation. Positivism is the view “that only “factual” knowledge gained through observation (the senses), including measurement, is trustworthy”[49]. This writer believes that this is the best approach for this project as the data we collect will be as a result of experimentation, the results of which will be independent of the subject under study, and therefore both verifiable and the same should the experiment need to be run again, barring any change in variables. The train of thought in positivism is focusing on what is observable and consistent. While positivism is the main trait, it does share traits with realism, as should these tests be run under newer methods, the results will change, partially in due to the ever-evolving landscape of computer security. Now that we have the philosophy, we can move onto the approach, this aspect determines the approach of the research we can/will perform. This project will be more akin to the deductive approach that is ‘theory>hypothesis>observation>confirmation’, rather than the inductive approach which does so vice versa. As we have identified the problems, and then create an ‘observation’ platform of which to test our solution to said problems, confirming or denying our solution, it is more in line with a deductive approach than inductive.

2. Strategy

The strategy, being the next stage, focuses on *how* the project will be carried out. While this project does share some key characteristics with most of the strategies, mainly the experimental strategy, the strategy we will be utilising is the action research. Action research is the method by which we have a problem and therefore try and find a way to solve the problem in *response* to said problem. As this project was started in response to the growing problems small businesses find themselves in, it suits the parameter. Admittedly while we will be using experimentation, making some believe that experimental method would be more beneficial, here we are mainly using experimentation by a means to verify that the solution worked and to what degree, rather than the main focus of the project, which in our case, is more likely to be the research rather than the experiments. Additionally, action research first identifies the problem and then a set of solutions are “prepared and presented as recommendations to solve the issue”[50], which we will aim to do so. While action research does have a soft requirement of industry links or business-backing, as you can imagine, in our example, that is not so.

In regard to the method choice, there are three choices, mono, mixed and multi-method. These layer is focused on qualitative and quantitative methodology, in regard to the type of information you are going to collect and use to analyse. The difference between the three is that monomethod relies on either quantitative *or* qualitative data, whereas mixed and multi-method rely on a mixture of the two, with mixed doing so in an equal manner, and multi doing so in a less-equal but none-the-less present mixture of the two data.

3. Contingency Planning

There are a number of happenings that could occur over the time of this project that can disrupt the project. To this effect a number of strategies may be put into place as to either avoid or mitigate the effects of said disruptions, that is what this section will focus on.

The number one concern would be that of Covid and the subsequent lockdown, minimising human interaction. Understandably, this was a continuing concern from the project proposal with the first lockdown, and as such, this project has been designed to not use the human interaction-based attacks as experiments as there are no viable people to test on without concern.

The next main concern is to that of data, as there are multiple software being used, PFSense, Unifi and Parrot OS, to be the main ones, the likelihood of them or their hardware failing is not negligible, PFSense in particular seeing as the hardware it is running on is four to seven years old and is running on a mechanical hard drive. To mitigate these risks, each software will be backed up on a weekly basis or after particularly large changes have been made, this data of which will then be stored in 'cold' storage in a separate location, as well as being encrypted and stored in two separate cloud storage services. This concern also propagates to this project documentation, but that is of lesser concern as the documentation is automatically backed up by OneDrive, Google Cloud and locally as changes are made.

4. Risk Assessment

As you can imagine, all projects come with varying degrees of risk associated with their development, and as such we must take steps to minimise said risk. Luckily, risk was a focus point in this project from the start and as such, steps have already been taken to avoid them. The first and main risk would be of experimentation, as many attacks can damage their target in one way or another. This is why the attacks we will use for experimentation will be non-damaging/harmless attacks, as there is little point in developing a more secure network if you are going to accidentally destroy it all by deploying ransomware into it.

Another rather large risk is that of the outcome, while this project aims to improve security in a small business environment, the focus is *network* security. As such, should this document be taken as a *sole* response to address weak security throughout the 'network', the business will both be sorely disappointed and in a dangerous position due to weak security in other aspects of the network. Therefore it has been stated many times in this document that *this is a project focusing on network security, and as such should not be taken as an all-in-one solution*.

5. Timing

Of course, like any project, this project is restricted by time constraints, said time being the until the 20th of November 2020. To facilitate completing the project before this deadline, we can break it down into sections via the use of a Gantt Chart, of which can be found in the appendix due to the size of the chart having an issue with Word's formatting. As you may see, while the timing may be quite liberal, this is mainly so that arrangements can be made should something go awry, without affecting the tasks that rely on their predecessors.

4. Development Methodology

1. Problem Identification

As we are aiming to develop the security of a small business network, there must be a problem we are aiming to address. The main constraints come under the following categories;

- Cost

As mentioned before, one of the chief concerns is cost, as this is one of the more common entry barriers for many small businesses when it comes to network security. Costs of security implementations will attempted to be kept low, not only as this will increase the viability of businesses using these security measures, but it is not as if this writer can afford an over-the-top security network, on par with a higher-grade small business.

- Representation of target

In the case of this test-network, while it is a *test* network , it must still be representative of a small businesses, with some liberties made, without compromising the nature of the small business network. Also, as this is a *business* network, the equipment shall be kept to a standard, and as such consumer grade hardware will not be used. Understandably, many small businesses do use consumer hardware as cost saving measures, but just because it is commonly done, does not mean it is proper to do so.

- Feasibility

As the point of this document is to give an insight in improving network security, technically speaking this writer could suggest no wireless access, no non-static DHCP, static ARP, firewall rules on a port-per-host basis and no access via the WAN. Of course, this would achieve the target of improving security, but for a business, it is completely unfeasible, and as such a compromise must be made between security and usability.

- Complexity

As mentioned before, one of the more concerning issues with security is that of complexity, as you can imagine, security systems are a tad more complex than basic computer knowledge. Unfortunately, a balance must be struck between how advanced the system is to the average user, while still being advanced enough to keep out attacks. This will likely be one of the polarising factors of using PFSense, as its complexity is both a boon and a hindrance.

2. Network Design

With these requirements in mind, the equipment we will be using is as follows.:

- Ubiquiti UAP-AC-LR Access Point
- Ubiquiti 24-Port Switch Non-POE
- 1 x Dell OptiPlex 390 SFF running PFSense 2.4.5-RELEASE-p1
- 1 Network Service PC running Unifi Controller Software (Version 6.0.28.0)
- A PC to be used as an Admin PC, mainly used for configuring the network and others.
- A smartphone, to be used as both victim of attacks and tester due to its 3G capabilities.

In regard to the Ubiquiti devices being used, as opposed to most devices that are managed via either their own UI or via SSH or other console-based connections, Unifi devices are configured, monitored, and updated via a centralised controller, which is why there is a need for a separate system to host them. This is a net positive, as easier means of maintaining the network can be done via said interface, allowing those who are uncomfortable with console interfaces to successfully configure and maintain their network. While this writer could also suggesting the use of an Ubiquiti router to allow all devices to be managed from a singular interface, PFSense is, in this writer's opinion, a *much* better choice. Whilst it may not have the same interface as the Unifi devices, it does have its own Graphical UI (GUI) for its configuration and comes *much* more features than the Unifi alternative, because Unifi routing devices are still very much beta and as such many of the more advanced features are dubious in terms of reliability. This also means that there will be a clear disconnect between layer 2 and layer 3, all switching is done via the Unifi devices, whereas routing is done by PFSense, as the switch being used is only has layer 2 capabilities, while this disconnect is not necessarily useful per se, the clear disconnect between the two makes management of either side much easier. While Unifi devices are cheaper than competitors and advertised as enterprise-grade, but many in the community see them as a sort-of pseudo enterprise, as they often do not have many of the features of their competitors, but due to their lower price point and good building, they are in a sweet spot for small businesses that are looking for enterprise equipment at a good price point. In addition, while Unifi lacks some of the common features in enterprise environments, we will be making up for it by using PFSense as the router, to make up for what Unifi lacks.

3. Network Implementation

Now, moving onto the development of the network, as mentioned before, we will be using PFSense as the router, which during setup requires port allocation. Technically speaking, PFSense can run on a singular port using VLAN-ing to virtually segment the WAN and LAN traffic, but as we have two network interface ports available, they can be used for WAN and LAN independently. Whilst this is a test-network, internet connectivity is warranted for downloading, updating, remote access and verification of configuration. It is worth noting that while physical security is *very* important, it will be deferred for the time being, as it is not the main focus of building the network, in favour of digital security. The networks being used in this test network are listed below:

VLAN ID	Name/Purpose	Network	Gateway
1	LAN	10.0.0.0/24	10.0.0.1
5	Networking	10.0.5.0/24	10.0.5.1
10	Trusted Wired	10.0.10.0/25	10.0.10.1
11	Trusted Wireless	10.0.10.129/25	10.0.10.130
50	Guest	10.0.50.0/23	10.0.50.1

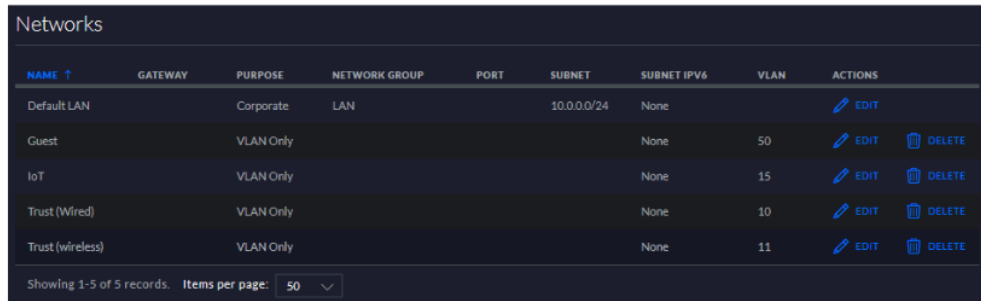
In regard to the networking convention, as you can see it is quite simplistic, using the first half of the host address as an indicator for the IP's VLAN tag, with the only exceptions being the latter 254 IP addresses of the guest subnet, the trusted wireless, and the OpenVPN server, the latter of which will be addressed later in the document. In regard to the address spacing, as we are using IPv4 private addressing, which is behind NAT translation, we see no reason to conserve addresses and needlessly complicating the network. A possible additional interface was to be Internet of Things, as a more restrictive network for IoT devices, but as this writer has no IoT devices, therefore this is unlikely to be done. As there is only two ports available, one of which internal, the LAN, the VLAN's parent interface will all be the same. While it would be preferable to physically separate them via different *physical* interfaces, VLAN-ing them will be sufficient for this test network performance. For the purpose of connection, at this stage in the project, the LAN interface had been set up with a standard DHCP pool for its entire subnet. The creation of the VLANs is done via either the initial setup of PFSense or later, once

access to the admin interface is established and at this point, they are unassigned to parent interface. As the initial setup uses a wizard, this will be skimmed over as it is as linear as it can be.

Now that we have established the initial PFSense setup, we move onto the Unifi setup, so that we can access the PFSense admin interface over the switching environment. Here, the Unifi controller is being loaded as part of a docker-compose stack. Technically speaking, this is an unofficial image, not provided by Ubiquiti itself, but a 3rd party repackaging the controller as a docker image. Whilst there are other options, such as configuring it from a browser, it is not available 24/7, meaning that should anything go wrong on the Unifi section of the network, you, the administrator, will be completely unaware. On the other hand, there are official Unifi controller mini pc's, but seeing as they cost £90-180, and do the exact same as what this writer can achieve on existing hardware using said docker container, it is seemingly not worth it. Another option is installing docker and the container on the PFSense machine, as FreeBSD, the OS of which PFSense is based does support docker, but there is the security concern of increasing the attack surface on an edge router as well as the fact that it is not officially supported on PFSense itself and is installed via scripts via the cli. Now that the controller is in place, once the network equipment is installed, they automatically find the controller via multicast, at which stage we can 'adopt' them. As mentioned before, we had set up a DHCP server, meaning that the devices were able to be assigned an IP from the LAN interface, allowing for easier connection to the controller, where it can receive the rest of its configuration. In the event that a device cannot find a DHCP server, it defaults to 192.168.0.0/24, meaning that the user must SSH into the device and assign the controller connection and IP manually, which, on larger networks can cause significant problems.

Now, the 'difficulty' in using two separate configuration interfaces is that here, the Unifi switching environment is unable to get VLAN tagging information from the router, and as such we must manually configure it ourselves. This is not difficult, just creating networks in the controller is simple, creating a 'corporate' network as default, and assigning creating the rest of the VLAN's as VLAN-only. As we are using a separate router and/or DHCP server, there is very little difference between a corporate and VLAN network, only Unifi requires at least one corporate network, so we are keeping it simple by allocating VLAN 1 as such. Whilst

discussing these networks, Unifi allows for DHCP snooping on these networks, and as such we have applied them to point to each networks' default gateway, as the DHCP server for each will reside on the PFSense router, therefore in the event that a device tries to use a different DHCP server than those chosen, this writer, as the network administrator, will receive an email about a rogue DHCP server.



Networks								
NAME ↑	GATEWAY	PURPOSE	NETWORK GROUP	PORT	SUBNET	SUBNET IPV6	VLAN	ACTIONS
Default LAN		Corporate	LAN		10.0.0.0/24	None		EDIT
Guest		VLAN Only				None	50	EDIT DELETE
IoT		VLAN Only				None	15	EDIT DELETE
Trust (Wired)		VLAN Only				None	10	EDIT DELETE
Trust (wireless)		VLAN Only				None	11	EDIT DELETE

Showing 1-5 of 5 records. Items per page: 50

Figure 6- Short Summary of Unifi-based Networks

Now, we have created the interfaces and VLANs, we can connect devices, but any devices connected will be provided a basic IP from the LAN interface, as whilst we have created the VLAN, we have not assigned them to an interface. To do so, in the admin interface of PFSense, under 'Interfaces>Assignments', from here we can assign the VLANs we made earlier in the CLI-setup of PFSense. As we only have one internal network, they all are assigned as sub interfaces of re0, becoming re0.10, re0.11, respective of the VLAN tag. These interfaces by default are given names of 'OPTX', X being the number of optional interface number. From there, under the Interface tab, we go to each VLAN port, rename them to a better name than OPTX, and assign them, using the network names given earlier in this section, as well as their static IPv4 addresses and subnetting.

As we are using PFSense as the DHCP Server, we must enable and configure each DHCP pool for each interface. At this point in time, we are using the WAN-provided DNS servers. Each interface will be using the first IP as their gateway, with the rest of the subnet being used as the DHCP pool or static IPs, as in PFSense, any static assignments must be outside interface's DHCP pool.

Now, at this stage, there is no connection to the internet available as by default the firewall of any PFSense interface has no rules, ending in a 'deny any' rule, the only exception being that

it allows access to the admin portal on the LAN interface. Therefore, to allow and test for internet connectivity we create an ‘allow any’ rule, allowing any sources across all protocols.



Figure 7- Rule allowing all external connections established from internal networks.

As you can imagine, this is not the type of rule you would want in a live network. That being said, PFSense automatically blocks all incoming connections on the WAN side, unless the connection was initially created from an internal interface network or if there is a rule in place allowing the connection on the WAN interface. As we now have internet connectivity, we can use this time to update PFSense, the docker image the Unifi Controller container is running off of, as well as the packages that come with PFSense.

A. VPN Client Configuration

At this point in time, as we have the networks set up, we can start securing them. One major component in this is the VPN, allowing us to secure outgoing communications on certain networks. For this test network, we will be securing all networks apart from the guest network via VPN. Also worth noting is that the VPN this writer will be using is NordVPN, as it is one, he has a subscription to but is a consumer version, while it would be more representative to use a business-grade VPN, it would be quite expensive for something that is only going to be used for testing and requires a business consultation to get prices and such. As such, we will be using the consumer version, which for securing our outbound traffic, will be sufficient. This initial VPN usage will be as a client using a public server, giving us additional anonymity.

Now, to start, we need to create a certificate to authenticate against the NordVPN server we are going to be using server UK1852. This is done under ‘System>Cert. Manager>CAs’, then adding a certificate, giving it a name, and selecting ‘Import an Existing Certificate Authority’. In order to import the CA, we need certificate information, in this case it is gathered from the NordVPN server OpenVPN config catalogue[51]. Here, you find the server you want to use and download the, in this case UDP, config file. In said file there is a section with ‘--BEGIN CERTIFICATE—’ and ‘--END CERTIFICATE—’, this section is what we put into the

Create / Edit CA

Descriptive name

NordVPN Cert

Method

Import an existing Certificate Authority

Existing Certificate Authority

Certificate data

-----BEGIN CERTIFICATE-----
MIIFCjCCAvEgAwIBAgIBATANBgkqhkiG9w0BAQ0FADASMQswCQYD
VQQGEwJQQTEQ
MA4GA1UEChMHNTM5ZjZQTjEYMBYGA1UEAxMPNTM5ZjZQTjE3B3B290
IENBMB4XDTE2
MDEwMTAwMDAwMFoKDTE1MTIzNTk1OjowOTEIMAAkGALUERhMC

Paste a certificate in X.509 PEM format here.

Certificate Private Key
(optional)

Paste the private key for the above certificate here. This is optional in most cases, but is required when generating a Certificate Revocation List (CRL).

Serial for next certificate

0

Enter a decimal number to be used as the serial number for the next certificate to be created using this CA.

Now, for the creation of the VPN client we go to 'VPN>OpenVPN>Clients' and press '+Add'. This part has *a lot* of configuration, so rather go one by one we will instead only include the fields that had been changed, anything not included below was left as default.

General Information	
Field	Input
Server Mode	Peer to Peer
Protocol	UDP on IPv4 only
Device Mode	Tun – Layer 3 Tunnel Mode
Interface	WAN
Server Host or Address	<NordVPN Server Address>=uk1852.nordvpn.com
Server Port	1194 (for UDP, 443 for TCP)
Proxy Authentication	None
Description	<Used for administration purposes, use as inclined>

User Authentication Settings	
Field	Input
Username	<VPN Account Username>

Password	<VPN Account Password>
----------	------------------------

Cryptographic Settings	
Field	Input
TLS Configuration	Check
TLS Key	From the config file we grabbed the CA Key from, there is another block with begin and end 'OPENVPN STATIC KEY V1', paste that here, including the begin and end lines
TLS Key Usage Mode	TLS Authentication
Peer Cert. Authority	Use Cert. created earlier in this process
Client Certificate	WebConfigurator default
Encryption Algorithm	AES-256-GCM
Enable NCP	Check
NCP Algorithm	AES-256-GCM and AES-256-CBC
Auth Digest Algorithm	SHA512(512-bit)
Hardware Crypto	No Hardware Crypto Acceleration

Tunnel Settings	
Field	Input
Limit Outgoing Bandwidth	Leave blank unless this client is for certain situations, such as if you do not want a select network to exceed a certain limit. (Bytes per second)
Compression	No LZO Compression [Legacy style, comp-lzo no]
Don't add/remove routes	Check

Advanced Configuration	
Field	Input
Custom Options	Custom options will depend on your VPN provider, as each has their own options that can be found on their OpenVPN configuration page

Gateway Creation	IPv4 Only
Verbosity Level	3 is recommended, increasing gives more detailed output in logs

And Save.

Now we have created the VPN Client, but have not assigned it as in interface, do so under 'Interfaces> Interface Assignments', in a similar fashion to how we assigned the VLANs to their interfaces. Now enable it, leaving everything else as default, barring the description and name, as OPT1 is not exactly indicative of its use.

The next step is setting up the DNS resolver, which resolves DNS queries, providing an IP address from the domain name. It is installed by default in PFSense, but by default they use the WAN DHCP authoritative root DNS servers, so in this case they are using the ISP-provided servers, but as we are using a NordVPN setup in this testing, we will have to change that. So, navigating to 'Services>DNS Resolver', from here we can make the necessary changes.

General DNS Resolver Options	
Field	Input
Enable SSL/TLS Service	Uncheck
SSL/TLS Certificate	WebConfigurator default
Network Interfaces	All
Outgoing Network Interfaces	<Previously Made VPN Interface> WAN (If you want certain interfaces to not use VPN)
System Domain Local Zone Type	Transparent
DNSSEC	Uncheck
DNS Query Forwarding	Check (Allows us to forward to DNS servers provided under 'System>General Setup' as opposed to root DNS)
DHCP Registration	Check
Static DHCP	Check

General DNS resolver settings is complete, so we move onto advanced tab.

Advanced Privacy Options	
Field	Input
Hide Identity	Check
Hide Version	Check

Advanced Resolver Options	
Field	Input
Prefetch Support	Uncheck
Prefetch DNS Key Support	WebConfigurator default

Now, we have a VPN Client established and using the correct DNS servers, we just need to control the flow of traffic towards it. So, under 'Firewall>NAT>Outbound', we must first change the outbound NAT to hybrid or manual, the VPN provider suggesting manual. After saving said option, we can create rules to apply Network Address Translation to networks, allowing them to interact properly with the VPN tunnel. Below is an example rule applying NAT translation to the LAN subnet for VPN support, as you can see, we apply it to the VPN interface we created earlier. As NordVPN only supports IPv4, we only translate IPv4.

Edit Advanced Outbound NAT Entry

Disabled
☐ Disable this rule

Do not NAT
☐ Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules
In most cases this option is not required.

Interface
NORDVPN_UK_1852
The interface on which traffic is matched as it exits the firewall. In most cases this is "WAN" or another externally-connected interface.

Address Family
IPv4
Select the Internet Protocol version this rule applies to.

Protocol
any
Choose which protocol this rule should match. In most cases "any" is specified.

Source
Network
10.0.0.0 / 24
Type
Source network for the outbound NAT mapping.
Port or Range

Destination
Any
/ 24
Type
Destination network for the outbound NAT mapping.
Port or Range

☐ Not
Invert the sense of the destination match.

Figure 9- Example NAT rule

These NAT rules must be created for any interface wanting to use the tunnel. Whilst you can create individual rules for each, PFSense allows for the use of aliases. Under 'Firewall>Aliases.', we can create 'aliases' or terms that allow us to group networks/subnets together, allowing for the easier referencing of them later on. Simply add an alias, add the networks you want to refer to, and then refer to them later, below is an example rule, and it

being used in NAT translation.

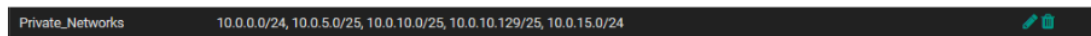


Figure 10- Alias for Non-guest connection.

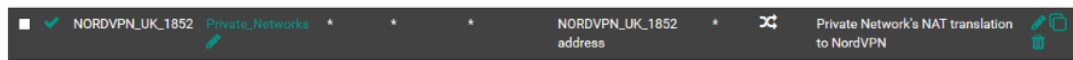


Figure 11- NAT translation rule for any network defined in the alias.

Now, applying it to the firewall; Under 'Firewall> Rules', first of all disable or delete the IPv6 rule auto created by PFSense, assuming your VPN provider doesn't support IPv6 tunnelling. Now, create a rule on any internal interface you want to use the VPN, for this example this writer will use the LAN interface. When creating the rule, under 'Advanced Options', there is a gateway variable, choose your VPN interface and save. The rule this writer has made allows for any protocol and destination coming from 1.0.0.2 to access the gateway, as seen below.

Figure 12-Gateway Rule Generation

The reasoning of this is that 1.0.0.2, of which acts as the Unifi controller is the only device that needs access to the internet, while the switch and access points may need updates and such, they are done so via the Unifi controller. Now, as PFSense firewall rules read from top to bottom, we much put this rule as low as possible, meaning that this rule and gateway is a 'last resort', should no other rule interfere. Now, should you want this done on any other interface, such as this writer is doing, simply recreate said rule, only on the other interface's firewall, assuming they are part of the previously made alias/rule in NAT translation.

Now all that is left is to redirect DNS queries to NordVPN’s servers. Under ‘System > General Setup’, change or add the DNS servers, in this case, 103.86.96.100 and 103.86.99.100, assigning at least one of them to the gateway, as shown below. Each gateway needs at least one unique DNS server.

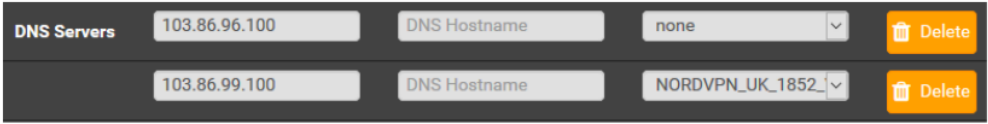


Figure 13-General Setup DNS Servers

It is worth noting that while NordVPN is used here, for the most part, when using another VPN provider, the process will stay the same, barring some nuances in custom rules ,encryption and other tunnel and DNS settings, at least when using PFSense.

To make sure the tunnel is up and running correctly, under ‘Status>OpenVPN’, there should be a client connect such as the one below.

Name	Status	Connected Since	Local Address	Virtual Address	Remote Host	Bytes Sent	Bytes Received	Service
NordVPN Connection via UK-1852 UDP4	up	2020	192.168.0.10:52442			4.84 GiB	88.85 GiB	

Figure 14- Tunnel Status

Assuming the tunnel is up, use a ‘Check your IP’ website to check whether your PC is actually using it in accordance with the firewall rules, and how external websites are perceiving it.

As we have just discussed aliases, this would-be good time to point out that by default PFSense allows communication between all VLANs, and as such you must create dedicated firewall rules blocking off those interfaces you do not want to communicate with each other. This is where aliases come in handy as you can create blocking aliases for an interface, detailing all the networks you do not want an interface to communicate with, and put it into a rule. Should any changes need to be made at a later date, simply change the alias rather than the multiple rules.

While using a VPN, there is the concern that select websites block VPNs due to either both tracking and/or security concerns, but this is mainly for public VPNs, which we used in testing, due to anonymity. On Enterprise VPNs, a separate IP pool is used, reducing the chances of such.

As for the VPN server, from which external clients can access the internal network, please refer to the appendix, section “OpenVPN Server Configuration”.

B. DNS Web Filtering

This next security method is going to be DNS filtering, essentially web filtering, just using DNS to filter domains rather than websites by their URL. This will allow us to block suspicious websites or other sources of malware before the request is made to the DNS server to actually access said website. While there are many options to achieve this, such as Pi-hole, OpenDNS and Cisco Umbrella, among others, but we will be using PFBlockerNG, as it is the 'go to' when it comes to DNS filtering on PFSense, controlling packets accessing the firewall based off IP blacklists.

The first step will be to install the PFBlockerNG package, in 'System>Package Manager', from here you can search for it and install it. As the package relies on a DNS resolver, that must be set up first, but seeing as we have already done so in the VPN client step before, it will be overlooked here.

Now that PFBNG is installed and its prerequisites set up, we can move onto configuring it. Under 'Firewall>PFBlockerNG', we will be brought to the configuration wizard set up. This will set up a default instance of PFBNG, with small variables selected by the user. So, for inbound interfaces, any and all WAN interfaces should be selected, and likewise for outbound and LAN interfaces that you want the blocker to run on. For webserver configuration we will keep the default ports and IP at 10.10.10.1, as it is not in use by our other networks. Once the wizard has been completed, the program will start downloading default blacklists. Now, go to the DNSBL tab, under configuration, make sure that the 'permit firewall rules' is active, assuming you have more than one LAN/VLAN interface.

While this section is called DNS filtering, PFBNG works blocking both IPs and DNS and as such we will first move onto enabling IP blocking. This is under the IP tab, while most settings will be kept as is, the Maxmind license key option, while not *necessary* per se, is very useful for geoIP blocking and as such is recommended. Whilst on this page, make sure the WAN interfaces are selected on the 'inbound firewall rules' and the LAN interfaces on the 'outbound firewall rules'. If you did register a Maxmind license key, the GeoIP tab appears, from here we can block access to and from servers based on their geographical location. Technically speaking, unless you are hosting services on your network, and therefore have holes in your WAN interface, blocking access to your network from said locations is technically unnecessary as, by default, PFSense blocks all inbound communications unless they were started from an

internal network. From this GeoIP tab, you can permit or deny access to and from countries, either by doing so for the entire continent, or by editing them, you can do so on a country-by-country basis, blocking access to websites hosted in said country. There is also an instance of the ‘top scammers’, countries that have the highest rate of malicious websites and while it would be a good idea to block them, as the UK is one of them, you can block yourself out of many websites you would normally access, for testing purpose, as the only access this writer would need from external sources would be a device using the VPN server, he has blocked all inbound apart from the UK, as well as outbound from uncertain sources such as south America, china, japan and a number of other countries as well, largely due in part due to the insecure http/https used on websites. Worth noting to be careful in what you block as some websites are commonly hosted elsewhere from where the actual business is situated.

Then there is the DNS Blacklist or DNSBL category, this is where the DNS lists come into play, where you can create lists of sources, blocking the websites contained within. These source lists can be found quite easily, varying from the business-orientated to those sourced by the community, as well as those included in the ‘Feeds’ tab. The Feeds tab comes with predefined lists based on certain topics, simply add, enable, and select the unbound option for them to be included.

Category	Alias/Group	Feed/Website	Header/URL
IPv4 Category	PR01	Abuse Feodo Tracker	Abuse_Feodo_C2
IPv4	PR01	> Abuse Feodo Tracker	Abuse_Feodo_C2_Agr
IPv4	PR01	Abuse SSL Blacklist	Abuse_SSLBL
IPv4	PR01	> Abuse SSL Blacklist	Abuse_SSLBL_Agr
IPv4	PR01	Bambenek Consulting	BBC_C2
IPv4	PR01	> Bambenek Consulting	BBC_C2_Agr
IPv4	PR01	CINS Army	CINS_army
IPv4	PR01	Emerging Threats	ET_Block
IPv4	PR01	Emerging Threats	ET_Comp
IPv4	PR01	Internet Storm Center	DSHield
IPv4	PR01	Pulsedive	Pulsedive
IPv4	PR01	Spamhaus	Spamhaus_Drop
IPv4	PR01	Spamhaus	Spamhaus_eDrop
IPv4	PR01	Talos-Snort	Talos_BL
IPv4	PR02	Alienvault	Alienvault

Figure 15- The Feeds Tab Lists

On the other hand is categories, essentially a ready-sourced DNS blacklist that is separated into categories allowing the admin to block websites at the resolver, such as adult, drugs, spyware,

malware, essentially websites that you would prefer your users not to access. These categories are derived from either Shallalist or Université Toulouse and while not part of the *official* PFSense team, neither is the PFBlockerNG package, and both are well received by users of PFSense, none the less there is some level of trust the admin must take when using these types of packages. Word of warning, some of these categories such as adult are *very* large lists and as such may take up a significant amount of RAM, often maxing out the DNSBL limit set in the general tab which by default is 20,000 lines. For the purposes of testing, only the categories blocking items that are inherently malicious are blocked such as malware, spyware, trackers, etc, in addition to the DNSBLs both produced by default and derived from Firebog's 'ticked' site lists[52] and are both active.

Now, at this stage, technically speaking, this blocker is not connected to interface, but during the setup wizard, if everything went right, in the DNS resolver additional config section, there is a line including PFBlockerNG, '**server:include: /var/unbound/pfb_dnsbl.*conf**'. This means that any device using the DNS resolver will be affected by the DNS blocking configured in the PFBlockerNG 'firewall'. Secondly, these rules do not come into effect as they are saved, but once the resolver has been reloaded under the 'Update' tab, otherwise they will come into effect on the standard reload which by default is at the start of every hour.

As a last note, DNS filtering alone is not enough to block malicious advertisements and websites, of course it is not all encompassing, just a step in the right direction. The difficulty is that being that it works against DNS means that to block a host, you must block the domain, and in doing so, you may block legitimate subdomains. A good example of this is Amazon, as they have a massive advertising domain, automatic rules may block them, but doing so would likely block access to several sites, and break those that rely on it to some effect. Therefore, although a DNS-level block is in place, the use of a good anti-virus package and browser-level Adblock are advised, to target those that 'slip through the cracks', both in meaning of advertisements and other connections.

While on the point of DNS, the *enforcement* of its use can be done either manually, through DHCP allocation or NAT redirection, the latter being the more effective of the two. In this instance for testing purposes, the gateway of each VLAN was set as the primary DNS Server, and NordVPN being the secondary, should the local DNS resolver go down, as that is the authority server for the local resolver anyway. As a backup, and means of security, in the 'Firewall> NAT' section, this writer created a port forward/redirection rule for each interface

that specifies any DNS request sourced from their respective networks will be redirected to the DNS resolver, so should anyone try to use a different DNS, it will still go through the local DNS resolver. An example from the Wired_VLAN can be seen below.

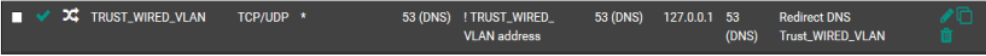


Figure 16- Example of DNS NAT redirection rule

Now, despite this enforcement, there are ways to avoid it such as client-side VPN and DNS-over-HTTPS, the difficulty in blocking these is that different VPN providers use different ports, so while you may block some, you may not block them all. In addition, DNS-over-HTTPS is a means of securing the DNS, which while it technically *does* do so, it also means you, the administrator, cannot control it unless you set up SSL-inspection, a form of allowed/official Man In The Middle attack, which while pfSense does allow, there are concerns that it weakens the security of HTTPS as there is no longer a direct connection, and misconfiguration means that often the re-encryption after inspection is significantly weaker than the initial encryption. Then there is the concerns when creating, transferring, and installing root certificate on each machine wanting to use the SSL-inspection proxy server, which has many points to go wrong. In some modern browsers, such as Firefox, the network can signal browsers to disable DNS-over-HTTPS, allowing for enforcement of the DNS resolver and local blocking. In pfSense, this setting can be enabled under the 'DNSBL>Safe search' tab in PFBlockerNG, on the Firefox DoH setting.

As an example of how effective the blocking is, having used it for roughly a week during general browsing of the internet, according to the package, ~30% of all queries have been blocked.

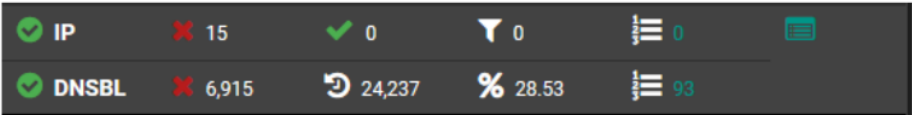


Figure 17- Unbound Resolver Queries Widget

C. Wireless Networks

Now, although we have secured the network to a certain degree, we still only have wired connectivity, so we must create the wireless networks, while this can be done in PFSense, here we will be using Unifi to create them. This is a rather simple process, on the controller under the ‘Settings>wireless’ tab, simply create a new wireless network. This wireless network by default will be distributed to each access point in the Unifi environment, but as we only have one access point, it will make little difference. Simply give the network an SSID/name, enable WPA security (Unifi only allows WPA-2) and apply a strong password. As a basic means of giving wireless access to the network, by default on VLAN 1, under advanced settings, this can be changed using the VLAN settings. Below you can see a default wireless network using the Trust_Wireless network, the only missing setting being the combining of 2GHz and 5GHz into a singular SSID, as to not flood the area with multiple SSIDs.

EDIT WIRELESS NETWORK - L57WIFI

Name/SSID: L57Wifi

Enabled: ☒ Enable this wireless network

Security: ☐ Open ☐ WEP ☐ WPA Personal ☒ WPA Enterprise ☐ Hotspot 2 OSEN

Security Key:

Guest Policy: ☐ Apply guest policies (captive portal, guest authentication, access)

ADVANCED OPTIONS ▾

Multicast and Broadcast Filtering: ☒ Block LAN to WLAN Multicast and Broadcast Data ⓘ

Excepted Devices ⓘ
ⓘ No MAC addresses have been configured.

+ ADD

+ ADD BATCH + ADD CLIENTS

VLAN: ☒ Use VLAN 11

Figure 18- Trusted Wireless Network

Assuming the networks setup in Unifi match those set up in PFSense, namely the VLAN tags, and their DHCP servers are configured, these wireless networks will be successful, contacting

PFSense for their DHCP reservations, and other routing-provided information. For testing purposes, a trusted wireless and a guest network were created. While on the topic of wireless networks, we should also discuss the static addressing, the access point collects an IP address for each VLAN it uses, and so a static reservation would be much preferable. While discussing static IP reservations, an additional form of security in this realm would be MAC filtering, which while it does have significant uses, in wireless security, it is nearly worthless. As you may see in a later experiment section, finding the MAC address of a *wireless* client is *very* easy, effectively nullifying the point of MAC filtering, that is not to say it does not have its uses; in wired networks it is *very* effective as it is much more difficult to intercept the MAC address of the device using a wired connection as opposed to a wireless one.

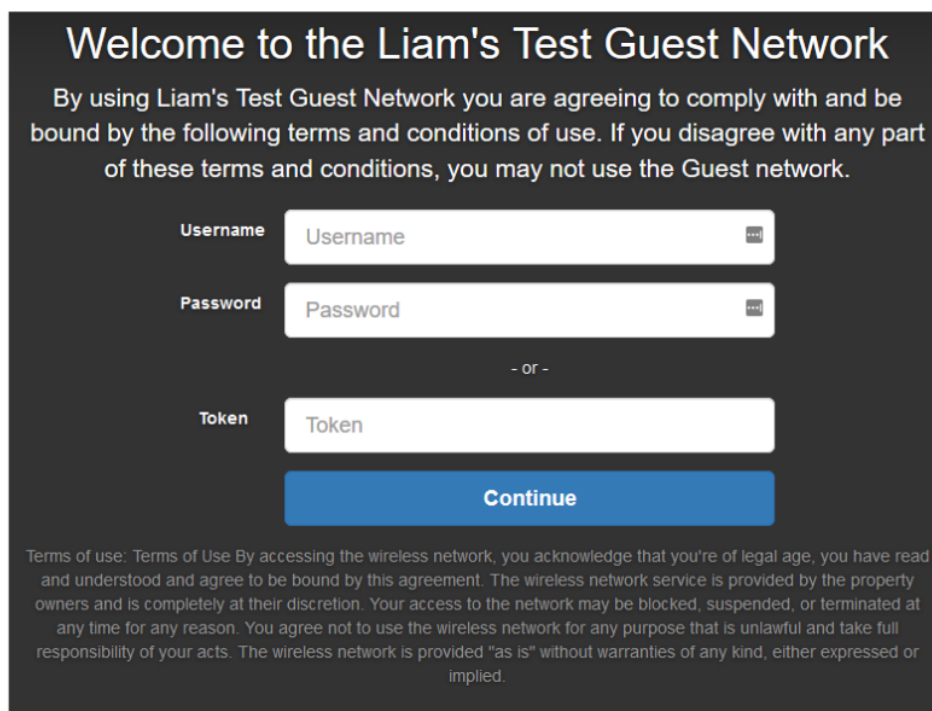
In this regard, on the Networking VLAN, where the network and network-service-providing devices reside, all devices are statically addressed, both IP and ARP as well as denying any client not listed on the DHCP client list, and the fact that they are all wired devices, makes them much more ‘secure’. In addition, should anything be disconnected, the admin is warned by the Unifi controller, assuming .

D. Guest Network

As we are discussing the wireless network, we might as set up the guest network. So, as mentioned before, the guest network does have WPA-2 password on its wireless access, but it is a bit weaker as you need to enter an additional password afterwards. If you refer back to figure 15, you will see an ‘Apply guest policies’ option, that has been enabled in this case, as has Layer 2 isolation, which was not pictured. While it would be good to use the Unifi guest portal, it *really* does not like the PFSense radius, and as such we will be using the PFSense Captive portal, just directing Unifi to use the captive portal once complete. To create a guest portal, go to ‘Services>Captive Portal’ and ‘Add’. As this is a *guest* network, this writer also created firewall rules specifically blocking access to any other network/IP on the network, essentially only allowing access to the WAN and the internet.

On the following captive portal configuration page, the settings here depend on what kind of guest portal you want, except for the interface, as we only want the Guest_VLAN to use it. For this test scenario, we will keep everything default in the first section except for the interface, per-user bandwidth restriction, of which has been set to 5000kb/s down and 1000kb/s up, and the use of a custom portal. This custom portal is from a GitHub project from a user named Kobaltz[53], simply because this writer has no experience with web

design, even at this level. While the default PFSense captive portal page is sufficient, this is simply as an example of loading a custom page. The resulting portal can be seen below.



The image shows a dark-themed captive portal interface. At the top, it says 'Welcome to the Liam's Test Guest Network'. Below this is a paragraph of terms and conditions. There are three input fields: 'Username' with a placeholder 'Username', 'Password' with a placeholder 'Password', and 'Token' with a placeholder 'Token'. Each field has a small icon on the right. Below the 'Token' field is a blue 'Continue' button. At the bottom, there is a small text block for 'Terms of use'.

Welcome to the Liam's Test Guest Network

By using Liam's Test Guest Network you are agreeing to comply with and be bound by the following terms and conditions of use. If you disagree with any part of these terms and conditions, you may not use the Guest network.

Username

Password

- or -

Token

Continue

Terms of use: Terms of Use By accessing the wireless network, you acknowledge that you're of legal age, you have read and understood and agree to be bound by this agreement. The wireless network service is provided by the property owners and is completely at their discretion. Your access to the network may be blocked, suspended, or terminated at any time for any reason. You agree not to use the wireless network for any purpose that is unlawful and take full responsibility of your acts. The wireless network is provided "as is" without warranties of any kind, either expressed or implied.

Figure 19-Guest Network Captive Interface

As you can see, there are two methods of accessing the guest network, a login, or a voucher. This is designed so that those with an account, such as employees can gain internet access on their personal devices, without risking harm to the rest of the network, whereas guests can collect a voucher code from, say, the front desk, giving them guest-internet access for a determined amount of time, or simply guest access should you not give the token field a backend, as it will accept a blank input as successful should there be no backend. At this stage, both of these fields do not do anything as there is no backend to support them, this is what we will move onto now.

On the next section, titled 'Authentication', set the authentication method as 'Use an Authentication backend', and the Authentication server we will use is Freeradius, using the local database as a secondary/backup. While we could just use a local database, we will need a radius server for a OpenVPN server to be detailed later.

Under the 'vouchers' tab, we also set up voucher authentication, essentially a time-allotted code that allows temporary internet access, similar to those used in hotels. Before the vouchers can be created, we must give parameters by which to do so, realistically the default settings are more than sufficient, and seeing as we are not going to be using that many, they will suffice. The one option you may want to change is ticket bits, as if left as default you may only generate 1023 tickets per roll, having said that, that many will be sufficient for most small businesses and as such will be kept as default. This writer has also added the rest of the ASCII symbols to the character set, as PFSense defaults on using 2-9 and uppercase and lowercase lettering. Once the settings are saved, we can create the actual vouchers, start by creating a new 'roll', giving it a number between 1-65535, a time allotment (this writer used 86400, equal to 24 hours), a number of vouchers to generate (count), and an administrative comment, and done. These vouchers are then generated and printed to an Excel spreadsheet, whereby they can be given to those needing temporary internet access. You may also create multiple rolls at once, with different time allotments as well, so you may give some people 24 hours, or others 7 days.

E. Radius Authentication

This next section we will create a radius server to use as user authentication for both the guest network and OpenVPN server we create at a later step, radius being the protocol that's main duties are centralised Authentication, Authorisation, and Accounting (AAA)[54]. While there are many different ways of creating a radius server, we will be using the Freeradius3 package in PFSense, as it does not come installed as default, make sure to install it first of all. As we are using Freeradius on the firewall, go to 'Services>Freeradius>Interfaces', from here either keep the * interface for listening on all interfaces or localhost/127.0.0.1 as we will use here. Now from the 'Client' tab, we can create a local client using the below settings;

General Configuration	
Client IP Address	127.0.0.1 Enter the IP address or network of the RADIUS client(s) in CIDR notation. This is the IP of the NAS (switch, access point, firewall, router, etc.).
Client IP Version	IPv4
Client Shortname	LocalFreeRadiusServer Enter a short name for the client. This is generally the hostname of the NAS.
Client Shared Secret	***** Enter the shared secret of the RADIUS client here. This is the shared secret (password) which the NAS (switch, accesspoint, etc.) needs to communicate with the RADIUS server. <i>FreeRADIUS is limited to 31 characters for the shared secret.</i> Warning: Single quotes in shared secret must be escaped with a backslash (\'). Backslash must be escaped by using two backslashes (\\).
Miscellaneous Configuration	
Client Protocol	UDP Enter the protocol the client uses. (Default: UDP)
Client Type	other Enter the NAS type of the client. This is used by checkrad.pl for simultaneous use checks. (Default: other)

Figure 20- Local Freeradius Server

The shared password will act as a form of security between the server and client, here they both are on the same device so it is not too important, but a strong password should be used none-the-less. Now, under ‘System>User Manager>Authentication Servers’, we can add the Freeradius Server as a proper authentication server, in this case we used the settings below;

Server Settings	
Descriptive name	FreeRadius
Type	RADIUS
RADIUS Server Settings	
Protocol	MS-CHAPv2
Hostname or IP address	127.0.0.1
Shared Secret	*****
Services offered	Authentication and Accounting
Authentication port	1812
Accounting port	1813
Authentication Timeout	5 This value controls how long, in seconds, that the RADIUS server may take to respond to an authentication request. If left blank, the default value is 5 seconds. NOTE: If using an interactive two-factor authentication system, increase this timeout to account for how long it will take the user to receive and enter a token.
RADIUS NAS IP Attribute	WAN - 192.168.0.10 Enter the IP to use for the "NAS-IP-Address" attribute during RADIUS Access-Requests. Please note that this choice won't change the interface used for contacting the RADIUS server.

Figure 21- Freeradius Authentication Server

The shared secret is the same as we used before, assuming you are to link the two. Now, back to the Freeradius ‘Users’ tab, and we can start creating credentials for users of the guest network, not to be confused with *actual* guests who should use the voucher system. Using ‘+Add’ to create a credential, first of all is username and password they will use, which is quite self-

explanatory, then password encryption, as this is all localhost and therefore cannot be intercepted as if it were traversing the network, *technically* speaking, cleartext will suffice, and should be used to authenticate that the user exists by using the 'Diagnostics>Authentication' tab. While it may seem beneficial to use MD5 instead, unfortunately if that is chosen, the login will not work.

We can then test it on the guest network using an actual device, and should it work, the user will be allowed access to the internet amongst other restriction.

F. Switch configuration

Now that the networks are created and both Unifi and PFSense are aware of them, we can apply the VLANs to their ports. Important distinction to make here is that Unifi does not allow for simply assigning ports, but works off of profiles, by default each network is given an automatic port profile, giving the same effect that if you would apply a VLAN to an access port. Trunks on the other hand, unless you want all VLANs, which is the default status, you must create a port profile for it. The port profiles are made in 'Settings>Profiles>Switch Ports' and by default there are All, Disabled and any networks you have created. As all the VLANs use the same interface for their gateway, we can simply use the 'All' profile for the gateway, but for the access point, it has been restricted to both guest and trusted wireless, as they are the only VLANs that rely on wireless for access. As for the network-service PC hosting the Unifi controller and the other PC deemed the 'admin PC', they have been restricted to the Networking VLAN, but still has access to the LAN network, using specific ports, this is because in the event that a device needs to be adopted into the Unifi environment, it first gains an IP address from the LAN DHCP, after which case it can be adopted and moved into the Networking VLAN. In regard to actually securing the switch itself, there are two ways of interacting with it, SSH and via the controller. The controller is secured using the admin's Unifi Account, which assuming you have a decent password, should be sufficient as not too many devices should have access to the controller anyhow. In regard to SSH, by default is ubnt for both username and password but after the device has been adopted by a controller, is changed in accordance with the 'site'-wide SSH login, changeable in the controller site settings, the 'site' being the section of the network designate-able by the Unifi environment. While we could have done this section at an earlier stage, locking oneself out of the network was a distinct possibility, and as such was left till last. Below is the switch diagram from the Unifi device. As you can see, most of the ports have been used or blocked, barring port 4 which was left open should this writer accidentally lock himself out of the network. This action is only condonable due to the test-nature of this network, in an actual environment this would be a *grave* error, assuming it is truly open, without any form of sticky or static addressing. Of course, all devices are using Networking VLAN for management.

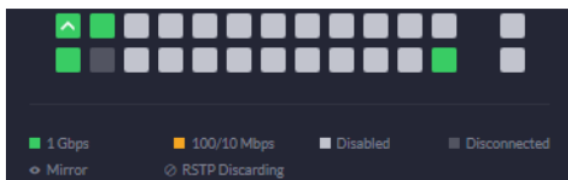


Figure 22- Unifi Switch Config

G. Network Maintenance

When it comes to updating PFSense and the packages it uses, it is quite easily done as all packages belong to the PFSense team's repository. This means, should an update become available, it will not be pushed directly to the repository before being checked beforehand. Updating PFSense and packages are as simple as selecting the 'Install Update' button under 'System > Package Manager' for packages and Update tab for upgrading PFSense itself. Having said this, occasional backups should be made when any changes are being made, using the 'Backup and Restore' tool under 'Diagnostics'.

Another method of securing the networks is via the DHCP, in PFSense, on the Networking and Trust_Wired networks, each client is assigned an IP and static ARP via DHCP, any clients not listed on the static DHCP reservations list is denied and will have to get an IP manually. Having said that, due to the setting of static ARP, only those listed on the DHCP reservations may communicate with the firewall, and therefore those not listed will not be routable. Reason being is that in a wired set up and management VLAN, there is not going to be constant DHCP activity as there is on a wireless network where clients are connecting and disconnecting and as such, we can implement features that require previous setup. It may also be used on wireless connections, but if many devices are connecting, it can quickly become very bothersome to administer.

As for Unifi, should anything go wrong, if set up, the admin will get an email with information on the event, assuming the internet connection or switch connecting the controller to the router has not failed. As for upgrading firmware or updating, the controller notifies the admin, but can be done at the admin's console. While this writer would suggest always updating as soon as possible, Ubiquiti does have a bad reputation with pushing updates that break certain features, so caution is advised.

5. Network Testing

To measure the security of the network, we will have to perform tests to give a better understanding of where we can improve, or if it needs improvement at all. Whilst security is not a numerical scale of measurement, attempting attacks against the network, allows the user to better understand the types of attacks they are going to face.

1. Wi-fi Attacking.

The first type of attack we are going to attempt is a wireless attack, against the wireless access points. One increasingly common means of wireless attacking is wardriving, the use of a small GPS-enabled, single-board computer that captures the location, handshake, and information of wi-fi networks as the user walks past, the collection of handshakes can then be cracked in another location. A good example of this would be the Pwnagotchi, a Linux project leveraging the capabilities of single board computers such as the Raspberry Pi 0 to more efficiently and discretely attack wi-fi hotspots. Another would be warshipping, again, leveraging the use of smaller single-board computers, this time with a 3g connection to enable 'remote' connections to networks the attacker is not physically present. This type of attack is become more popular mostly due to the rise of ecommerce and the increase in deliveries, allowing them to sneak under the radar of their target.

Now, the wireless attacks to be performed will consist of a wordlist attack and a hybrid attack, both forms of authentication attacks, just different means of cracking it. We are doing this type of attack first as they are the first forms of defence for entry to a network, and as people are constantly connecting to them, they also act as the easiest form of data interception. Both of these attacks require the initial interception of a handshake, for this purpose we will use Parrot OS, a pentesting Linux-based operating system that comes with a multitude of software, for this stage in particular we will be using the aircrack suite. Starting with airmmon-ng, we must first put our wireless interface into monitor mode to monitor the traffic, after which we can use airodump-ng to monitor all traffic coming from access points in the immediate area, as well as any clients connecting or connected to them, using the command ;

'Sudo airmmon-ng start <Name of Interface>'

Now we have an interface in monitor mode we can start monitoring using the command;

‘Sudo airodump-ng wlan1mon’

From here, a list of local access points and clients will appear, allowing for you to pick the target MAC address of both client and access point, those with higher data are likely more active, and therefore you are more likely to intercept a handshake. Below, you can see this writers’ output of said command.

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
9C:A3:A9:62:9C:11	-1	0	150	0	4	-1	WPA	<length: 0>
3A:E8:29:FE:BD:1F	-47	101	0	0	6	195	WPA2 CCMP	PSK <length: 0>
1A:E8:29:FE:BD:1F	-47	103	0	0	6	195	WPA2 CCMP	PSK L57Guest
18:E8:29:FE:BD:1F	-47	111	14	0	6	195	WPA2 CCMP	PSK L57Wifi_2G
2A:E8:29:FE:BD:1F	-47	108	0	0	6	195	WPA2 CCMP	PSK L57IoT
60:32:B1:06:4F:4E	-63	401	74	0	4	130	WPA2 CCMP	PSK VM342
90:02:18:4B:67:5C	-81	33	16	0	11	130	WPA2 CCMP	PSK SKYZMZA1
5A:D3:43:02:31:D9	-83	187	0	0	1	130	WPA2 CCMP	MGT Virgin Media
7E:61:66:7A:BC:16	-83	34	0	0	11	130	WPA2 CCMP	PSK DIRECT-ek-FireTV_2005
6A:D3:43:02:31:D9	-84	191	0	0	1	130	WPA2 CCMP	PSK VM-guest9432514
B0:95:75:0C:40:6E	-84	24	30	0	11	270	WPA2 CCMP	PSK TP-Link_406E
48:D3:43:02:31:D9	-83	188	0	0	1	130	WPA2 CCMP	PSK VM342
D2:05:C2:74:64:89	-94	78	0	0	1	130	WPA2 CCMP	PSK VM-guest6479683
C0:05:C2:74:64:89	-91	74	1	0	1	130	WPA2 CCMP	PSK VM6647968
7A:65:59:A7:E0:D3	-91	64	0	0	1	195	OPN	BTWi-fi
78:65:59:A7:DE:D2	-90	62	2	0	1	195	WPA2 CCMP	PSK BTHub6-NS2R
D0:58:FC:5D:5C:7E	-1	0	5	0	6	-1	WPA	<length: 0>
80:72:15:97:71:BA	-75	17	14	0	11	260	WPA2 CCMP	PSK SKYZMZA1
BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes	
(not associated)	00:FC:8B:E4:10:3A	-53	0 - 1	0	36		VM342	
(not associated)	30:10:B3:4E:EB:1F	-82	0 - 1	0	29		virginmedia3588268	
9C:A3:A9:62:9C:11	9C:A3:A9:6B:5E:2D	-86	0 - 0e	819	128			
9C:A3:A9:62:9C:11	9C:A3:A9:6D:81:3B	-93	0 - 1e	0	22			
18:E8:29:FE:BD:1F	8C:B8:4A:AB:E4:0F	-52	0 - 1	49	216		L57IoT	
60:32:B1:06:4F:4E	E0:94:67:97:78:D6	-73	1e- 2e	0	18			
60:32:B1:06:4F:4E	24:18:1D:16:5D:9E	-82	1e-24	0	5			
60:32:B1:06:4F:4E	88:A3:03:3C:7D:1B	-89	0e- 1	13	62		VM342,SOMBRA18	
D0:58:FC:5D:5C:7E	D0:7F:A0:F8:78:7F	-83	0 - 1e	0	6			

Figure 23- Airodump-ng log

Now, from this list we must choose a client and station to try and intercept the WPA handshake from, [un]fortunately this handshake is only done at the point of connection, not during. For the purpose of testing, this writer could simply disconnect and reconnect to the network, but as you can imagine, this is not something that is going to happen when attacking a real network. For this purpose, we can use a deauthentication attack, essentially sending packets to the device telling it to disconnect from the network, at which point it will automatically reconnect, allowing us to intercept the handshake. It is worth pointing out, this is where password cracking becomes legally probable, if you are to simply intercept the handshake, then there is no legal problem, but if you deauthentication someone, then technically speaking, as it is a type of Denial-of-Service (DOS) attack, it can lead to fines or prison time, even if using it against a

single target it is very difficult to spot. To start interception between target of client we use the command;

‘Sudo airodump -c 6 --bssid 18:E8:29:FE:BD:1F -w networktest wlan1mon’

This command basically intercepts traffic from the SSID specified, on channel 6, using wlan1mon and saves it to the networktest file. From this command, you should see a target, copying its MAC address, we can then use a deauth attack against it using the command;

‘Sudo aireplay-ng -0 2 -a 18:E8:29:FE:BD -c 8C:B8:4A:AB:E4:0F wlan1mon’

This specifies sending two deauth packets to the client in -c, which should then reconnect, allowing us to intercept the handshake. Below, we can see the result of the airodump terminal, signalling a captured handshake.

```
$ sudo aireplay-ng -0 2 -a 18:E8:29:FE:BD:1F -c 8C:B8:4A:AB:E4:0F wlan1mon
11:57:14 Waiting for beacon frame (BSSID: 18:E8:29:FE:BD:1F) on channel 6
11:57:14 Sending 64 directed DeAuth (code 7). STMAC: [8C:B8:4A:AB:E4:0F] [31/59 ACKs]
11:57:15 Sending 64 directed DeAuth (code 7). STMAC: [8C:B8:4A:AB:E4:0F] [ 0/65 ACKs]
```

Figure 24- Deauthentication attack

CH 6] [Elapsed: 2 mins] [2020-10-25 11:59] [WPA handshake: 18:E8:29:FE:BD:1F									
BSSID	PWR	RXQ	Beacons	#Data,	#/s	CH	MB	ENC CIPHER	AUTH ESSID
18:E8:29:FE:BD:1F	-48	100	1622	102	0	6	195	WPA2 CCMP	PSK L57wifi
BSSID	STATION		PWR	Rate	Lost	Frames	Notes	Probes	
18:E8:29:FE:BD:1F	8C:B8:4A:AB:E4:0F		-63	6e- 1	0	642	EAPOL		

Figure 25- Captured Handshake

So, now that we have a captured handshake in the form of a .cap file, but hashcat, the hashing tool we will use accepts a .hccapx file for simplicity's sake we will be using the converter tool at <https://hashcat.net/cap2hccapx/>, which is an official tool. Using this file, we can then use hashcat to 'crack' it, gaining the password if successful.

The first hashcat attack will be a basic wordlist, using a wordlist 29GB in size, comprising of 2649982129 passwords gathered from leaks, then essentially trying each and every one of them against the hashed hccapx file. The command to do so is:

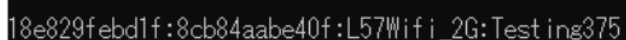
‘Hashcat -m 2500 -a 0 WPA2Test.hccapx weakpass_2’

'-m 2500' indicates it is a WPA2 hash, '-a 0' indicates a wordlist attack followed by the hashed file, and subsequent wordlist to be used. [Un]fortunately, this attempt was a failure, the password was not contained in the wordlist. and took roughly two hours to complete, at a rate of 315,000 hashes per second.

The next attack will use the same captured file, except this time we will be using a hybrid attack with hashcat, essentially it is a dictionary attack with amendments, in this instance specifically on the left-hand side of the word from the word list. The command we will use is;

'hashcat -m 2500 -a 6 WPA2TEST.hccapx probable-v2-top12000.txt ?d?d?d'

This takes the wordlist, this time a smaller wordlist, and amending the numbers 000-999 onto the end, as indicated by the '?d', of which basically is any number from 0-9. While we could use the previous wordlist, it, plus the amendments, would be too massive, taking roughly 83 days to fully check, therefore we are using a smaller wordlist here.

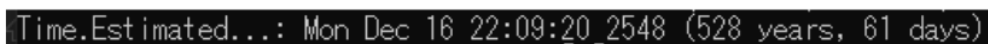


```
18e829febd1f:8cb84aabe40f:L57Wifi_2G:Testing375
```

Figure 26- Cracked Password

As you can see here, the cracked password was 'Testing375', which while not a strong password, due to the uncommon number amended on the right, meant that a wordlist attack was not going to work without additional variables. Also, this attempt took only two minutes with a wordlist of 9000 words, in addition to the amended numbers.

Simply for means of comparison, this writer also attempted a brute-force attack, assuming we have no information and must try every conceivable combination, and while this writer would like to show that it worked, there was one problem that is common with brute force attacks; time. Below is the estimated time of trying to crack a 12-character password.



```
Time.Estimated...: Mon Dec 16 22:09:20 2548 (528 years, 61 days)
```

Figure 27- Problem with brute force attacks

So, can we improve the wireless security? Of course, obviously the use of a stronger password is the most common security prevention method, on the other hand there is also the use of WPA2-Enterprise, essentially the use of a radius server to authenticate rather than a singular password. Now, for a small business WPA2-Personal, of which we tested here may be sufficient, assuming the use of a secure password, if you would rather not have to set up radius

user accounts for every person but is an option none the less. Lastly, a newer option would be WIFI 6/WPA3, which some devices are starting to support, and does away with the interceptable 4-way handshake, replacing it with a relatively more secure 'dragonfly' handshake, as well as other security improvements, but as it is in an alpha stage, where they are still finding vulnerabilities and making it a comparatively risky choice at this time.

Interesting point to make, while this access point attacked uses both 2.4Ghz and 5Ghz, the adapter used to attack could only attack the 2.4Ghz band. Therefore, if possible, use of only the 5Ghz band will filter out some attackers, admittedly only those who are doing so as a hobby and not seriously, but some none-the-less. Having said this, many networks still make use of devices and clients that are unable to use 5Ghz networks, many IoT devices especially, so while it is more secure, it is not too viable.

On another note, this type of attack is not the be all to end all, there are other types of attacks against wireless networks such as Man In the Middle attacks, phishing, WEP, evil twin, rogue access points, etc . Unfortunately, these require some sort of human interaction, of which these attacks take advantage of and due to current home restrictions, as well as the moral ambiguity of tricking someone to prove an attack, it was decided to leave these be. The 'upgrading' implementation can be found in the appendix, under; 'Wi-Fi EAP-TLS Authentication'.

2. DNS Filtering

This section of testing is not an attack as the password attack was, but rather a verification of DNS filtering in different scenarios, as well as means to avoid it altogether, which while *technically* it could be called an attack, a *loophole* would be a more apt description. We have disabled DNS-over-HTTPS, although due to the Firefox DOH blocking on the DNS resolver, it is still susceptible to the same blocking that normal DNS queries are. As such when trying to access ‘https://www.nordvpn.com’, the website is blocked as we have blocked VPN provider websites on the DNSBL, you can see the error page below;

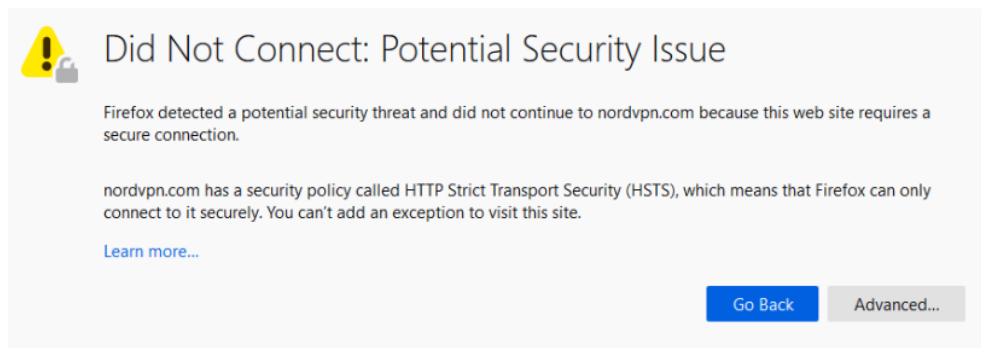


Figure 28- DNS Blocking Error

As you can see, while the page has technically been blocked, while it is because of PFBlockerNG, it does not show the ‘correct’ error. This is due to the fact that the website uses HTTP Strict Transport Security (HSTS), an enhancement of the standard HTTPS protocol, reinforcing some of the weaknesses in the standard version, meaning that the browser realises the connection has been intercepted. This is because the DNS Resolver is trying to redirect to the error page of which is HTTP, which is not the requested page, and that the DNSBL is not providing the proper certificate for the website and therefore is interpreting it as a Man In The Middle attack, which it technically is, and then is blocking the connection.

On a website that does not have HSTS, the DNS resolver can redirect to the proper error page;

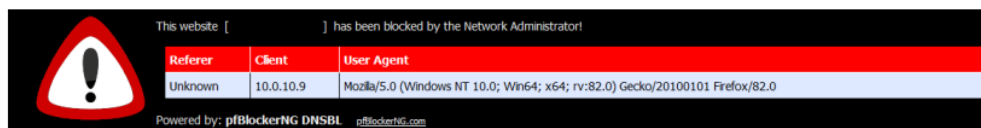


Figure 29- DNSBL Blocking Page

As you can see, this is more informative, detailing who has been blocked and details on said user, as well as showing a proper error page rather than a broken one as seen above. This is the blocked webpage, when DNSBL blocks ads or such they are replaced with a 1x1 pixel to minimise load on the systems involved.

Unfortunately, when using a client-based VPN, we can simply blindside the DNS resolver, which makes sense seeing as VPNs are often used in countries where restrictive filters are in place. Ideally, you would restrict admin control on the user's devices, assuming said devices are company property, and as such a VPN programme would not be installed in the first place. Items such as this which rely a great deal on application control are one of PFSense's weaknesses and is why there is usually a separate system in place to limit the use of unauthorised software. While not perfect, a means of partially tracking client website usage is via an IDS using OpenAppID, the implementation of which can be found in the appendix.

3. Evaluation

Now that we have implemented security methods and tools into the network, and tested a select few of them, we can start to analyse whether we have achieved our objective of '**Enhancing of network security within a small enterprise environment**'. While we can show that the security implementations were successful, to what extent? Security is not a linear scale and as such is much more difficult to quantify, technically speaking this project would have completed its main objective by simply increasing the complexity of the wireless password, as security had been improved. As you can imagine, that is not sufficient. Therefore, upon evaluation, has the network security been improved? In this writer's opinion, yes, it has been improved and would be successful in areas where the standard comparison would fail.

The answer to this is yes, while we have improved the security of the network it can definitely be improved again, as the previous experiments have shown us. For the password-related attacks we could make the password more complex or use WPA2-Enterprise as opposed to WPA2-Personal, as it is much more difficult to 'crack', relying instead on radius authentication in a similar vein to the guest network's login feature. Using the newer WPA3 could also improve security, as it uses a different handshake model that is lesser susceptible to interception but comes with the downside that not so many devices support it, and it is still *technically* in its early stages as it has yet to go through any additional renditions as they find more vulnerabilities, such as the WPA3 vulnerabilities deemed 'dragonblood'[55] and may be patched as more WPA3 specifications become available. Additionally, just because these options are *more* secure does not mean they are completely, as WPA2-Enterprise is still susceptible to interception attacks such as evil twin attack, therefore, we can implement WPA2 EAP-TLS authentication, which uses certificates as its means of authentication, of which are much more difficult to intercept, due to the presence of certificates as a means of authentication. This additional implementation can be found in the appendix.

Then there is the DNS filtering, could that be improved? Yes, as mentioned before the biggest weakness of the DNS resolver is that it can be bypassed via DNS-over-HTTPS or VPN usage. While we can *try* to block all VPNs, it will be a hard task due to the nature of a VPN being used to access what they should not. Unfortunately, the application filtering that would prevent many VPNs is one of PFSense's weak points, as mentioned before, and while there are packages that could attempt to track their usage, many modern VPNs use HTTPS over port 443, and as many IDS's track software via their port, it would prove futile.

6. Conclusion

In essence, through the implementations and subsequent experimentation, we have shown that we have and can improve the security of the network with the means available to us within the project boundaries, to what degree is a matter of perspective, but an improvement none-the-less. As a result, this documentation can be used by small-to-micro businesses looking to increase their network security beyond the less-than-adequate configuration that many smaller businesses find themselves using nowadays. Whether or not this guide is actually used by the small business owners is a matter of both opinion and reach.

When it comes to the objectives, some were met more than others; an example being research into what is an 'average' small business network was, due to the current restrictions and lockdowns, getting such information was more difficult than first anticipated, and as such we had to rely on 2nd hand information to ascertain it. Apart from that small trouble, we did successfully research the landscape that smaller businesses find themselves in, the security threats and related defences. In regard to the security tool research, while it has been done, the only written aspect was of those chosen as should all tools be documented and justified against each other, they would take up *much* too much of this project. Then there was the creation of a test network, implementing security features researched beforehand, experimentation against said network and subsequent improvement, suffice to say this writer believes these objectives to be completed to a satisfactory degree.

While we can say that we have achieved the aim of this project by improving the network security environment, but it is worth noting that this is only a small section towards the larger problems that are currently looming over businesses across the UK as mentioned earlier in the report.

1. Recommendations

As this project is quite limited in scope for reasons of current happenings and target area, there are a number of various options for future study. An interesting option would be cloud-based firewall configuration that is becoming increasingly popular, while it may be difficult to test due to the legal aspects of attacking a cloud-hosted service, it is an interesting option none-the-less. Then of course there is the option of doing the same type of implementations on differing systems, so where we used PFSense and Ubiquiti, others may use MicroTik and/or Cisco, comparing the two as to ascertain which is the better product. Unfortunately, such an approach was outside of the financial scope of this project but could provide interesting results.

Another option would be the inclusion of hosted web services and their subsequent security measures, of which was put aside in this project due to the fact that the test network was not WAN facing/ a perimeter firewall and allowing external connections would put the external LAN devices at risk. Therefore, implementing such features could be considered an additional course of action, additionally, comparing the positives and negatives of said hosting with those hosted on cloud services would also prove beneficial.

Of course there is the option of simply continuing the project further, but this would likely require additional systems in place to facilitate the additional security features, as well as a total revamp in regard to both the firewall, router, and its services. Whether or not this more expensive and expansive option would be viable for many smaller businesses is another matter entirely. However, as this is a recommendation for future work, there are allowances for editing the scope, so while this option may not suit as many smaller businesses, it will still be viable for a minority of them.

7. Reflection

This project has largely been constricted both in scope, financially and by current happenings as of the time of writing. While scope restrictions were of *design*, others were not. In hindsight, while PFSense *can* do a lot of what a firewall needs to do, the ‘learning’ curve is quite steep in comparison to other options. While this writer preferred PFSense, using a more entry/user-friendly option such as Untangle would arguably been a better option, though it does have its detriments. Untangles’ higher system requirements may have been an issue in the latter stages, as even when using PFSense, the less resource intensive of the two, RAM and Swap space usage would reach 80-100% quite quickly, so it may have been an issue. Another aspect is spending, this writer made some purchases that he regretted, such as the Unifi USG router, which was ultimately useless. Therefore, more logical spending would have proved beneficial in the long run as it would have allowed additional investment elsewhere. Additionally, the inclusion of more human-based weaknesses to the system would allow for exploration in their defence, but due to current conditions they would be very difficult to test against, as we would need actual unbiased participants which would be considerably more difficult to acquire in the conditions as of the time of writing.

A point of concern was the implementation of Snort, while useful, for a time it would simply not work, flooding itself with broken http alerts to the point where it would overload the snort interface, and shut itself down. After a number of days of trying to fix it, it turns out that it was not PFSense or Snort that was the problem, but the NIC that the computer was using, as it did not properly support the ‘Hardware Checksum Offloading’ that PFSense uses.

8. Bibliography

- [1] National Cyber Security Centre, "Cyber Security Breaches Survey 2019: Micro/Small Business findings visualisation," 2019.
- [2] S. Rebner and Cyleron, "The State Of Cybersecurity Pertaining To Small Business," *Forbes*, 2019. [Online]. Available: <https://www.forbes.com/sites/theyec/2019/09/18/the-state-of-cybersecurity-pertaining-to-small-business/>.
- [3] D. Mort, "Business Statistics," *UK Stat. A Guid. Bus. users*, no. 06152, pp. 93–136, 2019.
- [4] Beaming, "UK Cyber Threat Report Q2 2020," *Beaming Cyber Reports*, 2019. [Online]. Available: <https://www.beaming.co.uk/cyber-reports/cyber-threat-report-q2-2020/>.
- [5] Beaming, "Cyber report 2019: Volume of attacks doubles," *Beaming Cyber Reports*, 2019. [Online]. Available: <https://www.beaming.co.uk/cyber-reports/cyber-report-2019-volume-of-attacks-doubles/>. [Accessed: 13-Aug-2020].
- [6] GCHQ, "The cyber threat," *GCHQ.gov*, 2019. [Online]. Available: <https://www.gchq.gov.uk/information/cyber-threat>. [Accessed: 21-Aug-2020].
- [7] E. Johns, "Cyber Security Breaches Survey 2020," *Comput. Fraud Secur.*, vol. 2020, no. 4, p. 4, 2020.
- [8] GOV.UK, "Cyber Security Breaches Survey 2019 - GOV.UK," 2019.
- [9] R. Klahr *et al.*, "Cyber Security Breaches Survey 2017, Micro/Small Business Findings," no. October 2016, 2017.
- [10] R. Klahr, S. Amili, J. N. Shah, M. Button, and V. Wang, "Cyber Security Breaches Survey 2016," *Cyber Secur. Breaches Surv. 2016*, no. May, p. 56, 2016.
- [11] HM Government, "2015 Information Security Breaches Report," p. 49, 2015.
- [12] PWC and Department for Business Innovation and Skills, "Information Security Breaches Survey 2014," 2014.
- [13] pwc, "2013 INFORMATION SECURITY BREACHES SURVEY," pp. 1–19, 2013.
- [14] DETICA and Cabinet Office, "THE COST OF CYBER CRIME. A DETICA REPORT IN PARTNERSHIP WITH THE OFFICE OF CYBER SECURITY AND INFORMATION ASSURANCE IN THE CABINET OFFICE.," 2011.
- [15] MalwareBytes Labs, "2020 State of Malware Report," *Malwarebytes*, no. February, pp. 1–57, 2020.
- [16] SecureTeam, "The Small Business Guide to Cyber Attacks | Secure Team," *Secureteam.co.uk*, Oct-2019. [Online]. Available: <https://secureteam.co.uk/articles/the-costs-of-cyber-attacks-on-uk-small-businesses/>. [Accessed: 13-Aug-2020].
- [17] "Hiscox Cyber Readiness Report 2019," *Netw. Secur.*, vol. 2019, no. 5, p. 4, 2019.

- [18] Spectrum Internet, "Ransomware statistics that will shock your business." [Online]. Available: <https://spectruminternet.com/news-views/10-shocking-ransomware-stats-for-businesses/>. [Accessed: 19-Aug-2020].
- [19] Sophos, "The state of Ransomware," 2020.
- [20] BVA-BDRC, "SME Finance Monitor Report Q4 2019," no. March, 2020.
- [21] BitSight and J. Olcott, "How Much Does a Data Breach Cost in 2019?," *Bitsight Blog*, 2019. [Online]. Available: <https://www.bitsight.com/blog/calculating-the-cost-of-a-data-breach>.
- [22] Dell Small Business Advisor, "5 steps to scaling up your small business." Dell, 2018.
- [23] IAPP, "IAPP-EY Annual Governance Report 2019," 2019.
- [24] GDPR.eu, "GDPR Small Business Survey," 2019.
- [25] Staatscourant, "Beleidsregels van de Autoriteit Persoonsgegevens van 19 februari 2019 met betrekking tot het bepalen van de hoogte van bestuurlijke," 2019.
- [26] TrendMicro, "Developing Story: COVID-19 Used in Malicious Campaigns - SecurityNews - Trend Micro FR," *TrendMicro Security*, 2020. [Online]. Available: <https://www.trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains>. [Accessed: 26-Aug-2020].
- [27] Interpol, "CYBERCRIME : COVID-19 IMPACT," no. August, 2020.
- [28] National Cyber Security Centre, "Alert: APTs exploiting multiple vulnerabilities in several VPN products used worldwide," 2019.
- [29] Sophos, "The State of Cloud Security 2020.," 2020.
- [30] Office of National Statistics, "Coronavirus and the economic impacts on the UK - Office for National Statistics," 2020.
- [31] "London, Scottish and North East SMEs worst hit by coronavirus." [Online]. Available: <https://www.simplybusiness.co.uk/about-us/press-releases/sme-worst-hit/>. [Accessed: 08-Sep-2020].
- [32] Sam Bromley, "17% of businesses wouldn't survive another Covid-19 lockdown," *SimplyBusiness*, 2020. [Online]. Available: <https://www.simplybusiness.co.uk/knowledge/articles/2020/09/one-fifth-small-businesses-wont-survive-second-coronavirus-lockdown/>. [Accessed: 08-Sep-2020].
- [33] "Changes to the Coronavirus Job Retention Scheme - GOV.UK," *GOV.UK*, 2020. [Online]. Available: <https://www.gov.uk/government/publications/changes-to-the-coronavirus-job-retention-scheme/changes-to-the-coronavirus-job-retention-scheme>. [Accessed: 24-Sep-2020].
- [34] "Furlough: Rishi Sunak reveals replacement support scheme - BBC News." [Online].

Available: <https://www.bbc.co.uk/news/uk-wales-54279110>. [Accessed: 24-Sep-2020].

- [35] K. Bindley, "Remote Work Is Reshaping San Francisco, as Tech Workers Flee and Rents Fall - WSJ," *WSJ*, 2020. [Online]. Available: <https://www.wsj.com/articles/remote-work-is-reshaping-san-francisco-as-tech-workers-flee-and-rents-fall-11597413602>. [Accessed: 27-Sep-2020].
- [36] S. Ashman, "City Limits: The Remote Working Revolution And What It Means For Enticing Talent," *Forbes*, 2020. [Online]. Available: <https://www.forbes.com/sites/sairahashman/2020/09/22/city-limits-the-remote-working-revolution-and-what-it-means-for-enticing-talent/#1ad66d373231>. [Accessed: 28-Sep-2020].
- [37] N. Ammachchi, "COVID-19 Gives Rise to Third Wave of IT Outsourcing: Goldman Sachs," *Nearshores America*, 2020. [Online]. Available: <https://nearshoreamericas.com/covid-19-gives-rise-to-third-wave-of-it-outsourcing-goldman-sachs/>. [Accessed: 05-Oct-2020].
- [38] E. Jon, M. G. E., and S. Nigel, "Global sourcing trends in 2008," *Strateg. Outsourcing An Int. J.*, vol. 1, no. 2, pp. 173–180, Jan. 2008.
- [39] Bitdefender, "Bitdefender: Mid-Year Threat Landscape Report 2020," *Comput. Fraud Secur.*, vol. 2020, no. 9, p. 4, 2020.
- [40] ACS, "Cybersecurity Threats Challenges Opportunities," 2016.
- [41] W. Smart, "Lessons learned review of the WannaCry Ransomware Cyber Attack," *Lessons Learn. Rev. WannaCry Ransomware Cyber Attack*, no. February, pp. 1–42, 2018.
- [42] Bitdefender, "Bitdefender GravityZone Administrator's Guide," 2019.
- [43] R. Gafni and T. Pavel, "The invisible hole of information on SMB's cybersecurity," *Online J. Appl. Knowl. Manag.*, vol. 7, no. 1, pp. 14–26, 2019.
- [44] S. Mukherjee, "Overview of the Importance of Corporate Security in Business," *SSRN Electron. J.*, 2019.
- [45] S. Mansfield-Devine, "Securing small and medium-size businesses," *Netw. Secur.*, vol. 2016, no. 7, pp. 14–20, 2016.
- [46] Netgate, Electric Sheep Fencing LLC, and Rubicon Communications LLC, *The pfSense Documentation*. Netgate, 2020.
- [47] Department for Business Energy and Industrial Strategy, "Longitudinal Small Business Survey Year 2 (2016)," 2016.
- [48] 15writers.com, "Understanding the Research Onion," *15writers.com*. [Online]. Available: <https://15writers.com/research-onion/>.
- [49] J. Dudovskiy, "Positivism - Research Methodology," *Business Research Methodology*.

[Online]. Available: <https://research-methodology.net/research-philosophy/positivism/>. [Accessed: 27-Oct-2020].

- [50] UK Dissertation Writers, “Saunders Research Onion – A Step-By-Step Guide To Structuring Research Methodology Chapter For PhD And Master-Level Researchers,” *UKDissertationWriters.com*, 2019. [Online]. Available: <https://www.ukdissertationwriters.com/saunders-research-onion-a-step-by-step-guide-to-structuring-research-methodology-chapter-for-phd-and-master-level-researchers/>.
- [51] NordVPN, “Download OpenVPN configuration files | NordVPN,” *NordVPN*, 2020. [Online]. Available: <https://nordvpn.com/ovpn/>. [Accessed: 22-Oct-2020].
- [52] Firebog, “The Big Blocklist Collection: Text-only lists,” *The Firebog*. [Online]. Available: <https://v.firebog.net/hosts/lists.php>.
- [53] Kobaltz, “pfSense Captive Portal,” *Github*, 2015. [Online]. Available: https://github.com/kobaltz/pfsense_captive_portal.
- [54] RADIUS SARL, “The Freeradius Technical Guide,” 2014.
- [55] M. Vanhoef and E. Ronen, “Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd,” *Proc. - IEEE Symp. Secur. Priv.*, vol. 2020-May, pp. 517–533, 2020.

9. Appendix

1. Security Tools Evaluation

In regard to the tools to be used, mainly focusing on PFSense and Parrot OS, there were many different options to be used, but these were chosen despite considering alternatives, this section will act as justification of these choices.

When it comes to routers, there are *many* choice, too many in fact. The main reasons behind choosing PFSense mainly focused on four factors; cost, resources, documentation, and expandability. The cost of PFSense is between £0-50 a year, depending on whether you need support from Netgear, in addition to the initial hardware investment which can vary greatly. This low cost, largely due to its open-source nature, has allowed it to be used by businesses globally as it can often outperform the 'premium'/costly alternatives, the Unifi routers coming to mind. While PFSense may not be the easiest tool to use, in this writer's opinion, it *looks* difficult, but after using it for a day or two, it becomes significantly easier to use and navigate. The second factor is the resourcefulness of PFSense, even when compared to other router/firewall alternatives, it uses considerably lower resource requirements, and can be run on any PC with a NIC, but two is preferable. As mentioned earlier in the documentation, PFSense, due to its community-driven, open-source nature and the fact that it has been around since 2004 means that there is no *end* to the documentation. Some of it may be outdated, but you would be hard pressed to not find an updated version. This means that there is hardly an undocumented problem someone else has not experienced and hopefully fixed, making troubleshooting much easier. PFSense, like most software packages, is not an all-in-one package, and the development team understands that there are some features it does not have, this is why there is an official repository for software packages that have been built for PFSense, assuming they are given approval by the development team. This means that although PFSense may have its shortcomings, odds are there is a software package that can make up for their shortcomings.

2. OpenVPN Server Configuration

As mentioned before in this document, the need for remote working/access is greater now more than ever for most businesses. In this section this writer will show how to use OpenVPN to set up remote access to a network using OpenVPN in PFSense. Depending on the number of users, it may be best to do so on a separate server, as to remove strain from the PFSense machine as itself is already acting as a firewall and router for the whole network, but as we do not have a separate machine, this will suffice.

To start, we will need a domain and DNS service, so for this test this writer will be using Cloudflare. Technically speaking, this domain is not *needed*, but makes the task much simpler via dynamic DNS. Technically speaking, you could just do so with an IP address, but unless said address is static, it will change and break configurations. By using Dynamic DNS, we can avoid said situations while still properly mapping a domain to our IP address. Under 'Services>Dynamic DNS' you can add a DDNS client, the options you must input vary greatly depending on your service type/provider. For Cloudflare it is simply hostname to register on domain and Cloudflare login information and API key, once 'Save & Force Update' been chosen, the DDNS will register the hostname to your domain via your service and direct it back at public IP address. If successful, the IP should be coloured green.

Another step we must do before creating the actual server is setting up a Certificate Authority(CA) for the OpenVPN server and its users. For this purpose, we will create a private/self-signed CA in PFSense specifically for this OpenVPN server. Under 'Cert. Manager>CAs' add a new CA, filling out the steps, by default this CA will last for 10 years, which should be long enough. In regard to the 'Key Length', this may be increased for a more secure form of encryption at the cost of increased CPU process time, but as we are running this on less-than-great hardware, we will keep it as is, as it is a good balance between security and CPU process time. Once it has been saved, PFSense will then generate certificate data and a private key using said information amongst others. Now, we can generate a server and user certificate, in the 'Certificate' tab, create a new one, using the previously made CA as the authority for the server and for 'Certificate type' choose server. Ideally, do not use SHA1 as the digest algorithm, PFSense documentation recommends SHA256 at a minimum, or at least as high as your client device can support, some *older* devices will not work with newer hashes. We will be using SHA512, as we will only have up to 2 users using newer devices. The common name does not have to be the domain name used in the DDNS, as it is an internal

name, it can be anything, for example it could just be 'OpenVPNServer'. To create the user in PFSense, go to 'System>User Management' and add a new user, creating a username and password for them to use. Select 'Generate a user certificate', and make sure you use the previously created CA, giving it a descriptive name in the process. While here you may also set for the account to expire after a certain amount of time or group membership, if no group membership is given, they cannot access the PFSense interface, which this writer does not want to do anyway.



Figure 30-Example User

Above is an example user for this writer given membership to the remote group, of which has no access to the PFSense interface. Along with this account comes the certificate generated, as seen below, this certificate is what the client will use to access the server.

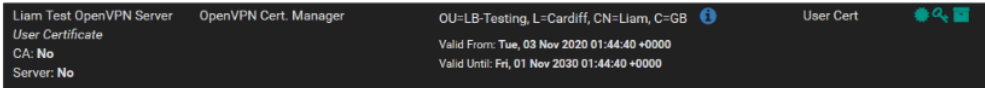


Figure 31- Account Created Certificate

Now, for the creation of the Server, go to 'VPN>OpenVPN>Wizards', this will start the server creation wizard. While we could do so manually, this is a much easier option. For the options we will use 'Local user access', while we could use Radius, seeing as this is all done in one machine, the PFSense box, local user access is simply more convenient. For the CA and server cert., use those created earlier. For the configuration steps, those used in the test scenario can be seen below.

General OpenVPN Server Information	
Interface	WAN
Protocol	UDP on IPv4 only (Would recommend not using default, but we are proxying the connection as well as port forwarding)
Local Port	1194
Description	<Simply for admin purposes>

Cryptographic Settings	
TLS Authentication	Tick
Generate TLS Key	Tick
Diffie-Hellman Parameter Length	2048 bit

Encryption Algorithm	AES-256-GCM (256 bit key, 128-bit block)
Auth Digest Algorithm	SHA512(512-bit)
Hardware Crypto	None (Hardware used does not support, if Hardware does support this, enable it)
Tunnel Settings	
Tunnel Network	192.168.147.0/24 (Out of the way of most IP schemes as to not conflict) (Completely outside of regular scheme to reinforce that they are external VPN connections)
Redirect Gateway	Tick (If you want all client info to go through VPN)
Local Network	10.0.0.0/24 (Only network that has resources for VPN members to access, will be further restricted by firewall rules)
Concurrent connections	<Max number of connections> (Left Blank during testing)
Compression	Omit Preference (Leaving compression decision to OpenVPN)
Inter-client communication	Tick (allows OpenVPN client to communicate with each other)
Client Settings	
Dynamic IP	Tick
Topology	Subnet- One IP per client in common subnet
DNS Default Domain	<Using Domain from DDNS here>
DNS Servers	192.168.147.1 (PFSense DNS Resolver, may include additional backup DNS Servers)

The last steps are simply whether you want OpenVPN to automatically create a firewall rule on the WAN interface or whichever interface you assigned the server to, as well as an OpenVPN rule, of which this writer allowed it to do both. Once the wizard is complete, the server will automatically be started, if it is down, something likely went wrong in configuration and troubleshooting and/or a restart will be required, but seeing as this used a 'wizard', the chances of such are minimal.

In regard to the clients connecting, there are two options, manually and via importing. This is where the OpenVPN-client-export package comes into play, it allows for you to 'export' a file for clients so that they can import it, minimising the chances of misconfiguration. Of course this package will have to be installed in the PFSense package manager. Once installed, go to 'VPN>OpenVPN>Client Export', then select the server, in this case we only have the one. The rest of the options are optional barring the 'hostname resolution' and 'verify server CN', of which can be set to the hostname and domain combination created at the DDNS stage, and

Automatic, respectively. These files can be saved as default for other client export files or kept as is, only being applied for the singular client you will export at the next step. Under the OpenVPN Clients list will be a list of clients associated with the certificate authority created earlier, as well as a number of different options for exporting configurations to different operating systems/devices. As you can see below, there is quite a selection, depending on OS.

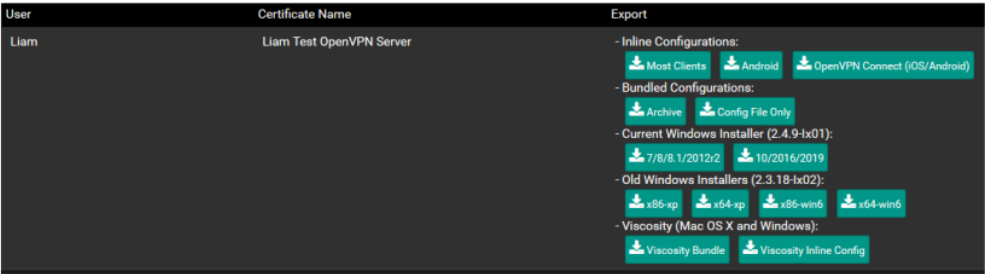


Figure 32- Export OpenVPN Client

As an example for testing means, this exported file will be loaded on this writer's phone, seeing as it is the only device able to connect to an external network, using 3g in this scenario. Using the OpenVPN android application, we can import the file, creating a VPN entry as can be seen below. Upon selecting this entry, the user prompted for the username and password.

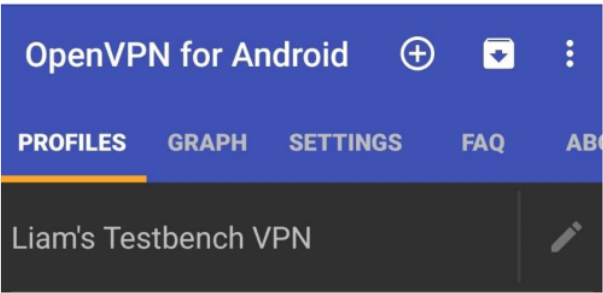


Figure 33- Imported VPN Entry

Using the user we created in the PFSense local database earlier, the VPN will connect, at which point we are given a log.

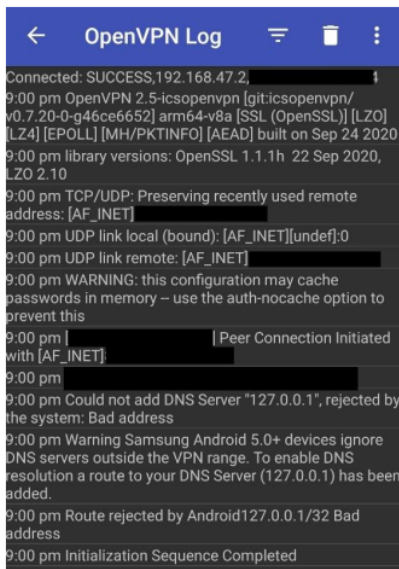


Figure 34- OpenVPN Connection Success

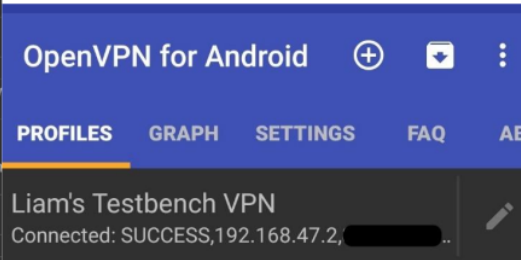


Figure 35- OpenVPN Connection Log

As you can see, the connection was successful, the only error was as a result of this writer's test on what would happen if given a localhost DNS server, not so much a proper test, but as a result of curiosity. The blacked-out information is the URL and IP of this writer's network, which he would rather not disclose for security's sake. The main downside to this VPN connection is speed and as a result, internet connectivity. This is due to the fact that this testbench is running on a residential ISP, using an asymmetrical connection, in other words as this uses both upload and download, the upload being the limiting factor, it can barely reach 1mb download speed. Having said this, in this use case it would be for a more secure means of accessing the network-connected services rather than a means of proxying an internet connection or opening them to the outside world via a reverse proxy.

3. Wi-Fi EAP-TLS Authentication

As mentioned in the experimentation phase, a means of defending against cracking attacks is via WPA2-enterprise wi-fi as opposed to the more common WPA2-Personal. This means rather than using a singular password, we instead use a username and password combination, in this case using FreeRadius, in a similar way to how the guest network does except this is from the Wi-fi access point rather than the PFSense-hosted captive portal. While we could use the same server as we did previously, for security sake we will create a new FreeRadius authentication server for authenticating this wireless network. As the initial set up has been covered before, it will be ‘glossed over’ at this stage.

The first step is creating an interface for the access point to contact the radius server, both authentication and accounting, and as this access point uses the management VLAN, we will be creating the FreeRadius interface for 10.0.5.1, the management VLAN, ports 1812 and 1813 for authentication and accounting, respectively. Then we will create a client entry for the access point, as we only have the one, the one entry will suffice, on larger networks, more client devices means more entries. The settings used can be seen below.

The screenshot displays the configuration interface for a Unifi AP Client. It is divided into two main sections: 'General Configuration' and 'Miscellaneous Configuration'.

General Configuration:

- Client IP Address:** 10.0.5.4. Description: Enter the IP address or network of the RADIUS client(s) in CIDR notation. This is the IP of the NAS (switch, access point, firewall, router, etc.).
- Client IP Version:** IPv4.
- Client Shortname:** UnifiAP. Description: Enter a short name for the client. This is generally the hostname of the NAS.
- Client Shared Secret:** A masked field (dots). Description: Enter the shared secret of the RADIUS client here. This is the shared secret (password) which the NAS (switch, accesspoint, etc.) needs to communicate with the RADIUS server. FreeRADIUS is limited to 31 characters for the shared secret. Warning: Single quotes in shared secret must be escaped with a backslash (\'). Backslash must be escaped by using two backslashes (\\).

Miscellaneous Configuration:

- Client Protocol:** UDP. Description: Enter the protocol the client uses. (Default: UDP)
- Client Type:** other. Description: Enter the NAS type of the client. This is used by checkrad.pl for simultaneous use checks. (Default: other)
- Require Message Authenticator:** No. Description: RFC5080 requires Message-Authenticator in Access-Request. But older NAS (switches or accesspoints) do not include that. (Default: no)

Figure 36-Unifi AP Client

Now, under ‘System>User Management>Authentication Servers’, we will create an interface on the Networking _VLAN’s gateway, so that the access point[s] can access it. Below is the

settings used, using MS-Chapv2 as it is the strongest protocol for Freeradius, as well as the shared password we created on the interface.

Server Settings

Descriptive name

FreeRadius Trusted Wireless

Type

RADIUS

RADIUS Server Settings

Protocol

MS-CHAPv2

Hostname or IP address

10.0.5.1

Shared Secret

.....

Services offered

Authentication and Accounting

Authentication port

1812

Accounting port

1813

Authentication Timeout

5

This value controls how long, in seconds, that the RADIUS server may take to respond to an authentication request. NOTE: If using an interactive two-factor authentication system, increase this timeout to accommodate the user's response time and enter a token.

RADIUS NAS IP Attribute

NETWORKINGVLAN - 10.0.5.1

Enter the IP to use for the "NAS-IP-Address" attribute during RADIUS Access-Requests. Please note that this choice won't change the interface used for contacting the RADIUS server.

Figure 37- Freeradius Wi-fi Authentication Server

As you can imagine, this means that these Freeradius clients will authenticate their devices over the management VLAN, being one of the number of reasons it must be kept restrictive. As for the Unifi environment, we must now direct it towards this interface, to do this we create a Radius profile under ‘Settings>Profile>Radius’, adding a new profile, the result of which can be seen below.

EDIT RADIUS PROFILE - TRUSTED WIRELESS

Profile Name: Trusted Wireless

VLAN Support:

- ☐ Enable RADIUS assigned VLAN for wired network
- ☒ Enable RADIUS assigned VLAN for wireless network

RADIUS Auth Server:

- IP Address: 10.0.5.1
- Port: 1812
- Password/Shared Secret: [REDACTED]
- + ADD AUTH SERVER

Accounting:

- ☒ Enable accounting

Interim Update:

- ☐ Enable Interim Update

RADIUS Accounting Server:

- IP Address: 10.0.5.1
- Port: 1813
- Password/Shared Secret: [REDACTED]
- + ADD ACCOUNTING SERVER

Figure 38- Unifi Radius Profile

Now, under ‘wireless networks’, we can change the security to ‘WPA Enterprise’, and assign said Radius profile. Although the controller calls it WPA, Unifi does not allow WPA and as such all instances of WPA are actually WPA2.

As we plan to use EAP-TLS protocol on our client devices, we will need to create a user and user certificate on Freeradius and PFSense, respectively. So, we first of all create a user in the same way we did in the guest network, assigning a VLAN to the user account. From there we can then create the certificate needed to authenticate the user against the server, for which we will need to create a Certificate Authority under ‘System>Cert Manager’, the CA used in testing can be seen below.

Create / Edit CA

Descriptive name: FreeRadius CA

Method: Create an internal Certificate Authority

Internal Certificate Authority

Key length (bits): 4096

Digest Algorithm: sha512
NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.

Lifetime (days): 3650

Common Name: FreeRadius-InternalCA

The following certificate authority subject components are optional and may be left blank.

Country Code: None

State or Province: e.g. Texas

City: Cardiff

Organization: e.g. My Company Inc.

Organizational Unit: e.g. My Department Name (optional)

Figure 39- Freeradius CA

Now, using this CA, we can then, the under ‘Certificate’ tab, create both a user and server certificate. The Certificates can be seen below.

Add/Sign a New Certificate		Add/Sign a New Certificate	
Method	Create an Internal Certificate	Method	Create an Internal Certificate
Descriptive name	FreeRadius Server Cert	Descriptive name	FreeRadius Test User Cert
Internal Certificate		Internal Certificate	
Certificate authority	FreeRadius New Cert	Certificate authority	FreeRadius New Cert
Key length	4096	Key length	4096
Digest Algorithm	sha512	Digest Algorithm	sha512
NOTE: It is recommended to use an algorithm stronger than SHA1 when possible		NOTE: It is recommended to use an algorithm stronger than SHA1 when possible	
Lifetime (days)	3650	Lifetime (days)	3650
Common Name	Freeradius-Internal/CA	Common Name	LiamBlunt
The following certificate subject components are optional and may be left blank		The following certificate subject components are optional and may be left blank	
Country Code	GB	Country Code	GB
State or Province	e.g. Texas	State or Province	e.g. Texas
City	Cardiff	City	Cardiff
Organization	e.g. My Company Inc	Organization	e.g. My Company Inc
Organizational Unit	e.g. My Department Name (optional)	Organizational Unit	e.g. My Department Name (optional)
Certificate Attributes		Certificate Attributes	
Attribute Notes	The following attributes are added to certificates and requests when they are selected mode. For Internal Certificates, these attributes are added directly to the certificate	Attribute Notes	The following attributes are added to certificates and requests when they are selected mode. For Internal Certificates, these attributes are added directly to the certificate
Certificate Type	Server Certificate	Certificate Type	User Certificate
Add type-specific usage attributes to the signed certificate. Used for placing		Add type-specific usage attributes to the signed certificate. Used for placing	

Figure 41- Freeradius Server Cert

Figure 40-Freeradius User Cert

Lastly, we need to configure the ‘Certificates for TLS’ settings on the EAP tab in Freeradius and assign the server CA and server certificate. In the ‘Certificates for TLS’ section, apply the certificates for the CA and server, respectively. While not essential, in this section, this writer also disabled the weaker EAP types such as MD5, GTC and LEAP as making sure the EAP-TLS tab settings were correct, the only changes this writer made here were ticking the ‘Check Cert Issuer’ and ‘Check Client Certificate CN’ options. This is why the user’s ‘common name’ in the user certificate is the same as the username for the Freeradius user this writer created. Now, back to the Cert manager, for our authentication method, the device needs both the CA and user certificate, these can be gathered by clicking the ‘Export Certificate’ button next to both the CA and user entries. Then, preferably securely, get those cert files onto the device that

is going to be connecting to the Wi-Fi. For testing purposes we will once again be using an Android phone. Upon executing the certificates, android asks for their purpose, of which we select Wi-fi. Then, connecting to the network is as simple as selecting TLS for the EAP method, putting the CA and user certificates in their field and Identity, of which is the Freeradius user's username. The filled form for this writer's android mobile can be seen below.

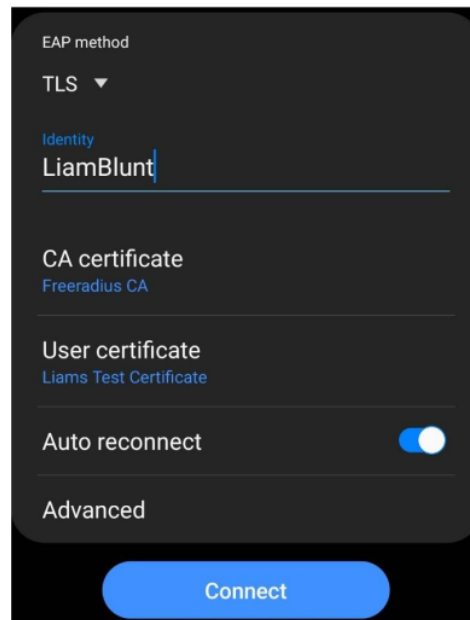
A screenshot of an Android application interface for configuring a Wi-Fi connection. The interface is dark-themed. At the top, it says 'EAP method' with a dropdown menu showing 'TLS'. Below that is an 'Identity' field with the text 'LiamBlunt'. Further down are two certificate selection fields: 'CA certificate' with 'Freeradius CA' and 'User certificate' with 'Liams Test Certificate'. Below these is a toggle switch for 'Auto reconnect' which is turned on. At the bottom is an 'Advanced' section header and a large blue 'Connect' button.

Figure 42- EAP-TLS Wi-Fi Connect

Now, while this is more secure, it is more complicated to get users set up. Having said that, this authentication is set up on the 'Trust_Wireless' network, and as indicated by the name, is for only the most trusted of devices/clients due to the less-restrictive firewall ruling set up on the interface, and as such there are not going to be hundreds of users connecting to this VLAN, at least not in a small business scenario.

4. Snort IDS Configuration

An Intrusion Prevention System is a means of detecting unfamiliar or incorrect traffic through the firewall, the example we will be using is Snort, as it is one of two IDS packages available in PFSense. First of all Snort must be installed in PFSense, as we have gone over installing packages, this will be overlooked.

One snort is installed, under the 'Services>Snort>Global Settings' tab, this is where snort retrieves the rules it applied to the network. Snort has a number of free rulesets and premium rulesets, and some require an account to use, their usage depends fully on the administrator's needs, for test purposes we will use all the free options available. Additionally there is OpenAppID, an opensource means developed by Cisco to identify software running on client machines, allowing for administrators to better control their clients use of unauthorised software, assuming its traffic has passed the firewall. Once the rulesets have been selected and saved, please refer to the 'Update' tab as to actually download them, as well as set an update interval and time. This writer has the rules updating every 24 hours at 03:00, as to avoid disrupting the network.

Now, to apply Snort we must create an interface, under the 'Interfaces' tab. Important to note here, while PFSense refers to the LAN interfaces as separate to the other VLANs, Snort does not, recognising it as a parent interface, so should a snort interface be applied to the LAN network, it will instead be applied to all sub-interfaces of LAN, AKA every internal VLAN we have. As such we will instead create an interface per VLAN. Here, we will create a Snort interface for the Networking VLAN, as it is the one that arguably needs the most security.

Luckily, when creating an interface at this stage, most settings can be kept as default, the only ones that are recommended to change are the interface to the VLAN you want it assigned to, and the description, for administrative purposes. You may also choose to 'block offenders', but at this point this writer would *highly* advise against that. The reason for this is the next step, assigning the rulesets, under the 'X Categories' tab, where X is the interface you assigned it to. This tab is where you select what rulesets you downloaded you want to apply to the interface, so that you can be alerted should something flag those rules. These rulesets are essentially criteria for matching signatures of traffic to ascertain its purpose and should it match an alert rule, alert the admin to its presence. Here you may use an IPS policy, essentially a selection of rules ranging from light(Connectivity) to heavy(Max detect) detection, or simply select those

you want to. If you are unsure, this writer would suggest an IPS policy. For testing purposes, and to see *what* would be flagged, this writer enabled every rule. Back at the interface tab, you may now start the Snort interface.

As expected, the alert logs lit up like a Christmas tree, alerting to nearly every instance of HTTP, browsers, programs, STUN traversal, etc. This is where some admin intervention is needed. To lower these false positives, there are two methods, suppression, and deletion. In the 'Alerts' tab, you can look at the list of alerts, and suppress or delete a rule should you deem it false. As OpenAppID is enabled, there will be many instances of Firefox or Chrome alerts, luckily these can simply be deleted. In regard to suppression and deletion, deletion simply deletes the rule, avoiding it being inspected and can be said to be the more efficient of the two methods, as suppression still inspects it, but does not create an alert.

Ideally, this IDS/IPS interface should be left running for a week or so as to remove as many false positives as possible. Once you believe you have suppressed or deleted all false positives, you may choose to change from alerting, to blocking. This means that any client not whitelisted that generates an alert will be blocked for a set amount of time. As you can imagine, this can accidentally block a good number of trusted clients, and that is why it is ill advised unless you are *very* confident you have eliminated all false positives, or at the very least added those clients you fully trust to the whitelist, or 'passlist' as Snort refers to the list that prevents blocking certain clients.

This implementation of IDS/IPS can then be copied to other interfaces such as the WAN interface, or another creation of a Snort Interface to match it.

It is worth mentioning that Snort mainly checks HTTP, and while it can check HTTPS/SSL, in their readme file, they say mention that Snort should not be used for SSL inspection for reasons of performance and false positives.

5. Interface Firewall Rules

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗ 0 / 122 KB	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks	⚙️
✗ 0 / 7.37 MB	IPv4 *	EasyRuleBlockHostsWAN	*	*	*	*	none		Easy Rule: Blocked from Firewall Log View	📄 ⚙️ 🗑️
^ ^ <Default Rules> ^ ^										🗑️
✓ 1 / 11 KB	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		OpenVPN Server Access	📄 ⚙️ 🗑️
✗ 0 / 0 B	IPv4 TCP	RFC1918	*	*	*	*	none			📄 ⚙️ 🗑️

Figure 43- WAN Firewall

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<Per-Client Rules>										🗑️
✓ 0 / 0 B	IPv4 TCP	AllowedAccessToAdmin	*	This Firewall	PFSense_Admin	*	none		Allow Trust_VLAN access to admin interface	📄 ⚙️ 🗑️
✓ 0 / 10.34 GB	IPv4 *	TRUST_WIRED_VLAN net	*	Private_Networks	*	*	none		Allow Access From Trust_VLAN to Private Networks	📄 ⚙️ 🗑️
<Interface-Wide Rules>										🗑️
✓ 0 / 0 B	IPv4 TCP/UDP	*	53 (DNS)	127.0.0.1	53 (DNS)	*	none		NAT Redirect DNS Trust_WIRED_VLAN	📄 ⚙️ 🗑️
✓ 0 / 0 B	IPv4 *	TRUST_WIRED_VLAN address	*	192.168.0.1	*	*	none		Allow Access From Trust_VLAN to External Gateway	📄 ⚙️ 🗑️
⚙️ 6 / 39.84 GB	IPv4 *	TRUST_WIRED_VLAN net	*	*	*	NORDVPN_UK_1852_VPNV4	none		Default Trust_VLAN to NordVPN gateway	📄 ⚙️ 🗑️

Figure 44- Trusted_Wired Firewall

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<Per-Client Rules>										🗑️
⚠️ 0 / 0 B	IPv4 TCP/UDP	WAN address	UnifiRemote	10.0.5.2	*	*	none		Block Unifi Remote	📄 ⚙️ 🗑️
✓ 0 / 0 B	IPv4 TCP/UDP	10.0.5.2	*	This Firewall	PFSense_Admin	*	none		Allow NetworkPC Access to Admin Interface	📄 ⚙️ 🗑️
<Interface Wide Rules>										🗑️
✓ 0 / 0 B	IPv4 TCP/UDP	NETWORKING_VLAN net	53 (DNS)	127.0.0.1	53 (DNS)	*	none		NAT Redirect DNS Networking_VLAN	📄 ⚙️ 🗑️
⚙️ 13 / 887.13 MB	IPv4 *	UnifiDevices	*	*	*	NORDVPN_UK_1852_VPNV4	none		NordVPN Gateway	📄 ⚙️ 🗑️

Figure 45- Networking_VLAN Firewall

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
Custom Rules											
■	✓	0/0 B	IPv4 TCP/UDP	TRUST_WIRELESS_VLAN net	*	10.0.5.2	Docker_Containers	*	none	Allow Access to Network Service PC	
V Default Rules V											
■	✓	0/0 B	IPv4 TCP/UDP	10.0.10.129/25	53 (DNS)	127.0.0.1	53 (DNS)	*	none	NAT Redirect DNS Trust_Wireless_VLAN	
■	🔒	0/0 B	IPv4 TCP/UDP	*	*	This Firewall	PFSense_Admin	*	none	Block Access to Admin Interface	
■	✓	0/5.67 GB	IPv4 *	TRUST_WIRELESS_VLAN net	*	*	*	NORDVPN_UK_1852_VPNV4	none	Default Trust_Wireless_VLAN to NordVPN gateway	

Figure 46 Trust_Wireless Firewall

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
■	✓	0/37 K/B	IPv4 TCP/UDP	GUEST_VLAN net	*	This Firewall	GuestCaptivePortal	*	none	Guest Portal	
Blocking											
■	🔒	0/0 B	IPv4 TCP/UDP	*	*	This Firewall	PFSense_Admin	*	none	Block Access to Admin Interface	
■	🔒	0/0 B	IPv4 *	GUEST_VLAN net	*	Private_Networks	*	*	none	Block Access to Certain Networks	
■	✗	0/0 B	IPv4 TCP	GUEST_VLAN address	*	*	1194 (OpenVPN)	*	none	Blocking Openvpn Access	
Gateway											
■	✓	0/0 B	IPv4 TCP/UDP	GUEST_VLAN net	53 (DNS)	10.0.50.1	53 (DNS)	*	none	NAT Redirect DNS Guest	
■	✓	0/0 B	IPv4 *	GUEST_VLAN address	*	GUEST_VLAN address	*	WANGW	none	Allow Internet Guest	

Figure 47- Guest VLAN Firewall

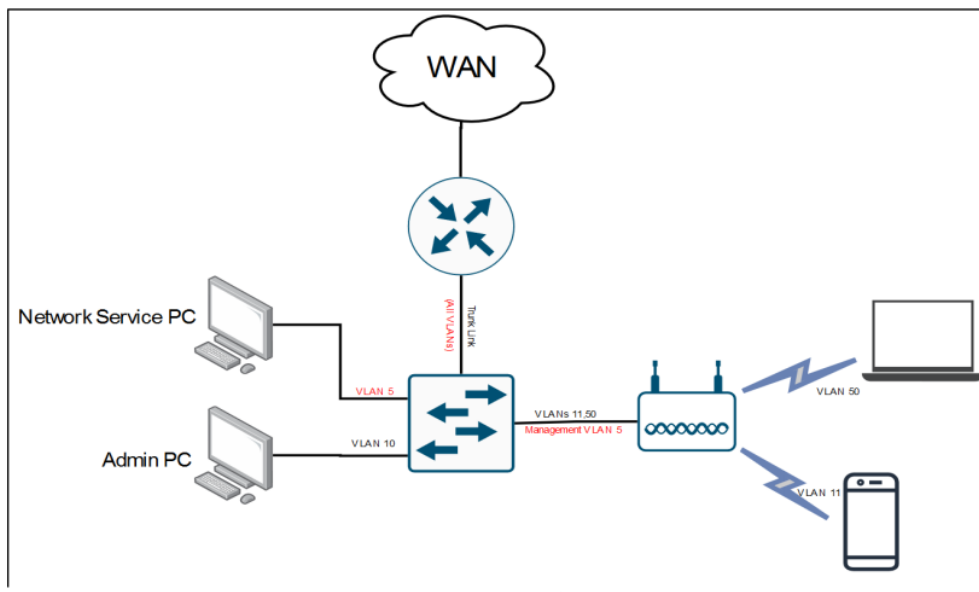


Figure 48- Larger Network Diagram

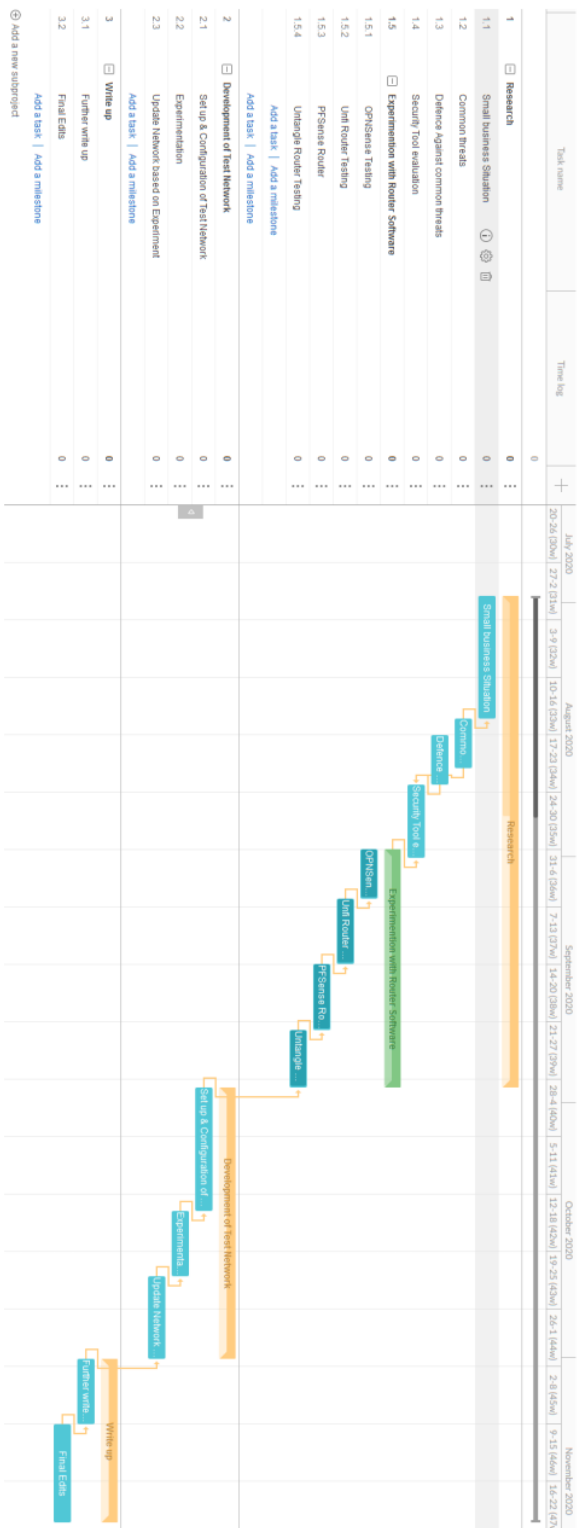


Figure 49- Project Gantt Chart

MSC Project Report Liam Blunt Final

GRADEMARK REPORT

FINAL GRADE

/100

GENERAL COMMENTS

Instructor

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

PAGE 16

PAGE 17

PAGE 18

PAGE 19

PAGE 20

PAGE 21

PAGE 22

PAGE 23

PAGE 24

PAGE 25

PAGE 26

PAGE 27

PAGE 28

PAGE 29

PAGE 30

PAGE 31

PAGE 32

PAGE 33

PAGE 34

PAGE 35

PAGE 36

PAGE 37

PAGE 38

PAGE 39

PAGE 40

PAGE 41

PAGE 42

PAGE 43

PAGE 44

PAGE 45

PAGE 46

PAGE 47

PAGE 48

PAGE 49

PAGE 50

PAGE 51

PAGE 52

PAGE 53

PAGE 54

PAGE 55

PAGE 56

PAGE 57

PAGE 58

PAGE 59

PAGE 60

PAGE 61

PAGE 62

PAGE 63

PAGE 64

PAGE 65

PAGE 66

PAGE 67

PAGE 68

PAGE 69

PAGE 70

PAGE 71

PAGE 72

PAGE 73

PAGE 74

PAGE 75

PAGE 76

PAGE 77

PAGE 78

PAGE 79

PAGE 80

PAGE 81

PAGE 82

PAGE 83

PAGE 84
