

design your future

# Cyber Security bij EFFIX

Auteur:

Pieter Verheyen

Handelswetenschappen en  
bedrijfskunde

Opleiding:

Systeem-en Netwerkbeheer

Campus Kortrijk

Academiejaar 2020-2021



# Woord vooraf

---

Een onderdeel van het tweede jaar Systeem- en Netwerkbeheer is om een praktisch project uit te werken bij onze stageplaats. Ik heb mijn project uitgevoerd bij het bedrijf EFFIX. Het project dat ik deed was gebaseerd op security. Dit vind ik persoonlijk het interessantste in de IT. Daardoor zal ik volgend jaar ook verder studeren in deze branche. Ik zal namelijk toegepaste informatica, afstudeerrichting cyber security studeren. Het beveiligen van data en het de hackers moeilijk maken is iets waar ik mij graag wil in verdiepen. Het project dat ik uitvoerde bij het bedrijf EFFIX draait om security. Iets waar ik al lange tijd erg geïnteresseerd in ben. Dit begon toen ik voor de eerste keer een firewall mocht instellen. Door dit te doen ontdekte ik dat er in deze sector van de IT enorm veel werk is en dat dit een heel diep onderwerp is. Ik wil me hier dan ook graag verder in verdiepen en dat heeft dit project me al een pak in geholpen.

Ik heb deze opdracht dan ook zeer positief ervaren. Door het zelfstandig uitvoeren van een project leer ik enorm veel bij. Ik heb mijn kennis over security enorm moeten uitbreiden om dit project tot een goed einde te brengen.

Werken bij EFFIX was altijd heel leuk. Er was elke dag wel iets te doen waardoor ik veel heb bijgeleerd. Ook stond elke collega klaar om ons te helpen en ons nieuwe uitdagingen te geven. Ik kreeg van elkvlak in de IT wat te proeven: zo mocht ik eens meedraaien op de helpdesk, meegaan met collega's naar klanten om het netwerk in orde te zetten, alleen kleine interventies uitvoeren en op kantoor kleine zaken in orde brengen.

Ik zou graag ook enkele mensen bedanken. Als eerste wil ik heel graag mijn stageplaats EFFIX voor het uitlenen van materiaal en vooral kennis. In het bijzonder zou ik graag Geoffrey Vander Schelden bedanken voor het toekennen van deze stageplaats aan mij. Verder wil ik graag alle medewerkers van EFFIX bedanken voor

het altijd paraat staan om te helpen. Ik leerde niet enkel dingen bij op mijn stageplaats maar ook op school. Daarom wil ik graag ons opleidingshoofd Wim Engelen bedanken voor de goeie organisatie in deze studierichting. Ook wil ik graag elke leerkracht bedanken voor het overbrengen van hun kennis naar mij.

# Inhoudsopgave

---

Lijst met afkortingen.....	1
Inleiding .....	3
1      Opdrachtomschrijving.....	4
2      Componenten .....	5
2.1    Watchguard Firewall.....	5
2.2    De Subscription services .....	6
2.3    HPE Aruba switch.....	11
2.4    Vlan's .....	11
2.5    Super-microserver .....	15
2.6    RAID-controller.....	15
2.7    VMWare (ESXI) .....	17
2.8    Unifi controller .....	18
3      De configuratie .....	19
3.1    De Firewall .....	19
3.2    De netwerkswitch.....	30
3.3    De Supermicro server.....	33
3.4    De Acces Point .....	37
4      Mailboxen .....	38
4.1    Microsoft 365 .....	38
5      Overige beveiliging .....	45
5.1    Hardware beveiligen.....	45
5.2    Opleiden van eindgebruikers .....	45
6      Hacking.....	47
6.1    Penetration testing.....	47
6.2    Bekende aanval methoden.....	49
6.3    Waarom Pentesten uitvoeren.....	63
7      Moeilijkheden en problemen .....	64
7.1    Falen van hardware .....	64
7.2    Falen synchronisatie Microsoft 365 en licenties.....	64
7.3    Watchguard licentie.....	65
8      Conclusie.....	67

Afbeeldingenlijst.....	69
Bijlagen.....	71
Bijlage 1: Netwerkschema.....	71
Bijlage 2: Configuratie switch .....	72
Bijlage 3: XML Watchguard .....	75

# Lijst met afkortingen

---

Afkorting	Uitleg
AI	Artificiële intelligentie
Xss	Cross-site scripting
RED	Reputation Enabled Defense
DLP	Data Loss Prevention
APT	Advanced Persistent Threat
TDR	Threat Detection and Response
PoE	Power over Ethernet
ESXI	VMWare
AP	Acces Point
LAN	Local Area Network
VLAN	Virtual Local Area Network
RDP	Remote Desktop protocol
DDoS	Distributed-denial-of-service
DoS	Denial-of-Service
DC	Domain Controller
AD	Active Directory
OS	Operating system

MFA	Multi Factor Authentication
Pentest	Penetration testing
MitM	Man-in-the-middle

# Inleiding

---

Mijn stageproject gaat over de beveiliging binnen de IT. We kozen dit omdat ik dit een zeer interessant onderwerp vind. Het probleem bij IT-security is dat dit een zeer ruim en complex onderwerp is. De specialisten moeten constant mee evolueren met de hedendaagse technologieën. De opdrachtomschrijving is zeer ruim: maak een netwerk en beveilig deze zo goed mogelijk, probeer daarna je eigen beveiliging te kraken.

Tijdens het uitwerken van mijn stageproject ontdekte ik dat ik mij op bepaalde zaken moet focussen. Het volledige beveiligen is namelijk een te groot begrip. Ik koos om een firewall in te stellen en de mailboxen die ik had zo goed mogelijk te beveiligen. Maar voor ik aan dit project kon starten moest ik mijn componenten uitzoeken. Dit kan je lezen in hoofdstuk één. Hoe ik mijn componenten instelde kan je terugvinden in hoofdstuk drie. Het instellen en beveiligen van de mailboxen staat in hoofdstuk vier.

Beveiligen in de IT is niet alleen softwarematig maar ook hardware matig. In hoofdstuk vijf kan je terugvinden hoe je dit het beste doet.

Na het beveiligen van het netwerk is het de bedoeling dat we proberen het netwerk te kraken. Dit is niet zo simpel, wat natuurlijk wel een goed teken is. Anders zouden er veel meer mensen dit kunnen en dat is natuurlijk niet de bedoeling. Meer uitleg hierover vind je terug in hoofdstuk zes.

In hoofdstuk zeven leg ik uit welke problemen ik tegenkwam toen ik werkte aan dit project. En in hoofdstuk acht kan je mijn conclusie terugvinden.

# 1 Opdrachtomschrijving

---

De opdracht die ik in overleg met mijn stageplaats kreeg is gebaseerd op het beveiligen van een netwerk en alles wat in het netwerk zit. Het beveiligen van een netwerk is natuurlijk een zeer ruim begrip en hier kan je zeer diep in gaan. In een netwerk heb je servers, computers, acces points, mobiele apparaten en netwerk switchen. Daarnaast heb je ook eindgebruikers die software gebruiken van het bedrijf, mailboxen en deze surfen ook op het internet. Niet alleen softwarematig kan alles beveiligd worden maar ook hardware matig. Bijvoorbeeld een slot op de serverkast. Dit zijn allemaal zaken die dienen beveiligd te worden. Als we de eindgebruikers vrij spel geven op het internet, is de kans zeer groot dat er binnen de kortste keren een virus of bepaalde malware in het netwerk sluipt. Dit kan enorme gevolgen hebben voor het bedrijf. In mijn opdracht wordt de focus gelegd op het buiten houden van malware, virussen en DDOS-aanvallen. Dit doe ik met een firewall. Daarnaast wil ik ook zorgen dat de mailboxen veilig zijn. Dit wil zeggen dat ik alle phishing-mails wil tegenhouden, malware die in een mail verstopt zit, nep domeinnamen, spammails en vreemde URL's. Dit zal ik doen met Microsoft defender for Office 365.

Nadat alles beveiligd is zal ik ook een Penetration test (pen test) proberen uit te voeren en verschillende andere soorten populaire aanvallen. Een Pen test dient om alle zwakheden bloot te leggen in het netwerk. Zo kunnen eventuele fouten na het beveiligen nog rechtgezet worden.

# 2 Componenten

---

In dit hoofdstuk bespreken we de componenten van mijn eindwerk. Deze zijn belangrijk om een goed overzicht te krijgen van wat we zullen gebruiken en waarvoor deze dienen. Later in deze scriptie gaan we dieper in op de configuratie, hoe veilig deze is en wat voor problemen ik ondervond. De Firewall is het belangrijkste component. Deze wordt daarom als eerste besproken. Daarna gaan we ook dieper in op de netwerkswitch, de server en de acces point.

## 2.1 Watchguard Firewall

De Watchguard firebox T35 is één van de belangrijkste componenten van mijn eindwerk. Dit is namelijk de firewall. Deze zorgt ervoor dat mensen met slechte bedoelingen het netwerk niet kunnen bereiken. Het opereert als het ware als een filter. Je kan in de firewall regels instellen om bepaalde poorten te blokkeren, websites te blokkeren, protocollen te blokkeren of door te laten. Als er een IP-pakketje aankomt die aan geen enkele regel voldoet of die voldoet aan een regel die aangeeft dat het verkeer niet door mag gaan, zal de firewall het pakketje een halt toeroepen. Het IP-pakketje wordt dan ‘gedropt’.

### 2.1.1 Werking firewall

Zoals eerder vertelt werkt de firewall als een soort filter voor het netwerk. De firewall die ik gebruik heeft veel mogelijkheden. Als eerste moeten we regels instellen voor wat mag en wat niet mag. Hier moet je wel oppassen, want de firewall leest de regels van boven naar onder. Als er in een regel staat dat een specifiek IP-

pakketje moeten worden geblokkeerd, kan een regel eronder deze niet meer toelaten. Je hebt niet enkel regels die een bepaald verkeer blokkeren of toelaten, je hebt ook andere services. Bij mijn firewall zijn dit betalende functies.

## 2.2 De Subscription services

Om deze subscription services te kunnen gebruiken moet je wel een licentie hebben. Je hebt 3 licenties: Support, Basic Security en Total Security. De support-licentie bezit maar enkele services, de Basic Security bezit er al wat meer en de Total Security bezit alle services. Ikzelf zal gebruik maken van de Total Security. Dit doe ik omdat ik dan kan gebruik maken van APT Blocker en DNS watch. Hieronder bespreek ik elke mogelijke service.

- Gateway antivirus

Als er iemand met slechte bedoelingen, zoals bijvoorbeeld een hacker, een virus of een trojan horse loslaat op je netwerk zal de Gateway antivirus dit stoppen. Gateway antivirus werkt met verschillende protocollen: SMTP, IMAP, POP3, HTTP, FTP, Explicit en TCP-UDP. Wanneer er een nieuwe aanval wordt gedetecteerd wordt er gedetecteerd wat dit virus maakt. Dit wordt ook wel de ‘handtekening’ van het virus of trojan horse genoemd. De Gateway antivirus onthoudt deze handtekeningen en gebruikt deze om virussen te vinden. Wanneer dit is ingesteld kunnen ook compressed files gescand worden op virussen.

- IntelligentAV

Dit is een functie die gebruik maakt van artificiële intelligentie (AI). Het dient om een nog betere verdediging te geven tegen malware. IntelligentAV kan door middel van AI bepaalde aanvallen maanden op voorhand voorspellen.

Het grote verschil hier is dat je nu ook beschermd bent tegen virussen die nog niet gecreëerd zijn.

- **Intrusion Prevention Service**

Deze functie is gemaakt om de installatie te beschermen tegen spyware, SQL- injectie, cross-site (xss) scripting en buffer overflows. Ook hier wordt er gebruik gemaakt van de 'handtekening' van de aanval. Aan de hand van die handtekeningen wordt de aanval herkend en geblokkeerd.

- **WebBlocker**

Deze functie dient om gebruikers de toegang te ontzeggen tot bepaalde websites. Webblocker gebruikt een database die websites in een categorie zet. Daarna kan je kiezen om een bepaalde categorie te blokkeren, toe te laten of een waarschuwing te geven. Indien er een waarschuwing staat ingesteld kan de gebruiker kiezen om de website al dan niet te raadplegen.

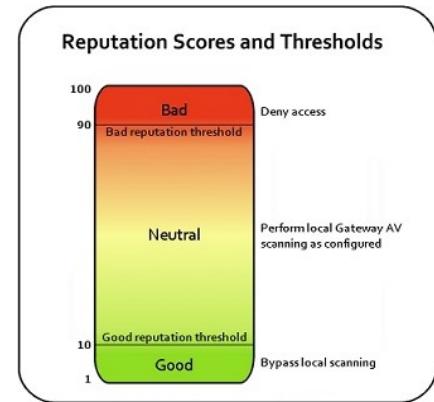
- **SpamBlocker**

Deze functie dient om ongewenste e-mails (spammails) te blokkeren.

Spamblocker scant alle e-mails en detecteert alle URL's die in de mail zitten. Ook wordt er gekeken of het geregistreerde domein niet al geblokkeerd is. Verder wordt er een patroonherkenning uitgevoerd, wordt er gekeken naar de reputatie van de afzender, wordt de koptekst en voettekst worden geanalyseerd en de grafische bijlagen gescand.

- Reputation Enabled Defense (RED)

Watchguard RED maakt gebruik van een cloud-gebaseerde WatchGuard reputatieserver die een reputatiescore tussen 1 en 100 toekent aan elke URL's. Als iemand naar een website surft zal de RED de website naar de reputatieserver sturen. Daarna zal de server antwoorden met een score van 1 t.e.m 100. Afhankelijk van wat er is ingesteld zal de gebruiker kunnen surfen naar de website. Hoe lager de score hoe veiliger de website is.



FIGUUR 1: REPUTATION ENABLED DEFENSE

- Application Control

Deze functie laat ons toe om de applicaties die de gebruikers ter beschikking hebben te beheren. Ook hier wordt er weer gewerkt met handtekeningen. Zo kan Application Control meer dan 1000 applicaties identificeren en blokkeren. Je kan in Application Control ook bepaalde functies van applicaties uitschakelen zoals file transfer.

- Data Loss Prevention (DLP)

Met DLP kunnen we het lekken van vertrouwelijke data opsporen, monitoren en voorkomen. In de DLP-service zitten er ingebouwde auditsensoren die gebruikt kunnen worden voor het naleven van HIPAA- of PCI-vereisten. Er is ook een mogelijkheid om zelf sensoren in te stellen. DLP gebruikt regels voor inhoudscontrole om gevoelige inhoud te vinden. Wanneer DLP-inhoud vindt

die overeenkomt met ingeschakelde DLP-regels, wordt de inhoud behandeld als een DLP-overtreding.

- APT Blocker

Een APT-aanval (Advanced Persistent Threat) is een type netwerkaanval waarbij geavanceerde malware en zero-day-exploits worden gebruikt om toegang te krijgen tot het netwerk en vertrouwelijke gegevens. APT-aanvallen maken gebruik van de nieuwste malwaretechnieken en zero-day exploits (zwakke plekken in de software). Daardoor is het niet meer mogelijk om met het zoeken naar de handtekening de aanvallen te herkennen. APT-Blocker gaat op zoek naar deze aanvallen op een andere manier. Deze service maakt gebruik van 'Full-system emulation' (virtualisatie) om de malware te detecteren. Alle bestanden die in ons netwerk komen worden gescand en daar wordt een MD5-hash van gemaakt. Deze wordt dan later vergeleken met een MD5-Hash in de database van Watchguard. Als die vergelijking een overeenkomst geeft met een gekende malware kan Watchguard direct acties ondernemen.

- Botnet Detection

Een botnet is een groot aantal geïnfecteerde computers die gecontroleerd worden door een server. Die server kan de geïnfecteerde computers bevelen om volgende aanvallen te doen: DOS, Spam verzenden en private data stelen. De detectie gebeurt op gekende IP-adressen van botnet-sites. Ook wordt deze al gedeeltelijk geblokkeerd bij de webblocker. Dit komt omdat botnets gebruik maken van HTTP en IRC-protocols.

- Network Discovery

Deze service dient om uw netwerk in kaart te brengen. Alle netwerken op ons intern netwerk kunnen worden weergegeven. Ook staan de volgende gegevens erbij: IP-adres, Hostname, MAC-adres, OS en open netwerkpoorten.

- Threat Detection and Response (TDR)

TDR is een Cloud gebaseerde service die samenwerkt met onze firewall om de gevolgen van het verliezen van data en penetraties tot een minimum te beperken door middel van vroegtijdige en geautomatiseerde beveiligingen te gebruiken. Het verzamelt informatie van alle eindpunten op het netwerk om zo makkelijker en sneller beveiligingsrisico's op te sporen.

- DNSWatch

DNSWatch is een cloud-gebaseerde service die gebruikt wordt om het netwerk te beschermen tegen 'slechte' domeinen. De service monitort alle DNS-aanvragen ongeacht type, protocol of poort. Wanneer een gebruiker verbinding maakt met een 'slecht' domein zal deze geblokkeerd worden.

- Geolocation

Met deze functie kunnen we websites uit bepaalde landen blokkeren. Als we België blokkeren dan kunnen we niet meer surfen naar websites die eindigen op .be.

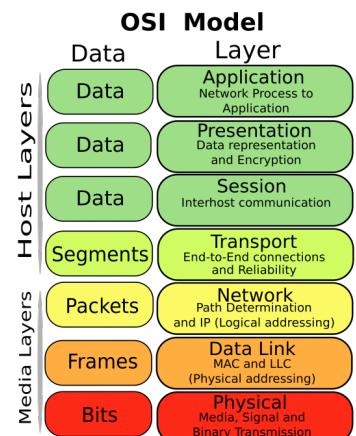
## 2.3 HPE Aruba switch

Na de firewall komt de netwerkswitch in ons netwerk. Voor dit project kreeg ik een HPE Aruba j9776a 2530-24g ter beschikking. Deze switch heeft 26 poorten. 24 daarvan hebben Power over Ethernet (PoE). De switch dient als uitbreiding op het bekabelde netwerk. Alles wat op de netwerkswitch wordt aangesloten zal ook op ons netwerk terechtkomen.

## 2.4 Vlan's

Om het netwerk overzichtelijk te houden en het ook te beveiligen maakte ik gebruik van Vlan's. Een Vlan oftewel een virtual local area network is een type virtueel netwerk.

Als we naar het OSI-model kijken bevindt deze zich op layer 2, de datalinklaag. Een Vlan bestaat uit een groep end devices en switches die samen een gemeenschappelijk Local Area Network (LAN) hebben. Maar door de Vlan kunnen we deze in één of meerdere fysieke netwerken opsplitsen. Zo kunnen we verschillende componenten en end devices in verschillende netwerken steken. Dit geeft ons extra beveiliging en overzicht omdat de gebruikers niet van het ene netwerk naar het andere kunnen surfen (tenzij dit in de firewall anders ingesteld staat). We kunnen gebruikers die op de publieke wifi zitten minder toegang geven dan de gebruikers die op de private wifi zitten. We kunnen ook een logica steken in het netwerk. Dit geeft ons meer overzicht.

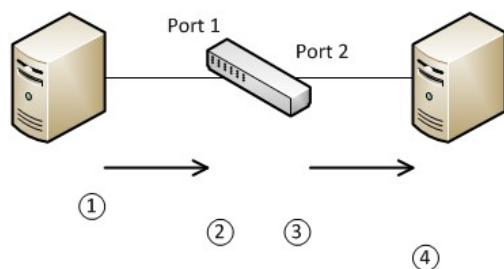


FIGUUR 2: OSI MODEL

### 2.4.1 Untagged Vlan's

Een poort op een switch kan tagged of untagged zijn. Als je poort untagged is dan zal de host niet op de hoogte zijn van de Vlan configuratie. De host die

geconnecteerd is met de switch zal een IP-pakketje sturen naar de switch. Als het pakketje toekomt op de switch zal de Vlan in kwestie eraan gekoppeld worden. Als het pakketje de switchpoort verlaat zal ook de Vlan verwijderd worden van het pakketje.



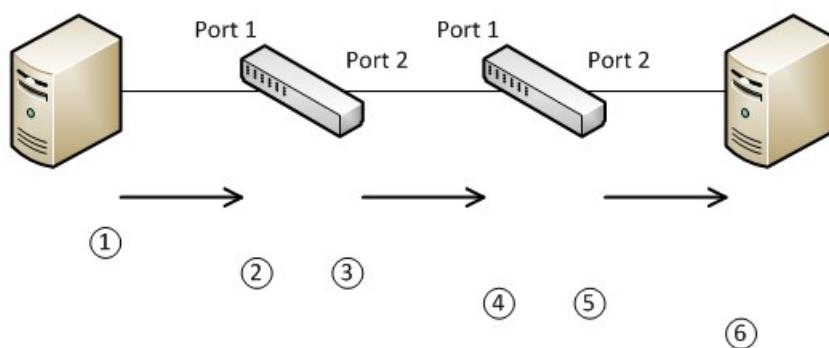
**FIGUUR 3: UNTAGGED VLAN**

Op de foto hierboven zie je een heel simpel netwerk. Om untagged Vlan duidelijk te maken kunnen we het gebruiken als een voorbeeld.

1. De linker computer stuurt een IP-pakketje naar de switch. Het pakketje bezit nog geen Vlan.
2. Het IP-pakketje is toegekomen op poort 1 van de switch. Deze poort is ingesteld als Untagged. Op deze poort is ook Vlan 25 ingesteld. Omdat het IP-pakketje op een Untagged poort komt met Vlan 25 erop zal aan het IP-pakketje vlan 25 worden toegevoegd.
3. De switch beslist dat het IP-pakketje via poort 2 moet worden verstuurd naar de andere computer. Omdat poort 2 ook untagged is wordt het IP-pakketje ontnomen van Vlan 25.
4. De rechter computer ontvangt een Untagged IP-pakketje.

## 2.4.2 Tagged Vlan's

Als de switchpoort tagged is dan verwacht de interface een IP-pakketje met die bepaalde VLAN tag. Omdat de switchpoort is ingesteld op tagged verwacht de poort dan ook een IP-pakketje met die bepaalde Vlan. De switch die dat IP-pakketje ontvangt ziet de tagged vlan en zal controleren of deze is toegelaten. Daarna wordt deze doorgestuurd naar de volgende tagged of untagged poort.



FIGUUR 4: TAGGED VLAN

Op de foto hierboven zie je een heel simpel netwerk. Om tagged Vlan duidelijk te maken kunnen we het gebruiken als een voorbeeld.

1. De linker computer verstuurde een IP-pakketje naar poort 1 op de switch. Het IP-pakketje bezit geen Vlan Tag.
2. Het IP-pakketje komt toe op poort 1. Dit is een Untagged poort van Vlan 10. De switch voegt aan het IP-pakketje Vlan 10 toe.
3. De netwerkswitch ontdekt dat het pakketje via poort 2 moet worden doorgestuurd. Poort 2 is een tagged poort van Vlan 10. Omdat deze tagged is controleert de switch of het IP-pakketje een tag van Vlan 10 bezit. Als dit

zo is wordt het pakketje doorgestuurd. Als dit niet zo is dan zal het pakketje gedropt worden.

4. De tweede switch krijgt het pakketje op poort 1. Poort 1 is een tagged poort van Vlan 10. De switch bekijkt of het IP-pakketje een tag van VLAN 10 bezit. Als dit zo is wordt het pakketje doorgestuurd. Indien dit niet zo is zal het pakketje gedropt worden. Daarna ontdekt de tweede switch dat het IP-pakketje naar poort 2 moet worden doorgestuurd.
5. Omdat poort 2 op de tweede switch een untagged poort is wordt Vlan 10 van het IP-pakketje verwijderd. Daarna wordt het doorgestuurd.
6. Als laatste ontvangt de rechter computer het IP-pakketje.

## 2.5 Super-microserver

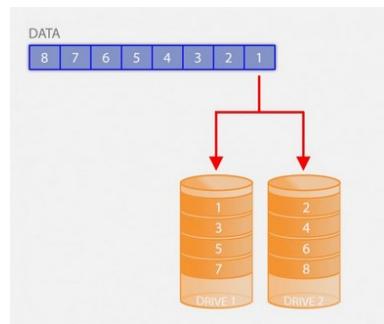
De server die ik gebruik is een Supermicro. Deze server heeft 32 GB RAM (werkgeheugen), bezit een RAID-controller en heeft 4 schijven van 2 TB. Op deze server draait het virtualisatieprogramma VMWare (ESXi). Dit geeft ons de mogelijkheid om op de server verschillende soorten servers te laten draaien. Het enige verschil met vroeger is dat we nu één fysieke server hebben met verschillende servers erop. Vroeger was er telkens een fysieke server nodig.

## 2.6 RAID-controller

Een RAID-controller is een apparaat dat de schijven beheert en als logische eenheden doorgeeft aan de server. Je hebt verschillende soorten RAID-sets. Hieronder worden deze allemaal besproken.

- RAID 0 (Striping)

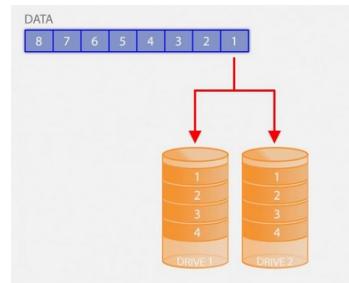
In RAID 0 wordt alle data verdeeld over de beschikbare schijven. Het eerste blok met data gaat naar schijf 1; Het andere blok met data gaat naar schijf 2 enzovoort. Het voordeel van deze manier is dat het enorm snel gaat. Het grote nadeel is hier dat deze manier niet betrouwbaar is. Als schijf 1 uitvalt, is alle data weg ook degene die op de andere schijf staat.



FIGUUR 5: RAID 0

- RAID 1 (spiegelen)

Bij een RAID 1 wordt de data gespiegeld over de schijven. Alles wat wordt opgeslagen op de eerste schijf zal ook op de 2<sup>de</sup> schijf worden opgeslagen.



FIGUUR 6: RAID 1

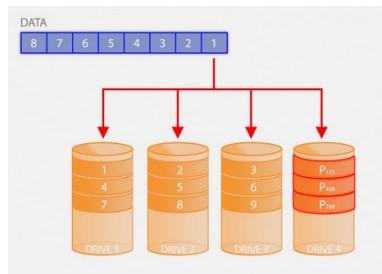
Als er een RAID 1 gebruikt wordt, moet je wel altijd een even aantal schijven hebben. Het voordeel hier is dat als de eerste schijf uitvalt, alle data ook nog op de tweede schijf staat. Het nadeel hier is dat je niet efficiënt gebruikt maakt van de opslagcapaciteit van de schijven.

- RAID 2 (Bit level striping)

Raid maakt gebruik van striping op bit-niveau. Dit zorgt ervoor dat we erg hoge snelheden kunnen halen. Het grote nadeel hier is dat er bijna geen enkele raid-controller RAID 2 ondersteund.

- RAID 3 en RAID 4

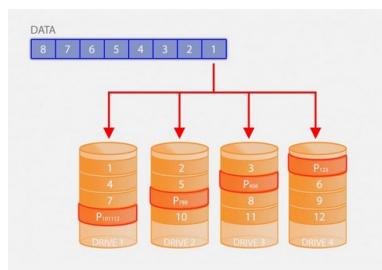
RAID 3 en RAID 4 zijn erg gelijkwaardig. Het enige dat anders is dat RAID 3 werkt op byte-niveau en RAID 4 werkt op blok-niveau. Het nadeel hier is terug dat deze zeer traag werkt.



FIGUUR 7: RAID 3 EN RAID 4

- RAID 5

RAID 5 werkt een beetje hetzelfde als RAID 4. De data worden via verschillende blokken over verschillende schijven verdeeld. Doordat alles

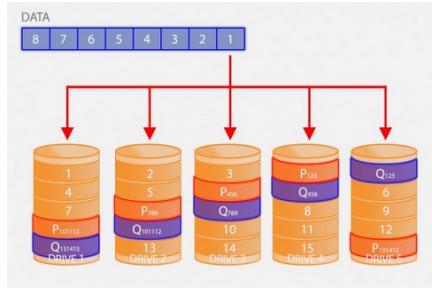


FIGUUR 8: RAID 5

gelijk verdeeld is kan de RAID-controller data terugvinden als er een schijf uitvalt. RAID 5 wordt veel gebruikt.

- RAID 6

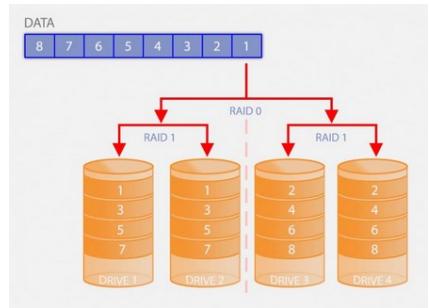
RAID 6 is een soort upgrade op RAID 5. Bij RAID 5 werden blokken met data verdeeld over de schijven. RAID 6 doet dit ook maar doet dit op 2 schijven. Hij zal dus 1 blok data op 2 verschillende schijven zetten. Als er dan 2 schijven falen kan nog altijd de data worden achterhaald.



FIGUUR 9: RAID 6

- RAID 10

RAID 10 is een combinatie van RAID 1 en RAID 0. De data worden eerst geschreven over 2 verschillende schijven zoals in RAID 0. Daarna worden die schijven gekopieerd zoals

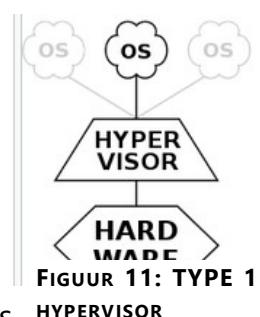


FIGUUR 10: RAID 10

in RAID 1.

## 2.7 VMWare (ESXI)

Op onze server zal VMWare draaien (ESXI). Dit is software die het mogelijk maakt om servers te virtualiseren. Dit zorgt dat de kost om servers aan te kopen nadrukkelijk daalt. Ook is alles wat makkelijker te beheren. VMWare is een type 1 hypervisor. Dit houdt in dat er geen operating system (OS) draait op de server. Op de hardware installeren we de software van ESXI en als deze is



FIGUUR 11: TYPE 1 HYPERVERVISOR

geïnstalleerd, kunnen we door naar het IP-adres te surfen verschillende servers aanmaken. Het grote voordeel is hier dat alles schaalbaar is. Als er meer ruimte nodig is kunnen we de schijf vergroten in ESXI. Als er meer geheugen nodig is kunnen we die ook toevoegen.

## 2.8 Unifi controller

In mijn netwerk gebruik ik een Acces Point (AP) van Unifi. Deze werken via een controller. In de controller kan je allerlei dingen instellen en aanpassen. We kunnen daar het wifiwachtwoord en de wifinaam. We kunnen ook toestellen op de zwarte lijst zetten.

# 3 De configuratie

---

In dit hoofdstuk bespreek ik hoe alle componenten zijn ingesteld en waarom ik deze zo ingesteld heb.

## 3.1 De Firewall

Als eerste veranderde ik de standaardwachtwoorden op mijn firewall. Zo kan alleen gemachigde personen inloggen.

Daarna maakte ik op mijn Firewall mijn verschillende netwerken aan. Dit is belangrijk omdat onze Firewall ook functioneert als DHCP-server en omdat deze moet communiceren met onze netwerkswitch. Onder het kopje netwerk kunnen we de VLAN's aanmaken. Ik heb 4 VLAN's aangemaakt, deze zijn VLAN100 – management, VLAN10 – Public-Wifi, VLAN20 – Private-Wifi en VLAN30 – computers. We moeten ook instellen onder welke interface deze gebruiken. Hieronder meer uitleg over de verschillende interfaces.

In de digitale bijlage vindt u de volledige XML en configuratie terug.

### 3.1.1 Trusted Interface

Trusted interfaces connecteert met de LAN of het interne netwerk. Een trusted interface is meestal een connectie voor gekende mensen of medewerkers. Het dient om mensen die niet elke dag op het netwerk komen niet aan bepaalde bestanden te laten komen of rechten te geven. Op ons netwerk vallen VLAN100, VLAN20 en VLAN30 onder de trusted interface.

### 3.1.2 Optional Interface

Optional interface zijn mixed-trust of DMZ-omgevingen. Deze staan los van het netwerk. Deze geven al minder rechten en vallen onder een andere Alias in de Firewall. Voorbeelden hiervan zijn FTP en mailservers. Ook kan een publieke wifi hieronder vallen. VLAN10 valt bij ons onder de optional interface.

The screenshot shows the 'Network Configuration' interface with the 'VLAN' tab selected. The title bar says 'Network Configuration'. Below it is a navigation bar with tabs: Interfaces, Link Aggregation, Bridge, VLAN, Loopback, Bridge Protocols, WINS/DNS, Dynamic DNS, Multi-WAN, Link Monitor, SD-WAN, and PPPoE. The 'VLAN' tab is highlighted. The main area is titled 'Virtual Local Area Network (VLAN) settings'. A table lists four VLAN entries:

ID	Name (Alias)	Zone	IPv4 Address	IPv6 Address	Secondary	Interfaces	Add...
100	VLAN100 - Management	Trusted	192.168.25.100/24 (DHCP server)			2	
20	VLAN20 - Private-Wifi	Trusted	192.168.20.100/24 (DHCP server)			2	
30	VLAN30 - Computers	Trusted	192.168.30.100/24 (DHCP server)			2	
10	VLAN10 - Public-Wifi	Optional	192.168.10.100/24 (DHCP server)			2	<button>Edit</button> <button>Delete...</button>

FIGUUR 12:AANMAAK VLAN'S EN INTERFACE

Nu de VLAN's zijn aangemaakt en we hebben meegegeven welke interface deze heeft moeten we ook nog meegeven of er tagged of untagged verkeer wordt verwacht. Onder het tabblad interfaces kunnen we dit instellen. Hier moeten we wel goed opletten want als we bezig zijn met te configureren en we stellen een tagged VLAN in dan kan het zijn dat we de connectie verliezen met de firewall. Ik heb ervoor gekozen om op interface 1 alle VLAN's onder tagged verkeer te plaatsen. Dit doe ik omdat dit de uplink naar mijn switch is.

Interface Name:	Optional-1					
Interface Description:	UPLINK switch					
Interface Type:	VLAN					
<input checked="" type="checkbox"/> Send and receive tagged traffic for selected VLANs						
You can add one or more VLANs to this interface.						
<a href="#">New VLAN</a>						
Member	ID	Zone	Name	IPv4 Address	IPv6 Address	Secondary
<input checked="" type="checkbox"/>	30	Trusted	Computers	192.168.40.100/24 (DHCP serv...		
<input checked="" type="checkbox"/>	20	Trusted	Private wifi	192.168.35.100/24 (DHCP serv...		
<input checked="" type="checkbox"/>	10	Optional	Public wifi	192.168.30.100/24 (DHCP serv...		
<input checked="" type="checkbox"/>	100	Trusted	management	192.168.25.100/24 (DHCP serv...		

FIGUUR 13: TAGGED INTERFACE

### 3.1.3 Firewall regels

Alleen de VLAN's instellen is niet genoeg. We moeten nu ook regels aanmaken wat deze VLAN's mogen en wat niet. Het is belangrijk dat een Firewall de regels van boven naar onder leest. Als er op de eerste lijn staat dat we niet mogen surfen naar een bepaalde website dan zal dit effectief uitgevoerd worden ook als er een regel later staat dat dit wel mag. Vandaar is de soort regel en de positie zeer belangrijk. Hier onder zal ik de regels uitleggen die ik heb ingesteld.

Regel 1 FTP: Deze regel laat het toe om van een any-trusted of een any-optional naar een any-external te verbinden over poort 21. Poort 21 wordt gebruikt voor FTP-servers (fileservers)

Regel 2 allow computers - management: Deze regel laat toe dat de gebruikers in VLAN30 naar any-external, any trusted mogen surfen. De policy Type is een http-proxy. Deze wordt gebruikt om naar alle websites die buiten het netwerk liggen te verbinden over poort 80. Op deze regel heb ik ook een webblocker actief gezet en de application control staat ook actief. Later komen we terug op de instellingen hiervan.

Regel 3 allow-port-443: Deze regel laat toe dat gebruikers uit VLAN 30 en gebruikers uit VLAN 20 toegang hebben naar VLAN 100. Dit komt omdat de systeem administrators ook in deze VLAN zitten en als ze toegang nodig hebben tot de server er zo connectie kunnen naartoe maken. Op deze regel staat ook een application control en webblocker ingesteld.

Regel 4 allow Computers – mangement: Deze regel laat toe dat de gebruikers in VLAN30 naar any-external, any trusted mogen surfen. De policy Type is een https-proxy. Deze wordt gebruikt om naar alle websites die buiten het netwerk liggen te verbinden over poort 443. Op deze regel heb ik ook een webblocker actief gezet en de application control staat ook actief. Later komen we terug op de instellingen hiervan.

Regel 5 Allow RDP: Deze regel laat toe om een Remote Desktop protocol (RDP) te starten naar één van de servers. Deze regel is alleen voor de gebruikers uit VLAN 30 die naar VLAN 100 willen een verbinding maken. Door deze regel staat poort 3389 open. Op deze regel staat ook een application control ingesteld.

Regel 6 en regel 7: Dit zijn automatisch gegenereerde regels van Watchguard. Deze zorgen ervoor dat de authenticatie goed verloopt.

Regel 8 allow port - 8080: deze regel laat het toe om vanaf VLAN 30 en VLAN 20 naar VLAN 100 te surfen over poort 8080. Op deze regel staat ook een application control ingesteld.

Regel 9: Dit is een automatisch gegeneerde regel die ervoor zorgt dat we de Watchgaurd Web UI kunnen raadplegen.

Regel 10 allow port - 8443: Deze regel laat de connectie tussen VLAN 30 en VLAN 100 over poort 8443 toe. Dit is omdat de AP moet geadopteerd worden in de Unifi

Controller. Als deze poort niet open staat dan kunnen we niet de AP in onze Unifi controller adopteren en zal er dus ook geen wifi zijn. Op deze regel staat ook een application control ingesteld.

Regel 11 DNS-proxy-firebox: Deze regel is een DNS-proxy. Alle regels die in de Firewall komen zullen worden bekeken. Indien nodig zal onze Watchguard er zelf een DNS aan toevoegen. Dit geld alleen op het verkeer dat effectief wordt verstuurd naar de Watchguard.

Regel 12 DNS-proxy-DomainController: Hier zal al het verkeer dat vanuit de domaincontroller komt de DNS gegevens meekrijgen van de Domain Controller.

Regel 13: DNS-proxy-Blocked: Indien er geen match is met regel 11 en regel 12 worden de IP-pakketjes gedropt.

Regel 14 denied-Ping: Deze regels blokkeert het pingen van VLAN 30 naar het IP-adres 192.168.30.100. Dit doen we om een distributed-denial-of-service (DDOS) aanval tegen te gaan. Op deze regel staat ook een application control ingesteld.

Regel 15 ping: Dit is een automatisch gegeneerde regel die het pingen naar andere toestellen toelaat.

Regel 16: Dit is een automatisch gegeneerde regel die het toelaat om de Watchguard policy manager te raadplegen. Op deze regel staat ook een application control ingesteld.

Regel 17 Domain join: Deze regel laat het toe om de computers een domein te laten joinen. Deze regel zorgt dat er verschillende poorten worden opengezet.

Regel 18 Outgoing: Dit is een automatisch gegeneerde regel die het overige verkeer doorlaat.

Order /	Action	Policy Name	Policy Type	From	To	Port	PBR	SD-WAN	App Control	Geolocation	Tags
1	✓	FTP	FTP	Any-Trusted, Any-Optional	Any-External	tcp:21		None	Global		
2	✓	allow Computers - management	HTTP-proxy	VLAN30 - Computers	Any-External, Any-Trusted	tcp:80		praktijkproject	Global		
3	✓	allow-port-443	allow-port-443	VLAN30 - Computers, VLAN20 - Private-Wifi	VLAN100 - Management	udp:443		praktijkproject	Global		
4	✓	allow Computers - management	HTTPS-proxy	VLAN30 - Computers	Any-External, Any-Trusted	tcp:443		praktijkproject	Global		
5	✓	Allow RDP	RDP	VLAN30 - Computers	VLAN100 - Management	tcp:3389		praktijkproject	Global		
6	✓	WG-Auth-WebBlocker	WG-Auth	Any-Trusted, Any-Optional	Firebox	tcp:4100		None	Global		
7	✓	WatchGuard Certificate Portal	WS-Cert-Portal	Any-Trusted, Any-Optional	Firebox	tcp:4126		None	Global		
8	✓	allow-port-8080	allow-port-8080	VLAN30 - Computers, VLAN20 - Private-Wifi	VLAN100 - Management	tcp:8080		praktijkproject	Global		
9	✓	WatchGuard Web UI	WG-Fireware-XTM-WebUI	Any-Trusted, Any-Optional	Firebox	tcp:8080		None	Global		
10	✓	Allow-port-8443	Allow-port-8443	VLAN30 - Computers	VLAN100 - Management	tcp:8443		praktijkproject	Global		
11	✓	DNS-proxy_Firebox	DNS-proxy	Any-Trusted, Any-Optional	Firebox	tcp:53 udp:53		Global	Global		
12	✓	DNS-proxy_DOMAINCONTROLLER	DNS-proxy	DOMAINCONTROLLER	Any-External	tcp:53 udp:53		Global	Global		
13	✓	DNS-proxy_BLOCKED	DNS-proxy	Any-Trusted, Any-Optional	Any	tcp:53 udp:53		None	Global		
14	✗	denied-Ping	Ping	VLAN30 - Computers	192.168.30.100	icmp (type: 8, ...)		praktijkproject	Global		
15	✓	Ping	Ping	Any-Trusted, Any-Optional	Any	icmp (type: 8, ...)		None	Global		
16	✓	WatchGuard	WS-Firebox-IGMPT	Any-Trusted, Any-Optional	Firebox	tcp:4105 tcp:4...		praktijkproject	Global		
17	✓	domain join	domain join	VLAN30 - Computers	VLAN100 - Management	tcp:88 tcp:135...		praktijkproject	Global	Global	
18	✓	Outgoing	TCP-UDP	Any-Trusted, Any-Optional	Any-External	tcp:0 (Any) u...		None	Global		

FIGUUR 14: REGELS FIREWALL

### 3.1.4 Instellingen subscription services

In hoofdstuk 2.2 legde ik uit wat alle subscription services doen. Hieronder laat ik zien welke ik gebruik heb en waarom ik deze gebruik heb.

- Webblocker

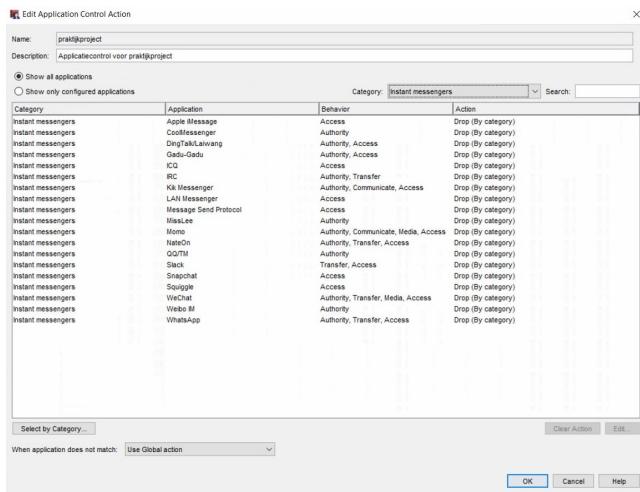
Als eerste stelde ik de webblocker in. Deze policy gaan de eindgebruikers het meest mee in aanraking komen omdat dit gaat over welke websites ze al dan niet mogen raadplegen. Op de foto hieronder ziet u dat er onder andere abortion, adult material, bandwidth en drugs wordt geblokkeerd. Vanaf de eindgebruiker een site raadpleegt met deze categorie zal die worden geblokkeerd. Deze webblocker stelde ik in bij mijn http en https-proxy. Dit komt omdat al het verkeer van websites over poort 80 of 443 loopt. Als ik daar mijn webblocker op actief zet dan weet ik zeker dat elke website gefilterd wordt.

praktijkproject						
webblocker voor praktijkproject						
Categories Exceptions Advanced Alarm Server						
Action	Category	Subcategory	Override	Alarm	Log	Quick Action
Deny	Abortion	Abortion	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Deny	Abortion	Pro-Choice	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Deny	Abortion	Pro-Life	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Deny	Adult Material	Adult Material	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Deny	Adult Material	Adult Content	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Deny	Adult Material	Lingerie and Swimsuit	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Deny	Adult Material	Nudity	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Deny	Adult Material	Sex	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Deny	Adult Material	Sex Education	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Deny	Advocacy Groups	Advocacy Groups	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Allow	Bandwidth	Bandwidth	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Allow	Bandwidth	Educational Video	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Allow	Bandwidth	Entertainment Video	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Allow	Bandwidth	Internet Radio and TV	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Allow	Bandwidth	Internet Telephony	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Deny	Bandwidth	Peer-to-Peer File Sharing	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Allow	Bandwidth	Personal Network Storage and Backup	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Deny	Bandwidth	Streaming Media	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Allow	Bandwidth	Surveillance	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Allow	Bandwidth	Viral Video	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Allow	Business and Economy	Business and Economy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Allow	Business and Economy	Financial Data and Services	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Allow	Business and Economy	Hosted Business Applications	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Allow	Collaboration - Office	Collaboration - Office	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Deny	Drugs	Drugs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Deny	Drugs	Abused Drugs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

**FIGUUR 15: WEBBLOCKER**

- Application control

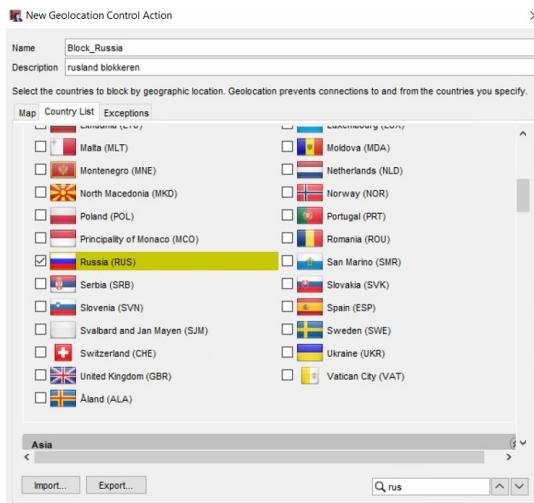
Na de webblocker stelde ik application control in. De reden hier is ook zoals bij de webblocker. De eindgebruikers zullen hier het meeste mee in aanraking komen. Met application control kunnen we verschillende functies uitschakelen op een website. Ik schakelde de onder andere instant messengers uit. Vanaf een website een bericht wilt sturen zal dit nu worden geblokkeerd.



**FIGUUR 16: APPLICATION CONTROL**

- Geolocation

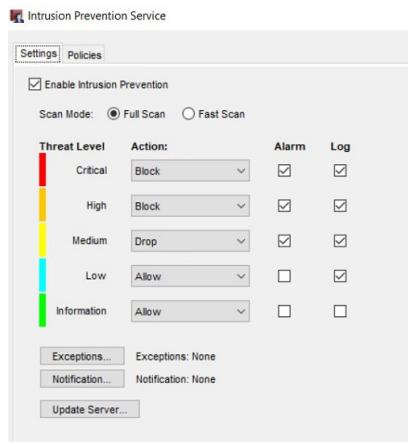
Hier heb ik besloten om alle websites die uit Rusland komen te blokkeren. Dit komt omdat daar vreemde websites zijn met al dan niet fake nieuws en malware. Deze staat ook actief op de http en https-proxy omdat daar al het verkeer over loopt.



**FIGUUR 17: GEOLOCATION**

- Intrusion prevention Service

Hier stelde ik in dat alles van een critical, high en medium level moet worden geblokkeerd. Daarnaast moet ook alles gelogd worden. Ook moet er altijd een full scan gebeuren in plaats van een fast scan. Dit kost iets meer tijd maar de risico's zijn dan ook minder.

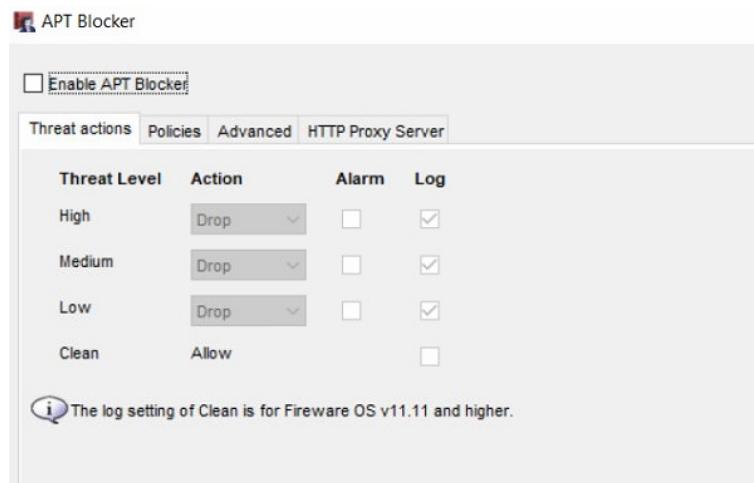


**FIGUUR 18: INTRUSION PREVENTION**

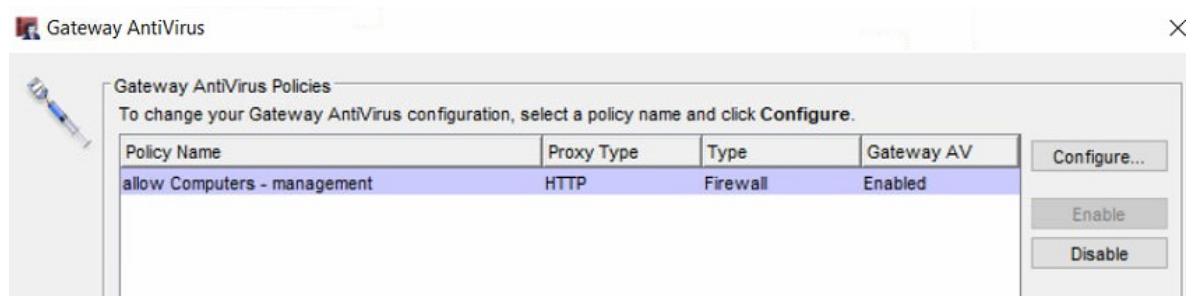
- APT blocker en Gateway antivirus

Daarna wou ik APT blocker instellen. Het probleem hier is dat deze samenwerkt met de functie gateway antivirus. Ik stelde eerst gateway antivirus in. Dit deed ik op de http-proxy. Dit komt omdat deze voor http-proxy is gemaakt en niet voor de https proxy.

Daarna vinkte ik APT blocker aan en stelde in dat hij altijd de pakketjes moest droppen. Het probleem hier was dat ik op een beta software werk van Watchguard. Als ik na het instellen kreeg ik een foutmelding dat een PDF-file niet kon worden gevonden. Dit is nog een bug in de software. Ik maakte daarom een case aan bij Watchguard.



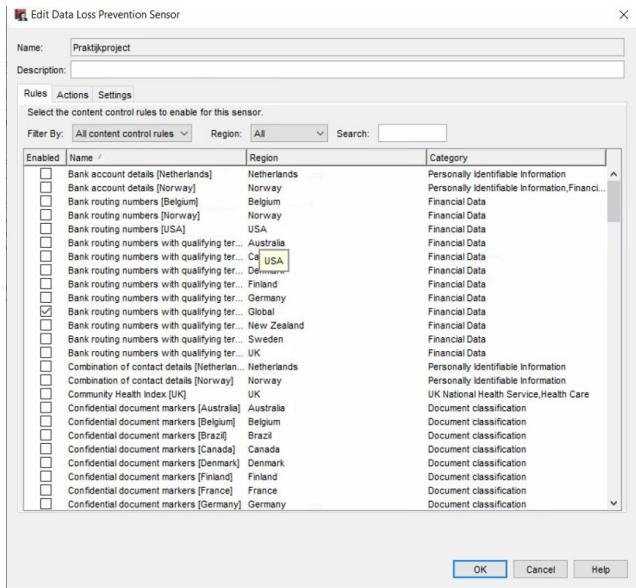
FIGUUR 19: APT BLOCKER



FIGUUR 20: GATEWAY ANTIVIRUS

- Data loss prevention

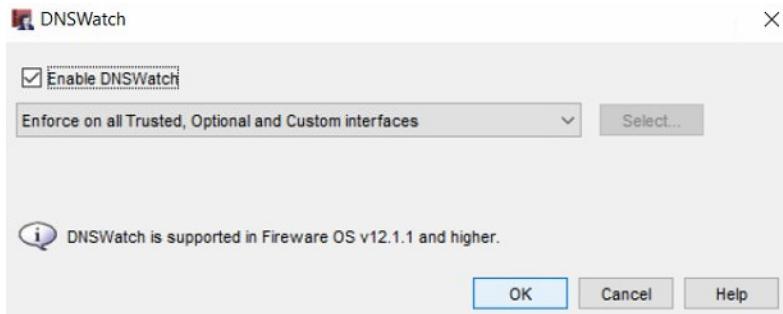
Hier stelde ik in dat er vooral moet gekeken worden naar bankgegevens. Ook stelde ik in dat er niet moet worden gekeken naar een specifieke regio. Er moet gemonitord worden over heel de wereld. Dit is ook zo ingesteld voor vertrouwelijke data.



**FIGUUR 21: DATA LOSS PREVENTION**

- DNSwatch

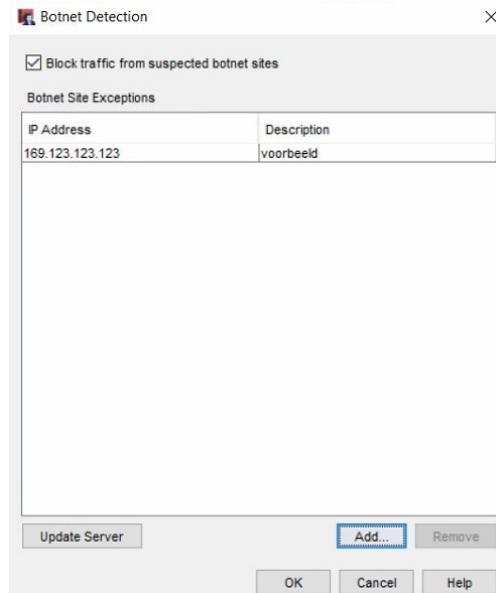
Ik schakelde dit in op alle trusted, optional en custom interfaces.



**FIGUUR 22: DNSWATCH**

- Botnet detection

Hier stelde ik een fictief IP-adres in van een eventueel botnet. Als het bedrijf al eens aangevallen door een botnet of als iemand een IP-adres kent van een botnet kan deze hier worden geblokkeerd.



**FIGUUR 23: BOTNET DETECTION**

## 3.2 De netwerkswitch

Op de netwerkswitch maakte ik enkele VLAN's aan. Deze dienen om structuur en logica te brengen in mijn netwerk. Ikzelf maakte op de netwerkswitch 4 VLAN's aan: VLAN 100, VLAN 10, VLAN 20 en VLAN 30.

VLAN 100 is het virtuele netwerk voor de management toestellen. De IP-range in deze VLAN is 192.168.25.1/24. Hierin zit de server en de Acces Point. De VLAN is getagged op poort 10, 23 en 24. Dit komt omdat de Acces Point is ingeplugged in poort 10, de server is ingeplugged in poort 23 en de uplink van de switch die van de firewall komt is ingeplugged in poort 24. Dit dient allemaal tagged verkeer te zijn

omdat we hier spreken over management toestellen en omdat de firewall ook tagged verkeer verwacht.

VLAN 10 is het virtuele netwerk voor de publieke wifi. De IP-range in deze VLAN is 192.168.10.1/24. Dit wifi netwerk is opgesteld voor bezoekers die het bedrijf zouden bezoeken. Omdat de Acces Point al in een tagged VLAN zit heb ik op poort 10 gekozen voor untagged. Zo is het wel mogelijk om de netwerken te scheiden en de Acces Point in het management VLAN te laten zitten. Op poort 24 is VLAN 10 ook getagged. Dit komt omdat de interface op de firewall ook staat op tagged verkeer ontvangen.

VLAN 20 is het virtuele netwerk voor de private wifi. De IP-range in deze VLAN is 192.168.20.1/24. Dit is het wifi netwerk voor de werknemers van het bedrijf. Zoals bij VLAN 10 is hier ook VLAN 20 untagged op poort 10 omdat de Acces Point al getagged is. Daarnaast is VLAN 20 getagged op poort 24 omdat deze de uplink naar de firewall verzorgt en de firewall tagged verkeer wil ontvangen.

VLAN 30 is het virtuele netwerk voor de computers. Op die poorten zitten alleen computers. De VLAN is enkel op poort 24 getagged omdat de firewall ook hier tagged verkeer verwacht. Op alle andere poorten is deze VLAN untagged. Dit komt omdat enkel speciale netwerkkaarten tagged verkeer kunnen verdragen. Deze zitten meestal in management toestellen. Omdat de meeste computers dit niet hebben stellen we untagged verkeer in. Daardoor komt deze toch in de VLAN en doordat poort 24 tagged is zal het verkeer goed terechtkomen op de firewall.

Om dit te configureren in de netwerkswitch gebruikte ik de volgende commando's: als eerste gaan we naar de configurerbare pagina met het commando 'enable', daarna gaan we naar het tablad om de switch in te stellen met het commando 'configuration terminal', daarna maken we een VLAN aan door VLAN XX in te typen

(de X wordt vervangen door het nummer van de VLAN). Daarna kunnen we kiezen voor tagged en untagged verkeer. Dit doen we met het commando tagged X of untagged X (X staat voor een getal). Om te controleren of de poorten juist staan gebruiken we het commando show VLAN xx (xx staat voor getal).

```
HP-2530-24-PoEP# configure terminal
HP-2530-24-PoEP(config)# vlan 30
HP-2530-24-PoEP(vlan-30)# tagged 24
HP-2530-24-PoEP(vlan-30)# untagged 1
HP-2530-24-PoEP(vlan-30)#[REDACTED]
```

FIGUUR 24: VLAN AANMAKEN, TAGGED, UNTAGGED

```
HP-2530-24-PoEP(vlan-30)# show vlan 30

Status and Counters - VLAN Information - VLAN 30

VLAN ID : 30
Name : VLAN30
Status : Port-based
Voice : No
Jumbo : Yes

Port Information Mode      Unknown VLAN Status
----- ----- -----
1           Untagged Learn      Up
2           Untagged Learn      Up
3           Untagged Learn      Down
24          Tagged  Learn      Up

HP-2530-24-PoEP(vlan-30)#[REDACTED]
```

FIGUUR 25: SHOW VLAN

Voor veiligheidsregels heb ik elke poort die niet in gebruik is dicht gezet. Dit deed ik via de volgende commando's: als eerste gaan we naar de configurerbare pagina met het commando 'enable', daarna gaan we naar het tablad om de switch in te

stellen met het commando 'configuration terminal', als dat gedaan is selecteren we de juiste poort met 'interface X' en als laatste schakelen we de poort uit met het commando 'disable'. We kunnen dit controleren door het commando 'show interface brief' te gebruiken.

```
HP-2530-24-PoEP> enable
Your previous successful login (as manager) was on 1990-01-02 02:32:34
from 192.168.30.1
HP-2530-24-PoEP# configure terminal
HP-2530-24-PoEP(config)# interface 15
HP-2530-24-PoEP(eth-15)# disable
```

FIGUUR 26: DISABLE INTERFACE

```
HP-2530-24-PoEP(eth-15)# show interfaces brief

Status and Counters - Port Status

Port Type | Intrusion
           | Alert     Enabled Status Mode
-----+-----+
 1 10/100TX | No       Yes    Up   100FDx  MDI off 0
 2 10/100TX | No       Yes    Up   10FDx   MDI off 0
 3 10/100TX | No       Yes   Down 10FDx   MDI off 0
 4 10/100TX | No       Yes   Down 100FDx  MDI off 0
 5 10/100TX | No       Yes   Down 10FDx   MDI off 0
 6 10/100TX | No       Yes   Down 10FDx   MDI off 0
 7 10/100TX | No       Yes   Down 10FDx   MDI off 0
 8 10/100TX | No       Yes   Down 10FDx   MDI off 0
 9 10/100TX | No       Yes   Down 10FDx   MDI off 0
10 10/100TX | No       Yes   Up   100FDx  MDI off 0
11 10/100TX | No       Yes   Down 10FDx   MDI off 0
12 10/100TX | No       Yes   Down 10FDx   MDI off 0
13 10/100TX | No       Yes   Down 10FDx   MDI off 0
14 10/100TX | No       Yes   Down 10FDx   MDI off 0
15 10/100TX | No       No    Down 10FDx   MDI off 0
16 10/100TX | No       Yes   Down 10FDx   MDI off 0
```

FIGUUR 27: SHOW INTERFACE BRIEF

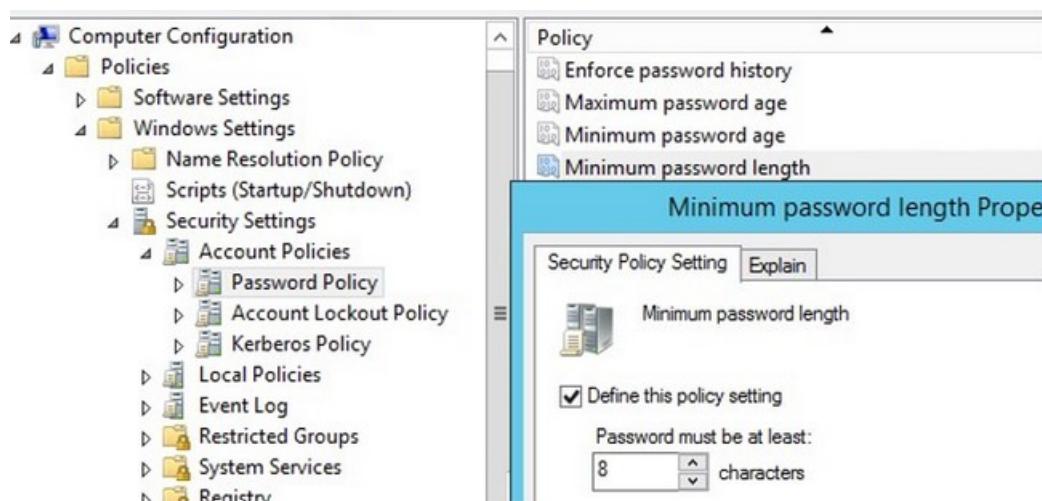
### 3.3 De Supermicroserver

Op de server installeerde ik ESXI. Dit werd besproken in hoofdstuk 2.5. Op deze virtualisatie software liet ik 3 servers draaien. Een Domain Controller, een back-up server en een Unifi controller (Ubuntu 20.04).

### 3.3.1 Domain Controller (DC)

Een domain controller is een server die antwoord biedt op alle authenticatie aanvragen en alle gebruikers op het netwerk. Een domein is een manier om alle gebruikers en computers op een hiërarchische manier te ordenen. Op een DC draait altijd een Active Directory (AD). Dit is het allerbelangrijkste om te beschermen. Als een aanvaller toegang krijgt tot de DC en bij gevolg ook tot de AD kan hij aan alles waar de gebruikers ook aan kunnen. Hij kan de wachtwoorden resetten naar een wachtwoord naar keuze en zo inloggen met verschillende accounts.

Onze DC is een heel kleine versie van een DC voor een bedrijf. Ik maakte maar twee gebruikers aan en gebruikte ook niet veel policies. Ik stelde een password policy in voor als de gebruikers zelf hun wachtwoord willen veranderen. Deze kan wel omzeild worden als je een wachtwoord ingeeft op de DC zelf.

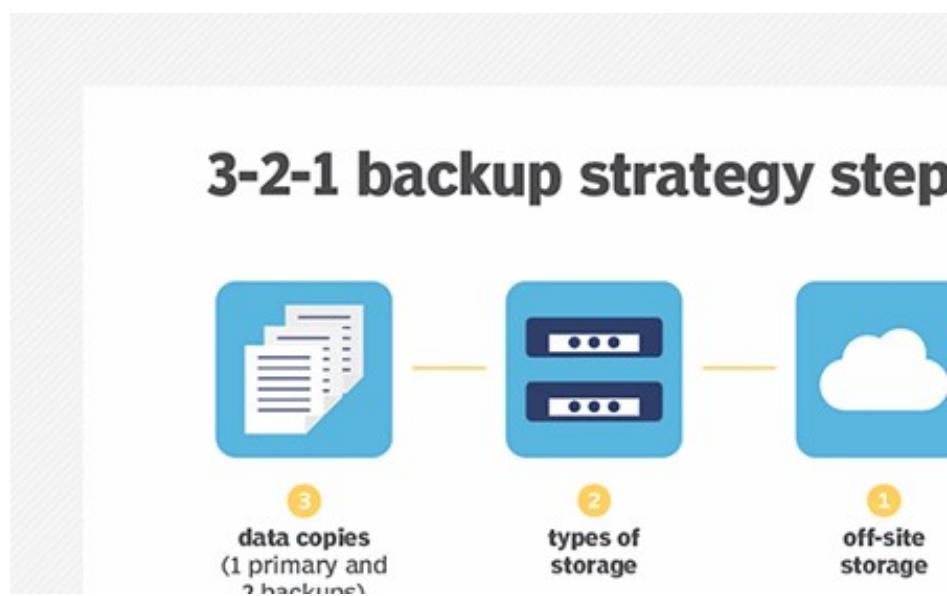


FIGUUR 28: PASSWORD POLICY

Mijn DC fungeert ook als een DNS-server. Dit deed ik om daar wat veiligheid in te bouwen. Dit konden we dan ook meennemen naar de regels die ik instelde op de firewall.

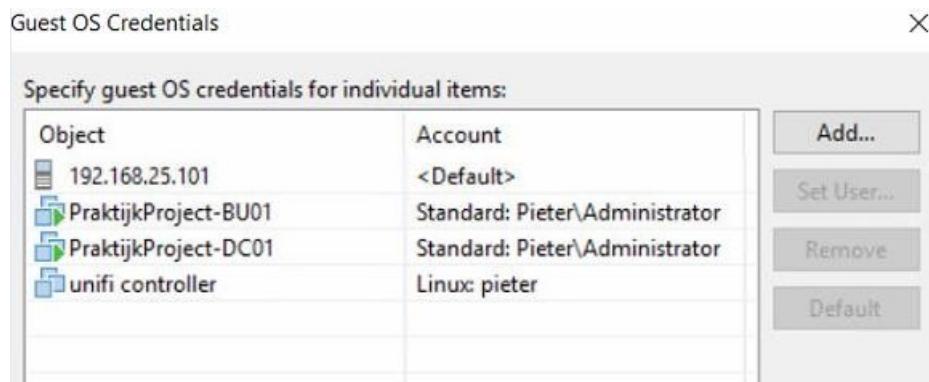
### 3.3.2 Back-up Server

Back-ups zijn zeer belangrijk in een bedrijf. Als er een hacker aanvalt of het gebouw is volledig vernield door een brand dan kunnen we altijd nog de back-ups gebruiken en kunnen de medewerkers nog verder werken. Het is dus belangrijk dat we onze back-ups werken en dat we deze ten allen tijden kunnen raadplegen en gebruiken. De beste back-up strategie is gebaseerd op een regel van drie. We nemen ten allen tijden drie kopies van de data. Eén op de server zelf, één on site en één op een andere locatie. Bij die drie kopies is het belangrijk dat deze niet op dezelfde media zijn geback-upt. Je kan er één uploaden op een harde schijf en een andere op een tape. Het is ook het beste om elke week een full back-up te maken en elke dag een incrementele back-up. Dit wil zeggen dat we elke week onze volledige installatie gaan back-uppen en elke dag alleen de veranderingen gaan back-uppen. Als er dan data loss is kunnen we aan de hand daarvan alles goed terugzetten. Ik werkte ook met 21 restore points. Dit wil zeggen dat ik 21 dagen terug kan gaan om mijn back-up terug te zetten.



FIGUUR 29: 3-2-1 BACK STRATEGIE

Wat ik praktisch deed is verschillend van de best mogelijke manier. Ik installeerde eerst het programma Veeam Back-up and replication. Als eerste moest ik mijn ESXI-server adopteren op deze server. Zo kan ik alles back-uppen. Daarna kan ik alle servers die op de ESXI staan instellen.



FIGUUR 30: BACKUP SERVERS

Omdat ik niet veel data bezit, maak ik gebruik van de daily-monthly-yearly methode. Dit wil zeggen dat ik elke dag een incrementale back-up neem en deze maandelijks naar een tape upload. En daarna ze jaarlijks zal bijhouden. Zo kan je tot jaren terug tot op de maand nauwkeurig al de data terugzetten. In mijn project heb ik daarvoor negen jobs voor nodig. Drie voor de daily routine omdat er drie servers moeten geback-uppt worden. Drie voor de maandelijks routine en drie voor de jaarlijks routine.

### 3.3.3 Unifi Controller (Ubuntu 20.04)

Mijn derde en laatste server is een Ubuntu 20.0 server. Dit is een andere server dan de DC en back-up server. Het operating system (OS) is hier niet Windows maar Linux. Deze server gebruik ik als Unifi Controller. Een Unifi controller is de draadloze managementsoftware waar we al onze wifinetwerken mee kunnen beheren en onze acces points. We kunnen hierin onze SSID veranderen van onze wifi, de

wachtwoorden aanpassen, VLAN's toevoegen aan wifinetwerken, MAC-adres filter toevoegen en nog veel meer. De mogelijkheden gaan heel ver.

De configuratie van mijn wifinetwerken zijn vrij eenvoudig. Ik maakte twee netwerken aan. Project-Public en Project-Private. Aan die twee netwerken gaf ik de juiste VLAN ID mee. Als dat in orde was kon ik mijn wifi netwerken aanmaken. Omdat de netwerken verbonden zijn aan de VLAN's krijgen we als we ermee verbinden een andere IP-range.

### **3.4 De Acces Point**

Aan de AP was er niet zoveel configuratie. Deze moest alleen geadopteerd worden in de Unifi controller. Om dit te kunnen laten slagen moest ik op mijn netwerkswitch de en op de firewall de configuratie aanpassen. Op de switch moest ik VLAN 100 tagged zetten op poort 10 en op de firewall moest ik poort 8443 openzetten. Daarna kon ik via SSH inloggen op de Acces Point en daar via het commando set-inform <http://192.168.25.2:8080/inform> de AP te laten adopteren in de controller.

# 4 Mailboxen

Nadat we in de vorige hoofdstukken effectief de beveiliging en de configuratie van onze componenten bespraken zal ik in dit hoofdstuk de configuratie van de mailboxen en bij gevolg de beveiliging van de mailboxen bespreken.

## 4.1 Microsoft 365

Al onze mailboxen draaien op de services van Microsoft 365. Als we dus willen dat we onze mailboxen kunnen gebruiken met de gebruikers die in mijn AD zitten zullen we deze eerst moeten synchroniseren. Daarvoor heeft Microsoft 365 een handige tool ontwikkeld. Deze moet je downloaden op je DC en daarna de stappen doorlopen. Als die klaar is dan komen na maximaal 48 uur wachten de gebruikers ook in het Microsoft 365 Admin center.

The screenshot shows the 'Active users' section of the Microsoft 365 Admin Center. At the top, there are buttons for 'Add a user', 'Refresh', 'Delete user', 'Reset password', 'Manage product licenses', 'Manage roles', 'Export users', and a '...' menu. To the right, there is a status indicator '1 selected' with a delete icon, a 'Filter' button, a search bar 'Search active users list', and a 'Choose columns' button. The main table lists five users:

Display name	Username	Licenses	Sync status
EFFIX Helpdesk	admin@praktijkprojectPV.onmicrosoft.com	Unlicensed	Cloud
On-Premises Directory Synchroniza...	Sync_PROJECT_0ba17aff856e@praktijkprojectPV.onmicrosoft.com	Unlicensed	Cloud
On-Premises Directory Synchroniza...	Sync_PROJECT-DC01_4538edbc08dc@praktijkprojectPV.onmicrosoft.com	Unlicensed	Cloud
Peter Parker	PeterParker@pieterverheyen.be	Microsoft Defender for Office 365 (Plan 1), Exchange Online	Cloud
Tony Stark	TonyStark@pieterverheyen.be	Office 365 E3, Microsoft Defender for Office 365 (Plan 1)	Cloud

FIGUUR 31: GEBRUIKERS MICROSOFT 365

Daarna kan je aan je gebruikers de nodige licenties koppelen. Ik gebruikte twee verschillende licenties. Als eerste gebruikte ik een Office 365 E3 licentie. Deze licentie koos ik omdat je hier meer beveiligingsopties hebt. Je krijgt Information

Protection, compliance-functies en azure information protection erbij. Als andere licentie koos ik voor een microsoft defender for Office 365. Deze licentie laat ons toe om via Microsoft defender onze beveiling in te stellen.

#### 4.1.1 Configuratie Microsoft Defender

Het instellen van de Microsoft Defender lijkt in eerste instantie zeer complex. Als we het admin center openen staat alles zeer vol en is het moeilijk uit te maken waar we wat instellen. Bijna alles van mijn instellingen staat onder het kopje "Threat management". De eerste en voor mij ook één van de belangrijkste policies is de anti-phising policy. Deze zal ervoor zorgen dat de meeste phising e-mails eruit zullen gefilterd. Ik stelde in dat de e-mail moet in quarantaine gezet worden als deze als phising wordt gedetecteerd.

The screenshot shows the 'Edit your policy test' interface. At the top, there are buttons for 'Delete policy', 'Increase Priority', and 'Decrease Priority'. Below this, the 'Applied to' section is set to 'pieterverheyen.be'. The main table lists policy rules under 'Impersonation' and 'Spoof' categories. Under 'Impersonation', rules include 'Users to protect' (2 users), 'Protect all domains I own', 'Protect specific domains', 'Action > User impersonation', 'Action > Domain impersonation', 'Safety tips > User impersonation', 'Safety tips > Domain impersonation', 'Safety tips > Unusual characters', 'Mailbox intelligence', 'Mailbox Intelligence > Protection', and 'Mailbox Intelligence > Action'. Under 'Spoof', rules include 'Spoof intelligence', 'Unauthenticated sender > ? symbol', and 'Action'. Each rule has an 'Edit' button next to it.

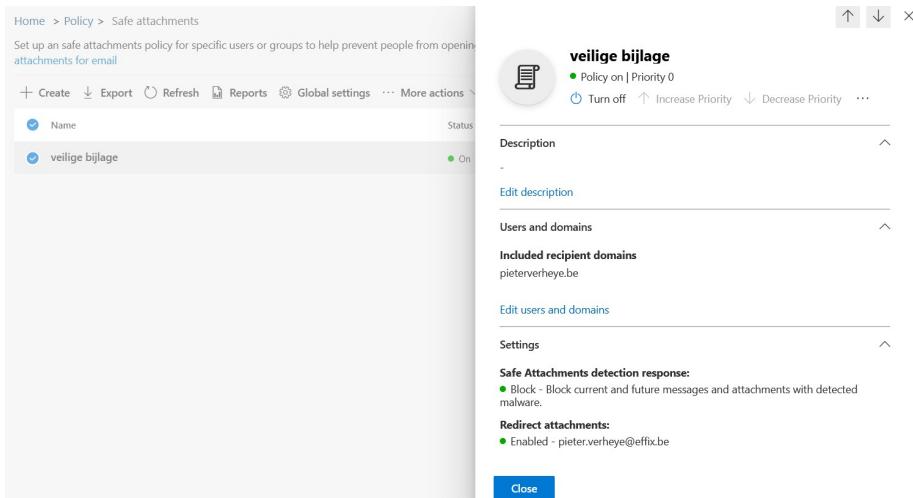
FIGUUR 32: ANTI-PHISING

De policy die ik daarna instelde was de Anti-spam policy. Deze zal ervoor zorgen dat er geen spam e-mails zullen toekomen. Ik gebruikte hiervoor de standaardinstellingen. Dit komt omdat er niet veel extra opties zijn. Je kan instellen op welke gebruikers deze niet actief moet zijn maar dit is hier niet van toepassing omdat we spam e-mails overal willen blokkeren.

Anti-spam settings			
Use this page to configure various anti-spam policies that control how messages are handled by Office 365 anti-spam. These policies include how messages identified as spam, bulk or phish are handled, settings for outbound messages including sending limits, and settings to control spoof intelligence. <a href="#">Learn more about anti-spam settings</a>			
<a href="#">+ Create a policy</a>		<a href="#">+ Create an outbound policy</a>	
Name	On	Type	Priority
Default spam filter policy (always ON)	<input checked="" type="checkbox"/>		Lowest
Connection filter policy (always ON)	<input checked="" type="checkbox"/>		Lowest
Outbound spam filter policy (always ...)	<input checked="" type="checkbox"/>		Lowest
Spoof intelligence policy	<input checked="" type="checkbox"/>		Lowest

**FIGUUR 33: ANTI-SPAM**

Daarna zorgde ik ervoor dat er geen geïnfecteerde bijlagen of verkeerde URL linken in ons netwerk binnengingen. Dit zijn twee verschillende policies maar lijken heel erg op elkaar. Bij de policy voor veilige bijlagen stelde ik in dat de verzender van een e-mail met een slechte bijlage zou worden geblokkeerd van het netwerk en dat er een e-mail wordt gestuurd naar de administrator. Zo kunnen fouten die gemaakt worden door het systeem direct rechtgezet worden. Bij safe links stelde ik in dat elke URL moet worden gescand en ik vinkte uit dat we kunnen zien waar de gebruiker op klikt.



FIGUUR 34: VEILIGE BIJLAGE

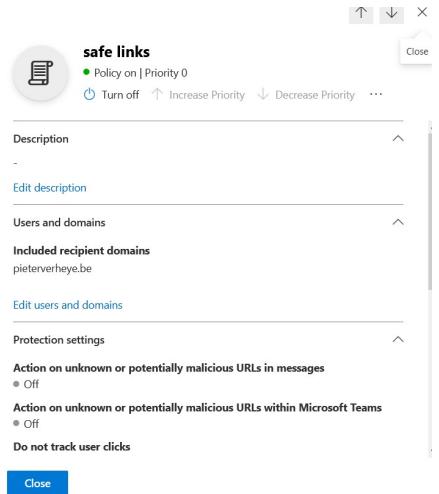
Home > Policy > Safe links

Safe Links helps prevent your users from following links in email and documents that go to web sites specific users in your organization interact with. Learn more about Safe Links

+ Create ⏪ Export ⏪ Refresh Reports Global settings More actions

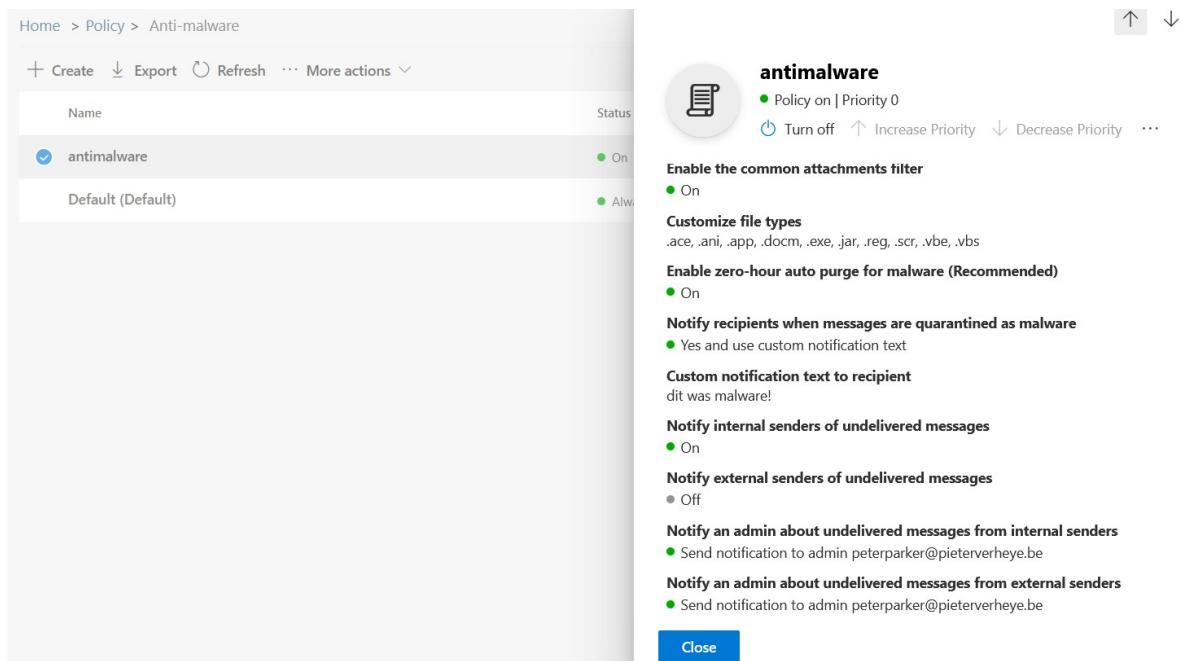
Name Status

safe links On



FIGUUR 35: SAFE LINKS

Als laatste stelde ik een anti-malware policy in. Deze zal ook alle bestanden en URL's scannen op potentiële malware. Het zorgt ervoor dat we geen virussen of andere slechte bestanden toelaten op ons netwerk.



FIGUUR 36: ANTI-MALWARE

Al deze instellingen zijn terug te vinden op het dashboard onder Threat management. Het enige nadeel aan Office 365 Security & Compliance is dat we ons dashboard niet zelf kunnen maken. Dit wil dus zeggen dat op ons dashboard nog allerlei andere niet nuttige zaken staan. Dit maakt het monitoren wat moeilijker. Ook worden de grafieken niet altijd geüpdateerd waardoor we niet direct kunnen zien hoeveel spam, fishing en malware er is onderschept.

## Insights



### Likely spoofed domains over the past 7 days

0 domains were likely impacted within your organization by senders attempting to spoof

0

#### Suspicious domains

Spoof intelligence had good signals that these domains may be suspicious

0

#### Nonsuspicious domains

Spoof intelligence had good signals that these domains should pass extended authentication checks



### Impersonations over the past 7 days

Impersonation intelligence protected the domains and users below

0

#### Domains Impersonated

Domain Protection includes domains you own and custom domains

0

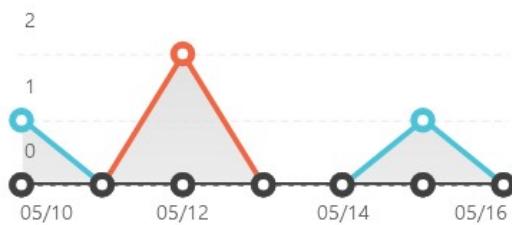
#### Users Impersonated

Protected users must be configured in an impersonation policy

## Trends

### ✉ Sent and received email

...



### ✉ Mailflow status report



FIGUUR 37: DASHBOARD O365

Verder is er op elk account een Multi Factor Authentication actief (MFA). Dit wil zeggen dat we telkens met het wachtwoord en een andere manier. Dit kan met de Microsoft Authenticator app of via het krijgen van een code per sms, het kan ook zijn dat je gebeld wordt. Dan moet je bepaalde toetsen indruwen. Dit zorgt ervoor dat als mensen met slechte bedoelingen je wachtwoord onderscheppen nog altijd de MFA op één of andere manier moeten omzeilen.



admin@praktijkprojectpv.onmicrosoft.com

## Aanmeldingsaanvraag goedkeuren

- 🔒 Open uw Microsoft Authenticator-app en keur de aanvraag om u aan te melden goed.

Hebt u problemen? [Meld u op een andere manier aan](#)

[Meer informatie](#)

**FIGUUR 38: MULTI FACTOR AUTENTICATION**

# 5 Overige beveiliging

---

We kunnen onze installatie en ons netwerk heel erg goed softwarematig beveiligen maar het is ook belangrijk dat we de hardware beveiligen en de gebruikers op de hoogte stellen van mogelijke gevaren. Dit zullen we in dit hoofdstuk bespreken.

## 5.1 Hardware beveiligen

Het is zeer belangrijk dat we onze hardware beveiligen. Als we dit niet doen dan kunnen mensen zomaar fysiek aan onze hardware. Uiteraard kunnen ze dan veel dingen verkeerd doen, denk maar aan het stelen van de harde schijven of de installatie gewoon kapot maken. Ook zijn die mensen al een stap dichter bij het ontmantelen van de softwarematige beveiliging. Hardware matig dingen beveiligen is eigenlijk zeer simpel. Het is belangrijk dat op elke serverkast een slot zit en deze dan ook gesloten is, ook leggen we best de sleutel op een andere plaats dan het serverlokaal. Een slot op de serverkast is handig maar het serverlokaal sluiten is ook belangrijk. Zodat alleen geautoriseerde gebruikers het serverlokaal binnen kunnen. Om dit te kunnen monitoren is het ook handig om een alarm en camerabewaking te hebben. Zo kan ten allen tijden het toetreden van het serverlokaal in de gaten worden gehouden.

## 5.2 Opleiden van eindgebruikers

Het is verder ook zeer belangrijk dat we de eindgebruikers opleiden. Zo kunnen we tegengaan dat ze het slachtoffer worden van social engineering hierop gaan we het volgende hoofdstuk dieper op in. Ook is het belangrijk dat we ze aanleren hoe we

een phising e-mail herkennen en wat we ermee doen als we deze zien. Het aantonen dat niet alles op het internet veilig is, en dat niet elke link op google veilig is is belangrijk. Als IT'er is het belangrijk om het niveau van de eindgebruikers te kennen zodat we daarop kunnen anticiperen als er dus verdachte bestanden of e-mails in het netwerk binnentreden.

We moeten ze ook aanleren dat niet elke bezoeker goede bedoelingen heeft. Deze kunnen USB-sticks in de computer steken zonder dat de gebruiker het weet en daardoor kan er malware of andere software op het netwerk komen. Ook hier komen we in het volgende hoofdstuk op terug.

# 6 Hacking

---

Het beveiligen van een netwerk is een grote en complexe taak. Omdat dit zo moeilijk en zo ruim is zijn er ook mensen die het netwerk zullen "hacken". Dit weliswaar met goede bedoelingen, om mensen iets bij te leren en mogelijke openingen voor echte hackers te dichten. In dit hoofdstuk bespreek ik wat penetration testing is, welke aanvallen vaak worden gebruikt en waarom het zo belangrijk is dat deze testen worden uitgevoerd in grote bedrijven.

## 6.1 Penetration testing

Penetration testing (pentest) zijn zogezegd white hat hackers die een bedrijf proberen te hacken. White hat hackers zijn mensen met goede bedoelingen. Deze zullen het netwerk van je bedrijf proberen binnen te breken maar zullen verder niets verkeerd doen met de informatie dat ze verkrijgen tijdens dat proces. Deze zijn precies het tegenovergesteld van de black hat hackers. Deze mensen zullen het netwerk van verschillende bedrijven aanvallen voor eigen bestwil. Ze proberen ransomware (het encrypteren van alle bestanden) te plaatsen in bedrijven om zo geld te verdienen.

Een Pentest kan op verschillende manieren gebeuren.

- Vulnerability assessment

Deze test brengt de kwetsbaarheid in kaart. Het identificeert, kwantificeert en brengt de prioriteiten van het netwerk in kaart. Deze test loopt meestal volledig automatisch. Het spoort dus bekende IT-fouten op in het netwerk.

Het nadeel hier is dat er niet wordt verteld of deze zwakheden effectief kunnen worden uitgebuit door black hat hackers. Daarom is dit een lichte versie van het effectief Pentesten. Het geeft wel veel informatie die gebruikt kan worden tijdens een pentest.

- Black box pentest

Deze test wordt uitgevoerd door een white had hacker. Deze heeft op voorhand geen informatie over hoe het netwerk of het bedrijf werkt. Meestal wordt er wel afgesproken welk deel er zal worden getest. De pentester zal het bedrijf aanvallen als een black hat hacker. Deze test geeft een goed algemeen beeld van de beveiliging.

- Grey box pentest

Deze test gaat iets dieper ten opzichte van de black box pentest. Meestal krijgt de pentester een account van een medewerker en wordt er vandaar verder getest. Deze test geeft aan hoe veilig het netwerk is vanuit het perspectief van klanten of van gebruikers. Het geeft ons een indicatie van wat er kan gebeuren als een black hat hacker zo een account in zijn handen krijgt.

- White box pentest

Deze test is de grondigste van de vier. Hier krijgt de pentester alle documentatie van het netwerk dat beschikbaar is. Hierdoor kan hij makkelijker beveiligingsrisico's vinden en deze dan ook verwerken. Deze test is ideaal voor het simuleren van realistische scenario's.

## **6.2 Bekende aanval methoden**

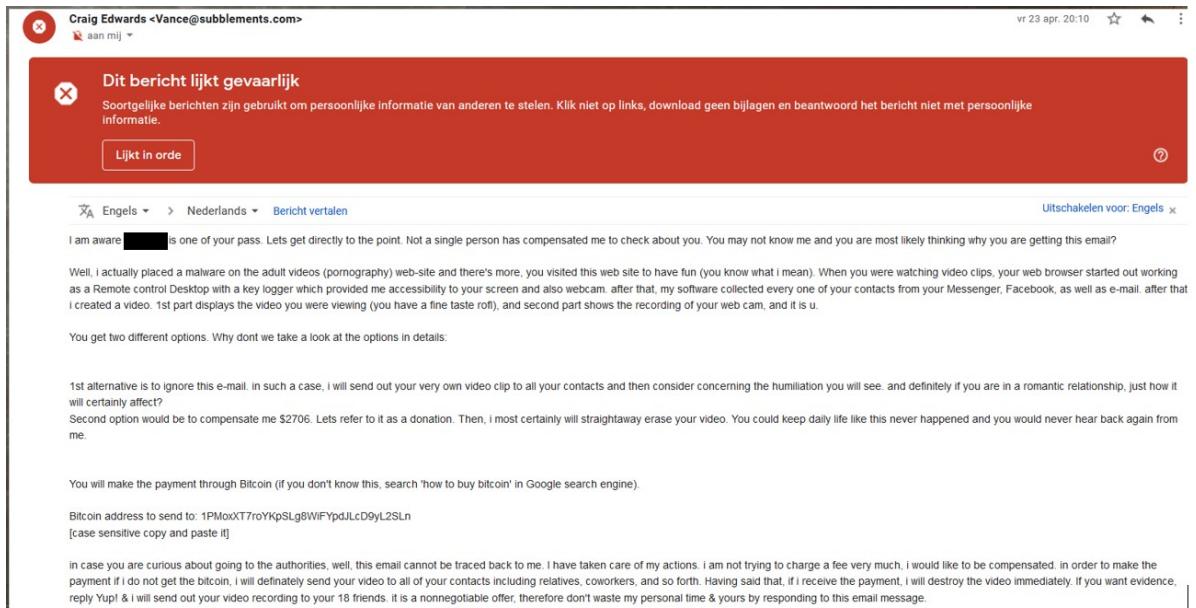
Er zijn enorm veel manieren om een netwerk binnen te dringen. Je kan hier gebruik maken van poorten dat open staan, het manipuleren van gebruikers en het echte aanvallen afvuren.

### **6.2.1 Social engineering**

Dit is één van de bekendste en efficiëntste manieren die er is. De hacker maakt gebruik van de eindgebruikers om zichzelf toegang te geven tot het netwerk of het netwerk plat te leggen. Hier zijn verschillende mogelijkheden voor. Hieronder zal ik de meest voorkomende social engineering manieren beschrijven.

- Phising

Een wel gekende term is phising. Een hacker of criminale zal verschillende e-mails verzenden en doen alsof ze iemand anders zijn of doen alsof ze informatie van u hebben bemachtigd. Dit in de hoop dat er iemand op de link klinkt en zo toegang tot zijn account verleend aan de hacker. Eenmaal de hacker dat wachtwoord heeft is de kans groot dat hij aan nog andere accounts kan. Dit is omdat erg veel mensen dezelfde wachtwoorden gebruiken voor verschillende accounts.



**FIGUUR 39: VOORBEELD PHISING**

- Dumpster diving

Een andere vorm van social engineering is dumpster diving. Dit is letterlijk hetgeen wat het woord zegt: in afval zoeken naar informatie. Dit kan effectief zijn als het bedrijf niet zorgvuldig is met het weggooien van documenten. Als er hier verslagen, brieven, namen met functies, facturen, ... worden gevonden dan kan dit voor iemand met slechte bedoelingen een schat met informatie zijn.

- Shoulder surfing

Shoulder surfing is ook wat het woord zegt. Over de schouder van iemand mee kijken terwijl deze een wachtwoord of pincode ingeeft. Ook meelopen met beveiliging en doen alsof je bij hen hoort is een vorm van Shoulder surfing. De beveiliging staat meestal in het begin van het gebouw. Eenmaal ze toelating gekregen hebben hebben ze vrij spel. Dit gebeurt meestal door een smoes, zoals het meenemen van een ladder, of een grote doos.

- Identity theft

Identity theft is het stelen van iemand zijn/haar identiteit. Dit kan bijzonder veel schade toebrengen aan die persoon. Als de persoon met slechte bedoelingen genoeg informatie heeft kan hij verzekeringen afsluiten, leningen aangaan en bijna alle andere financiële zaken controleren en er gebruik van maken.

- Reverse social engineering

Dit is een iets moeilijkere methode. Het beste is om dit uit te leggen aan de hand van een voorbeeld.

Firma A belt naar firma B en doet alsof het een bedrijf is dat zich specialiseert in het terug halen van verloren data. Firma B verteld dat ze hun gegevens zullen onthouden maar dat ze momenteel geen verloren data hebben en dus ook niet de diensten van firma A zullen gebruiken. Een tijdje later is er plotseling veel data verloren gegaan bij firma B en wordt er gebeld naar firma A om van hun diensten gebruik te maken. Natuurlijk heeft firma A ervoor gezorgd dat er plots zoveel data verloren is gegaan. En nu firma B van hun diensten gebruik maakt kunnen ze geld verdienen en programmatjes installeren dat hun altijd toegang geeft tot het netwerk van firma B.

Reverse social engineering is dus een techniek waarbij de hacker zich voorstelt als specialist. Na de voorstelling zal hij/zij iets breken bij zijn doelwit in de hoop dat ze hem terugbellen om het op te lossen en zo toegang tot hun netwerk geven.

- Een andere vorm van social engineering is het gebruik maken van key-loggers. Dit zijn meestal USB-sticks of software dat wordt geïmplementeerd

door een phising e-mail of als de aanvaller in het bedrijf een USB-stick plaatst in de computer. Als een niet opgeleide gebruiker deze handeling niet ziet dan is de kans groot dat als de aanvaller terugkomt dat hij elk getypt woord kan zien en zo de wachtwoorden en andere gevoelige informatie kan achterhalen.

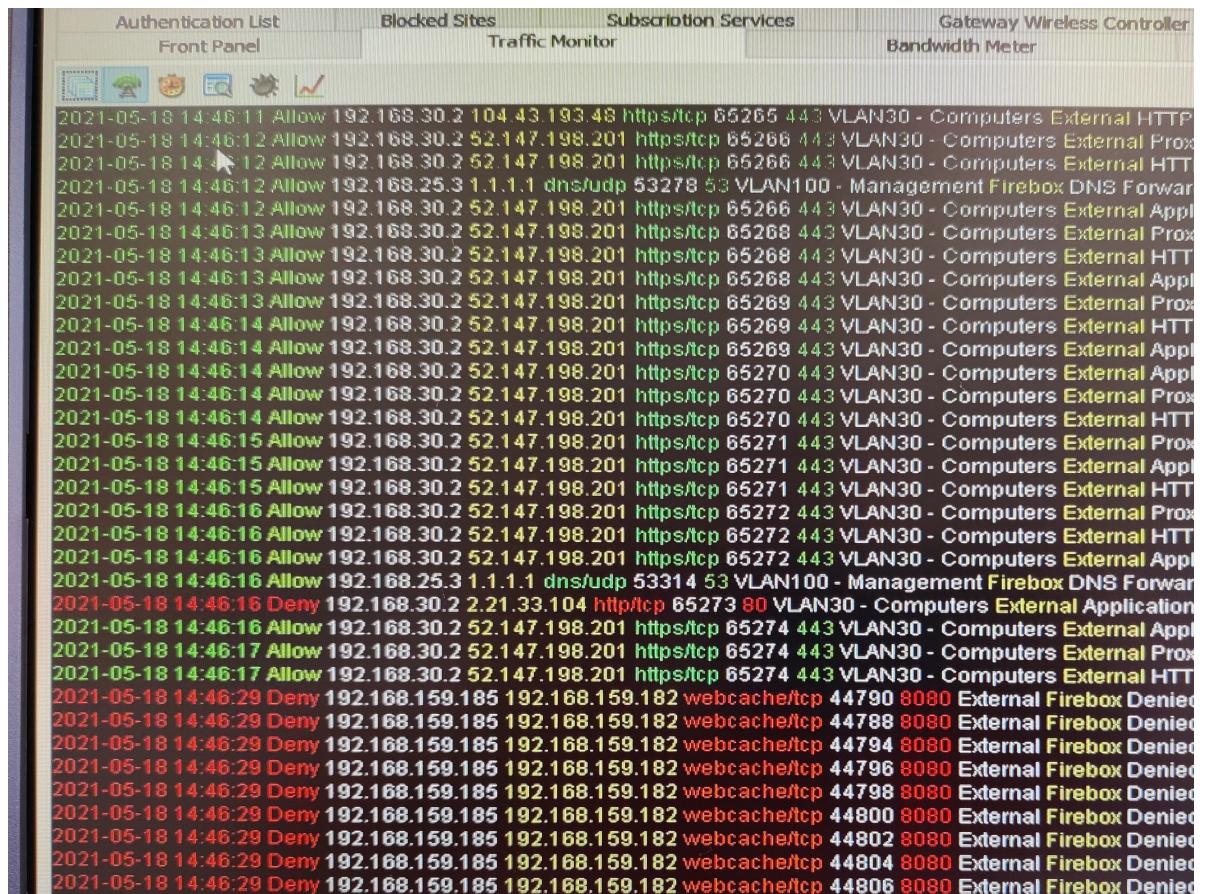
### **6.2.2 Denial-of-Service en distributed denial-of-service attack**

Een Denial-of-Service (DoS) en distributed denial-of-service (DDoS) aanval is een manier om servers, firewalls, computers, ... plat te leggen. Een DoS aanval zorgt ervoor dat er zodanig veel aanvragen toekomen bij bijvoorbeeld een server. Doordat er zoveel aanvragen toekomen wordt het systeem overbelast en kan het niet meer antwoorden op echte aanvragen. Hierdoor wordt het netwerk enorm vertraagd en zal er niets meer werken van software dat op die server draaide. Een DDoS aanval is helemaal hetzelfde als een DoS aanval. Het enige verschil is dat er bij een DDoS aanval niet vanop één computer wordt aangevallen maar vanaf verschillende computers die door de aanvaller worden beheerd. Dit noemen we ook wel een Botnet. Het beste om een DoS en DDoS aanval te begrijpen is om het te vergelijken met een autosnelweg. Als er plots enorm veel auto's op de weg rijden komt er een file en staat iedereen stil. Dit is hetzelfde bij een DoS of DDoS aanval. Als er plots enorm veel aanvragen naar de server komen dan zal hij uitvallen.

Een DDoS of DoS aanval levert de aanvaller geen informatie op of andere voordelen. Het is meestal genoeg voor de aanvaller om de diensten plat te leggen van het bedrijf. Het kan ook zijn dat een DDoS of Dos aanval de voorbode is van een echte aanval. Dit noemen we dan hijacking. Dit wordt later besproken.

Ik voerde een DoS aanval uit op mijn firewall. Daarvoor gebruikte ik als OS Kali Linux. Ik installeerde daarop een tool genaamd GoldenEye. Deze laat het toe om

DoS aanval te doen via het http-protocol. Je kan dan zien in de traffic monitor van mijn firewall dat al deze requesten gedropt worden. Dit komt omdat dit van één computer komt. Als er van verschillende computers zoveel aanvragen komen dan zal, hoe sterk de beveiliging ook is de firewall crashen.



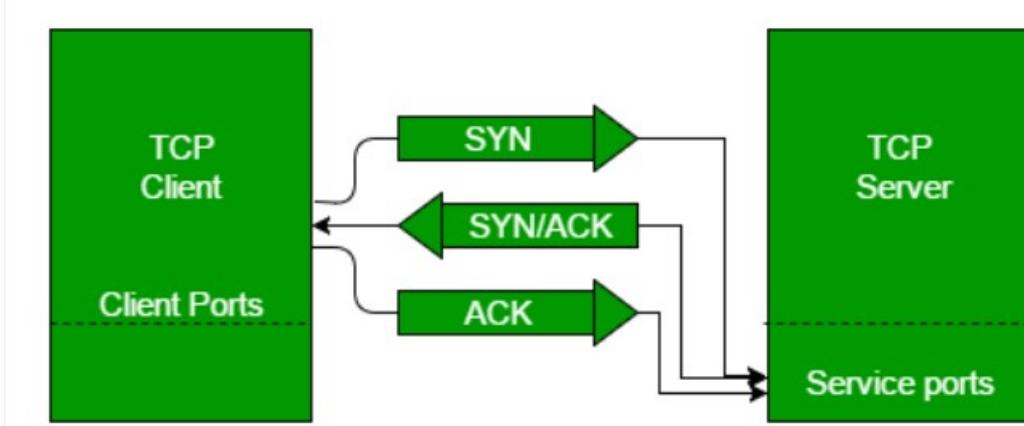
**FIGUUR 40: DoS AANVAL**

Er zijn verschillende manieren om een DDoS of Dos aanval uit te voeren. Hieronder bespreek ik de bekendste.

- TCP SYN flood attack

Deze aanval maakt gebruik van de 3-Way handshake in het TCP-protocol. Het misbruikt de bufferruimte tijdens de handshake. Het apparaat van de aanvaller overspoelt de kleine in-process pakketjes met

verbindingen verzoeken, maar antwoord niet wanneer het systeem op deze verzoeken antwoordt. Dit zorgt voor een time-out. Omdat de buffer van time-outs na enige tijd zal overlopen zal het systeem crashen.



FIGUUR 41: 3-WAY HANDSHAKE

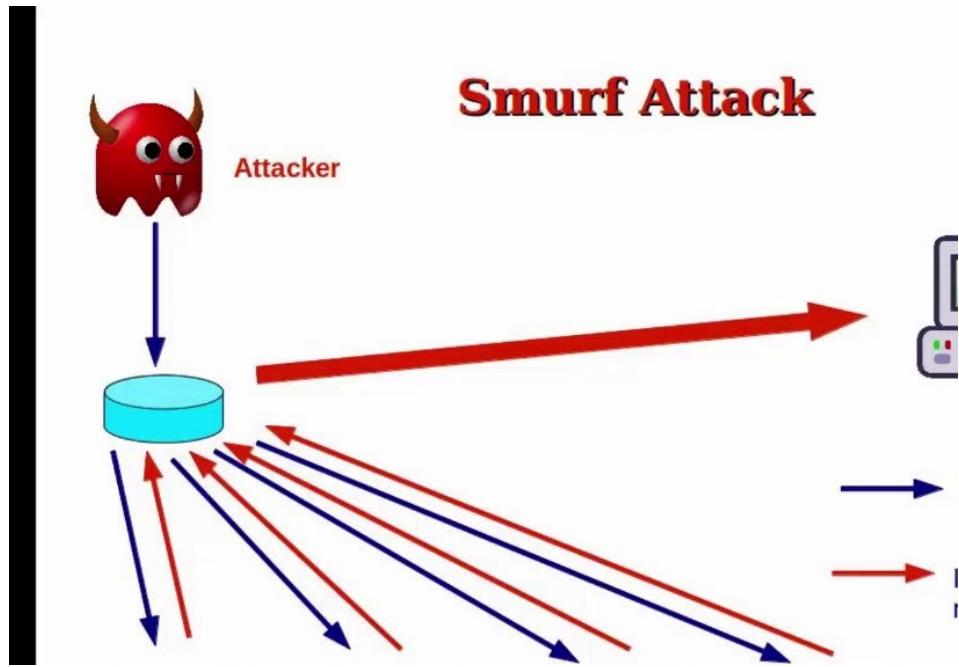
- Teardrop attack

Deze aanval zorgt ervoor dat de lengte en fragmentatie velden in opeenvolgende IP-pakketjes op de aangevallen host elkaar overlappen. Het aangevallen systeem probeert dan deze pakketjes terug goed te krijgen maar dit zal meestal falen. Het aangevallen systeem zal in de war geraken en zal na enige tijd crashen.



**FIGUUR 42: TEARDROP ATTACK** - Smurf attack

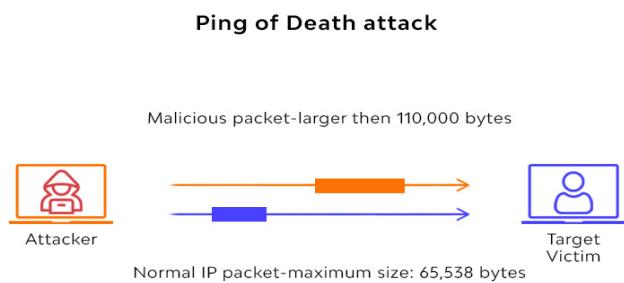
Deze aanval maakt gebruik van IP-spoofing en het ICMP-protocol. Spoofing is je voordoen als iets anders. Bij IP-spoofing doet een computer met IP-adres 192.168.0.1 zich voor als de computer met IP-adres 192.168.0.214. ICMP-protocol dient voor te kunnen pingen naar andere computers. Een smurf attack maakt gebruik van deze twee zaken om het netwerk te kunnen verzadigen met verkeer. Deze methode zal een ICMP-verzoek sturen naar broadcast IP-adressen. Deze ICMP-verzoeken komen van een gespoofed IP-adres. Als het beoogde IP-adres bijvoorbeeld 10.0.0.10 is, zou de aanvaller een ICMP-echo verzoek spoofen van 10.0.0.10 naar het broadcast adres 10.0.0.255/24. Dit verzoek zou naar alle IP's in het bereik gaan, waarbij alle antwoorden teruggaan naar 10.0.0.10, en zo het netwerk overweldigen. Dit proces is herhaalbaar en kan worden geautomatiseerd om enorme hoeveelheden netwerkverkeer te genereren.



**FIGUUR 43: SMURF ATTACK**

- Ping of death attack

Deze aanval gebruikt de manier van pingen om andere systemen hun buffer te laten overlopen. Een ping kan een maximale load van 65535 bytes meedragen. Als de ping een grotere load meedraagt dan zal de ontvanger de IP-pakketjes moeten defragmenteren daardoor kan de buffer vollopen en zal het aangevallen systeem crashen.



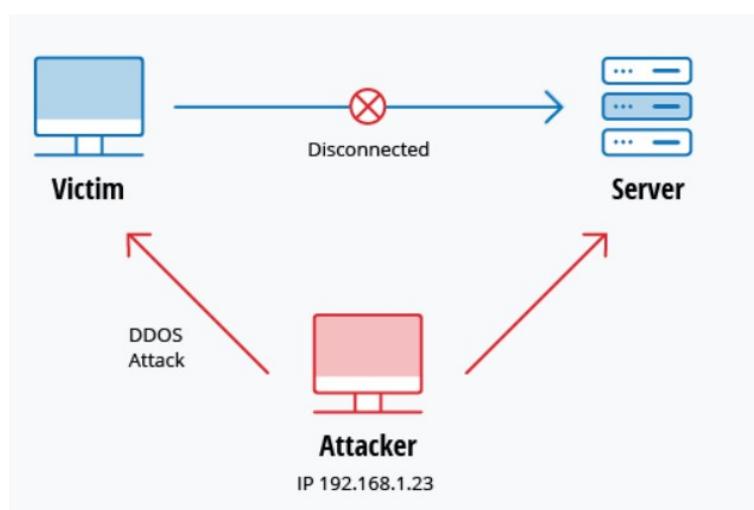
**FIGUUR 44: PING OF DEATH ATTACK**

### 6.2.3 Man-in-the-middle attack

Een man-in-the-middle (MitM) attack is wanneer een hacker zich tussen de effectieve antenne en de gebruiker zit. Zo kan de aanvaller al het verkeer dat de gebruiker naar de antenne stuurt onderscheppen. De eindgebruiker zal hier niks van merken. Ook hier zijn verschillende technieken voor die ik hieronder bespreek.

- Session hijacking

Bij dit type aanval zal de aanvaller zich voordoen als de gebruiker. Dit doet hij door zijn IP-adres te spoofen. Doordat dit lukt zal de server denken dat hij met de vertrouwelijke client aan het communiceren is. Zo kan de aanvaller al het verkeer onderscheppen.

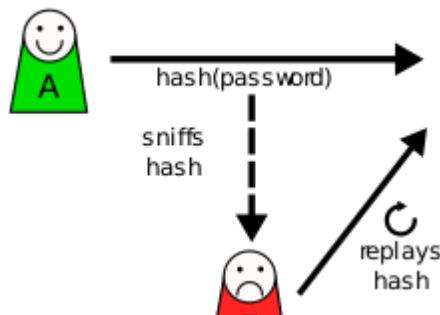


FIGUUR 45: MAN IN THE MIDDLE HIJACKING ATTACK

- Replay attack

Een replay-aanval doet zich voor wanneer een aanvaller oude berichten onderschept en opslaat en ze dan later probeert te versturen, waarbij hij zich voordoet als een van de eindgebruikers. Deze aanval is makkelijk tegen te gaan door sessiontimestamps in te stellen. Het gevaarlijke aan deze aanval is dat

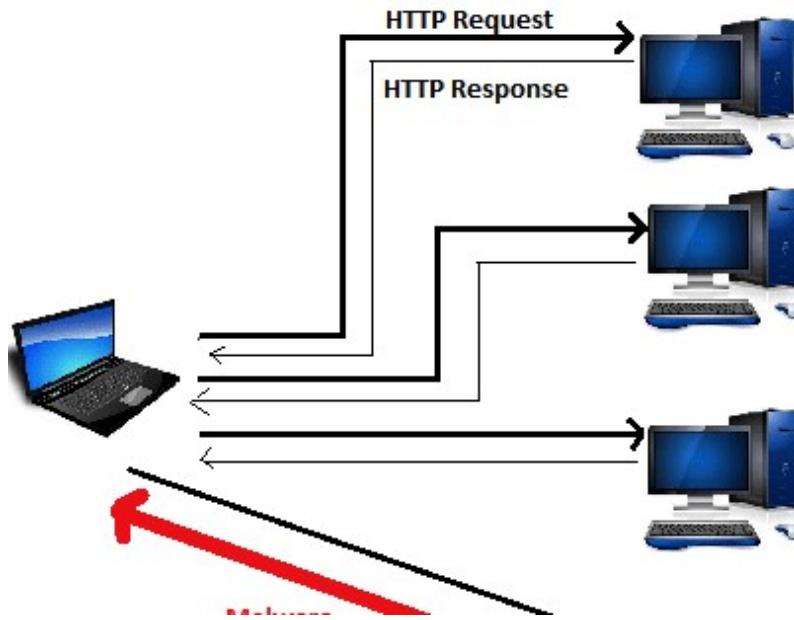
encryptie hier mogelijks niet altijd een oplossing biedt. Dit is omdat als we tijdens de communicatie ook de encryptiesleutel kunnen onderscheppen of deze kunnen vervangen we toch alle toegang hebben tot de data.



FIGUUR 46: REPLAY ATTACK

#### 6.2.4 Drive-by attack

Drive-by attack is een veelgebruikte methode voor het verspreiden van malware. Hackers gaan op zoek naar onveilige websites en plaatsen een kwaadaardig script in HTTP- of PHP-code op een van de pagina's. Dit script kan malware rechtstreeks installeren op de computer van iemand die de site bezoekt, of het kan de eindgebruiker doorsturen naar een site die door de hackers wordt gecontroleerd. Drive-by attacks kunnen plaatsvinden bij het bezoeken van een website of het bekijken van een e-mail. In tegenstelling tot veel andere soorten aanvallen is een drive-by niet afhankelijk van een handeling van de gebruiker. De gebruiker moet niet ergens inloggen of effectief iets downloaden. Dit gebeurd automatisch door de website in te laden.



**FIGUUR 47: DRIVE BY ATTACK**

### 6.2.5 Password attack

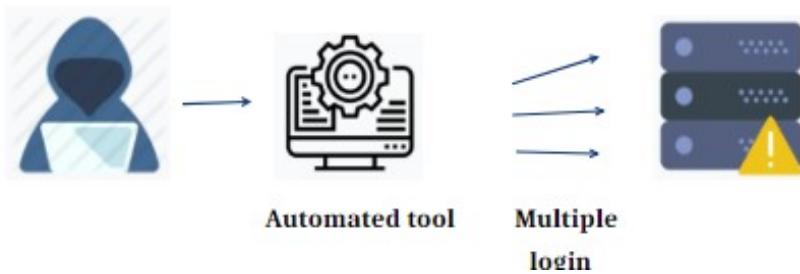
Wachtwoorden is de meeste gebruikte manier om eindgebruikers hun account te beveiligen en te zorgen dat de authenticatieaanvragen kunnen geverifieerd worden. Dit is dan ook de reden waarom een password attack een zeer efficiënte manier is om toegang te verkrijgen tot iemand haar/zijn data.

Wachtwoorden kunnen op verschillende manieren verkregen worden. Dit kan via social engineering, het rondkijken op iemand haar/zijn bureau, toegang verkrijgen tot de wachtwoord database, het netwerk afzoeken naar niet versleutelde wachtwoorden of door gewoonweg het wachtwoord te raden. Het wachtwoord raden kan op verschillende manieren gebeuren. Het kan willekeurig zijn en dat we dus geluk hebben of het kan op een systematische wijze uitgevoerd worden.

Als de aanval op systematische manier wordt uitgevoerd heb je twee opties. Brute force attack en een woordenboek attack. Hieronder wat meer uitleg.

- Brute force

Brute-force password guessing betekent een hoop willekeurige wachtwoorden te proberen en hopen dat dit lukt. Deze wachtwoorden kunnen gebaseerd zijn op voorkennis van de persoon doordat deze te veel informatie vrijgaf terwijl iemand bezig was met social engineering. Deze wachtwoorden zijn meestal een geboortedatum, woonplaats, etc ...



FIGUUR 48: BRUTE FORCE ATTACK

- Dictionary attack

Bij een dictionary attack wordt een woordenboek van veelgebruikte wachtwoorden gebruikt om toegang te krijgen tot de computer en het netwerk van een gebruiker. Er zijn ook manieren om zo versleutelde wachtwoorden te kraken.

### 6.2.6 SQL injection

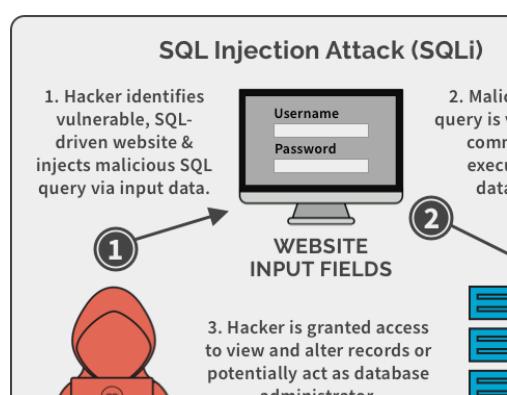
Een SQL injection aanval is een veel voorkomend probleem bij databases. Het gebeurt als een hacker een SQL-query uitvoert. Dit kan hij doen door bijvoorbeeld stukjes code te schrijven bij de invoervelden die op de website staan. Dit kunnen bijvoorbeeld de vakjes zijn waar je je gebruikersnaam en wachtwoord moet ingeven. Een succesvolle SQL-injectie kan gevoelige gegevens uit de database lezen,

databasegegevens wijzigen (invoegen, bijwerken of verwijderen), de database afsluiten, de inhoud van een bepaald bestand herstellen en commando's aan het besturingssysteem geven.

Een voorbeeld hiervan is wanneer een website de accountnaam opvraagt om bepaalde gegevens op te vragen en deze weer te geven aan de gebruiker. Een voorbeeld van een query is "SELECT \* FROM users WHERE account = "" + userProvidedAccountNumber + ";"

Deze query werkt als de gebruikers in dit voorbeeld dan hun juiste rekeningnummer doorgeven. Maar dit stukje code laat wel een gat open voor aanvallers. Als iemand bijvoorbeeld zou besluiten om een rekeningnummer op te geven van "" of '1' = '1'" dan geeft dit de volgende querystring: "SELECT \* FROM users WHERE account = "" of '1' = '1';" Omdat '1' = '1' altijd evalueert naar TRUE, zal de database de gegevens van alle gebruikers weergeven in plaats van slechts van één gebruiker.

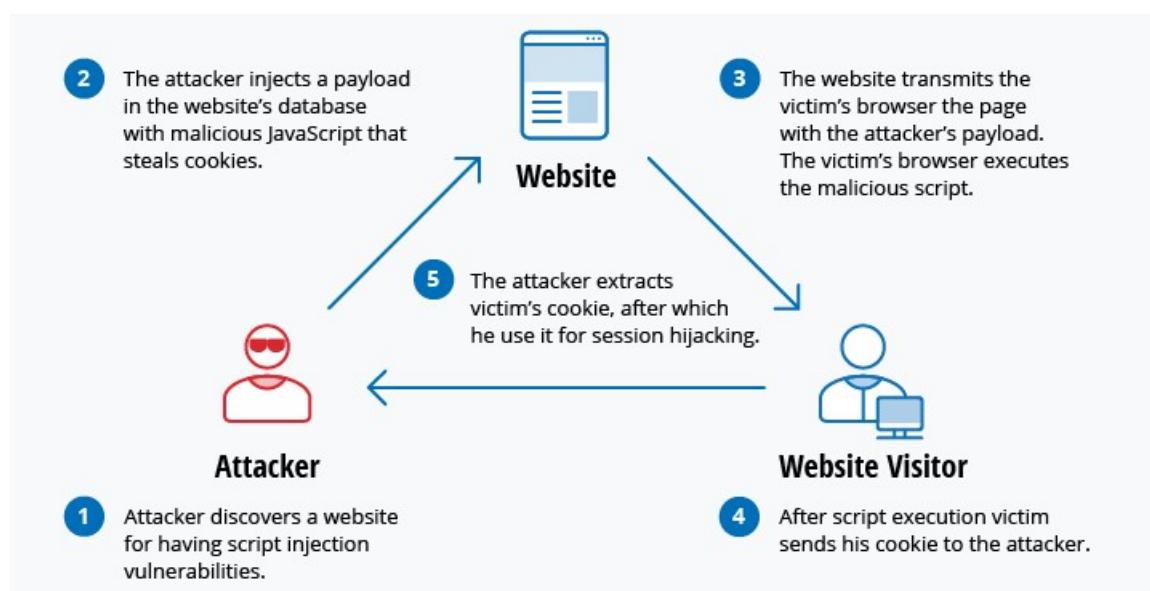
De kwetsbaarheid voor dit type cyberaanval hangt af van het feit dat SQL geen echt onderscheid maakt tussen het besturings- en het gegevensvlak. Daarom werken SQL-injecties vooral als een website dynamische SQL gebruikt.



FIGUUR 49: SQL INJECTION

### 6.2.7 Cross-site scripting (XSS) attack

XSS-attacks maken gebruik van webbronnen van een derde partij om bepaalde scripts uit te voeren in de webbrowser. De aanvaller injecteert de website met kwaadaardige javascripts in de database. Wanneer de eindgebruiker die bepaalde pagina opvraagt zal dat script mee ingeladen worden. De website kan bijvoorbeeld de cookies van de eindgebruiker naar een server van de hacker sturen, waarna de hacker deze kan gebruiken voor bijvoorbeeld een session hijacking attack. De gevaarlijkste gevallen treden op wanneer cross site scripting wordt gebruikt om extra kwetsbaarheden te gebruiken. Deze kwetsbaarheden kunnen een hacker helpen met het niet alleen stelen van cookies, maar ook toetsaanslagen op te slaan, screenshots te maken, netwerkinformatie te ontdekken en te verzamelen, en van op afstand toegang te krijgen tot de computer van de eindgebruiker.



FIGUUR 50: CROSS SITE SCRIPTING ATTACK

## **6.3 Waarom Pentesten uitvoeren**

Deze testen zijn dus uiteraard zeer belangrijk. Voor kleine bedrijven tot multinationals is het altijd belangrijk om de data van de klanten veilig te houden. Een pentest kan ons daarmee helpen. Deze testen geven ons enorm veel informatie over hoe sterk het entwerk is tegen de hierboven uitgelegde aanvallen. Hieronder bespreek ik aantal belangrijke zaken dat deze testen het bedrijf leren.

- Zo een test toont het beveiligingsteam hoe deze aanvallen plaatsvinden en wat er allemaal beïnvloed wordt in het bedrijf.
- Deze testen tonen de op dit moment grootste kwetsbaarheden in het netwerk. Een pentest prioriteert de mogelijke aanvallen die kunnen komen in een categorie van low, medium en large.
- Doordat deze test de grootste zwakheden weergeeft krijgt het bedrijf ook de kans om deze te verhelpen.
- Deze test toont niet alleen de zwakheden maar ook de sterke punten binnen de organisatie.
- Als laatste brengt deze ook slechte interne beveiligingsprocessen aan het licht.

# 7 Moeilijkheden en problemen

---

In dit afsluitend hoofdstuk zal ik bespreken welke moeilijkheden ik tegenkwam tijdens het uitvoeren van mijn project.

## 7.1 Falen van hardware

Het eerste grote probleem dat ik enkele keren ondervond was dat mijn hardware faalde. Dit wil zeggen dat ik op een dag toekwam en dat mijn server niet meer naar behoren werkte. Na wat onderzoek bleek dat het batterijtje van mijn raidcontroller was stuk gegaan. Daardoor was de raidcontroller een fractie van een seconde uitgevallen en zat ik met corrupte data. Dit in combinatie met een schijf dat niet meer werkte zorgde ervoor dat mijn RAID 5 onbruikbaar werd, wat resulteerde in het verliezen van alle data. Daardoor moest ik opnieuw mijn servers maken en de gebruikers aanmaken.

## 7.2 Falen synchronisatie Microsoft 365 en licenties

Doordat door het hardware falen mijn AD verdwenen was werkte mijn synchronisatie met Microsoft 365 niet meer. Deze zal altijd communiceren met de AD waarmee deze is gesynchroniseerd. Doordat deze server plotseling verdwenen is kan deze synchronisatie ook niet meer doorlopen en faalt deze ook. Het probleem is echter dat je alles wat gesynchroniseerd is niet kan aanpassen of verwijderen omdat Microsoft 365 niet meer kan communiceren met de AD. Om dit op te lossen

kan je via Microsoft 365 de synchronisatie laten loskoppelen. Dit duurt echter minstens 48 uur en slaagt ook niet altijd. Doordat ik mijn omgeving twee keer heb gesynchroniseerd kan je bij de gebruikers zien dat er een overbodige gebruiker in zit. Deze kan niet verwijderd worden maar doet ook verder niks.

Ook had ik wat problemen met mijn licenties van mijn gebruikers. Voor mijn doeleinden is het belangrijk dat we veel securityfeatures kunnen gebruiken. Dit zit echter niet bij alle licenties. De meest complete licentie is de E5 licentie. Dit was echter geen optie omdat deze €35 per gebruiker per maand kost. Dit is natuurlijk veel te duur voor te gebruiken in een testomgeving. Daarom kreeg ik één E3 licentie ter gebruik. Deze bezit ook alle securityfeatures alleen heeft deze geen geavanceerde beveiligings-, analyse- en spraakfuncties. Deze licentie kost €19.70 per gebruiker per maand. Omdat in de E3 licentie geen Microsoft defender voor Office 365 zit kreeg ik daar ook nog een licentie voor. Deze kost €1.64 per gebruiker per licentie.

### **7.3 Watchguard licentie**

Omdat er verschillende opties zijn bij de licenties van Watchguard was het kiezen al moeilijk. Echter toen ik besloot om de Total security licentie te gebruiken ontdekte ik dat de prijzen voor oudere toestellen enorm duur zijn. Ik had eerst een Watchguard T10 in gebruik. Deze zijn ondertussen al uit productie gehaald. Deze firewall zijn licentie was al een tijdje verlopen, en dat zorgde ervoor dat de prijs heel duur werd. Dit komt omdat je ook nog de periode dat je firewall geen geldige licentie had ook erbij moest betalen. Dit zorgde ervoor dat de prijs van de licentie nog eens keer 2 of 2.5 zou gaan. Dit was natuurlijk ook te duur.

Als oplossing kreeg ik van één van de collega's een firewall die gebruikt werd om het testen van beta-software van Watchguard. Deze had de juiste licenties en ik kon daarmee verder werken.

# 8 Conclusie

---

Het project dat ik gemaakt heb in EFFIX heb ik enorm veel uit geleerd. Nu dat het project op zijn einde koopt wil ik toch enkele conclusies neerschrijven. Het maken van het project vond ik niet simpel. Dit komt omdat het begrip security zeer ruim is en dat ik van alles iets wou proberen. Daardoor heb ik mijn eigen standaarden niet gehaald die ik graag wou halen. Na afloop was dit een logische uitkomst omdat ik heel veel hooi op mijn vork heb genomen. Ik heb wel veel geleerd over alle soorten security en hoe diep dit onderwerp gaat.

Toen ik van start ging met dit project ben ik zoals een kip zonder hoofd erin gedoken en alles beginnen instellen. Daardoor maakte ik veel fouten. Achteraf gezien was het eerst beter om een netwerkschema te maken zoals in bijlage 1 en daarna pas alles uit te werken. Nu heb ik het schema achteraf gemaakt als de opstelling al klaar was. Ik leerde dus dat het eerst beter is om alles goed uit te denken en te documenteren voordat je effectief eraan begint. Het opzoeken van informatie, VLAN's, hoe het netwerk in elkaar zit en hoe we een pentest uitvoeren deed ik allemaal terwijl ik effectief bezig was met het project. Deze informatie heb je beter al ter beschikking voor je de praktische uitvoering doet.

Verder was het beveiligen van mailboxen ook niet simpel. Het gebruik van Microsoft Defender for office365 is een goede oplossing maar het is niet de beste oplossing. Het gebruik van een spamfilter zoals Barracuda is zeker aan te raden. In de oplossing van Microsoft zit wel toekomst in. Er zijn enorm veel mogelijkheden maar ik heb nu het gevoel dat deze nog niet optimaal werken.

Het laatste deel van het oorspronkelijke project was een pentest uitvoeren. Toen de opdracht werd vastgelegd wist ik dat dit niet simpel zou zijn, maar het is zeer complex. Daardoor heb ik ook geen echte pentest uitgevoerd. Ik voerde enkel een DoS aanval uit om te kijken hoe de firewall erop reageert.

# Afbeeldingenlijst

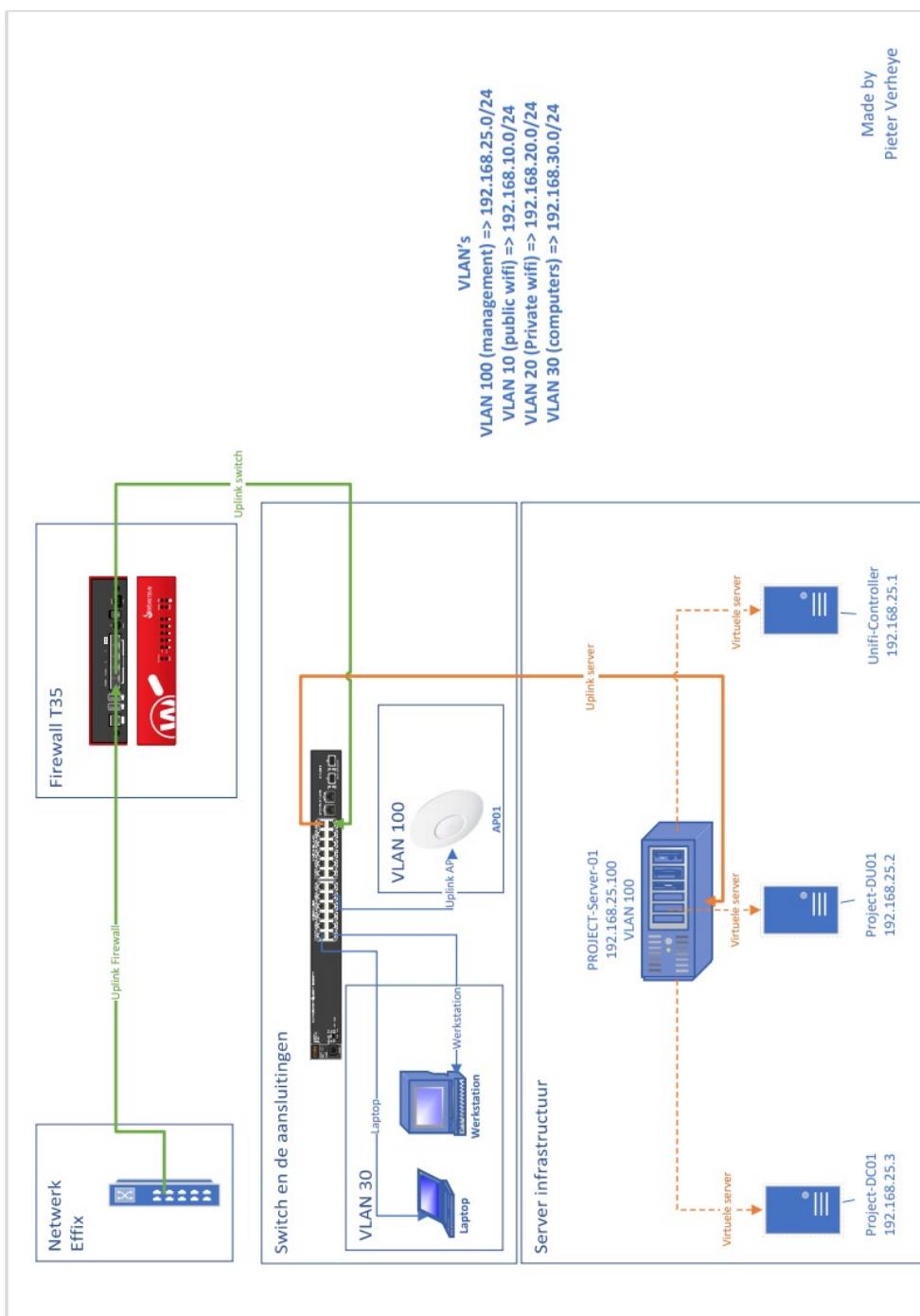
---

Figuur 1: Reputation Enabled Defense.....	8
Figuur 2: OSI model .....	11
Figuur 3: Untagged Vlan .....	12
Figuur 4: Tagged Vlan .....	13
Figuur 5: RAID 0.....	15
Figuur 6: RAID 1.....	16
Figuur 7: RAID 3 en RAID 4 .....	16
Figuur 8: RAID 5.....	16
Figuur 9: RAID 6.....	17
Figuur 10: RAID 10.....	17
Figuur 11: TYPE 1 hypervisor .....	17
Figuur 12:Aanmaak VLAN's en interface .....	20
Figuur 13: Tagged interface .....	21
Figuur 14: Regels Firewall .....	24
Figuur 15: Webblocker.....	25
Figuur 16: Application control.....	26
Figuur 17: Geolocation.....	26
Figuur 18: Intrusion prevention .....	27
Figuur 19: APT blocker.....	28
Figuur 20: Gateway antivirus.....	28
Figuur 21: Data loss prevention.....	29
Figuur 22: DNSWatch .....	29
Figuur 23: Botnet detection .....	30
Figuur 24: VLAN aanmaken, tagged, untagged.....	32
Figuur 25: Show VLAN .....	32

Figuur 26: Disable interface.....	33
Figuur 27: Show interface brief.....	33
Figuur 28: Password policy .....	34
Figuur 29: 3-2-1 back strategie.....	35
Figuur 30: Backup servers .....	36
Figuur 31: Gebruikers Microsoft 365 .....	38
Figuur 32: Anti-phising .....	39
Figuur 33: Anti-spam.....	40
Figuur 34: Veilige bijlage.....	41
Figuur 35: Safe links .....	41
Figuur 36: Anti-malware .....	42
Figuur 37: Dashboard O365 .....	43
Figuur 38: Multi Factor Autentication.....	44
Figuur 39: Voorbeeld phising .....	50
Figuur 40: DoS aanval.....	53
Figuur 41: 3-Way handshake .....	54
Figuur 42: Teardrop attack .....	55
Figuur 43: Smurf attack.....	56
Figuur 44: Ping of death attack.....	56
Figuur 45: Man in the middle Hijacking attack .....	57
Figuur 46: Replay attack .....	58
Figuur 47: Drive by attack .....	59
Figuur 48: Brute force attack.....	60
Figuur 49: SQL injection.....	61
Figuur 50: Cross site scripting attack.....	62

# Bijlagen

## Bijlage 1: Netwerkschema



## Bijlage 2: Configuratie switch

```
HP-2530-24-PoEP# show run
```

Running configuration:

```
J9779A Configuration Editor; Created on release #YB.15.12.0006
```

```
Ver #04:01.ff.37.27:ea
```

```
hostname "HP-2530-24-PoEP"
```

```
ip default-gateway 192.168.25.100
```

```
interface 15
```

```
    disable
```

```
    exit
```

```
snmp-server community "public" unrestricted
```

```
vlan 1
```

```
    name "DEFAULT_VLAN"
```

```
    no untagged 1-3,10,22-24
```

```
    untagged 4-9,11-21,25-28
```

```
    no ip address
```

```
    exit
```

```
vlan 10
```

name "public\_wifi"

tagged 10,24

no ip address

exit

vlan 20

name "private\_wifi"

tagged 10,24

no ip address

exit

vlan 30

name "VLAN30"

untagged 1-3

tagged 24

no ip address

exit

vlan 100

name "management"

untagged 10,22

tagged 23-24

ip address 192.168.25.231 255.255.255.0

exit

spanning-tree

no tftp server

no dhcp config-file-update

password manager

## **Bijlage 3: XML Watchguard**

Doordat dit een bestand is van 833 pagina's zal ik de URL naar het bestand hieronder plaatsen.

[https://vivesonline-my.sharepoint.com/:u/r/personal/r0784501\\_student\\_vives\\_be/Documents/WatchGuard-XTM.xml?csf=1&web=1&e=zsYdRt](https://vivesonline-my.sharepoint.com/:u/r/personal/r0784501_student_vives_be/Documents/WatchGuard-XTM.xml?csf=1&web=1&e=zsYdRt)

