

Het netwerk binnen een bedrijf

Senne Knaepkens
2020-2021

Inhoudsopgave

1	Wat is een bedrijfsnetwerk?.....	2
2	Waaruit bestaat een bedrijfsnetwerk?.....	2
2.1	Router:.....	2
2.1.1	Wat is een router?	2
2.1.2	Verschillende soorten routers:.....	2
2.2	Firewall:	4
2.2.1	Wat is een firewall?.....	4
2.2.2	Verschillende soorten Firewalls:	4
2.2.3	Veelgebruikte poorten bij een firewall:	5
2.2.4	Het TCP/IP Lagenmodel:.....	6
2.3	Switches:.....	6
2.3.1	Wat is een switch?	6
2.3.2	Verschillende soorten switches:.....	6
2.4	Servers:.....	7
2.4.1	Wat zijn servers?	7
2.4.2	Verschillende soorten servers:.....	7
2.4.3	Wat is het nut van een server:.....	7
2.5	Wifi	8
2.5.1	WiFi routers:.....	8
3	Het netwerk bij GET:	8
3.1	Hoe ik het netwerk zou maken:	8
3.2	Aanpassingen:	8
4	Hoe kan je een computer toevoegen aan een netwerk/domein	9
5	Interessante termen:.....	10
5.1	PoE	10
5.1.1	Wat is PoE?	10
5.2	Backbone switch	11
5.2.1	Wat is een backbone switch?	11

1 Wat is een bedrijfsnetwerk?

Een bedrijfsnetwerk is een computernetwerk met eventueel een telefoonnetwerk dat gebruikt wordt in een bedrijf voor interne communicatie. Dit is handig omdat men dan allemaal gebruik kan maken van dezelfde servers, databases, bestanden enzovoort. De administrator van dit netwerk kan bepaalde mensen dan ook bepaalde rechten etc. geven maar ook beperkingen indien nodig. Via een softwareprogramma kan de administrator bv. ook updates door “pushen” naar de gebruikers in het netwerk.

2 Waaruit bestaat een bedrijfsnetwerk?

2.1 Router:

2.1.1 Wat is een router?

Een router zorgt ervoor dat er switch(es) en/of pc('s) aangesloten kunnen worden op het internet met een draadloze of bekabelde verbinding via een RJ45-aansluiting. In de meeste routers zit een DHCP-server ingebouwd, deze server zorgt ervoor dat de apparaten die willen verbinden met de router automatisch een IP-adres krijgen uit de IP-range die de DHCP-server mag/kan uitgeven. Deze IP-adressen zijn dan voor een bepaalde tijd geldig, wanneer deze IP-adressen zijn geretourneerd kunnen deze opnieuw uitgedeeld worden aan een ander apparaat of terug aan het hetzelfde apparaat.

2.1.2 Verschillende soorten routers:

Breedbandrouters:

De meest gebruikte router voor thuisgebruik. Deze soort router heeft vaak al een modem geïntegreerd, je kan hierop meerdere computers aansluiten op één breedbandaansluiting.



Professionele routers:

Professionele routers krijgen niet 1 IP-adres maar ze krijgen een blok van opeenvolgende adressen toegewezen (een subnet) van unieke adressen. Zo kan men in een bedrijf bijvoorbeeld een printserver een eigen IP-adres toewijzen.



Backbone- of ISP-routers (Internet Service Provider-routers):

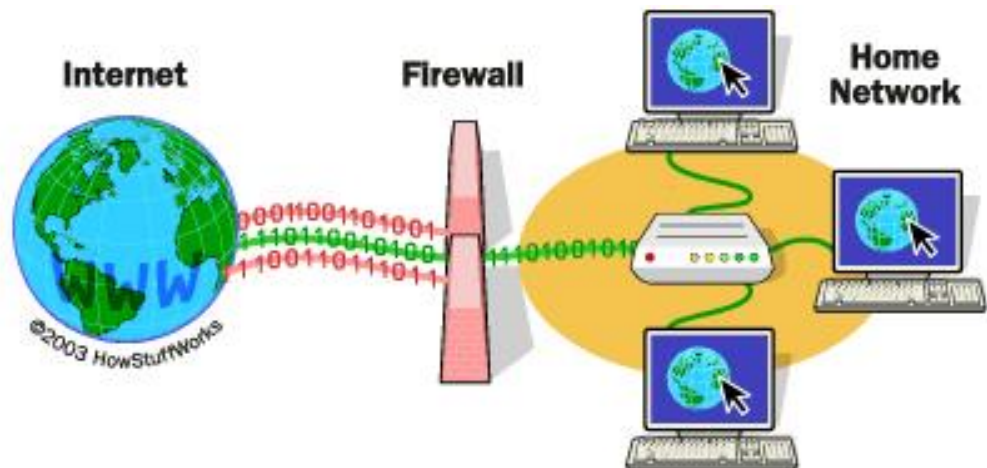
Deze routers worden gebruikt door bedrijven zoals Telenet, hun routers moeten enorm grote hoeveelheden verwerken en erg betrouwbaar zijn. Deze routers zijn vaak ook modulair zo kan men afhankelijk van het aantal nodige poorten de router verder “opbouwen”.



2.2 Firewall:

2.2.1 Wat is een firewall?

Een firewall is een beveiliging tegen het internetverkeer buiten een bepaald netwerk. In deze firewall kan men bepaald verkeer toelaten door bijvoorbeeld poort 443 open te zetten, dit wil dan zeggen dat er HTTPS-protocollen toegelaten worden om op sites te kunnen surfen vanuit het netwerk.



2.2.2 Verschillende soorten Firewalls:

Packet filtering firewall:

Deze soort firewall werkt op de "Network layer" van TCP/IP-protocol-stack. Deze firewall werkt enkel met de IP-header van het pakket en is hierdoor snel maar biedt niet de beste bescherming. Dit heeft dus als gevolg dat er sneller virussen, zwakheden in programma's etc. zullen optreden.

Application layer firewall:

Deze soort van een firewall grijpt in op de "Application layer" van de TCP/IP-protocol-stack. (hieronder staat een foto van de TCP/IP-protocol-stack) Een bepaalde software zal voor elk pakketje bepalen of deze wordt doorgelaten of tegengehouden. Deze vorm van een firewall is veiliger maar ook complexer en is dus iets trager.

Stateless firewall:

Deze firewall bekijkt elk pakketje en slaat geen tussentijdse informatie op van de connecties die de firewall heeft. Deze vorm van Firewall brengt grote beperkingen met zich mee, tegenwoordig wordt er meestal een stateful firewall gebruikt.

Stateful firewall:

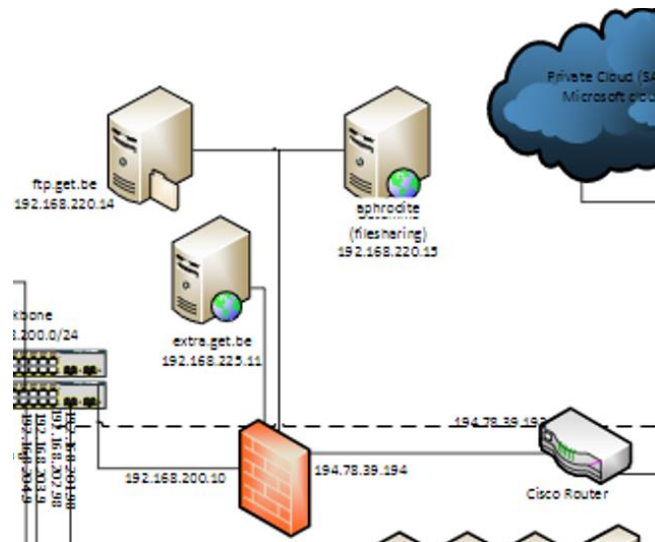
Deze firewall bekijkt ook elk pakketje MAAR slaat de tussentijdse informatie wel op, hierdoor kan de firewall beter bepalen of een pakketje doorgelaten moet worden of tegengehouden moet worden.

Personal firewall:

Dit is een firewall die enkel de computer zelf beschermt waarop hij is geïnstalleerd. Er zijn verschillende soorten regels die je kan geven voor deze firewalls maar sommige personal firewalls hebben de mogelijkheid tot het zelf schrijven van regels voor de firewall afhankelijk van het proces waar de computer mee bezig is. Een voorbeeld hiervan is dat je de mailbox toegang geeft tot poort 25, zo kan deze mails versturen.

Network Firewall:

Dit is een aparte computer/server tussen 2 of meerdere netwerken. De ruimte tussen deze 2 netwerken wordt ook wel DMZ of demilitarized zone genoemd. In de DMZ zitten computers of servers die bereikbaar moeten zijn vanuit het internet of een netwerk buiten je eigen netwerk. Een voorbeeld van een DMZ is bijvoorbeeld de site ftp.get.be



Managed firewall

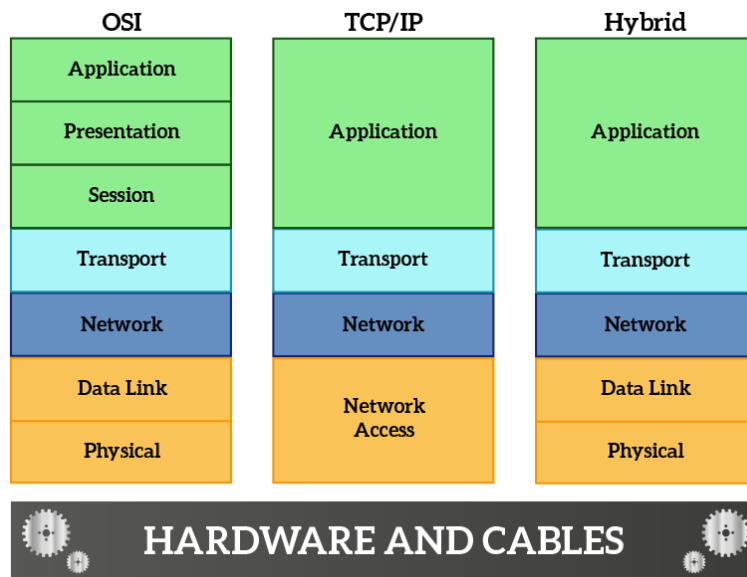
Dit is een firewall die door een third party bedrijf wordt gemanaged. Dit is vaak de oplossing voor bedrijven die zelf niet genoeg kennis hebben in het beveiligen van hun netwerk.

2.2.3 Veelgebruikte poorten bij een firewall:

HTTP gebruikt poort 80
HTTPS gebruikt poort 443
SSH gebruikt poort 22

Link naar andere poorten: https://nl.wikipedia.org/wiki/TCP- en_UDP-poorten

2.2.4 Het TCP/IP Lagenmodel:



2.3 Switches:

2.3.1 Wat is een switch?

Een switch is een zeer belangrijk onderdeel van een netwerk en al helemaal in een bedrijfsnetwerk zoals bij GET. Een switch wordt vaak gebruikt voor het uitbreiden van het aantal poorten op de router. Maar wordt ook zeer vaak gebruikt om bepaalde netwerken of apparaten met elkaar te verbinden, zo kan je zelfs zonder netwerkverbinding pakketjes sturen van de ene naar de andere computer, er vanuit gaande dat ze gelinkt zijn door een switch.

2.3.2 Verschillende soorten switches:

Unmanaged switches:

Aan dit type switches kan men niets instellen/aanpassen, de gebruiksvriendelijkheid van deze switches ligt vrij hoog en doorgaans probleemloos. Dit is een goede oplossing voor bedrijven die niet veel van netwerken kennen en een simpel netwerk willen in hun bedrijf.

Managed switches:

Dit type van switch is uiteraard geavanceerder en heeft voorzieningen voor configuratie en inspectie. Een voorbeeld hiervan is: Monitoring, met monitoring kan men de statistieken van het internetverkeer van de switch bekijken.

Multilayer switches:

Een normale switch kijkt enkel naar het MAC-adres en opereert dus op laag 2 van het TCP/IP-protocol. Maar een multilaagse of multilayer switch kan gegevens ook doorsturen op basis van informatie die zich op de hogere lagen van het TCP/IP-protocol bevindt.

2.4 Servers:

2.4.1 Wat zijn servers?

Een server is een "computer" die aan een client (een andere computer) een bepaalde dienst verleent. Deze dienst kan een actie op de server zijn of bepaalde informatie opvragen. Dit noemt men ook wel het "client-servermodel".

2.4.2 Verschillende soorten servers:

Dedicated server:

Op deze servers draait er maar 1 serverprogramma, dit is dan ook de enigste taak van de server. Voor een database gebruikt men dit soort servers vaak aangezien een database veel vraagt van de servers.

Clustered server:

Dit zijn een aantal aan elkaar gekoppelde computers/servers ook wel een "cluster" genoemd waarop één serverprogramma draait. Dit is nodig wanneer je veel clients tegelijk moet bedienen bv. In het geval van een bekende website zoals Facebook.

Servers met client -en servertaken:

Op één computer worden dan de client -en servertaken uitgevoerd.

Een server waarop meerdere serverprogramma's draaien:

Zoals de naam al zegt, 1 server met daarop verschillende serverprogramma's of toepassingen. Dit is zeer handig moest je een aantal kleine toepassingen draaien en hiervoor geen volledige server "verspillen".

Een cloud server:

Dit is een server in de "cloud", de gebruiker weet niet waar de server precies staat.

2.4.3 Wat is het nut van een server:

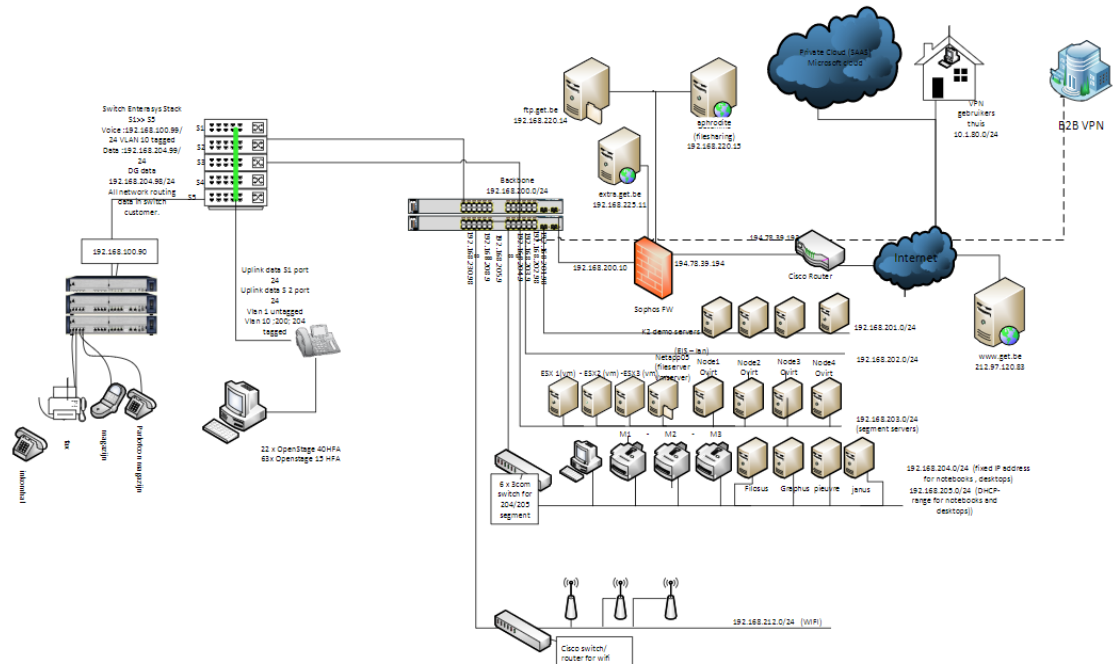
Dit hangt af van het type server. Als voorbeeld zullen we even een printserver nemen, een printserver heeft als bedoeling de mogelijkheid om met alle computers af te printen van één/meerdere bepaalde printers. Om dit mogelijk te maken staat de printserver in verbinding met een switch die op zijn beurt dan weer verbonden is met alle computers in het netwerk van het bedrijf.

2.5 Wifi

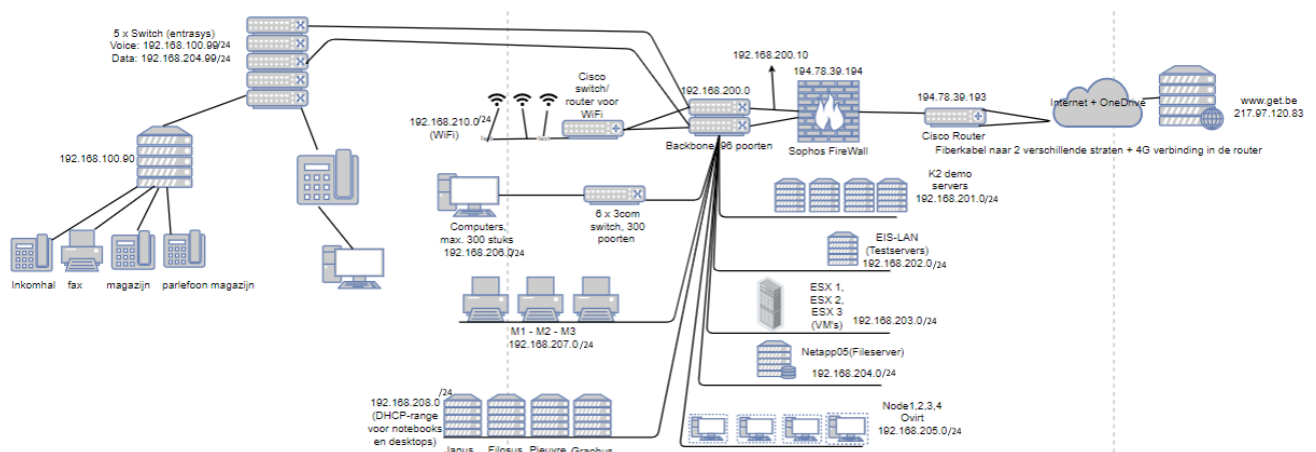
2.5.1 WiFi routers:

Binnenin GET staan er een aantal WiFi routers die ervoor zorgen dat de werknemers van GET overal in het kantoor verbinding hebben via WiFi voor bijvoorbeeld hun tablet of hun GSM. Deze WiFi routers staan in verbinding met de switch die dan weer in verbinding staat met de router.

3 Het netwerk bij GET:



3.1 Hoe ik het netwerk zou maken:



3.2 Aanpassingen:

3 ingangen van het internet naar de router binnenin GET:

2 Fiberkabels gebruiken, liefst van 2 verschillende straten. Dit is handig voor als er werken zijn op een bepaalde baan, dan is er nog de tweede fiberkabel om internet te ontvangen binnenin GET. Stel deze 2 fiberkabels zouden buiten werking zijn, is er nog een laatste ingang voor Wifi verbinding namelijk 4G, de router die men bij GET gebruikt ondersteunt dit ook. Zo is er altijd een WiFi-verbinding bij GET.

Twee verbindingen tussen de Firewall en de backbone switches:

Waarom zou je dit doen? Dit is in een normale situatie overbodig. Maar stel 1 van de 2 switches valt uit dan heb je nog steeds een netwerkverbinding omdat je de firewall met beide switches verbonden hebt.

2 verbindingen naar de Wifi router:

Dit heeft ook dezelfde reden stel 1 van de 2 switches valt uit is er nog steeds een Wifi netwerk.

Servers/virtuele machines/computers meer apart gezet:

Ik heb deze meer verdeeld met als bedoeling dat je via 1 IP-adres alle computers bijvoorbeeld kan laten updaten via een bepaalde software. Ik heb bijvoorbeeld ook alle printers bij elkaar gezet omdat dit iets makkelijker werkt volgens mij.

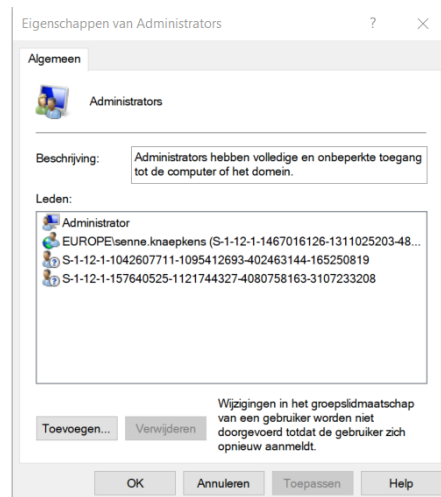
Superscopen in plaats van een subnet te gebruiken.

Men zou er ook voor kunnen kiezen om in plaats van een subnet gebruik te maken van een superscope. Wat is een superscope? Een superscope is een beheersfunctie van een DHCP-server die gebruikt kan worden om meerdere "scopes" toe te voegen aan één enkele "administratieve eenheid". Met behulp van een superscope kan een DHCP-server meerdere IP-adressen leasen aan toestellen die verbinding willen maken aan het fysieke netwerk. In een multinet-configuratie kan een DHCP-server door middel van superscopen een bepaalde reikwijdte van IP-adressen die in het netwerk liggen groeperen. Zo kan een DHCP-server dus ook uit verschillende scopes IP-adressen halen/gebruiken. Een superscope is de oplossing voor vele problemen, deze zorgt er bijvoorbeeld ook voor dat je een groter bereik van IP-adressen hebt. Maar een superscope maakt het ook makkelijker om clients naar een nieuw bereik te migreren. Er is nog maar één DHCP-server nodig in plaats van 2 DHCP-servers bij het gebruik van een tweede logische netwerk. Uiteraard kan je met het gebruik van een superscope ook nog gebruik maken van "fixed ip-adressen" dit wil zeggen dat je een vast IP-adres geeft aan een bepaalde computer, server,...

4 Hoe kan je een computer toevoegen aan een netwerk/domein

Eerst moet je zien dat de nieuwe gebruiker al is toegevoegd in het domein. Dit kan je doen door als administrator op het domein aan te melden en in de registry een nieuwe user toe te voegen. Daarna starten

we de laptop op, windows zal bepaalde vragen stellen in verband met land, taal en beveiligingsvragen. Na een aantal vragen zal de computer vragen of deze voor privégebruik is of voor gebruik in een domein. Hier kiezen we voor de optie "deze computer toevoegen in een netwerk/domein". Toen konden we aanmelden met een administrator account en de nieuwe gebruiker toevoegen aan de administrator accounts. Dit hebben we gedaan door de "Windowstoets" en "x" tegelijk in te drukken en dan door te klikken naar computerbeheer. Eens we in computerbeheer zijn gaan het tabje "lokale gebruikers en groepen". In dit tabje klikken we dan weer door naar "groepen" en dan dubbelklikken we op "administrators", dan zou je het volgende venster moeten krijgen:



Hier klikken we dan op toevoegen en vullen we de naam van de nieuwe gebruiker in het onderste vak, dan klikken we op "namen controleren" en dan kan je controleren of je de naam juist hebt ingevoerd. Als de naam en de gegevens kloppen klikken we op "ok" en dan op "toepassen". Indien je de vorige stappen hebt gevolgd zou de gebruiker toegevoegd moeten zijn aan je computer.

5 Interessante termen:

5.1 PoE

5.1.1 Wat is PoE?

Power over Ethernet (PoE) is een zeer handige feature, het is eigenlijk het gegeven dat er door een ethernetkabel zowel een signaal als stroom doorkomt. Dit zorgt er dus voor dat je voor een simpele telefoon geen stekker hoeft te gebruiken. Deze technologie wordt ook vaak gebruikt in CCTV, beter bekend als beveiligingscamera's dit is handig omdat er over 1 kabel dan zowel beeld als stroom wordt geleverd/ontvangen.

5.2 Backbone switch

5.2.1 Wat is een backbone switch?

Een backbone switch is de belangrijkste switch in een netwerk. Deze switch staat in verbinding met de firewall, deze backbone switch staat ook weer in verbinding met andere componenten van het netwerk. Een aantal voorbeelden van andere componenten zijn: een andere switch, een computer, een server.

Bronnen: Wikipedia, werknemers van GET, Tweakers, Microsoft support, strato.nl