

Cyber Threat Assessment Report

Autobedrijf A (geanonimiseerd voorbeeld)

Testperiode: 6 februari 2025 t/m 13 februari 2025

Rapportdatum: 20 februari 2025



1. Management samenvatting

We hebben de belangrijkste bevindingen van onze NGFW-beoordeling samengevat in de onderstaande Executive Summary. Hoewel de hoogtepunten hier worden vermeld, volgt een meer gedetailleerd overzicht van elke sectie verderop in het rapport. Zorg ervoor dat je de pagina met Aanbevolen Acties aan het einde van dit rapport bekijkt voor concrete stappen die jouw organisatie kan nemen om inkomende bedreigingen te beperken, beleid te implementeren en capaciteitsplanningsproblemen te voorkomen.

1.1. Beveiliging



35

Aanvallen via applicatie-kwetsbaarheden gedetecteerd



0

Malware en/of botnets ontdekt



7

Hoog-risico applicaties gedetecteerd

Let op: alle bedreigingen die in dit rapport worden vermeld, hebben effectief de bestaande netwerkbeveiliging omzeild. Ze moeten daarom als actief worden beschouwd en kunnen leiden tot verhoogde risico's, zoals een datalek.

1.2. Productiviteit



219

Totaal aantal gedetecteerde applicaties



6

Totaal aantal gedetecteerde proxy-applicaties



0

Totaal aantal peer-to-peer applicaties

Het gebruik van applicaties zou een sterke invloed moeten hebben op de netwerkarchitectuur. Inzicht in welke typen applicaties worden gebruikt, kan impact hebben op het beleid, controles op gesegmenteerde netwerken en het gebruik van cloudgebaseerde serviceplatforms.

1.3. Gebruik



266,3GB

Totaal gebruikte bandbreedte



22,4

Gemiddelde logfrequentie per seconde



84,8%

Percentage SSL-versleuteld verkeer

Naast individuele applicaties kan inzicht in het totale gebruik helpen bij capaciteitsplanning en het optimaliseren van netwerkverkeer op lange termijn.

2. Inhoudsopgave

1.	Management samenvatting	2
1.1.	Beveiliging	2
1.2.	Productiviteit	2
1.3.	Gebruik	2
2.	Inhoudsopgave	3
3.	Beveiliging	4
3.1.	Belangrijkste gedetecteerde applicatiekwetsbaarheden	4
3.2.	Belangrijkste malware, botnets en spyware/adware gedetecteerd	4
3.3.	Belangrijkste malware, botnets en spyware/adware gedetecteerd	5
3.4.	Kwetsbare apparaten en hosts	5
3.5.	Onbekende Malware	6
3.6.	Schadelijke en verdachte bestanden	6
4.	Productiviteit	7
4.1.	Cloudgebruik (SaaS)	7
4.2.	Cloudgebruik (IaaS)	7
	Proxy-applicaties	8
4.3.	Top webapplicaties	9
4.4.	Top websites op basis van browsing tijd	9
4.5.	Top webcategorieën	10
4.6.	Meest bezochte webdomeinen	10
5.	Netwerkverbruik	11
5.1.	Gemiddeld bandbreedteverbruik per uur	11
5.2.	Top bronnen/bestemmingen met het hoogste bandbreedteverbruik	12
5.3.	Top bronlanden van netwerkverkeer	12
5.4.	Gemiddelde logfrequentie per uur	13
5.5.	Gemiddelde logfrequentie per uur	14
5.6.	Gemiddeld FortiGate geheugengebruik per uur	15
6.	Aanbevelingen	16
6.1.	Verbeter detectie van schadelijke URL's en training	16
6.2.	Onderwijs en bescherm gebruikers tegen phishing-aanvallen	16
6.3.	Segmenteer het netwerk om risico's te beperken	16
6.4.	Beperk de inkomende Site-to-Site VPN tot strikt noodzakelijke communicatie	17

3. Beveiliging

Quick Stats



- **35** Aanvallen via applicatie kwetsbaarheden gedetecteerd
- **0** Bekende botnets gedetecteerd
- **1** Schadelijke website gedetecteerd
- **7** Hoog-risico applicaties gedetecteerd
- **1** Phishingwebsite gedetecteerd
- **0** Bekende malware gedetecteerd
- **15** Bestanden geanalyseerd door de sandbox
- **0** Verdachte bestanden gedetecteerd door de sandbox

3.1. Belangrijkste gedetecteerde applicatiekwetsbaarheden

Applicatiekwetsbaarheden kunnen worden misbruikt om de beveiliging van je netwerk in gevaar te brengen. Het FortiGuard-onderzoeksteam analyseert deze kwetsbaarheden en ontwikkelt vervolgens handtekeningen om ze te detecteren. FortiGuard maakt momenteel gebruik van een database met meer dan **5.800** bekende applicatiebedreigingen om aanvallen te detecteren die traditionele firewalls omzeilen. Voor meer informatie over applicatiekwetsbaarheden kun je terecht op FortiGuard:

<https://fortiguard.fortinet.com/services/ips>

#	Risico	Bedreigingsnaam	Type	Slachtoffers	Bronnen	Aantal
1	5	Linux.Kernel.Netfilter.xt_TCPMSS.DoS	DoS	1	1	1
2	2	Nmap.Script.Scanner	Anomalie	18	1	26
3	2	DNS.PTR.Records.Scan	Scan	2	1	8

3.2. Belangrijkste malware, botnets en spyware/adware gedetecteerd

Cybercriminelen maken gebruik van verschillende kanalen om malware te verspreiden. De meest voorkomende methoden verleiden gebruikers ertoe een geïnfecteerd bestand te openen via een e-mailbijlage, een schadelijk bestand te downloaden of op een link naar een kwaadaardige website te klikken.

Tijdens de beveiligingsbeoordeling heeft Fortinet malware- en botnet-gerelateerde gebeurtenissen geanalyseerd die wijzen op schadelijke bestanddownloads of verbindingen met botnet-commandocentra.

Geen records gevonden.

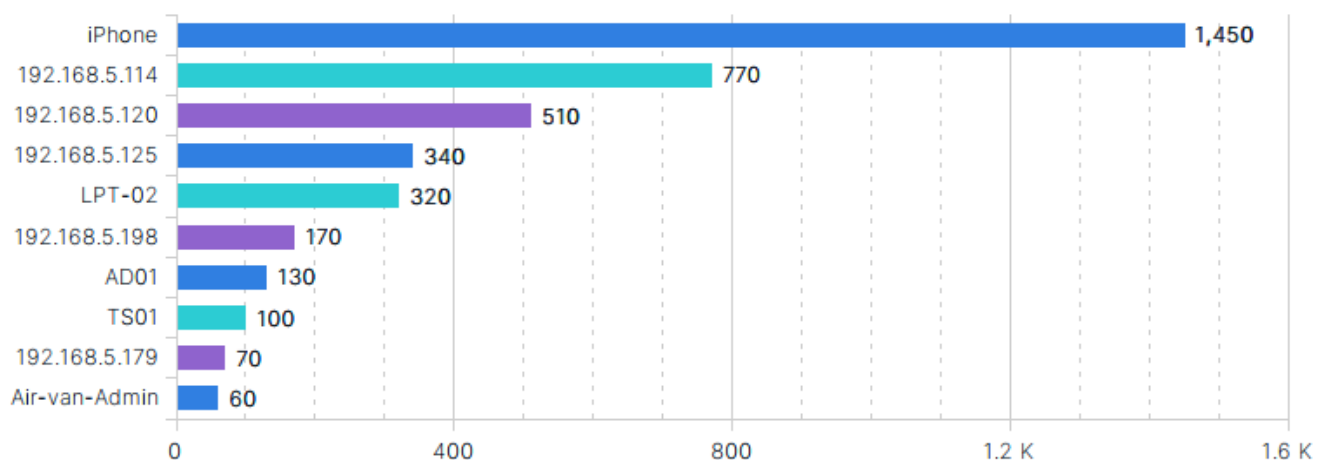
3.3. Belangrijkste malware, botnets en spyware/adware gedetecteerd

Het FortiGuard-onderzoeksteam kent een risicobeoordeling van 1 tot 5 toe aan een applicatie op basis van het gedragsprofiel van de applicatie. Deze risicobeoordeling helpt beheerders om snel hoog-risico applicaties te identificeren en beter te beslissen over het toepassingscontrolebeleid. De onderstaande applicaties hebben een risicoscore van 4 of hoger gekregen.

#	Risico	Applicatie	Category	Technology	Gebruikers	Bandbreedte	Sessies
1	5	Proxy.HTTP	Proxy	Netwerkprotocol	15	1,19MB	95
2	5	SOCKS4	Proxy	Netwerkprotocol	1	22B	2
3	5	SOCKS5	Proxy	Netwerkprotocol	1	6B	2
4	4	RDP	Remote.Access	Client-Server	27	16,67GB	257
5	4	TeamViewer	Remote.Access	Client-Server	3	90,98KB	13
6	4	Astrill	Proxy	Client-Server	1	21,10KB	2

3.4. Kwetsbare apparaten en hosts

Op basis van het activiteitstype van een individueel apparaat kunnen we een inschatting maken van de betrouwbaarheid van elke client. Deze clientreputatie wordt bepaald door belangrijke factoren zoals bezochte websites, gebruikte applicaties en inkomende/uitgaande connecties. Door de verzamelde activiteiten per apparaat te analyseren, kunnen we een algemene bedreigingsscore genereren. Bedreigingsscore per apparaat:



3.5. Onbekende Malware

De steeds geavanceerdere dreigingen van vandaag kunnen hun schadelijke intenties verbergen en traditionele antimalwarebeveiliging omzeilen. Conventionele antimalware-engines kunnen in de beschikbare tijd en met de vereiste zekerheid vaak bepaalde bestanden niet classificeren als goed of kwaad; hun intentie blijft onbekend. Sandboxing helpt dit probleem op te lossen door onbekende bestanden uit te voeren in een beveiligde omgeving, hun gedrag te observeren en hun risico te classificeren op basis van dat gedrag. Met deze functionaliteit ingeschakeld voor jouw beoordeling, hebben we een diepere analyse uitgevoerd van bestanden die door jouw netwerk circuleren.

Geen records gevonden.

3.6. Schadelijke en verdachte bestanden

Geen records gevonden.

4. Productiviteit

Quick Stats

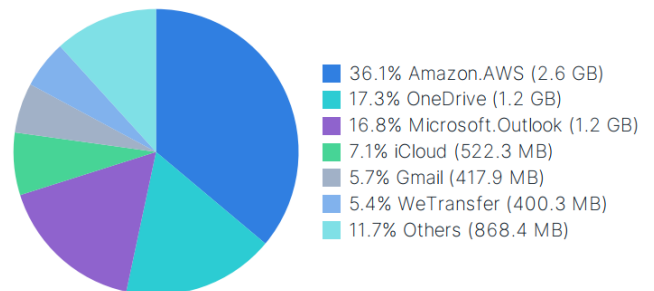


- **219** Totaal aantal gedetecteerde applicaties
- **6** Totaal aantal gedetecteerde proxy-applicaties
- **0** Peer-to-peer applicaties gedetecteerd
- **3** Remote access applicaties gedetecteerd

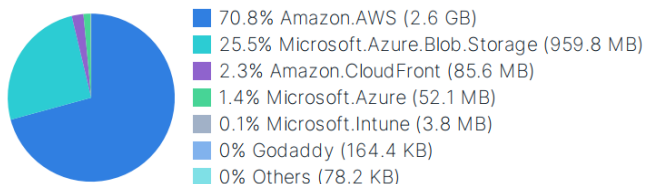
- **SSL** is de meest gebruikte applicatie
- **Network.Service** is de meest gebruikte applicatiecategorie
- **8029** Totaal aantal bezochte websites
- **go.microsoft.com** is de meest bezochte website

4.1. Cloudgebruik (SaaS)

IT-managers zijn zich vaak niet bewust van het aantal cloudgebaseerde diensten dat binnen hun organisatie wordt gebruikt. Soms worden deze applicaties gebruikt om bestaande bedrijfsinfrastructuur te omzeilen of zelfs te vervangen, simpelweg vanwege gebruiksgemak. Een mogelijk gevolg hiervan is dat gevoelige bedrijfsinformatie naar de cloud wordt overgedragen. Hierdoor kan jouw data worden blootgesteld als de beveiligingsinfrastructuur van de cloudprovider wordt geschonden.

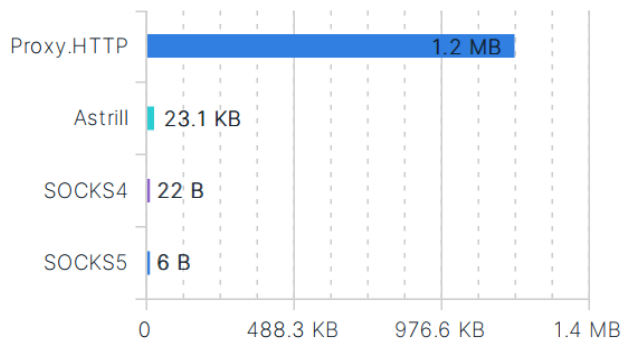


4.2. Cloudgebruik (IaaS)

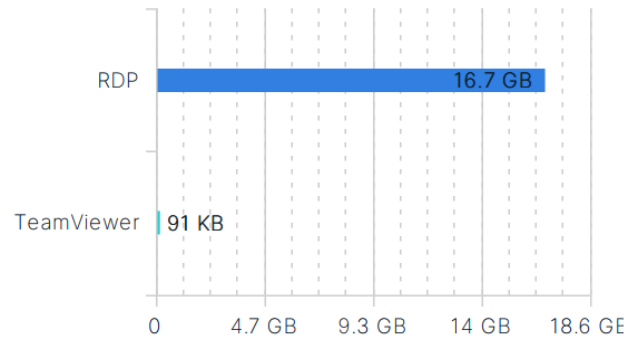


Het gebruik van Infrastructure as a Service (IaaS)-platformen is populair en kan zeer nuttig zijn wanneer computerresources beperkt zijn of gespecialiseerde vereisten hebben. Echter, het effectief uitbesteden van jouw infrastructuur moet goed worden gereguleerd om misbruik te voorkomen. Een periodieke audit van IaaS-applicaties is niet alleen nuttig voor beveiligingsdoeleinden, maar helpt ook om de kosten te minimaliseren die gepaard gaan met "pay-per-use" modellen of doorlopende abonnementsvergoedingen.

Proxy-applicaties



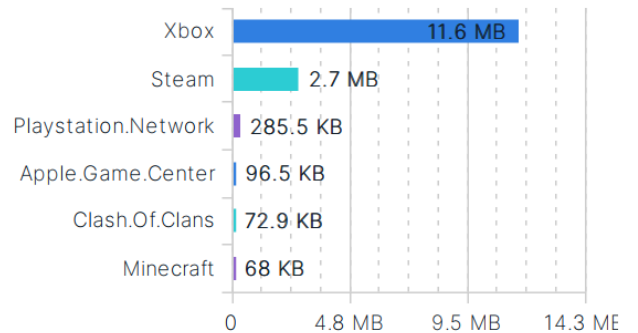
Remote Access-applicaties



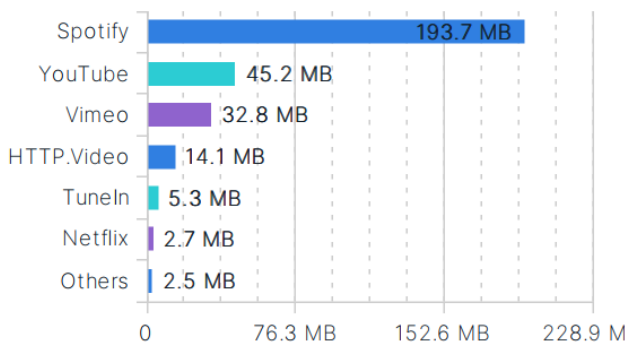
Top Peer-to-Peer Applications

Geen records gevonden.

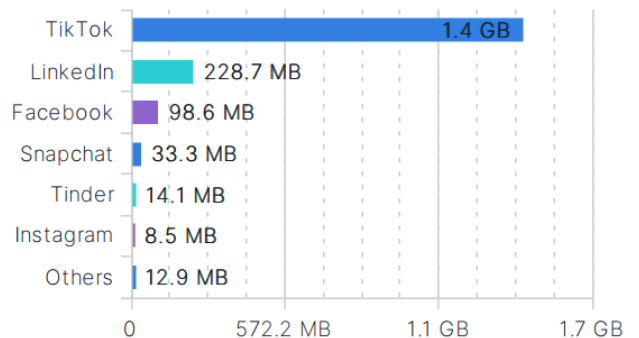
Top Gaming-applicaties



Top Video/Audio Streaming-applicaties



Top Social Media-applicaties



4.3. Top webapplicaties

In de huidige netwerkomgevingen maken veel applicaties gebruik van HTTP voor communicatie – zelfs applicaties waarvan je dit niet direct zou verwachten. Het belangrijkste voordeel van HTTP is dat de communicatie overal aanwezig, universeel geaccepteerd en (over het algemeen) open is op de meeste firewalls. Dit vergemakkelijkt de communicatie voor de meeste zakelijke en goedgekeurde applicaties, maar sommige niet-zakelijke applicaties gebruiken HTTP ook op een onproductieve of mogelijk schadelijke manier.

#	Applicatie	Sessies	Bandbreedte
1	HTTPS.BROWSER	484.660	122,65 GB
2	HTTPS	90.057	32,15 GB
3	Microsoft.Windows.Update	26.921	28,16 GB
4	Microsoft.365.Portal	44.503	6,14 GB
5	Microsoft.Portal	381.704	4,69 GB
6	Adobe.Update	416	3,78 GB
7	HTTP	1.860	3,60 GB
8	Apple.Services	2.098	3,41 GB
9	Amazon.AWS	834	2,60 GB
10	Google.Services	29.999	2,55 GB

4.4. Top websites op basis van browsing tijd

Geschatte browsing tijden per website kunnen nuttig zijn om een nauwkeurig beeld te krijgen van populaire websites. Deze lijst bevat vaak interne webresources zoals intranetten, maar kan ook wijzen op overmatig internetgebruik. Deze gegevens kunnen worden gebruikt om de implementatie van web caching-technologieën te rechtvaardigen of om zakelijke gebruiksbeleid vorm te geven.

#	Domein	Categorie	Browsing tijd (hh:mm:ss)
1	unifi.it-beheer.example	Informatie Technologie	129:48:28
2	avery-eu-west-1-svc.logicnow.us	Informatie Technologie	123:53:15
3	euce1-swprd2.sentinelone.net	Informatie Technologie	122:46:57
4	outlook.office365.com	Informatie Technologie	67:20:53
5	ctldl.windowsupdate.com	Informatie Technologie	65:15:55
6	eu-office.events.data.microsoft.com	Informatie Technologie, Web Hosting	57:56:51
7	signal.zetadisplay.com	Informatie Technologie	56:49:38
8	connectivitycheck.gstatic.com	Informatie Technologie, Zoekmachines en Portalen	55:38:51
9	checks-api.emea.system-monitor.com	Informatie Technologie	55:03:11
10	wcs.autosoftware.example	Zakelijk	53:06:09

4.5. Top webcategorieën

Webbrowsing-gedrag kan niet alleen wijzen op inefficiënt gebruik van bedrijfsresources, maar ook op suboptimale webfilteringbeleid. Daarnaast geeft het inzicht in het algemene surfgedrag van medewerkers en kan het helpen bij het definiëren van compliance-richtlijnen.

#	URL Categorie	Gebruikers	Aantal verzoeken	Bandbreedte
1	Informatie Technologie	93	964.620	95,66 GB
2	Zakelijk	70	43.244	7,81 GB
3	Zoekmachines en Portalen	80	40.899	2,12 GB
4	Persoonlijke Voertuigen	33	20.254	69,26 GB
5	Webgebaseerde E-mail	44	17.114	835,51 MB
6	Advertenties	53	15.409	444,08 MB
7	Webgebaseerde Applicaties	47	13.594	318,52 MB
8	Sociale Netwerken	44	12.243	403,25 MB
9	Nietszeggende Inhoud	37	10.982	126,42 MB
10	Content Servers	82	9.487	3,00 GB

4.6. Meest bezochte webdomeinen

De bezochte websites geven een goed beeld van hoe medewerkers bedrijfsresources gebruiken en hoe applicaties communiceren met specifieke websites. Door de toegangsgegevens van domeinen te analyseren, kunnen organisaties overwegen om hun bedrijfsinfrastructuur aan te passen. Dit kan bijvoorbeeld via websiteblokkering, diepgaande inspectie van cloudapplicaties, of de implementatie van webverkeersversnellingstechnologieën.

#	Domein	Categorie	Bezoeken
1	go.microsoft.com	Informatie Technologie	303.957
2	unifi.it-beheer.example	Informatie Technologie	76.729
3	uploadleuopel.systemmonitor.eu.com	Informatie Technologie	67.572
4	euce1-swprd2.sentinelone.net	Informatie Technologie	64.512
5	nc.softwarepakket.example	Informatie Technologie	49.508
6	outlook.office365.com	Informatie Technologie	33.562
7	watson.events.data.microsoft.com	Informatie Technologie	24.360
8	comserver-hb-eu1-fra-2.n-able.com	Informatie Technologie	23.358
9	checks-api.emea.system-monitor.com	Informatie Technologie	16.943
10	cwp.hosting.example	Informatie Technologie	16.668

5. Netwerkverbruik

Quick Stats



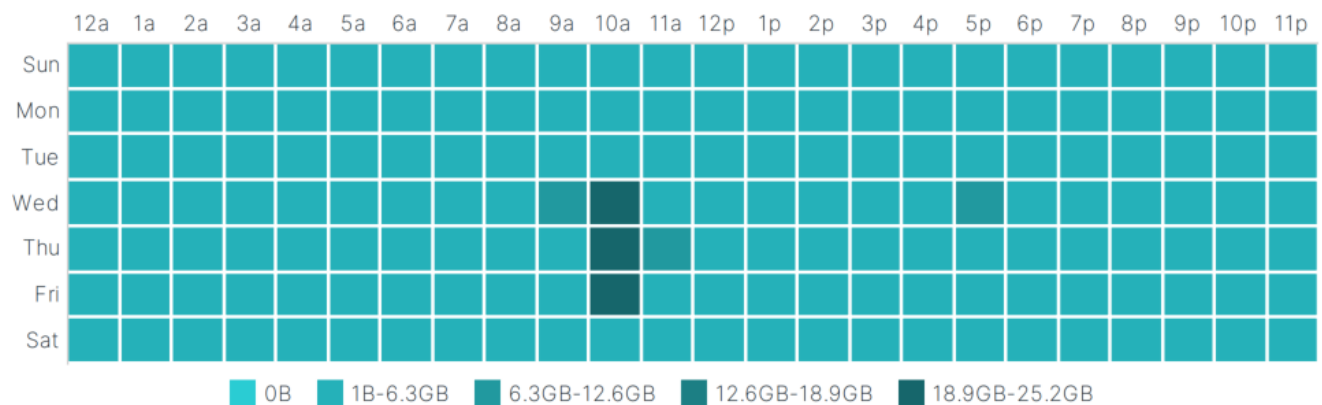
- **266,3 GB** Totale gebruikte bandbreedte
- **84,8%** Van het verkeer is SSL-versleuteld
- **10:00 - 11:00 uur** is het tijdslot met het hoogste dagelijkse piekverbruik
- **192.168.5.30** is de bron met het hoogste bandbreedteverbruik
- **192.168.5.3** is de bron met het hoogste aantal sessies
- **22,4** Gemiddelde logfrequentie per seconde
- **0,8%** Gemiddeld FortiGate CPU-gebruik
- **22,6%** Gemiddeld FortiGate geheugengebruik

5.1. Gemiddeld bandbreedteverbruik per uur

Door het bandbreedteverbruik per uur te analyseren, krijgen beheerders beter inzicht in de vereisten voor ISP-verbindingen en netwerksnelheden.

Daarnaast kan bandbreedte worden geoptimaliseerd door:

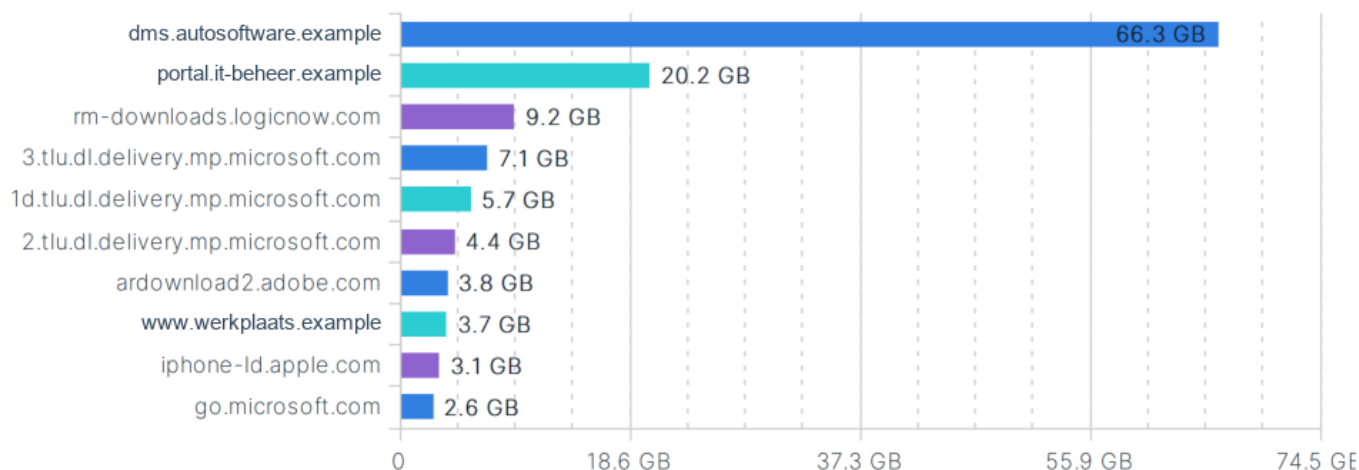
- Het toepassen van bandbreedtelimieten per applicatie
- Het prioriteren van specifieke gebruikers tijdens piekuren
- Het uitvoeren van updates buiten werktijden



5.2. Top bronnen/bestemmingen met het hoogste bandbreedteverbruik

Een van de meest effectieve manieren om bandbreedtegebruik te analyseren, is door te kijken naar de bronnen en bestemmingen die het meeste verkeer genereren.

- Veelvoorkomende externe bestemmingen (zoals OS/firmware-updates) kunnen worden begrensd (throttling) om zakelijk kritisch verkeer te prioriteren.
- Interne hosts met hoog bandbreedteverbruik kunnen worden geoptimaliseerd via verkeersbeheer of door het implementeren van gebruikersbeleid binnen de organisatie.



5.3. Top bronlanden van netwerkverkeer

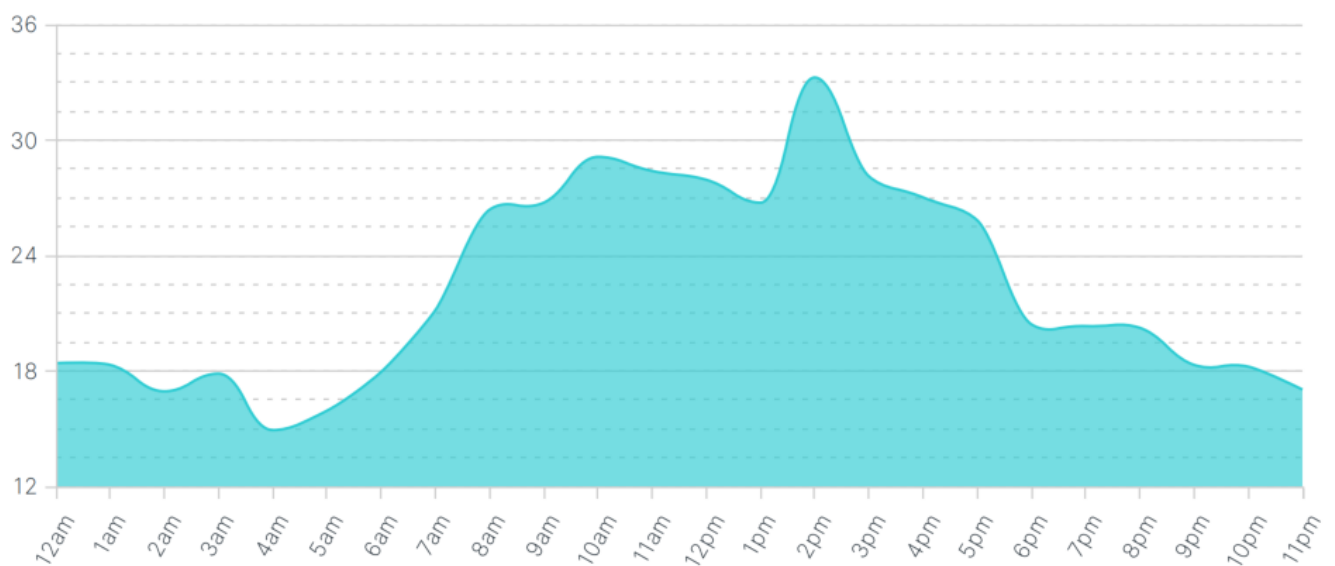
Door IP-verkeer te analyseren, kunnen we bepalen uit welk land specifieke aanvragen afkomstig zijn. Sommige botnets, command-and-control-functionaliteiten en zelfs externe toegang kunnen intensieve sessie-activiteit veroorzaken. Dit kan wijzen op gerichte aanvallen of aanhoudende dreigingen vanuit bepaalde landen. De onderstaande tabel geeft een overzicht van land-gebaseerd verkeer. Activiteiten uit specifieke landen kunnen afwijkend zijn en mogelijk verder onderzoek vereisen.

#	Land	Bandbreedteverbruik
1	Nederland	44,46 MB
2	Zwitserland	284,11 KB
3	Verenigde Staten	128,84 KB
4	Portugal	114,02 KB
5	Duitsland	92,43 KB
6	Verenigd Koninkrijk	38,77 KB
7	Frankrijk	14,23 KB
8	Zweden	10,48 KB
9	België	9,19 KB
10	Bulgarije	4,26 KB

5.4. Gemiddelde logfrequentie per uur

Inzicht in gemiddelde logfrequenties is essentieel voor het schaalbaar maken van een beveiligingsomgeving. Hoge logfrequenties in specifieke uren duiden meestal op piekmomenten in netwerkverkeer en doorvoersnelheid. Het berekenen van logfrequenties binnen een organisatie helpt bij het schaalbaar maken van logging- en analysetools zoals FortiAnalyzer. De hier getoonde logfrequenties zijn gebaseerd op volledige loggingcapaciteiten van FortiGate en omvatten alle logtypen, waaronder:

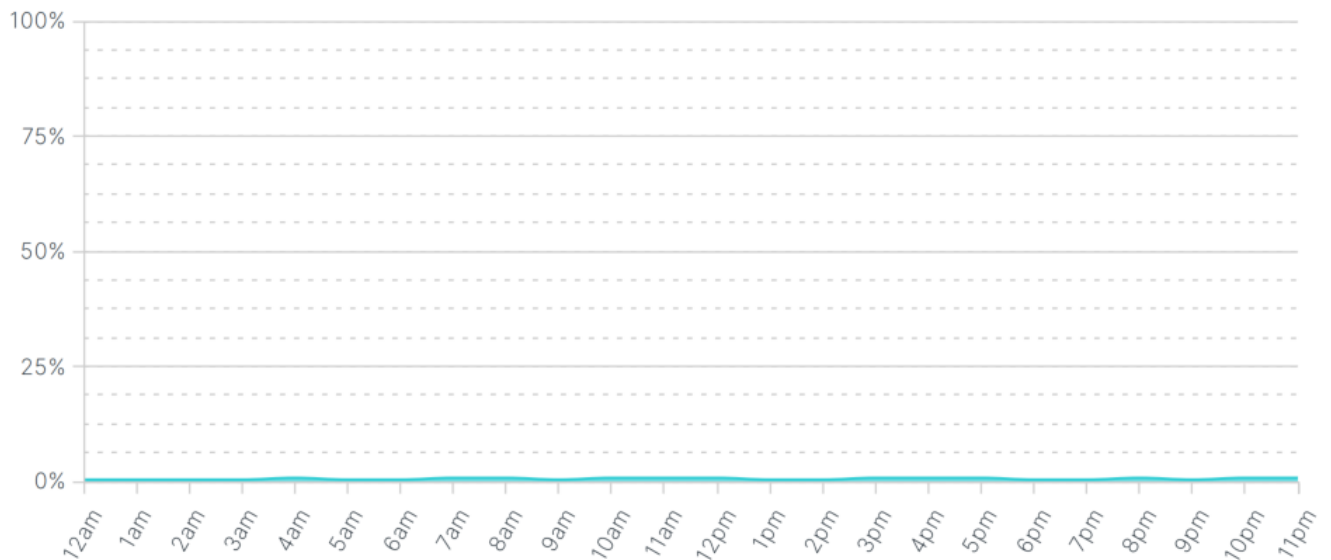
- Verkeer
- Antivirus
- Applicatiegebruik
- IPS-detecties
- Web- en systeemevenementen



5.5. Gemiddelde logfrequentie per uur

Het CPU-gebruik van een FortiGate wordt vaak gebruikt om de juiste netwerkoplossing te dimensioneren. Door een uurlijkse analyse van CPU-gebruik uit te voeren, kan een goed beeld worden gevormd van hoe FortiGate-apparaten zullen presteren binnen het doelnetwerk. Hoger dataverkeer leidt vaak tot meer gegenereerde logs, wat de CPU-belasting kan verhogen. Als het CPU-gebruik 75% of hoger blijft gedurende een lange periode, dan kan het nodig zijn om:

- Over te stappen op een krachtiger model
- De netwerkkarchitectuur te herzien
- Optimalisaties toe te passen, zoals verkeersbeheer en load balancing

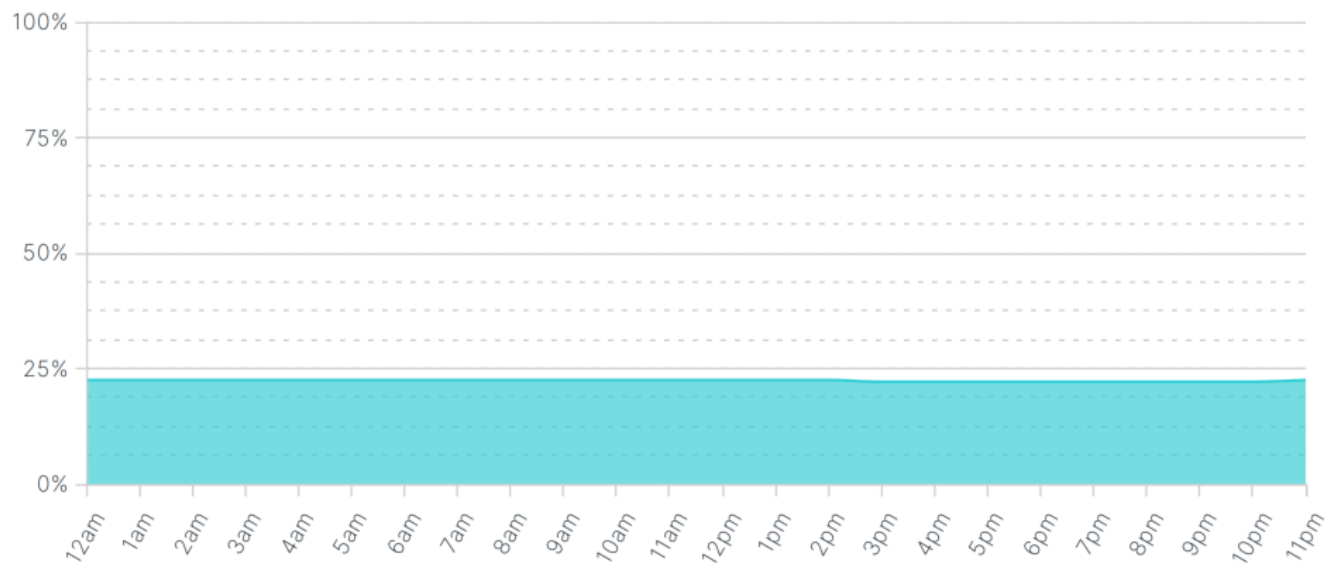


5.6. Gemiddeld FortiGate geheugengebruik per uur

Net als bij CPU-gebruik is geheugengebruik over tijd een belangrijke indicator voor de duurzaamheid en stabiliteit van een FortiGate in het netwerk. Hoge geheugengebruiksniveaus kunnen aanhouden, zelfs als het dataverkeer relatief laag is. Dit komt vaak door:

- Logging-activiteiten die veel geheugen vereisen
- Opgeslagen (gecachede) logbestanden die later worden verwerkt
- Intensieve inspectie van netwerkverkeer en beveiligingscontroles

Door het geheugengebruik per uur te analyseren, kan worden bepaald of de huidige FortiGate-configuratie optimaal is of dat aanpassingen nodig zijn voor betere prestaties en stabiliteit.



6. Aanbevelingen

6.1. Verbeter detectie van schadelijke URL's en training

Websites met bekende schadelijke URL's worden binnen jouw organisatie bezocht en kunnen mogelijk webfiltercontroles omzeilen. We raden de volgende acties aan:

- Zorg ervoor dat jouw webfilteringcontroles up-to-date zwarte lijsten gebruiken.
- Train jouw medewerkers om nooit te klikken op onbekende URL's in e-mails.

6.2. Onderwijs en bescherm gebruikers tegen phishing-aanvallen

We hebben gedetecteerd dat bepaalde bezochte URL's probeerden gevoelige informatie van interne gebruikers te verkrijgen. Zorg ervoor dat je:

- Medewerkers traint om echte en frauduleuze afzenders te onderscheiden.
- Een e-mailgateway implementeert die moderne phishing-aanvallen detecteert en blokkeert.

6.3. Segmenteer het netwerk om risico's te beperken

Tijdens de beoordeling is gebleken dat verschillende soorten apparaten zich op hetzelfde netwerksegment bevinden. Dit vergroot het aanvalsoppervlak en vergemakkelijkt laterale beweging bij een eventuele besmetting of aanval.

We adviseren een duidelijke netwerksegmentatie toe te passen, waarbij de volgende groepen apparaten in aparte VLAN's worden geplaatst:

- Servers
- Werkplekken (pc's/laptops)
- Printers
- Telefoons (VoIP)
- Tablets / mobiele apparaten
- Gastennetwerk (reeds benoemd)

Daarnaast adviseren wij om intra-VLAN traffic zoveel mogelijk te blokkeren (client isolation), tenzij dit expliciet nodig is voor de bedrijfsvoering. Hiermee wordt voorkomen dat een geïnfecteerd apparaat direct andere apparaten binnen hetzelfde segment kan benaderen.

Deze aanpak:

- Verkleint het risico bij malware-uitbraken
- Verbetert zichtbaarheid en controle per netwerkzone
- Maakt het eenvoudiger om beveiligingsbeleid per segment toe te passen

6.4. Beperk de inkomende Site-to-Site VPN tot strikt noodzakelijke communicatie

Tijdens de analyse is geconstateerd dat er een actieve Site-to-Site VPN-verbinding aanwezig is. Hoewel dit nuttig kan zijn voor samenwerking tussen vestigingen, vormt het ook een potentieel risico wanneer er geen restricties zijn op het type verkeer dat erdoorheen mag.

Wij adviseren daarom om:

- Alleen specifiek verkeer dat functioneel noodzakelijk is toe te staan (bijv. domeinverkeer, RDP naar een server, of specifieke applicatiepoorten)
- Overige communicatie tussen de netwerken standaard te blokkeren
- Logging in te schakelen op de VPN-interface voor monitoring van ongewenst verkeer
- Regelmatig te controleren of de toegestane communicatie nog actueel en noodzakelijk is

Deze maatregel helpt om de zogeheten aanvalsroute via interne tunnels te verkleinen en om ongeautoriseerde toegang of laterale beweging te voorkomen bij een eventuele besmetting in één van de vestigingen.

Kom je
er niet uit?

Bel ons!
0412 - 744 300

We helpen je graag!

#AltijdVeiliginBedrijf

