FORTINET

WHITE PAPER

Security-Driven Networking

Het hoe en waarom

1 Inleiding 3

1.1 Beveiligingsstrategie 3

1.2 Security by design 4

1.3 Integratie 4

2 Security-Driven Networking 5

2.1 Next Generation Firewall (NGFW) 5

2.1.1 Perimeter firewall 6

2.1.2 Interne segmentatiefirewall (ISFW) 9

2.2 Secure WLAN/LAN 10

2.2.1 Geïntegreerde netwerk- en securityinfrastructuur 11

2.2.2 Complete zichtbaarheid 11

2.3 Network Access 12

2.3.1 FortiNAC 12

2.3.2 FortiOS native NAC 12

2.4 Fabric Management Center 13

2.4.1 FortiManager 13

2.4.2 FortiAnalyzer 14

2.5 Topologie 15

2.5.1 Kleine organisatie (ca. 50 – 250 medewerkers) 15

2.5.2 Middelgrote organisatie (ca. 250 – 500 medewerkers) 16

2.5.3 Grote organisatie (> 500 medewerkers) 17

3 Conclusie 18

Bijlage 1 – Conformiteit met bestaande kaders 19

1 Inleiding

Dit semi-technische whitepaper heeft tot doel u als lezer mee te nemen in het hoe en waarom van Fortinets Security-Driven Networking propositie. Na het lezen van dit document zult u tenminste:

1. Begrijpen hoe een coherente en geïntegreerde netwerk- en securityinfrastructuur leidt tot een substantiële verbetering van de digitale weerbaarheid;
2. Begrijpen hoe het gebruik van slechts één managementinterface voor de gehele netwerk- en securityinfrastructuur bijdraagt aan een drastische verlaging van de beheerlast;
3. Begrijpen hoe u aan de hand van rapportages in een oogopslag in staat wordt gesteld de door u binnen de netwerk- en securityinfrastructuur geïmplementeerde maatregelen te toetsen op conformiteit.

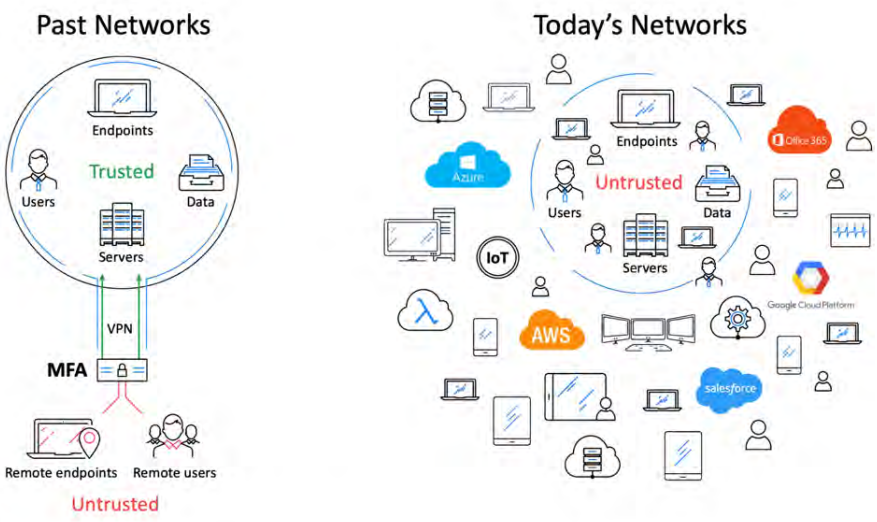
Leeswijzer

Alvorens de individuele onderdelen in detail te beschrijven en u enkele voorbeeld-designs mee te geven in hoofdstuk 2, beschrijft hoofdstuk 1 een aantal stappen en overwegingen waar u voorafgaand aan het vernieuwen van een netwerkinfrastructuur idealiter rekening mee dient te houden. Het derde hoofdstuk bevat een afsluitende conclusie en nawoord, waarna bijlage 1 u tot slot een handig overzicht biedt van de conformiteit van de beschreven oplossing ten aanzien van diverse veel in Nederland gehanteerde normen en standaarden.

1.1 Beveiligingsstrategie

De afgelopen jaren zien wij als Fortinet een aantal belangrijke ontwikkelingen die van invloed zijn op de aanpak van IT-security in het algemeen, waaronder:

- De zakelijke wereld draait in immer toenemende mate om digitalisering, sterker nog: data is tegenwoordig verreweg het waardevolste bezit van een organisatie. Schade aan deze data of zelfs verlies ervan is veelal desastreus voor het voortbestaan van de organisatie in kwestie;
- Consumentisering is een duidelijk waarneembare trend onder zakelijke gebruikers, wat zo veel wil zeggen dat deze gebruiker zakelijk minstens dezelfde mogelijkheden wil hebben als dat hij/zij privé – als consument – ook heeft. Denk aan: het altijd en onbeperkt online zijn, ongelimiteerde toegang tot data vanaf elk device, en de hoogst mogelijke snelheid (“ik wil het en ik wil het nú”).
- Een explosieve adoptie van clouddiensten – ongeacht of dit nu SaaS, PaaS of IaaS betreft –, introductie van Bring Your Own Device-initiatieven, en ingebruikname van IoT-/headless devices brengt nieuwe risico’s en vraagstukken met zich mee als: “waar staat mijn data en hoe beveilig ik deze?” tot aan “welke devices hebben toegang tot het netwerk en welke controle heb ik daar over?”.



Figuur 1 - Traditioneel versus modern netwerk

Deze en soortgelijke trends hebben ertoe geleid dat de aanpak van IT-security navenant efficiënter, effectiever en meer betrouwbaar dient te zijn. Een traditionele aanpak waarbij er een muur is getrokken rondom het interne netwerk met één enkel toegangspunt (zie figuur 1) volstaat anno 2020/2021 niet meer. Binnen een moderne netwerk- en securityinfrastructuur ontbreekt het aan een duidelijke perimeter, waardoor meer en andere security-maatregelen noodzakelijk zijn.

Normenkaders als de ISO-27001/27002 en NIST 800-53 kunnen zeer bruikbaar zijn om te bepalen welke middelen en/of maatregelen u als organisatie (nog) zou moeten nemen. In sommige gevallen is dit overigens niet zo vrijblijvend; bijvoorbeeld als uw organisatie een ISO-27001 certificaat wenst te behalen, of zelfs alleen maar omdat u door wet- en regelgeving daartoe verplicht bent. Wat de precieze aanleiding voor u ook is, het startpunt is vrijwel altijd dezelfde: begin met het bepalen van de beveiligingsstrategie en stel op basis daarvan het te voeren beleid vast.

Een tegenwoordig veel gehanteerde beveiligingsstrategie is het zogenaamde Zero-Trust-model. In plaats van te geloven dat alles achter de perimeter firewall veilig is heeft een Zero-Trust- beveiligingsmodel[1] een andere benadering; het gaat juist uit van inbreuk. In een Zero-Trust-model wordt daarom elk toegangsverzoek, zelfs als deze van binnen het eigen netwerk komt, middels stringente policies getoetst op basis van authenticatie en autorisatie, en geïnspecteerd op afwijkingen voordat daadwerkelijk toegang wordt verleend. Met ‘toegang’ wordt niet alleen toegang tot het netwerk bedoelt, maar bijvoorbeeld ook tot specifieke (gevoelige) applicaties en data. Uiteraard worden alle events gelogd teneinde het kunnen uitvoeren van een audit (denk aan compliance in geval van bijvoorbeeld eerdergenoemde ISO-27001 certificering en/of toepasselijke wet- en regelgeving), of het uitvoeren van een diepgaande analyse indien er sprake is van een securityincident.

Deze strategische aanpak van informatiebeveiliging wordt steeds meer als dé norm beschouwd in de ontwikkeling van beveiligingsbeleid, óók als het betrekking heeft op de netwerkinfrastructuur. Fortinet biedt binnen haar Security-Driven Networking propositie de capaciteiten die nodig zijn – en meer – om binnen de netwerkinfrastructuur op eenvoudige wijze een Zero-Trust-beleid te implementeren.

1.2 Security by design

Het moment waarop een bestaande netwerkinfrastructuur moet worden vervangen door bijvoorbeeld veroudering, of een nieuwe netwerkinfrastructuur moet worden gerealiseerd vanwege een verhuizing of de ingebruikname van een nieuwe locatie, is bij uitstek het geschikte moment om tot een ‘secure by design’ ontwerp te komen waarin ook is nagedacht over informatiebeveiliging.

Immers, wanneer informatiebeveiliging in de ontwerpfase centraal wordt gezet kan er reeds bij implementatie een geïntegreerde en coherente netwerk- en security-infrastructuur (NSI) tot stand komen dat voldoet aan alle wensen vanuit zowel het netwerkteam als ook het securityteam, zonder dat er later additionele investeringen nodig zijn of onnodige complexiteit ontstaat door het ‘aan elkaar moeten knopen’ van technologieën. Dit onderstreept dan ook direct het belang van het betrekken van de CISO in deze fase. Hij/zij weet aan welke eisen het netwerk dient te voldoen als het gaat om security en compliance, iets wat de netwerkarchitect of -beheerder uit hoofde van diens functie niet altijd weet (of hoeft te weten).

1.3 Integratie

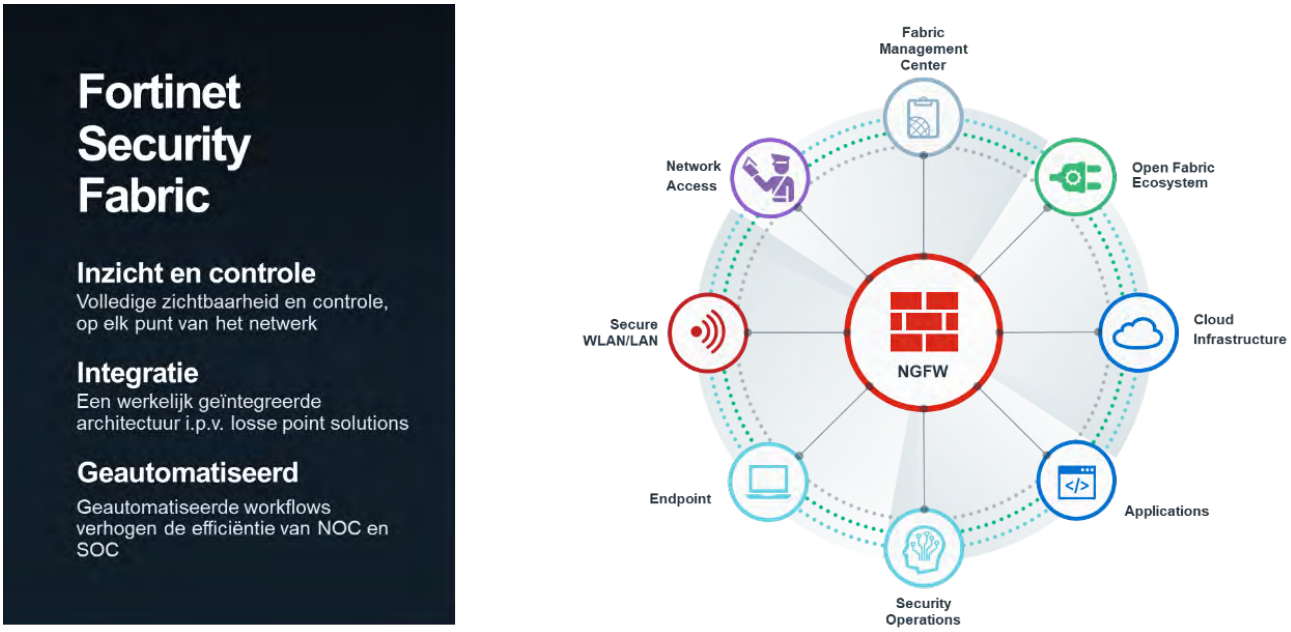
Veel organisaties kiezen vandaag de dag nog voor standalone oplossingen binnen hun netwerkinfrastructuur, soms gedreven door een multi-vendor beleid, vaker omwille van een subjectief ‘best of breed’ gedachtegoed. Feit is echter dat met een keuze voor standalone oplossingen vaak silo’s ontstaan die grotendeels onafhankelijk

[1] Zie: https://go.forrester.com/government-solutions/Zero-Trust/

van elkaar functioneren. Het gevaar is dat hierdoor de beheerlast juist onevenredig groot wordt én dat dit ten koste gaat van een adequate beveiliging.

Fortinet is ervan overtuigd dat het positioneren van standalone oplossingen in een netwerk- en security-infrastructuur niet de meest efficiënte en effectieve manier is om enerzijds malware, cryptolockers en aanvallers buiten de deur te houden, en anderzijds een beheersbare omgeving te creëren. Vanuit deze visie heeft Fortinet diens 'Security Fabric' ontwikkeld; hierbij werken producten/oplossingen van Fortinet zelf, maar ook die van technologiepartners, naadloos met elkaar samen. Deze samenwerking kan op vele manieren plaatsvinden, bijvoorbeeld van het realtime delen van threat intelligence tussen de verschillende componenten, tot aan het afdwingen van compliance over endpoints binnen én buiten het netwerk. Daarnaast vormt de geïntegreerde securityinfrastructuur een eenvoudig te beheren omgeving, out-of-the-box correlatie van events en een duidelijker overzicht over activiteiten in de IT-omgeving.

Deze overkoepelende fabric-visie kan worden toegepast op diverse IT-deelgebieden, zo ook op de netwerkinfrastructuur. Security-Driven Networking vloeit dan ook voort uit deze visie en omvat minimaal de onderdelen NGFW, Secure WLAN/LAN en Network Access (zie figuur 2). Het Fabric Management Center component is niet altijd benodigd, maar zeker van grote meerwaarde in het geheel.



Figuur 2 - Security Fabric

2 Security-Driven Networking

In dit hoofdstuk gaan we dieper in op de individuele onderdelen NGFW, Secure WLAN/LAN en Network Access welke tezamen onze Security-Driven Networking oplossing vormen. Ook wordt aandacht besteed aan het Fabric Management Center en welke waarde dit component toevoegt aan de andere onderdelen.

2.1 Next Generation Firewall (NGFW)

De FortiGate, zijnde het Next Generation Firewall platform van Fortinet, staat aan de basis van de Security Fabric en de daaruit voortvloeiende Security-Driven Networking propositie. Hoewel er qua positie in het netwerk meerdere deploymentopties zijn, concentreren we ons hier op twee, te weten: de perimeter firewall aan de rand van het netwerk, en de interne segmentatiefirewall in het hart ervan.

2.1.1 Perimeter firewall

De perimeter firewall – ook wel edge-firewall genoemd – vormt bij uitstek hét startpunt in een netwerk- en securityinfrastructuur. Primair is deze firewall verantwoordelijk voor de bescherming van het interne netwerk tegen de 'grote boze buitenwereld', bijvoorbeeld door het verkeer van/naar het internet – het zogenaamde Noord-Zuid verkeer – te inspecteren en te beveiligen tegen aanvallen van buitenaf. Daarnaast wordt de firewall veelal als gateway ingezet waarop VPN-tunnels van remote medewerkers worden getermineerd (in combinatie met multi-factor authenticatie), of zelfs als slimme router die dynamische routering toepast over het internet. De mogelijkheden die de FortiGate kan bieden op deze positie zijn legio en slechts beperkt tot de binnen FortiOS – Fortinets uniforme operating systeem van onder andere de FortiGate – geïntegreerde features.

2.1.1.1 Sizing

Een juiste sizing van de perimeter firewall is van belang om het risico op het creëren van een zogenaamde *bottleneck* aan de rand van het netwerk te voorkomen. Variabelen waar terdege rekening mee gehouden dient te worden bij de sizing zijn bijvoorbeeld de benodigde poortconfiguratie, het maximaal aantal simultane TCP/IP-sessies (rekening houdend met toekomstige groei in clouddiensten!), en de gewenste netto doorvoersnelheid, uitgaande van volledige content inspectie. Dit houdt in dat het Noord-Zuid verkeer gecontroleerd wordt op de aanwezigheid van malware en alle andere dreigingen waar signatures voor beschikbaar zijn. Gangbare termen voor deze netto doorvoersnelheid zijn *Threat Protection Throughput* of *Threat Prevention Throughput*.

2.1.1.2 Virtueel versus fysiek

Een trend die zich al jaren in IT-landschap voordoet is het virtualiseren van services om zo slimmer en efficiënter om te gaan met hardware resources. Ook Fortinet heeft virtuele appliances in haar assortiment, dat geldt tevens voor de FortiGate firewall. In geval van een on-premises deployment van een perimeter- of interne segmentatie firewall is ons advies echter hier een fysieke appliance voor in te zetten, omwille van een optimale performance. De virtuele appliance komt het best tot zijn recht als firewall in de (public) cloud, danwel als datacenter firewall in een (hyperconverged) datacenter omgeving; beide scenario's zijn echter buiten scope van dit document.

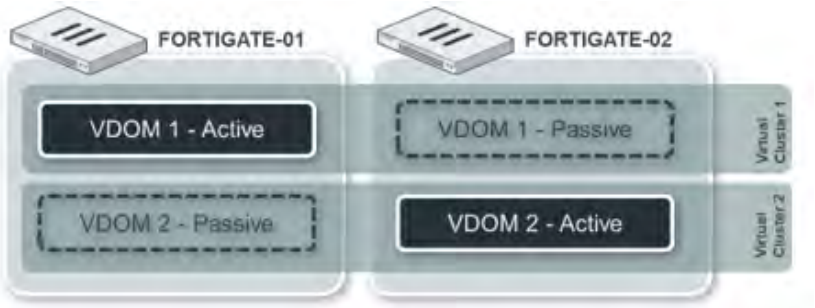
De fysieke firewall-lijn van Fortinet laat zich kenmerken door een zogenaamde hardware architectuur. Naast een standaard CPU bevat deze vrijwel altijd – desktopmodellen uitgezonderd – purpose-build ASICs welke netwerktaken en content inspectie in hardware uitvoeren en daarmee de CPU offloaden. Door deze hardware acceleratie, in combinatie met het volledig in eigen huis ontworpen operating systeem en securityfeatures, zal een FortiGate zelfs in veeleisende omgevingen tot zijn recht komen.

2.1.1.3 Beschikbaarheid

In geval van een perimeter-firewall omgeving is een hoge beschikbaarheid erg belangrijk. Een enkelvoudige deployment zou een zogenaamde *single point of failure* opleveren, met een verhoogd risico op een verbroken verbinding met de buitenwereld. Met behulp van twee FortiGate firewalls kan een hoog beschikbare firewallomgeving worden gecreëerd in de vorm van een zogenaamde High Availability (HA) cluster. Qua

ondersteunde modi operandi spreken we over active-active (beide firewalls verwerken actief verkeer) en active-passive (alleen de primaire firewall verwerkt actief verkeer, de ander staat standby). Voor het netwerk lijkt een HA-cluster te functioneren als een enkele FortiGate firewall die netwerkverkeer verwerkt en de gebruikelijke beveiligings-services biedt.

Virtual clustering breidt deze HA-functionaliteit verder uit door fail-over bescherming en load-balancing te bieden voor een FortiGate firewall die met meerdere VDOM's werkt (zie figuur 3). Door gebruik te maken van VDOM's en virtual clustering kunnen resources efficiënter worden ingezet, beide firewalls zijn immers actief.

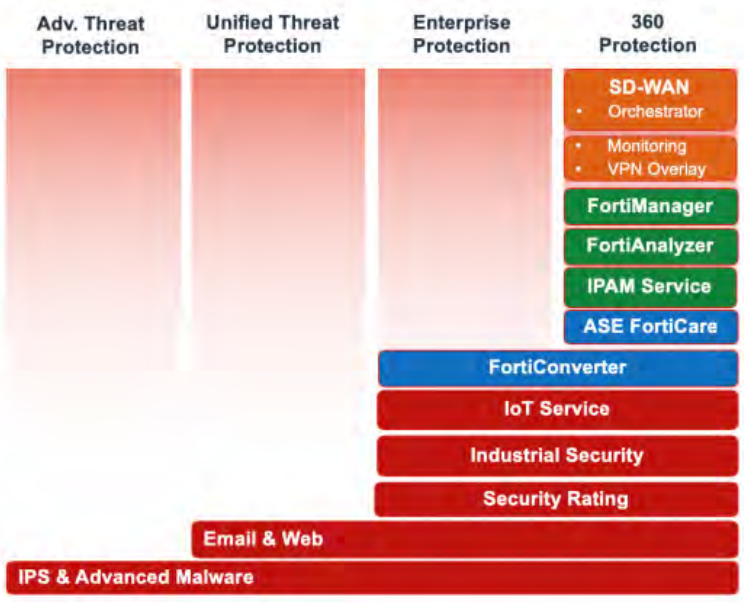


Figuur 3 - Virtual clustering

NB. Groot voordeel van firewall appliances van Fortinet is dat deze standaard het gebruik van zogenaamde Virtual Domains (VDOM's) ondersteunen. Ieder VDOM vertegenwoordigt een logische firewall met eigen dedicated resources. Met behulp hiervan kan naar wens een logische scheiding worden aangebracht tussen verschillende omgevingen en/of firewall-rollen.

2.1.1.4 Security

De FortiGate beschikt standaard over een aantal functionaliteiten waarvoor geen licentie of abonnement nodig is. Hierbij moet gedacht worden aan: integratie met een aanwezige IdM-oplossing ten behoeve van het verkrijgen van gebruikersinformatie (i.p.v. slechts een IP-adres), applicatieherkenning, SSL-inspectie en het kunnen blokkeren van specifieke bestandstypen.



Figuur 4 - Security bundels

Voor andere, meer specifieke securityfuncties zijn abonnementen (security bundels, zie figuur 4) beschikbaar waardoor de firewall meer mogelijkheden krijgt om verkeer te controleren op bedreigingen. Omdat de perimeter firewall de zogenaamde *first line of defense* is, is een uitgebreide set aan securityfeatures op deze positie aanbevolen.

De meest gekozen security bundel op de FortiGate welke als perimeter firewall dienstdoet is de Unified Threat Protection-bundel. Deze biedt o.a. advanced malware protection (incl. sandboxing), IPS, antispam en webfiltering. Goede tweede is de Enterprise Protection-bundel die – in vergelijk met de UTP-bundel – een aantal additionele zaken biedt,

waaronder een in hoofdstuk 2.3 nader besproken IoT-detectieservice (identificatie van IoT devices t.b.v. Network Access Control), industriële security op ICS/SCADA protocollen, FortiConverter service om bestaande firewall rules en policies van een ander merk firewall te converteren, en Security Rating als een proactieve dashboardservice waarbij de configuratie van de FortiGate wordt gecheckt tegen algemene best practices.

Welke bundel het beste past is natuurlijk afhankelijk van de specifieke behoefte van een organisatie, wel adviseren we minimaal de UTP-bundel als het gaat om een perimeter firewall deployment.

2.1.1.5 Advanced Threat Protection (ATP)

FortiGate Cloud Sandbox – onderdeel van alle voor de FortiGate beschikbare securitybundels – controleert onbekende uitvoerbare bestanden door:

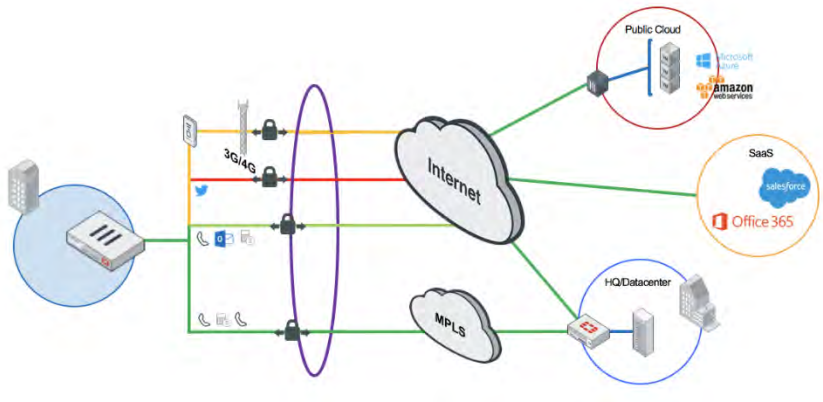
1. **Cloud query (statische analyse)** - Gebruikmaking van een realtime check tegen een enorme online threat-database van FortiGuard Labs (de threat researchafdeling van Fortinet).
2. **Sandboxing (dynamische analyse)** - Uitvoeren van het bestand in een of meer virtuele machines (VM's) om te bepalen of het bestand een hoog, gemiddeld of laag risico vormt op basis van het gedrag dat wordt waargenomen.

Door de combinatie van statische en dynamische analyse is de FortiGate in staat om ook beveiliging te bieden tegen zogenaamde Zero-Day bedreigingen. Dit zijn nog onbekende bedreigingen waarvoor nog geen signatures zijn ontwikkeld.

NB. Een advanced threat protection (ATP) oplossing zoals hierboven omschreven is, met het oog op risico's die gepaard gaan met Zero-Day bedreigingen, een *must have* in elke netwerk- en securityinfrastructuur en maakt om die reden onderdeel uit van al onze securitybundels.

2.1.1.6 Secure SD-WAN

Door een zelf ontwikkelde SD-WAN-oplossing in haar next generation firewalls te integreren, anticipeert Fortinet op een bij gedistribueerde organisaties momenteel populaire ontwikkeling. Waar de meeste SD-WAN-oplossingen echter voornamelijk gericht zijn op connectiviteit, heeft Fortinet dit ontworpen vanuit een security-by-design principe. Fortinet spreekt dan ook eerder over "Secure SD-WAN" dan over SD-WAN. De perimeter FortiGate firewall biedt deze functionaliteit zonder daartoe benodigde licentie.



Figuur 5 - Visualisatie Secure SD-WAN

Door de combinatie van laag-7 firewalling, advanced routing en next generation securityfeatures kan elke FortiGate niet alleen dynamisch omgaan met het gebruik van meerdere WAN-verbindingen maar kan het ook verkeer sturen op basis van beveiligingsbeleid, al dan niet voortvloeiend vanuit wet- en regelgeving. Zo kan bijvoorbeeld malware of botnet-verkeer worden gemitigeerd, terwijl tegelijkertijd op basis van applicatie-herkenning zakelijke applicaties worden onderscheiden van en voorrang krijgen op persoonlijke applicaties door deze over de WAN-verbinding met de beste performance te sturen.

Dankzij dit concept kunnen dure WAN-verbindingen met een extra hoge SLA uiteindelijk worden vervangen door normale internetlijnen van verschillende providers. Het concept wordt slechts beperkt door de aanwezigheid van IP-connectiviteit, op welke manier (ADSL/VDSL, kabel, glasvezel, 3G/4G, etc.) deze IP-connectiviteit wordt geleverd, is feitelijk niet belangrijk. De SD-WAN-oplossing binnen de FortiGate kiest automatisch het meest optimale pad, op basis van continue monitoring van meerdere kritieke parameters (latency, jitter en packetloss). Door eenvoudigweg meerdere WAN-verbindingen tot één logische interface te virtualiseren, is elke verbinding automatisch een back-up of failover voor een andere verbinding. In figuur 5 ziet u een visualisatie.

2.1.2 Interne segmentatiefirewall (ISFW)

Anno 2020/2021 zijn er talloze voorbeelden beschikbaar van security-breaches die zich bij organisaties hebben voorgedaan waarbij de schade beperkt had kunnen worden middels gedegen netwerksegmentatie. Het belang van segmentatie en L7 inspectie van verkeer tussen deze segmenten dient dan ook niet lichtvaardig te worden opgevat. Niet voor niets adviseert het NCSC in een netwerk niet langer te vertrouwen op uitsluitend access control lists (wat feitelijk niets anders is dan statische packetfiltering) en in plaats daarvan een segmentatie-firewall met IPS-functionaliteit te implementeren[2]. Het FortiGate platform biedt deze mogelijkheden en vormt hiermee een fundamenteel bouwblok voor een veilige en gesegmenteerde netwerkinfrastructuur.

2.1.2.1 ISFW als (collapsed) core-switch

In een tot voor kort gebruikelijke situatie waarbij het netwerk eerst wordt gerealiseerd en waar later securitymaatregelen – zoals een interne segmentatiefirewall – aan toe worden gevoegd, ontstaat een vaak onnodig complex geheel. In de core van het netwerk leidt dit bijvoorbeeld tot het moeten beheren van minstens een redundante core-switch én een redundante ISFW-opstelling met dus twee verschillende operating systemen. Bovendien staat de ISFW dan veelal niet *in-line* waardoor te inspecteren verkeer op een relatief omslachtige manier door de ISFW moet worden geleid, bijvoorbeeld door gebruikmaking van VRF-technieken. Deze aanpak brengt zoals gezegd onnodige complexiteit met zich mee, wat weer leidt tot een hogere foutgevoeligheid en verlaging van de digitale weerbaarheid.

Binnen de Security-Driven Networking propositie neemt de FortiGate die dienstdoet als ISFW ook de rol van core-switch/L3-router op zich, welke het verkeer tussen interne netwerksegmenten (VLAN's) zal gaan routeren. Groot pluspunt is dat dit dus gedaan gaat worden door een security-device, welke ook L7-inspectie voor haar rekening kan nemen. Hiermee wordt de eerdergenoemde complexiteit weggenomen en tegelijkertijd de weerbaarheid tegen interne dreigingen verhoogd.

NB. De te verwachten latency in dit scenario is verwaarloosbaar; met een sterke achtergrond in de hoek van telecommunicatie en internet service providers, heeft Fortinet in iedere FortiGate een krachtige routerings- en inspectieperformance ingebouwd. Vrijwel alle netwerk- en content inspectietaken worden in dedicated hardware uitgevoerd, zijnde eerdergenoemde co-processors (ASIC's) die de generieke CPU offloaden.

2.1.2.2 Sizing

Waar de perimeter firewall verantwoordelijk is voor routering, inspectie en beveiliging van het Noord-Zuid verkeer, is de interne segmentatiefirewall op gelijke wijze verantwoordelijk voor het interne Oost-West verkeer. Qua volume is dit verkeer van oudsher groter dan het Noord-Zuid verkeer waardoor het kiezen van een platform met voldoende capaciteit (denk aan poorten, sessies en doorvoersnelheid) des te meer van cruciaal belang is.

[2] Zie: https://www.ncsc.nl/documenten/publicaties/2019/mei/01/handreiking-voor-implementatie-van-detectie-oplossingen

2.1.2.3 Beschikbaarheid

Binnen de Security-Driven Networking propositie fungeert de ISFW ook als core-switch waar de volledige L3-routering binnen het netwerk plaatsvindt. Dit heeft als belangrijkste voordeel dat al het inter-VLAN verkeer door de firewall loopt en dus geïnspecteerd kan worden op o.a. ongewenste afwijkingen. Door deze positionering vormt de firewall een kritisch component en dient deze dus te allen tijde redundant te worden uitgevoerd.

2.1.2.4 Security

Qua minimaal benodigde securityfeatures op de ISFW lopen de meningen uiteen. U heeft kunnen lezen dat het NCSC op Oost-West verkeer het gebruik van Intrusion Prevention System (IPS) aanbeveelt; dit beschouwen wij dan ook als absoluut minimum. Met het oog op de snelle opkomst van *unmanaged* devices in het netwerk (bijvoorbeeld devices die privé-eigendom zijn van medewerkers) zijn features als antivirus en sandboxing echter een meer dan welkome toevoeging. Omdat deze devices reeds binnen het netwerk opkomen wordt een virus niet door de perimeter firewall opgemerkt, met alle mogelijke gevolgen van dien. Dit in ogenschouw nemende en realiserend dat features als webfiltering en antispam niet zinvol zijn op de ISFW, heeft Fortinet juist voor de interne segmentatiefirewall de Advanced Threat Protection bundel ontwikkeld (zie figuur 4), welke bestaat uit IPS, antivirus en sandboxing.

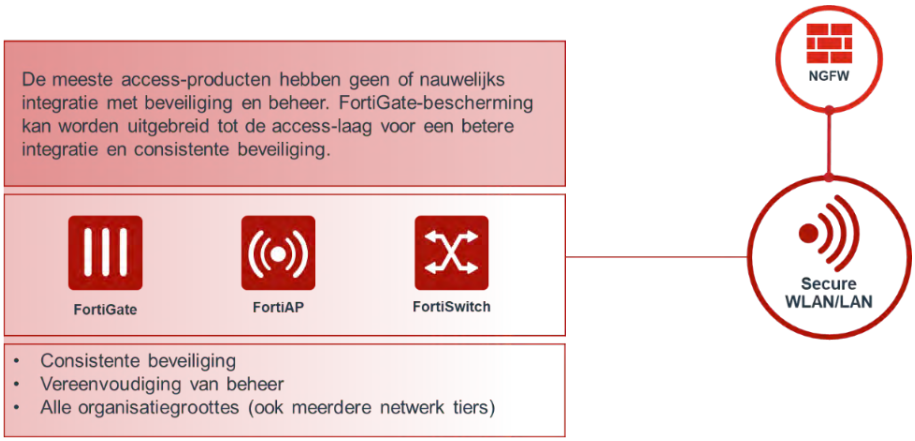
NB. Intrusion Prevention System (IPS) dient niet te worden verward met Intrusion Detection System (IDS). De eerste is in staat daadwerkelijk in te grijpen bij ongewenst/afwijkend verkeer, waar een IDS slechts een detectieve functie heeft. Een IPS staat dan ook *in-line* waar een IDS meestal *out-of-band* te vinden is.

2.1.2.5 Microsegmentatie

Een veel gehoorde term binnen securitylandschap is 'microsegmentatie'. Waar netwerksegmentatie met behulp van VLAN's bedoeld is om op netwerkniveau het aanvalsoppervlak te verkleinen (bij een aanval kan minder makkelijk *lateral movement* plaatsvinden in een gesegmenteerd netwerk), doet microsegmentatie dit op identiteit- of workload-niveau, oftewel nog een laag dieper dan VLAN's. Om microsegmentatie te kunnen toepassen met behulp van een firewall dient deze zich bewust te zijn van identiteiten (users en/of devices) en workloads (applicaties) en kan deze policies toepassen op verkeer daartussen. Daarbij maakt het dus niet uit of het inter-VLAN of intra-VLAN verkeer betreft. De FortiGate ISFW is vanwege een veelvoud aan identificatie-mogelijkheden en L7 firewall functionaliteit in staat om microsegmentatie toe te passen op Oost-West verkeer.

2.2 Secure WLAN/LAN

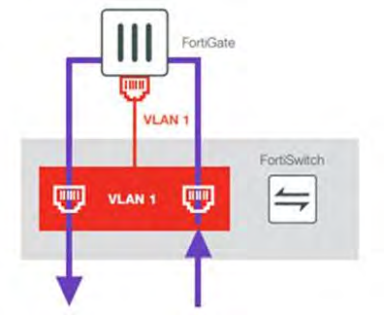
U heeft eerder kunnen lezen dat de interne segmentatiefirewall, welke binnen onze Security-Driven Networking propositie tevens dienstdoet als core-switch/L3-router, verantwoordelijk is voor inspectie en beveiliging van het interne Oost-West verkeer. Deze firewall functionaliteit kunnen we eenvoudig doortrekken naar iedere individuele access-poort en/of wireless SSID door FortiSwitches en FortiAP's te koppelen aan de FortiGate. Met behulp van een geïntegreerde LAN- en WLAN-controller vormt de FortiGate de *control plane* van deze onderliggende (downstream) switches en access points.



2.2.1 Geïntegreerde netwerk- en securityinfrastructuur

Door FortiSwitches en FortiAP's te combineren met de FortiGate interne segmentatiefirewall wordt een alomvattende netwerk- en securityoplossing gerealiseerd welke beheerd wordt vanuit de FortiGate GUI. Iedere (sub-)interface dat zich in het netwerk bevindt wordt hierdoor als het ware een interface op de firewall zelf. Security kan aldus op een veel dieper netwerkniveau worden toegepast, zonder additionele complexiteit met zich mee te brengen.

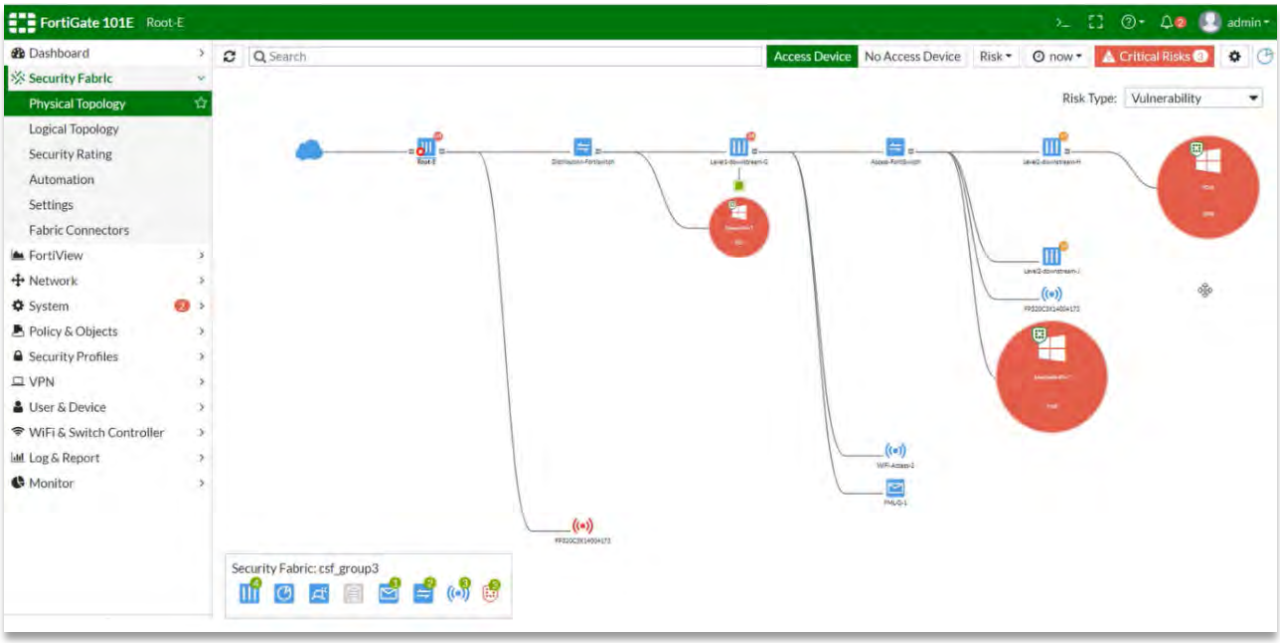
NB. FortiSwitches en FortiAP's fungeren in deze setup als L2 devices, L3 routering vindt immers uitsluitend plaats op de upstream FortiGate firewall. Op de switches zijn VLAN's actief; men kan er voor kiezen om verkeer dat binnen een VLAN blijft lokaal op de switch te laten i.p.v. door de firewall te laten lopen, dit wordt vaak geprefereerd bij bijvoorbeeld Top-of-Rack switches waarop een (hyperconverged) datacenter is aangesloten.



Uniek aan het Security-Driven Networking concept is echter de mogelijkheid ook dit intra-VLAN verkeer door de firewall te laten verlopen. Zo kunnen bijvoorbeeld protocolafwijkingen op L7 worden ontdekt, maar ook devices van elkaar worden geïsoleerd waardoor peer-to-peer traffic niet langer mogelijk is. We spreken hier over microsegmentatie, dat verder gaat dan alleen netwerksegmentatie (zie 2.1.2.5). Dit concept wordt vooral toegepast op access-VLAN's en sluit goed aan op een Zero- Trust beveiligingsbeleid.

2.2.2 Complete zichtbaarheid

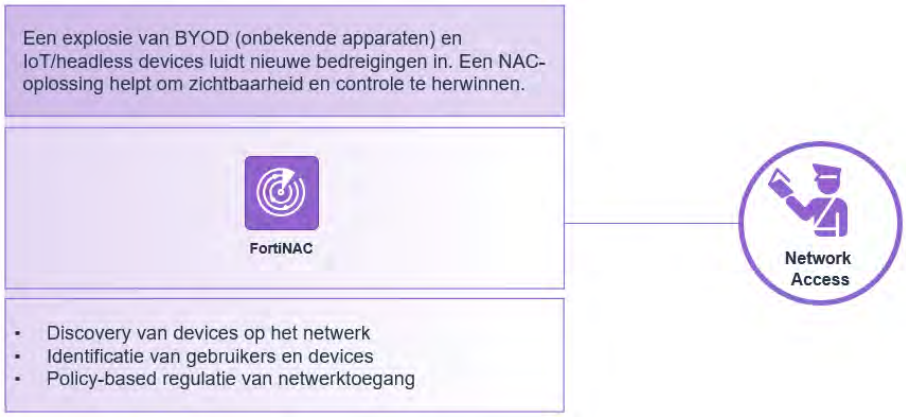
In de FortiGate GUI is tot op detail te zien achter welke switchpoort of access-point een gebruiker zich bevindt, met uitgebreide details zoals kwetsbaarheden, real-time bandbreedteverbruik en eventuele security incidenten. Doordat de FortiGate de onderliggende switches en de wireless architectuur beheert, kan een device zelfs eenvoudigweg de volledige toegang tot het netwerk ontzegd worden. Daarnaast is de gehele netwerk topologie op intuïtieve wijze grafisch weergegeven in de Security Fabric tab, zelfs als deze meerdere FortiGates, switches en access points bevat. Met behulp van deze integratie wordt het kinderlijk eenvoudig om de volledige infrastructuur centraal op een FortiGate te beheren (zie figuur 6).



Figuur 6 - Grafische toplogieweergave FortiGate GUI

2.3 Network Access

Met de introductie van Bring Your Own Device-initiatieven en de opkomst van IoT-/headless-devices is een nieuwe uitdaging geïntroduceerd in de vorm van het veilig toe moeten staan van netwerktoegang voor onbekende en/of unmanaged devices. Om grip te krijgen op deze almaar groter wordende groep devices is een Network Access Control (NAC) oplossing onontbeerlijk.



2.3.1 FortiNAC

Fortinet biedt een volwaardige NAC-oplossing in haar portfolio in de vorm van FortiNAC; een compleet overzicht van die oplossing is buiten scope van dit document, weet echter dat een separate en op open standaarden gebaseerde NAC-oplossing simpelweg noodzakelijk is binnen een op multi-vendor gebaseerde netwerk- en securityinfrastructuur. Voor de in dit document beschreven oplossing – combinatie van FortiGate, FortiSwitch en FortiAP – volstaat vaak de geïntegreerde NAC-functionaliteit als hierna beschreven in 2.3.2.

2.3.2 FortiOS native NAC

Uniek voor de in dit document beschreven oplossing is het feit dat deze vanaf FortiOS 6.4, standaard basis NAC-functionaliteit biedt zonder daartoe een separate NAC-oplossing in te hoeven zetten. Deze functionaliteit kan worden ingeschakeld op alle downstream FortiSwitches of op individuele FortiSwitch-poorten en helpt bij het verder implementeren van een Zero-Trust beveiligingsbeleid door de toegang tot het netwerk te beheren voor specifieke devices en apparaten.

Aanvankelijk worden apparaten die zijn aangesloten op poorten met de NAC-functie ingeschakeld, in een onboarding VLAN geplaatst met een restrictief beveiligingsbeleid. Het onboarding-VLAN heeft apparaatidentificatie, een DHCP-server en een captive portal ingeschakeld. De upstream FortiGate verzamelt informatie over het device en probeert het naar aanleiding daarvan te identificeren. De FortiGate maakt daarbij gebruik van een uitgebreide lokale database en kan ook, in geval van IoT devices, een cloud query naar FortiGuard (de threat researchafdeling binnen Fortinet) sturen opdat zij de identificatie kunnen doen aan de hand van hen bekende attributen. Voor deze laatste optie is wel een separate licentie benodigd in de vorm van de IoT-detectieservice. Eenmaal geïdentificeerd zal de FortiGate zorgdragen dat op een onderliggende FortiSwitch de dienovereenkomstige NAC-policy wordt afgedwongen, bijvoorbeeld het verplaatsen van het device naar een specifiek VLAN.

NB. Het op deze manier automatisch in het juiste VLAN kunnen plaatsen van een device wordt ook wel ‘dynamic VLAN assignment’ genoemd. Deze functie maakt het leven van een netwerkbeheerder een stuk aangenamer; hij/zij hoeft immers niet meer bij te houden wat voor device achter een specifieke poort zit en daar specifieke poortinstellingen voor te configureren.

2.4 Fabric Management Center

Het onderdeel van de Security Fabric dat wij Fabric Management Center noemen bestaat feitelijk uit een tweetal oplossingen, te weten:

1. **FortiManager** – Het beheerplatform voor dagdagelijks beheer in geval van een multi-site/-VDOM-omgeving;
2. **FortiAnalyzer** – De centrale log- en rapportageserver met SOC-capabilities.

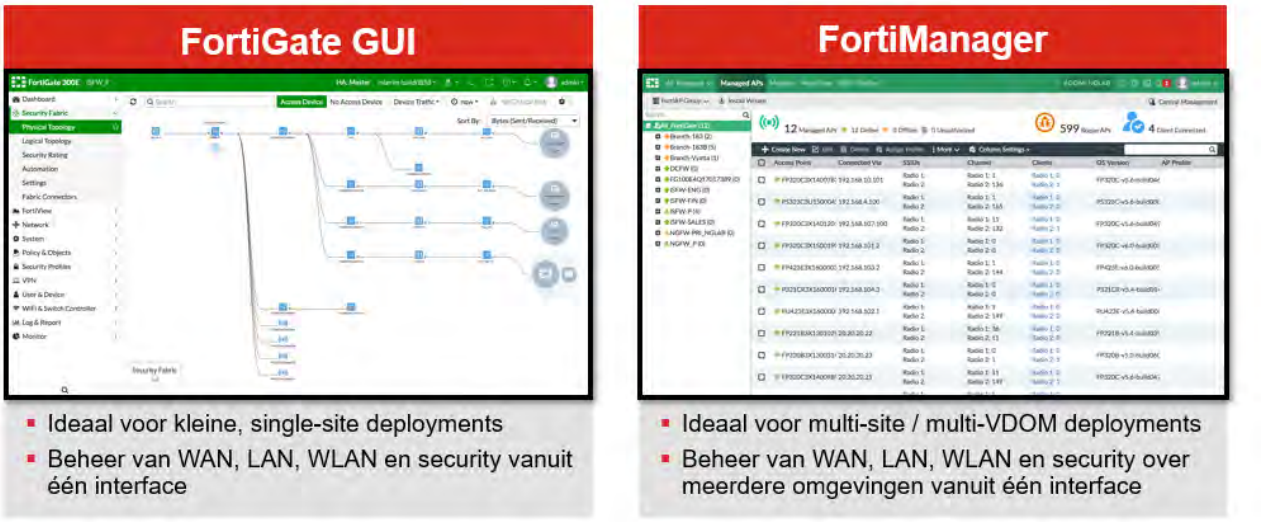
Beide oplossingen kunnen van grote waarde zijn in het geheel. Om die reden volgt een uiteenzetting van beide oplossingen in de hiernavolgende paragrafen.

2.4.1 FortiManager

Qua managementmogelijkheden onderscheiden we de FortiGate GUI zelf en FortiManager als centraal beheerplatform. De keuze tussen beide is vooral gedreven door beheergemak; waar de FortiGate GUI volstaat in geval van een te overzien aantal (logische) FortiGate firewalls, is FortiManager vooral gemakkelijk zodra dit aantal groter wordt bijvoorbeeld in een multi-site omgeving of in een gelaagd security-model met fysiek of virtueel gescheiden perimeter- en segmentatiefirewalls. FortiManager biedt in dat geval één GUI van waaruit alle FortiGates en VDOMs gelijktijdig kunnen worden beheerd, inclusief onderliggende netwerk-infrastructuur en gekoppelde (WAN-)verbindingen. Er is daarbij sprake van een hiërarchische structuur; indien FortiManager wordt gebruikt dan is deze preferent aan de FortiGate GUI.

NB. Voor auditdoeleinden dient voor administratieve toegang tot de FortiManager of de FortiGate GUI – conform best practices in cybersecurity – gebruik te worden gemaakt van rol-gebaseerde toegang. De beheerder in kwestie is daarbij als gebruiker vermeld in een gekoppelde identity-oplossing en kan zich als zodanig authentiseren (bijvoorbeeld middels TACACS+, RADIUS of LDAP). Hierbij dient tevens het gebruik van MFA te worden afgedwongen.

Beide platformen kennen verschillende reeds geconfigureerde beheerdersrollen, van super admin tot local user, elk met eigen privileges als het gaat om het al dan niet kunnen configureren van firewall rules en policies, maar ook bijvoorbeeld het kunnen lezen van gegevens met een bepaalde gevoeligheid (bijvoorbeeld persoons-gegevens). Afhankelijk van de behoefte kunnen ook andere, custom beheerprofielen worden aangemaakt.



Figuur 7 - FortiGate GUI versus FortiManager

2.4.2 FortiAnalyzer

FortiAnalyzer wordt in de praktijk op twee verschillende manieren ingezet; enerzijds als log- en rapportageserver, anderzijds als Security Operations (SecOps) device.

2.4.2.1 Log- en rapportageserver

Iedere FortiGate biedt – mits voorzien van lokale HDD/SSD – mogelijkheden tot het opslaan van log-data ten behoeve van analyses en het (periodiek) opstellen van rapportages. Feit is echter dat qua retentie op een FortiGate maximaal één week (= default) tot één maand (= na aanpassing configuratie) log-data beschikbaar is. Vaak is een dergelijke retentie te kort om een gedegen trendanalyse te doen, of er zijn andere (denk wederom aan compliance met interne richtlijnen en/of wet- en regelgeving) zwaarwegende redenen om log-data langer beschikbaar te hebben. Fortinet heeft daartoe een eigen log- en rapportage oplossing ontwikkeld in de vorm van FortiAnalyzer. Naast dat hiermee voldaan kan worden aan een langere retentieperiode, zijn de rapportagemogelijkheden binnen de FortiAnalyzer uitgebreider dan in de FortiGate zelf het geval is.

2.4.2.2 Security Operations (SecOps)

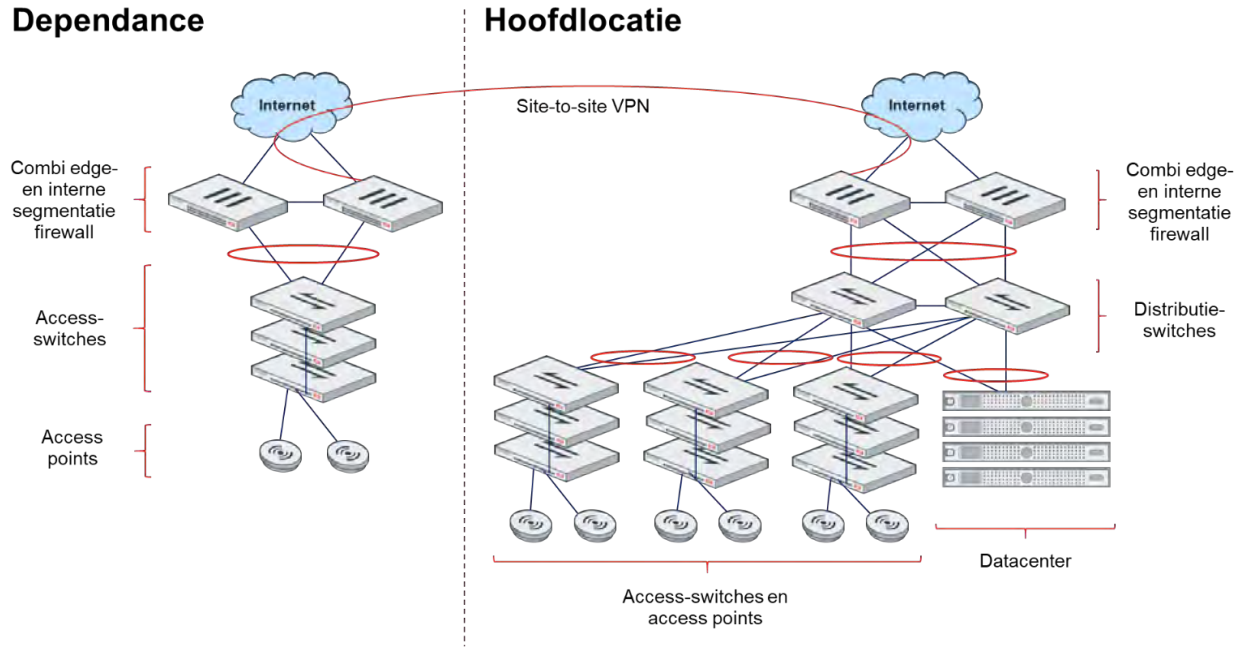
FortiAnalyzer biedt SecOps-functionaliteit door een intuïtief dashboard te bieden voor de weergave van events en eventuele incidenten die zich binnen de Fortinet Security Fabric voordoen. Deze events en incidenten worden door de separate onderdelen binnen de Fabric gesignaleerd en terstond gedeeld met de FortiAnalyzer. Een correlatie van events, welke kunnen duiden op een incident, gebeurt door de naadloze integratie van de diverse fabric componenten op verschillende plaatsen binnen en buiten (denk aan FortiGate Cloud Sandbox) het netwerk en dus niet per se binnen FortiAnalyzer. FortiAnalyzer speelt echter wel een centrale rol in de visuele weergave daarvan en de mogelijkheid om tot automatische responsacties over te gaan (voor deze laatstgenoemde SOAR-functionaliteit is de add-on SOC-subscriptie benodigd). Ook kan FortiAnalyzer een cruciale rol spelen in *threat hunting* activiteiten door periodiek historische log-data te checken op zogenaamde *command and control (C&C)* verkeer (hiertoe is de add-on Indicator of Compromise-subscriptie benodigd).

NB. Veel organisaties overwegen – vaak gedreven vanuit compliance – de aanschaf van een SIEM-platform ten behoeve van (security-)eventregistratie en correlatie. Ook een SOAR-platform om geautomatiseerde responsacties te bieden passeert daarbij vaak de revue. Een SIEM, al dan niet i.c.m. met SOAR is echter vaak niet de *holy grail*, het vereist namelijk veel specialistische kennis om deze optimaal operationeel te krijgen en te houden. Het gebruik van FortiAnalyzer als SecOps-device kan dan een prima alternatief zijn. De voorwaarde is echter wel dat er een keuze wordt gemaakt voor een meerlaags security-model waarbij diverse oplossingen van Fortinet worden geïmplementeerd.

2.5 Topologie

In deze paragraaf worden enkele topologie-opties besproken, met als doel een eenvoudige visuele weergave te bieden ten aanzien van de Security-Driven Networking propositie. Uiteraard zijn er talloze variaties mogelijk, iedere organisatie is immers uniek, qua componenten blijft ieder design echter grotendeels gelijk.

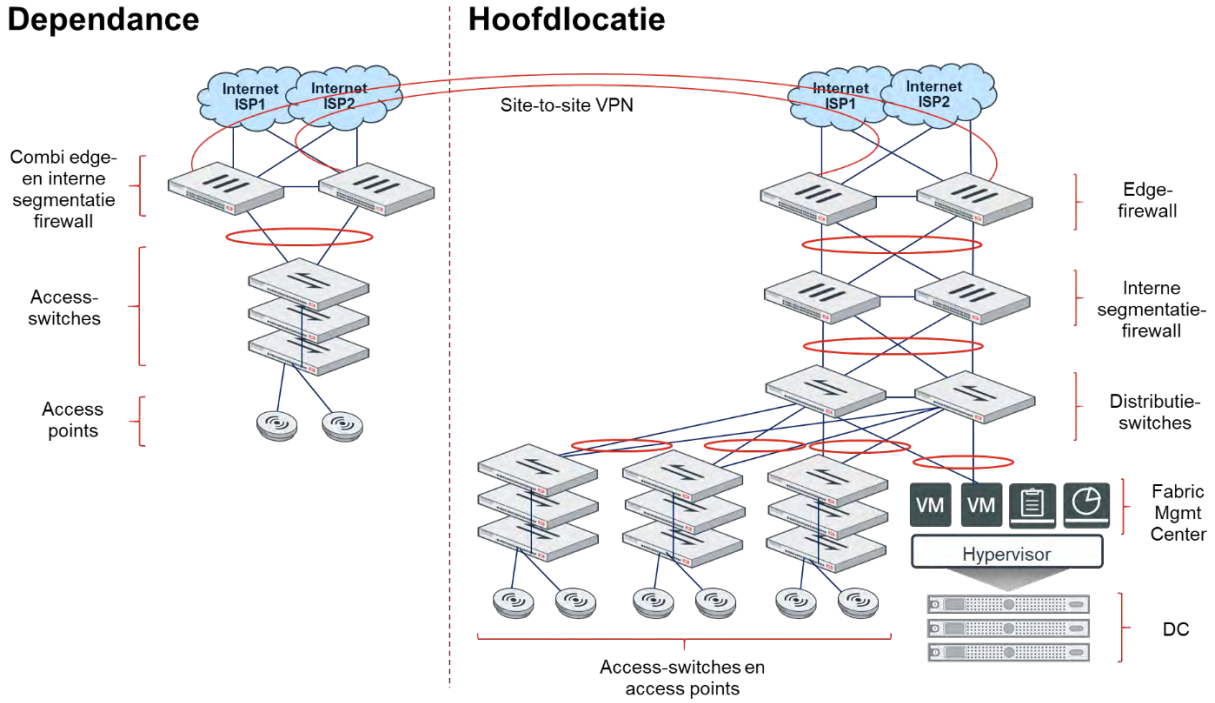
2.5.1 Kleine organisatie (ca. 50 – 250 medewerkers)



Uitgangspunten binnen het 'kleine organisatie' design:

- Lokale internet break-out
- Site-to-site VPN-verbinding tussen verschillende locaties
- Access-switches bieden standaard POE+ op alle poorten (uniformiteit)
- Gecombineerde edge- en interne segmentatie FW op zowel neven- als hoofdlocatie
- Loop-vrije redundante paden tussen alle tiers
- Nevenlocatie heeft alleen een MER, hoofdlocatie heeft een MER en diverse SER's
- Datacenter is on-premises en geconnecteerd op dezelfde distributieswitches als de access-laag

2.5.2 Middelgrote organisatie (ca. 250 – 500 medewerkers)

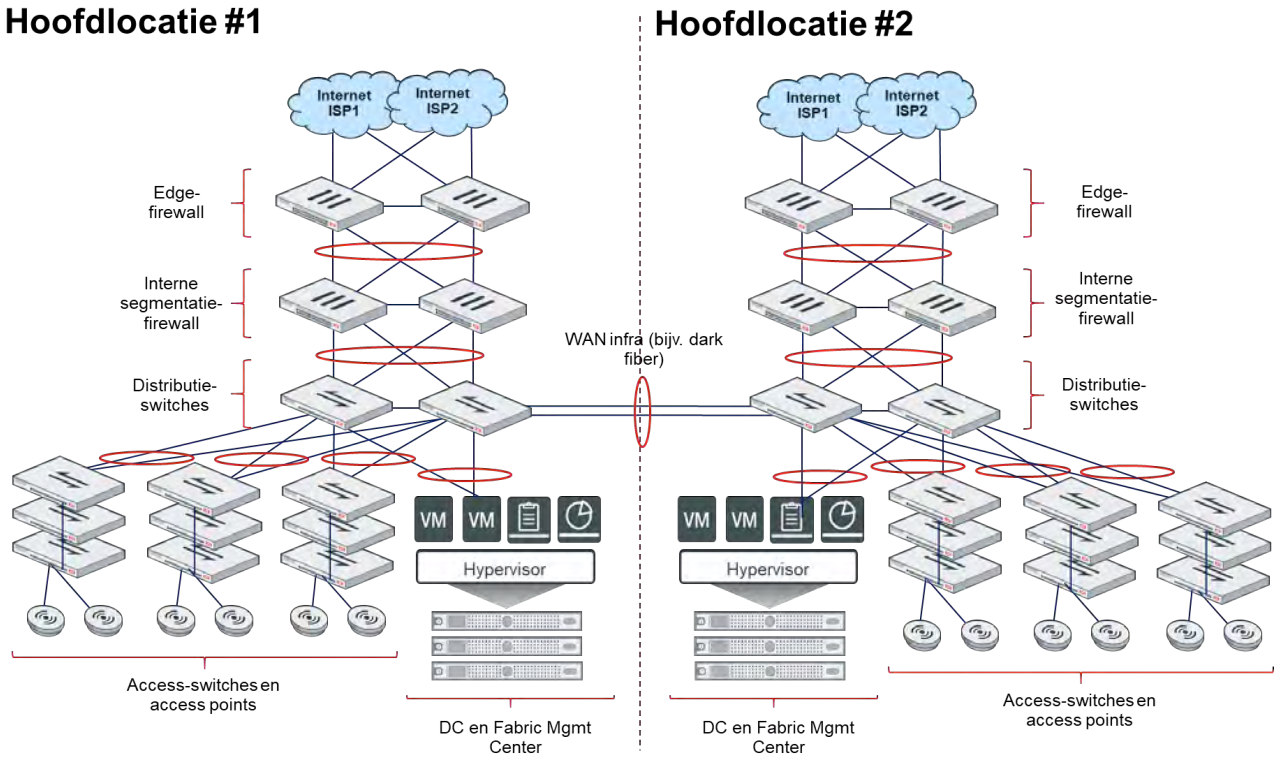


Uitgangspunten binnen het 'middelgrote organisatie' design (in rood de afwijkingen ten opzichte van kleine organisatie):

- Redundante lokale internet break-out
- Redundante site-to-site VPN-verbinding tussen locaties
- Access-switches bieden standaard POE+ op alle poorten (uniformiteit)
- Gecombineerde edge- en interne segmentatie FW op nevenlocatie, gescheiden op hoofdlocatie
- Loop-vrije redundante paden tussen alle tiers
- Nevenlocatie heeft alleen een MER, hoofdlocatie heeft een MER en diverse SER's
- Datacenter is on-premises en geconnecteerd op dezelfde distributieswitches als de access-laag
- Gebruik van Fabric Management Center t.b.v. NOC en SOC-diensten

NB. In sommige gevallen kiest een organisatie – met name kleine tot middelgrote organisaties – ervoor om de interne segmentatiefirewall als extra rol te definiëren op de perimeter firewall, al dan niet met gebruikmaking van VDOM's. Technisch gezien is dit goed mogelijk, mits een juiste sizing van het platform heeft plaatsgevonden. In kritische omgevingen daarentegen is het advies van Fortinet om beide rollen fysiek van elkaar te scheiden zodat een incident welke onverhoopt in staat is de perimeter firewall tijdelijk onbruikbaar te maken niet óók in staat is de gehele interne routering te corrumperen.

2.5.3 Grote organisatie (> 500 medewerkers)



Uitgangspunten binnen het 'grote organisatie' design (in rood de afwijkingen ten opzichte van middelgrote organisatie):

- Redundante lokale internet break-out
- Eigen WAN-infrastructuur om locaties te ontsluiten (bijvoorbeeld glasvezelring)
- Access-switches bieden standaard POE+ op alle poorten (uniformiteit)
- Gescheiden edge- en interne segmentatie firewall
- Loop-vrije redundante paden tussen alle tiers
- Volledig redundant on-premise datacenter (o.b.v. synchrone of asynchrone replicatie)
- Redundant uitgevoerd Fabric Management Center t.b.v. NOC en SOC-diensten

3 Conclusie

Een frequent door directie/management gemaakte fout is denken dat er zich binnen diens organisatie geen securityincidenten voordoen. Het feit dat er weinig of geen incidenten lijken te zijn, hoeft niet te betekenen dat er niets gebeurt. Besef dat er in elke organisatie incidenten zijn; in hoeverre een organisatie daartegen bestand is, hangt direct samen met de effectiviteit van de geïmplementeerde *controls* (administratief, technisch/ operationeel en fysiek).

De netwerk- en securityinfrastructuur is bij uitstek een omgeving waar diverse technische/operationele controls benodigd zijn om de digitale weerbaarheid op een acceptabel niveau te brengen. Het netwerk- en securityteam is daarbij verantwoordelijk voor het operationeel brengen en houden van deze controls op een zo efficiënt mogelijke wijze. Maar al te vaak wordt dit team echter gehinderd door een ontstane wildgroei aan standalone oplossingen, resulterend in:

1. Dagelijks een te groot aantal alerts waarop adequaat gereageerd moet worden, wat leidt tot een situatie waarbij sommige worden gemist of waar verbanden niet gelegd worden;
2. Door een veelvoud aan oplossingen is brede specialistische kennis noodzakelijk. Hier is simpelweg een gebrek aan op de markt, met als gevolg onderbezetting of ondergekwalificeerd personeel binnen het team;
3. Het gebrek aan out-of-the-box integratie tussen de vele standalone oplossingen leidt tot een situatie waarbij ‘alles aan elkaar geknoopt moet worden’. Dit maakt de architectuur in zijn geheel onnodig complex, met een hoge foutgevoeligheid in het operationeel beheer tot gevolg.

Fortinet kiest de frontale aanval als het gaat om het adresseren van deze veelvoorkomende uitdagingen. Met de introductie van diens Security-Driven Networking propositie worden twee – tot voor kort veelal gescheiden – werelden bij elkaar gebracht: networking en security. Doordat sprake is van een coherent, geïntegreerd geheel spreken we over een platform.

De benadering van Fortinet als gaat om diens Security-Driven Networking propositie is efficiënt en effectief te noemen; we hebben security als uitgangspunt genomen en het netwerk daar integraal onderdeel van gemaakt. Dit is een unieke benadering, en loopt jaren vooruit op de huidige ontwikkeling in de markt. Voor de critici onder ons: een vergelijkbare situatie heeft zich in de afgelopen jaren voorgedaan als het gaat om compute en storage; waar het tot voor kort gebruikelijk was om separaat servers, SAN, SAN-switches en hypervisor te implementeren en te beheren, is nu een hyperconverged omgeving – wederom een coherent, geïntegreerd geheel, maar dan in het datacenter – de norm geworden. Wij als Fortinet geloven dat eenzelfde resultaat te realiseren is met betrekking tot de netwerk- en securityinfrastructuur en hebben daar ook naar gehandeld.

Nawoord

Wij hopen dat deze whitepaper u meer inzicht heeft gegeven in wat Fortinets Security-Driven Networking propositie inhoudt en wat deze ook voor uw organisatie zou kunnen betekenen. Graag komen we met u in contact indien u behoefte heeft verder te spreken hieromtrent.

Team Fortinet NL

Bijlage 1 – Conformiteit met bestaande kaders

Voor de volledigheid van dit document gaat tabel 1 in op de conformiteit van Fortinets Security-Driven Networking propositie ten aanzien van in Nederland veel gehanteerde normenkaders en standaarden, te weten:

- **Baseline Informatiebeveiliging Overheid** – Kader van verplichte maatregelen voor de gehele overheid.
- **Edustandaard Certificeringsschema Informatiebeveiliging en Privacy ROSA** – Certificeringsschema m.b.t. informatiebeveiliging en privacy in onderwijssector. Maatregelen zijn verdeeld over 3 categorieën (Beschikbaarheid, Integriteit en Vertrouwelijkheid) en kennen 3 niveau's (1 = Laag, 2 = Midden en 3 = Hoog).
- **Center for Internet Security Critical Security Controls (CIS Controls)** – Publicatie van best practice richtlijnen aangaande informatiebeveiliging.

Tabel 1 – Security-Driven Networking in relatie tot veel gehanteerde normen en standaarden

Hoofdstuk-paragraaf	Omschrijving	Baseline Informatie-beveiliging Overheid[3]	Edustandaard Certificerings-schema Informatie-beveiliging en Privacy ROSA[4]	Center for Internet Security Critical Security Controls[5]
1.1	Bepalen beveiligingsstrategie en vaststellen beveiligingsbeleid	5.1	-	-
2.1	Gebruik perimeter firewall om interne netwerk te beschermen	13.1.2	B, niveau 3	12.2 t/m 12.10
2.1.1	Gebruik perimeter firewall als remote VPN-oplossing met MFA	9.4.2	V, niveau 3	12.11
2.1.1.3	HA-opstelling perimeter firewall (active-active of active-passive)	-	B, niveau 3	-
2.1.1.4	Gebruik antivirus en webfilter functionaliteit op perimeter firewall	12.2.1	I, niveau 3	7.4 t/m 7.7
2.1.2	Gebruik interne segmentatiefirewall t.b.v. logische netwerkscheiding	13.1.3	I, V, niveau 3	14.1, 14.2
2.1.2.3	HA-opstelling interne segmentatiefirewall (active-active of active-passive)	-	B, niveau 3	-
2.1.2.4	Gebruik netwerk-IPS om verkeer tussen netwerksegmenten te controleren op afwijkingen	NCSC-handreiking detectie-oplossingen	V, niveau 3	12.6, 12.7
2.1.2.5	Gebruik interne segmentatiefirewall om microsegmentatie toe te passen	9.4.1	I, V, niveau 3	14.3
2.3	Reguleren netwerktoegang voor onbekende en/of unmanaged devices	9.1	V, niveau 3	1.1, 1.6, 1.7
2.4.1	Rolgebaseerde administratieve toegang met MFA tot FortiManager of FortiGate GUI	-	I, V, niveau 3	11.5
2.4.2.1	Gebruik FortiAnalyzer als log- en rapportageserver (logretentie)	12.4.1	B, I, niveau 3	6.2 t/m 6.5
2.4.2.2	Gebruik FortiAnalyzer als SecOps device (SOC-diensten)	12.4.1	V, niveau 3	6.6 t/m 6.8

[3] Zie: https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/
[4] Zie: https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa/
[5] Zie: https://www.cisecurity.org/controls/