CISCO
SECURE

Whitepaper
Cisco – Public

De toekomst van de firewall

Vandaag een krachtiger postuur creëren en een brug bouwen naar de zakelijke en security vereisten van morgen

cisco The bridge to possible

Inhoud

Samenvatting

In deze whitepaper wordt de ontwikkeling van netwerk security beschreven en wat er nodig is om de omgeving van een organisatie in de toekomst te beschermen.

Naarmate netwerken heterogener worden, wordt het voor organisaties steeds lastiger consistent beleidsbeheer en -handhaving te garanderen met behoud van unified zichtbaarheid. De complexiteit van deze met elkaar verbonden netwerken leidt ook tot fouten of onjuiste configuraties, waardoor ze kwetsbaar worden voor zich steeds verder ontwikkelende geavanceerde bedreigingen.

Wat kan een organisatie doen om de controle weer terug te krijgen en consistentie te garanderen? Het begint allemaal met een geïntegreerde benadering van security waarbij de firewall centraal staat.

Firewalls vormen nog steeds de hoeksteen van de netwerk security strategie van organisaties, maar net zoals netwerken zich hebben ontwikkeld moeten firewalls dat ook doen. In het verleden was de firewall één applicatie aan de buitengrens van inkomend/uitgaand verkeer en fungeerde als een beleidsgestuurd controlepunt dat netwerkverkeer toegang toestond of weigerde. Om in de moderne digitale wereld te kunnen overleven, moeten organisaties van de inzet van losse firewalls overgaan op 'firewalling': een beleidsgestuurde methode voor het strategisch coördineren van geavanceerde security op logische controlepunten in het gehele heterogene netwerk.

Firewalling zal voor organisaties een kritieke stap zijn bij het beter afstemmen van security op veranderende bedrijfs- en netwerkbehoeften. Cisco heeft een geïntegreerd security platform ontwikkeld waarvan onze firewall de basis vormt. Dit platform biedt bedrijven de mogelijkheid de overstap te maken.

> "Firewalls vormen nog steeds de hoeksteen van de netwerk security strategie van organisaties, maar net zoals netwerken zich hebben ontwikkeld moeten firewalls dat ook doen."

Met firewalling kunnen organisaties die een digitale transformatie ondergaan vandaag een krachtiger security postuur creëren en een brug bouwen naar de zakelijke en security vereisten van morgen.

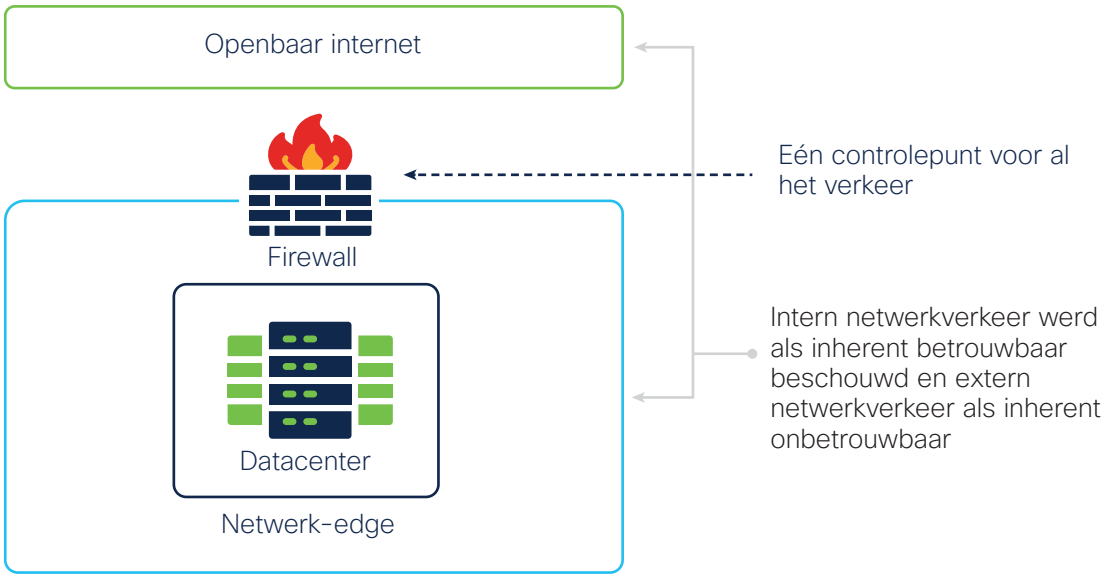
Deel 1: De geschiedenis van de firewall

De evolutie van netwerk security

De firewall werd traditioneel als poortwachter ingezet aan de netwerk-edge. Deze fungeerde als allesomvattend controlepunt dat netwerkverkeer aan de buitengrens inspecteerde. Op het punt waar verkeer inkomt/uitgaat was de firewall verantwoordelijk voor het valideren van communicatie: intern netwerkverkeer werd als inherent betrouwbaar beschouwd en extern netwerkverkeer als inherent onbetrouwbaar. Er werden op dit ene controlepunt regelsets en beleidslijnen gecreëerd en gehandhaafd om ervoor te zorgen dat gewenst verkeer het netwerk in/uit mocht en ongewenst verkeer werd tegengehouden.

Als we de buitengrens van het netwerk vergelijken met een slotgracht om een kasteel, fungeerde de firewall als een ophaalbrug die verkeer naar/uit de vesting regelde.

Traditionele netwerk security



Afbeelding 1. De traditionele netwerkfirewall

En toen kwam de cloud. En kwamen de apps.

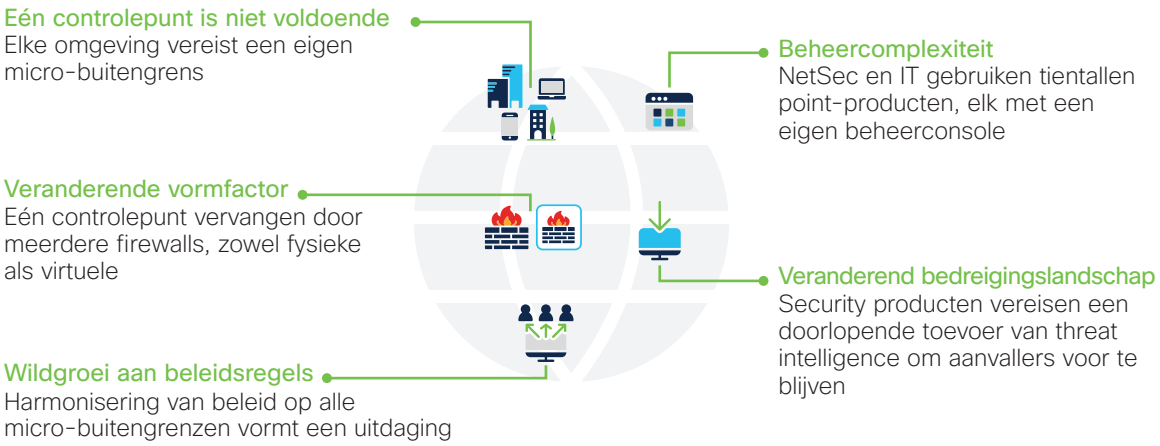
Het duurde niet lang voordat het principe van security via één controlepunt op losse schroeven werd gezet. Ten eerste was daar de opkomst van externe toegang en ondernemingsmobiliteit. Maar de transformatie werd pas echt in gang gezet door cloudcomputing. Toen bedrijven overgingen naar de cloud, werden apparaten en gebruikers massaal gemigreerd naar een plek buiten het beheerde interne netwerk, waardoor het model met één controlepunt ineffectief werd. Er was al snel sprake van meerdere buitengrenzen. En die moesten allemaal worden beveiligd. Er was geen effectieve manier om één slotgracht te creëren die het netwerk omringt.

Tegenwoordig is er sprake van data ver van de traditionele buitengrens – als gevolg van vestigingslocaties, medewerkers op afstand en toenemend gebruik van cloudservices – waarbij het traditionele security controlepunt volledig wordt omzeild. Bovendien hebben veel bedrijven het BYOD-model (Bring Your Own Device) geadopteerd, zodat medewerkers via hun eigen computers of mobiele apparaten toegang hebben tot gevoelige zakelijke toepassingen. Sterker nog, meer dan 67% van de medewerkers gebruikt eigen apparaten op het werk – een opwaartse trend die nog wel even zal aanhouden. Er zijn veel mobiele apparaten en laptops verbonden via publiek toegankelijke Wi-Fi-netwerken, en deze zijn zelfs cruciaal voor dagelijkse bedrijfsactiviteiten.

Bovendien is voor de overweldigende meerderheid van bedrijfslocaties en gebruikers ook directe toegang tot het internet vereist, waarbij een groeiende meerderheid van cloudgebaseerde kritieke toepassingen en data nu live is. Bedrijven blijven workloads implementeren via meerdere cloudservices, besturingssystemen, hardwareapplicaties, databases en meer. Toepassingen en data worden verder gedecentraliseerd, waardoor netwerken steeds diverser worden.

De nieuwe realiteit

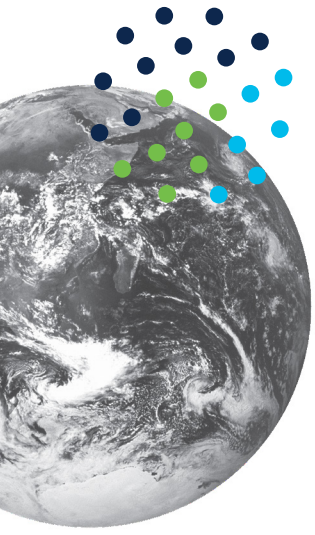
Deze 'one-size-fits-all' benadering is ineffectief gebleken in het huidige landschap.



Afbeelding 2. Netwerkcomplexiteit en veranderende bedreigingen zijn een probleem voor het traditionele firewallmodel

Een nieuwe, complexere realiteit

Hoewel deze innovaties een meer onderling verbonden en productieve werkomgeving mogelijk maken, hebben ze de manier waarop we zaken doen veranderd. De oude manier waarbij op kantoor toepassingen werden beheerd en gebruikers geautoriseerd is getransformeerd in een geheel van dynamische multicloud-ecosystemen die services en toepassingen in ondernemingen leveren. Bovendien worden bedrijfskritische relaties met derden beheerd. Enorme uitbreiding en uitbesteding bieden veel schaal en efficiëntie, maar er zijn ook nadelen. Deze evolutie van netwerkarchitecturen heeft het aantal aanvalsgebieden enorm vergroot en het beschermen van bedrijfsnetwerken, data en gebruikers aanzienlijk complexer gemaakt.

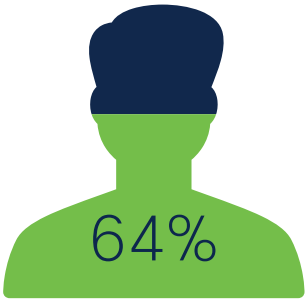


Bestrijding met point-producten

Organisaties hebben geprobeerd deze uitdagingen aan te gaan door de 'beste' point security oplossing toe te voegen om elk nieuw probleem dat optrad aan te pakken. Hierdoor ontstond een ongekende wildgroei aan apparaten, waarbij een gemiddelde onderneming tot wel 75 security tools gebruikte[1]. De inzet van meerdere security producten van verschillende leveranciers kan voor netwerk security teams tot grote beheerproblemen leiden. In de meeste gevallen resulteert een dergelijke wildgroei van security apparaten en mogelijkheden juist in een grotere kans op aanvallen. 94% van de ondervraagde professionals op het gebied van IT en InfoSec gaf aan zich zorgen te maken dat toegenomen netwerkcomplexiteit hen kwetsbaarder maakte; 88% gaf aan het wijzigen van netwerk security beleid flexibeler te willen maken[2].

Tussen januari en juli 2019 werden 3.800 datalekken bekendgemaakt: een toename van 54% in vergelijking met de eerste helft van 2018[3]. Deze sterke stijging is bewijs van de steeds geavanceerdere methoden die kwaadwillenden toepassen om netwerken binnen te dringen. Het toenemende aantal succesvolle inbreuken geeft ook aan dat traditionele methoden van netwerk security niet langer bestand zijn tegen moderne bedreigingen.

1 "Defense in depth: Stop spending, start consolidating", CSO, 4 maart 2016.
2 "Onderzoek naar de complexiteit van netwerk security," ESG Research Insights Report, juni 2019.
3 "Onderzoek naar de complexiteit van netwerk security," ESG Research Insights Report, juni 2019.



Menselijke fouten waren de belangrijkste oorzaak van een onjuiste configuratie

Meer bedreigingen, meer ruis en zelfs meer risico's

Naarmate kwaadwillenden nieuwe aanvalsvectoren vinden – van e-mail en vanwege BYOD-beleid niet-gecontroleerde endpoints tot webportals en IoT-apparaten – worden organisaties ook gestimuleerd andere benaderingen toe te passen om zich te beschermen.

Zoals hierboven aangegeven wordt het algehele security postuur van een organisatie er niet beter op door point-producten toe te voegen. Juist het tegenovergestelde. Er ontstaat meer 'ruis' waar security teams aandacht aan moeten besteden. Terwijl zij hun ogen openhouden voor onvermijdelijke nieuwe aanvallen en malware die wordt ingezet om misbruik te maken van een (bekende of onbekende) kwetsbaarheid, wordt door deze extra complexiteit het creëren, beheren en handhaven van security beleid nog lastiger.

En netwerk security teams moeten talrijke cloudbronnen een voor een configureren, waardoor de kans op een onjuiste configuratie toeneemt, wat weer tot een beveiligingslek kan leiden. Een niet-geïmplementeerde security controle, of een geïmplementeerde controle met fouten, kan het grootste probleem vormen: 64% van de organisaties geeft aan dat menselijke fouten de belangrijkste oorzaak waren van een onjuiste configuratie[4]. Of een dergelijke fout nu resulteert in schending van compliance of in uitval of de deur openzet voor een kwaadwillende: u kunt zich een dergelijk risico niet veroorloven.

Het is tijd voor een nieuwe kijk op de firewall

Netwerk security is een behoorlijke klus geworden. Het is gewoon niet mogelijk om een enorme hoeveelheid aan point security oplossingen, cloudbronnen en applicaties te beheren. Het is tijd voor een andere aanpak.

Het is tijd om de firewall tot de basis van een flexibel en geïntegreerd netwerk security platform te maken zodat bedrijven, nu en in de toekomst, een robuuster security postuur hebben.

Deel 2: Van firewall naar firewalling

Waarom firewalling?

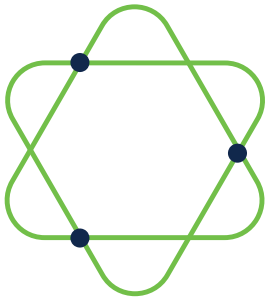
Onze netwerken ontwikkelen zich verder om nieuwe manieren van zakendoen te ondersteunen, en onze netwerk security moet gelijke tred houden. In de huidige wereld van gedistribueerde IT-middelen heeft de firewall een centrale functie in een robuust security postuur.

Firewall-vereisten zijn echter aanzienlijk toegenomen om het brede scala aan netwerkinfrastructuren, verbonden apparaten en besturingssystemen te kunnen beschermen tegen geavanceerde bedreigingen. Onze 'traditionele' firewall-apparaten worden aangevuld met een mix van fysieke en virtuele applicaties. Sommige hiervan zijn ingesloten in het netwerk, terwijl andere worden geleverd als een service, hostgebaseerd zijn of worden opgenomen in openbare cloudomgevingen. Er is zelfs sprake van nieuwe vormfactoren, zoals geclusterde applicaties die worden ingezet bij grote verkeersstromen, software die wordt uitgevoerd op persoonlijke apparaten, SD-WAN routers en veilige internetgateways. Het delen van threat intelligence op al deze afzonderlijke firewall-apparaten, ongeacht hun locatie, is essentieel voor uniforme zichtbaarheid van bedreigingen en een sterk security postuur.

Om huidige netwerken beter te beveiligen, moeten bedrijven afscheid nemen van de traditionele 'buitengrens'-benadering. Ze moeten strategische handhavingspunten instellen langs de gehele netwerkfabric, dichter bij de informatie of toepassingen die moeten worden beschermd. Hierbij is met name het creëren van micro-buitengrenzen op zowel fysieke als logische controlepunten essentieel.

De firewall moet niet meer worden gezien als een standalone fysiek netwerkapparaat: er moet meer aandacht worden besteed aan firewalling.

4 "Cloud Security Breaches and Human Errors", Fugue, 7 februari 2019.



Wat is firewalling?

Vergis u niet: de firewall is relevanter dan ooit tevoren. Sterker nog, om de huidige netwerken te beschermen zijn **overal meer** firewalls nodig. Bij firewalling ligt de nadruk op **hoe** u overal op beleid gebaseerde controles kunt instellen.

Firewalling kan een flexibele en geïntegreerde benadering bieden van gecentraliseerd beleid, geavanceerde security functionaliteit en consistente handhaving in uw steeds complexere heterogene netwerken. Een en ander resulteert in uitgebreide bescherming, zichtbaarheid, harmonisatie van beleid en krachtigere gebruikers- en apparaatverificatie. Met firewalling wordt ook het delen van threat intelligence op alle controlepunten voor uniforme zichtbaarheid en controle van bedreigingen mogelijk – en worden tijd en moeite bespaard bij het detecteren, onderzoeken en herstellen van bedreigingen.

Op die manier wordt firewalling een belangrijke strategie om uw complexe netwerk vandaag te beschermen. En vormt het een brug naar de toekomst terwijl uw bedrijf – en het bedreigingslandschap – zich verder ontwikkelt.

Hoe ziet het eruit?

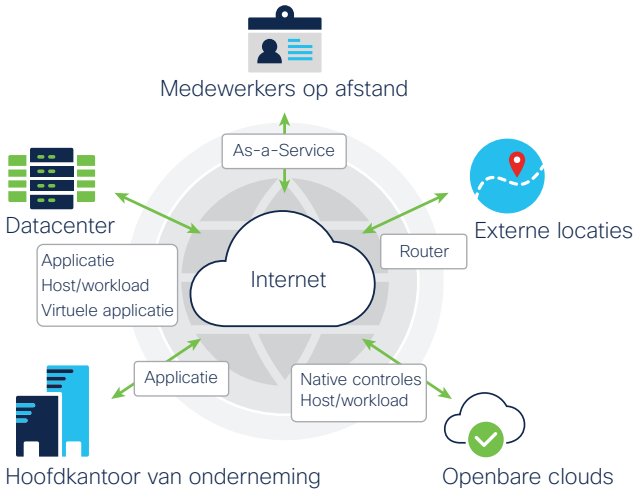
Of u nu middelen en data in de cloud, op kantoor of op een externe locatie beschermt: firewalling moet consistent geavanceerde bescherming tegen bedreigingen bieden, beleidshandhaving garanderen en threat intelligence delen. De uitdaging hierbij is ervoor te zorgen dat consistentie wordt toegepast in afzonderlijke omgevingen waar verschillende apparaten worden geïmplementeerd en gebruikt.

Beveiligingslekken kunnen ontstaan via elk apparaat met toegang tot het internet – op het hoofdkantoor, in het datacenter, op externe locaties, in openbare clouds of elke andere omgeving waar een medewerker op afstand werkt. Daarom is het belangrijker dan ooit om op meer logische locaties een robuuste set security controlepunten op te nemen om blootstelling aan bedreigingen te verminderen en risico's te beperken. Security mechanismen worden waar nodig in eigen omgevingen toegepast (fysieke of virtuele applicaties en netwerkapparaten zoals routers) en in externe omgevingen (Security as a Service [SECaaS]), native controles en workloads.

Wat is firewalling?

De huidige heterogene netwerken hebben overal handhavingspunten.

Firewalling biedt consistente preventie van bedreigingen met consistent beleid en zichtbaarheid van bedreigingen, zodat u overal aanvallen sneller en nauwkeuriger kunt voorkomen, detecteren en stoppen.



Afbeelding 3. De belangrijkste tenants van firewalling als mechanisme om de security uitdagingen van moderne netwerken aan te pakken

Security mechanismen uitbreiden

Aangezien bij de inzet van een traditionele firewall al het interne verkeer en geautoriseerde gebruikers als inherent betrouwbaar werden beschouwd (en extern verkeer als onbetrouwbaar) werd de gehele organisatie beschermd aan de buitengrens van het netwerk. Deze buitengrens van het netwerk werd het logische security controlepunt voor bescherming van de gehele organisatie. Al het netwerkverkeer, of dat nu afkomstig was van het hoofdkantoor, een datacenter of een medewerker op afstand, werd via dat ene controlepunt geleid.

Een dergelijk model werkt natuurlijk niet in de huidige complexe omgevingen, waarin de IT-infrastructuur van een organisatie een breed scala aan vormfactoren en leveringsmodellen omvat, inclusief fysieke en virtuele applicaties, in het netwerk geïntegreerde routers of switches, geleverd as-a-Service, hostgebaseerd of opgenomen in een openbare cloud.

Bij firewalling worden consistente security mechanismen geïmplementeerd om volledige zichtbaarheid, unified beleidsregels en uitgebreide zichtbaarheid van bedreigingen te bieden. Deze security mechanismen maken krachtigere gebruikers- en apparaatverificatie in steeds heterogenere cloudomgevingen mogelijk. Ze verzamelen, delen en reageren op context over gebruikers, locaties, apparaten en meer om ervoor te zorgen dat apparaten voldoen aan gedefinieerde security vereisten. Met consistente security mechanismen aan elke micro-buitengrens kunnen security teams taken automatiseren (zoals gebruikers en apparaten die de beleidsregels niet naleven automatisch in quarantaine plaatsen, twijfelachtige domeinen bij alle security mechanismen blokkeren en effectieve microsegmentatie ondersteunen). Bij firewalling wordt via volledige zichtbaarheid een holistisch overzicht gecreëerd van alle security waarschuwingen en aanwijzingen van besmettingen, en dankzij gedeelde threat intelligence wordt up-to-date bedreigingsdetectie bij elk verbonden apparaat mogelijk.

Cloudgebaseerd beheer

En het gaat niet alleen om point-producten. De enorme toename van het aantal buitengrenzen van het netwerk en van cloudbronnen heeft ook de blootstelling aan beveiligingslekken vergroot. Het beschermen van de belangrijkste bedrijfsmiddelen in complexe cloudomgevingen en het tegelijkertijd beheren van diverse security producten is een behoorlijke taak. Security teams hebben directe zichtbaarheid en gestroomlijnd beheer nodig om onjuiste configuratie te voorkomen.

Firewalling zorgt voor een sterker security postuur doordat het gecentraliseerd, cloudgebaseerd beheer ondersteunt en security teams de complexiteit kunnen verminderen en beleidsregels binnen de gehele organisatie kunnen afstemmen. Met sjablonen kan de opzet en consistentie van beleid verbeteren doordat een beleid maar één keer hoeft te worden opgesteld, waarna handhaving ervan wordt geschaald bij tienduizenden security mechanismen op een netwerk. Het gebruik van standaardbeleidssjablonen om snel nieuwe apparaten te implementeren vermindert het aantal configuratiefouten. Naarmate organisaties groeien, nemen nieuwe implementaties automatisch de nieuwste beleidsregels over. Een schaalbaar beleidsbeheersysteem integreert meerdere security functies in één toegangsbeleid en optimaliseert beleid bij alle security apparaten om inconsistenties te identificeren en deze snel te herstellen.

Sterker nog, een gecentraliseerde, cloudgebaseerde beheeroplossing zorgt ervoor dat de mogelijkheden voor een team enorm toenemen. Het kan snel risico's identificeren bij alle apparaten en zo een consistentere en veiligere status creëren. Met één beheerconsole kunnen objecten op alle apparaten worden vergeleken om inconsistenties te achterhalen en het huidige security postuur te optimaliseren. Teams kunnen beleidsbeheer stroomlijnen, de efficiëntie verhogen, consistentere security realiseren en tegelijkertijd de complexiteit verminderen.

Bestrijding met threat intelligence

Naarmate de buitengrens van het netwerk zich uitbreidt en steeds meer apparaten rechtstreeks verbonden zijn met het internet, nemen ook de aanvalsgebieden toe. Cyber security dreigingen, zoals malware, cryptovaluta, phishing en botnetactiviteiten, nemen toe en cybercriminelen maken steeds meer gebruik van machine learning en AI om misbruik te

maken van bestaande kwetsbaarheden en schadelijke aanvallen te versnellen. Er zijn maar zeer weinig organisaties die voldoende middelen hebben om alle kwetsbaarheidspatches van softwareleveranciers te testen en te kwalificeren. De meeste hebben moeite om opkomende en veranderende bedreigingen het hoofd te bieden.

Firewalling kan ook hierbij nuttig zijn. Door gebruik te maken van toonaangevende threat intelligence met het allernieuwste bedreigingsonderzoek en toegang tot security updates kan de constante stroom van bedreigingen worden beperkt. Bedreigingsonderzoekers identificeren snel aanwijzingen van besmetting en bevestigen en delen bedreigingen direct. Ze maken gebruik van schaalvoordelen om organisaties te beschermen tegen opkomende bedreigingen voordat deze plaatsvinden. Door threat intelligence te delen op alle onderling verbonden netwerken, endpoints, workloads en cloudomgevingen kunnen security teams ogenschijnlijk niet-verbonden gebeurtenissen correleren, ruis elimineren en bedreigingen sneller stoppen.

Wat zijn de risico's als firewalling niet wordt toegepast?

Naarmate networking zich heeft ontwikkeld, hebben organisaties zich aangepast en diverse point-producten geïmplementeerd ter ondersteuning van bedrijfsvereisten en -activiteiten. Dat hebben ze ook gedaan toen nieuwe aanvalsvectoren werden gepubliceerd, waardoor ze product na product na product hebben toegevoegd ter bescherming tegen de nieuwste XYZ-bedreiging. Organisaties die een traditionele firewall gebruiken om elk verbonden apparaat op meerdere buitengrenzen te beschermen, lopen het risico dat hun waardevolste data en middelen worden blootgesteld aan beveiligingslekken. Volgens de Cybersecurity Almanac uit 2019 zullen de jaarlijkse kosten van schade als gevolg van cybercriminaliteit in 2021 € 6 biljoen bedragen[5].

Deze bedreigingen kunnen een netwerk snel infiltreren en de activiteiten in gevaar brengen van een bedrijf dat geen uitgebreide netwerk security en zichtbaarheid van endpoints heeft.

Het beveiligen van het netwerk, de cloudomgevingen, de apparaten en data (waar deze zich ook bevinden) van een organisatie legt een zware druk op security teams.

Firewalling begint en eindigt met de firewall als hoeksteen van toekomstbestendige netwerk security

Bij Cisco doen we er alles aan om deze visie te verwezenlijken. We werken wereldwijd samen met bedrijven en ondernemingen van elke omvang die allemaal een flexibelere en meer in het netwerk geïntegreerde netwerk security nodig hebben. Daarom leveren we de veiligste architectuur die er bestaat: een krachtig en uitgebreid platform waarvan de firewall de basis vormt.

Een ongekend beschermingsniveau bieden door dit concept is een essentiële component van onze security strategie. De Cisco security portfolio en de firewallreeks van Cisco zorgen ervoor dat u veranderende bedreigingen overal waar nodig een stap voor kunt blijven met eersteklas security mechanismen, consistent beleid, zichtbaarheid en innovaties die security processen verbeteren.

In een tijdperk waarin het bedreigingslandschap dynamischer is dan ooit tevoren combineert Cisco leiderschap op het gebied van networking en grensverleggende technologie, zodat u vandaag en morgen profiteert van het sterkste security postuur dat er maar beschikbaar is.

5 "2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics", Cybercrime Magazine, 6 februari 2019.

Traditionele firewalls bieden slechts een beperkt beeld. IT vereist grotere zichtbaarheid van het gehele netwerk met gedeelde threat intelligence om bedreigingen eerder en sneller te detecteren en te blokkeren. Firewalling gaat verder door een uitgebreid security postuur te bieden op basis van unified management en uitgebreide security mogelijkheden, zoals inbraakpreventie, URL-filtering en geavanceerde bescherming tegen malware. Hierbij wordt gebruikgemaakt van automation en machine learning voor efficiëntie.

Zonder een firewalling-strategie kan netwerkcomplexiteit leiden tot onjuiste configuraties, waardoor het risico op een beveiligingslek toeneemt. Volgens een rapport van Gartner zal in 2022 95% van falende cloud security de schuld zijn van de klant.[6] Door een firewalling-strategie toe te passen en security beleidsregels op meerdere controlepunten te harmoniseren, kunnen organisaties hun algehele security postuur verbeteren.

Deel 3: Vier stappen voor het opzetten van uw firewalling-strategie

Stap 1: Leg de basis voor uw succesvolle firewalling-strategie met een moderne next-generation firewall. De juiste Cisco Secure Firewall zorgt voor consistent security beleid, zichtbaarheid en verbeterde respons op bedreigingen voor uw geïntegreerde security oplossing.

Stap 2: Wanneer u uw Cisco Secure Firewall heeft geselecteerd, moet u vervolgens voor één standaard beheeroplossing kiezen. Overweeg de volgende factoren bij het bepalen van de juiste oplossing voor uw organisatie:

- Bepaal de gewenste beheerlocatie (op kantoor of in de cloud) en welke groep verantwoordelijk wordt voor het beheren van security (SecOps of NetOps).
- Belangrijker nog: zorg dat de beheeroplossing wordt afgestemd op de huidige en toekomstige doelen van het IT-team. Als u workloads naar de cloud verplaatst, een leveranciersportal start, digitale transformatieprojecten begint of SaaS-toepassingen inzet, is het adopteren van cloudgebaseerd beheer een goed idee. Als uw organisatie gebruikmaakt van monolitische verouderde toepassingen, sluiten toepassingen op kantoor wellicht beter aan op uw behoeften. Over het algemeen vereisen verouderde toepassingen diverse aanpassingen voor optimale werking in de cloud. Als u geen directe plannen heeft om dergelijke toepassingen te upgraden, is een beheersysteem op kantoor doorgaans de beste keuze.
- Met een cloudgebaseerde beheeroplossing kunnen netwerkteams beleid in de gehele organisatie harmoniseren, complexiteit verminderen en alle security controlepunten beheren via een centraal dashboard. Op die manier kunt u beleidsregels consistent orkestreren en beheren vanaf één plek en bescherming bieden tegen de nieuwste bedreigingen. Met een gecentraliseerde, cloudgebaseerde toepassing kunt u security management stroomlijnen, nieuwe apparaten sneller implementeren met sjablonen en alle wijzigingen in uw omgeving in de loop van de tijd traceren.

Stap 3: Verbeter uw security postuur met integratie. Uw firewalling-strategie moet uitgebreide dekking bieden aan alle micro-buitengrenzen, en alle verbonden apparaten en security oplossingen beschermen en beheren. Door security in uw gehele heterogene netwerk te integreren – in cloud-apps en services, zakelijke e-mail en alle verbonden endpoints – wordt uw bedrijf beschermd tegen het steeds verder uitbreidende bedreigingslandschap.

Met deze stap kan uw security team meer bedreigingen blokkeren, sneller reageren op geavanceerde bedreigingen en automation toepassen in netwerk, cloud-apps en endpoints.

Stap 4: Zorg dat uw firewalling-strategie geavanceerde dreigingsanalyse omvat om uw bedrijfsmiddelen te beschermen, zodat u opkomende bedreigingen een stap voor kunt blijven. Een van de

6 "Is the Cloud Secure?" Gartner, 27 maart 2018.10

gemakkelijkste manieren is het selecteren van een oplossing die via uw firewall automatisch de nieuwste bedreigingsinformatie levert aan uw netwerk. Met up-to-date informatie en volledige zichtbaarheid krijgen security teams inzicht in de nieuwste kwetsbaarheden. En als een bedreiging toch een ingang vindt, kunt u identificeren waar en hoe. Ingebouwde next-generation IPS genereert een geautomatiseerde ranglijst van risico's en impactmarkeringen die prioriteiten identificeren, zodat de kritiekste middelen en informatie kunnen worden geïdentificeerd en geprioriteerd. Security teams kunnen direct corrigerende maatregelen nemen en bedreigingen herstellen. Hierbij kunnen ze zich op de kritiekste middelen richten in plaats van dat ze worden afgeleid door ruis, waardoor SOC-activiteiten veiliger worden.

Het begint met de juiste firewall als basis

Huidige security teams hebben het volgende nodig:

Betere security ondersteund door toonaangevende threat intelligence om uw complexe netwerk te beschermen en bedreigingen eerder en sneller te detecteren en aan te pakken.

Een manier om **security beleid efficiënt op te zetten, te schalen en te harmoniseren** op uw netwerk.

Zichtbaarheid en verminderde complexiteit met unified management en automation om security processen te versnellen en hun ervaring te verbeteren.

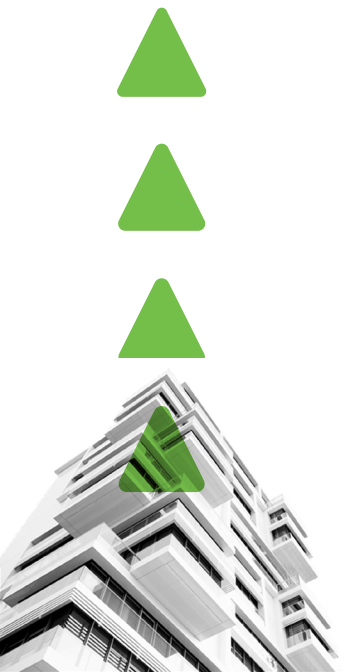
Networking en security die samenwerken om uw bestaande investeringen te maximaliseren. De juiste oplossing biedt een diepe set integraties voor uitgebreide security die alles overal beschermt.

De voordelen van een firewalling-strategie met Cisco Secure Firewall

Maak van uw gehele netwerk een uitbreiding van uw security architectuur: Door algemeen beleid, mogelijkheden voor inbraakpreventie en andere kernfuncties te delen met Cisco Secure Firewall kunnen switches en routers security handhaven en wordt de netwerkinfrastructuur gekoppeld aan een uitgebreide security portfolio. Deel snel threat intelligence in uw gehele infrastructuur om snel ogenschijnlijk niet-verbonden gebeurtenissen te correleren, ruis te elimineren en bedreigingen sneller te stoppen.

Eersteklas security mechanismen: Cisco Secure Firewall biedt superieure effectiviteit tegen bedreigingen om uw complexe netwerk te beschermen tegen steeds geavanceerdere aanvallen. Toonaangevende, geavanceerde threat intelligence helpt uw organisatie bij het zoeken naar nieuwe malwaredomeinen, schadelijke URL's en onbekende of niet bekendgemaakte kwetsbaarheden om bedreigingen eerder te detecteren en sneller te handelen. Ingebouwde IPS van de volgende generatie biedt uitgebreide zichtbaarheid door een geautomatiseerde ranglijst van risico's en impactmarkeringen te genereren om prioriteiten voor uw security team te identificeren en ruis te minimaliseren. Dankzij retrospectieve security blijft u op de hoogte, en doordat bedreigingen na de eerste detectie blijvend geanalyseerd worden, kunt u geavanceerde malware die in eerste instantie verborgen bleef beter identificeren.

Unified beleid en zichtbaarheid van bedreigingen: Security teams kunnen consistentie en harmonisering van beleid realiseren door security mechanismen op elk apparaat te standaardiseren en uit te voeren – van netwerkapplicaties en hosts tot in de cloud. Met Cisco's flexibele en gecentraliseerde beheer kan uw team op veel apparaten snel en eenvoudig schaalbare controles toepassen om consistent beleid te garanderen. Verminder complexiteit met unified management en automated bedreigingscorrelatie tussen nauw geïntegreerde security functies, waaronder toepassingsfirewalls, NGIPS en AMP. Stroomlijn security beleid en apparaatbeheer in uitgebreide netwerken en versnel belangrijke security processen, zoals detectie, onderzoek en herstel.



Deel 4: Een toekomstbestendige security oplossing

De manier waarop we werken is veranderd. Onze bedrijven en netwerken zijn getransformeerd, waardoor de regels van netwerk security zijn veranderd. Deze ontwikkelingen dwingen ons om de firewall te heroverwegen en firewalling te omarmen.

Cisco stimuleert innovatie om in te spelen op deze trends met een security platform dat eersteklas security mechanismen biedt waar dat nodig is, met consistent security beleid en zichtbaarheid, ondersteund door toonaangevende threat intelligence. De nieuwste generatie Cisco Secure Firewall vormt de basis van onze portfolio van nauw geïntegreerde producten.

Cisco's flagship cloudbeheeroplossing – **Cisco Defense Orchestrator** – maakt harmonisatie van beleid mogelijk bij diverse Cisco security producten.

In elk Cisco Security-product is **SecureX** ingebouwd, een oplossing voor automated respons op bedreigingen die reageert op nieuwe cyberaanvallen door automatisch tegenmaatregelen te delen en te implementeren in de gehele security architectuur.

Secure Endpoint biedt wereldwijde threat intelligence, geavanceerde sandboxing en blokkering van malware in real time. AMP analyseert doorlopend de bestandsactiviteiten in uw uitgebreide netwerk, zodat u snel geavanceerde malware kunt detecteren, inperken en verwijderen.

Talos Threat Intelligence is een wereldberoemd team van fulltime bedreigingsonderzoekers, datawetenschappers en engineers dat informatie verzamelt over bestaande en opkomende bedreigingen. Talos vormt het fundament van het gehele Cisco security ecosysteem en biedt bescherming tegen aanvallen en malware. Talos biedt zichtbaarheid van de nieuwste wereldwijde bedreigingen, praktisch bruikbare informatie over verdediging en beperking, en collectieve respons om alle Cisco-klanten actief te beschermen.

SNORT next-generation inbraakpreventiesysteem (SNORT NGIPS) is een toonaangevend, open-source NGIPS dat verkeersanalyses, sniffing/vastlegging van pakketten en protocolanalyses uitvoert. SNORT NGIPS gebruikt Talos threat intelligence om de gehele security community te helpen door beleid te delen dat bescherming biedt tegen opkomende bedreigingen.

Met Identity Services Engine (ISE) is overal aanpasbare, vertrouwde toegang op basis van context beschikbaar. Het biedt slimme, geïntegreerde bescherming via intent-based beleid en compliance-oplossingen.

Secure Access by Duo biedt multi-factor authentication, zichtbaarheid van endpoints, adaptieve verificatie en beleidshandhaving met externe toegang en eenmalige aanmelding om proactief de toegang tot toepassingen te beveiligen.

Secure Network Analytics, Secure Workload en Application Centric Infrastructure (ACI) werken samen en houden uw gebruikers (waar zij ook heen gaan) en hun toepassingsworkloads (waar deze zich ook bevinden) in de gaten. Hierbij wordt gebruikgemaakt van machine learning, gedragsmodellering, telemetrie van de netwerkinfrastructuur en segmentatie om opkomende bedreigingen te slim af te zijn.

Implementeer uw toekomstbestendige firewalling-strategie door te investeren in het Cisco security platform en Cisco Secure Firewall. U bent dan verzekerd van het sterkste security postuur dat nu beschikbaar is en bent klaar voor de toekomst.

Deel 5: Bouw vandaag uw toekomst van de firewall

Cisco combineert leiderschap op het gebied van networking en grensverleggende security technologie om de veiligste architectuur ooit te leveren. Of het nu gaat om het verbeteren van uw netwerk security door bestaande investeringen te optimaliseren of om het transformeren van uw routers in een firewall: Cisco blijft innoveren.

Cisco Secure Firewall is netwerk security die is ontwikkeld voor uw digitaal transformerende bedrijf – van het bedrijf dat het netwerk heeft gebouwd.

Leer meer over Cisco Secure Firewall en ga vandaag nog aan de slag om uw toekomst van firewalling vorm te geven. Lees meer over de nieuwste trends op het gebied van netwerken in het 2020 GlobalNetworking Trends Report.