Secure Access Service Edge (SASE)

At-a-Glance

Wat is SASE?

Secure Access Service Edge (SASE) combineert networking en security functies in de cloud voor veilige toegang tot toepassingen, waar gebruikers ook werken. De kernfuncties omvatten softwaregedefinieerde WAN (SD-WAN), Firewall-as-a-Service (FWaaS), veilige webgateway (SWG), Cloud Access Security Broker (CASB) en zero-trust netwerktoegang (ZTNA). Het doel van het SASE-model is om deze functies – traditioneel geleverd in point-oplossingen in silo's – te consolideren in één geïntegreerde cloudservice.

SASE ondersteunt organisaties bij:

Verbinding

Gebruikers naadloos toegang bieden tot de toepassingen en data die ze nodig hebben – in elke omgeving, vanaf elke locatie

Controle

De toegang beheren en de juiste security handhaven waar gebruikers ook werken

Convergentie

Networking en security functies convergeren om veilige connectiviteit as-a-service aan te bieden

Wat stimuleert de overstap naar Secure Access Service Edge?

Door de digitale bedrijfstransformatie en de verschuiving naar meer verspreide medewerkers is de behoefte om altijd en overal toegang te hebben tot bedrijfsmiddelen groter geworden. Hierdoor moeten networking en security naar de cloud worden gebracht en daar als een één geconvergeerde service worden aangeboden met flexibele implementatie- en verbruiksmodellen.

De verschuiving naar meer verspreide medewerkers is niet nieuw, maar is recent versneld. De principes van SASE zijn in de afgelopen jaren gevormd. SASE staat nu op de voorgrond omdat externe toegang tot toepassingen en 'overal vandaan kunnen werken' een topprioriteit van organisaties werden. Door deze verschuiving is het datacenter niet langer het middelpunt, maar de gebruiker. Om gebruikers veilige toegang tot bedrijfsmiddelen en toepassingen te bieden, moeten ze als een 'eenpersoonsvestiging' worden behandeld.

Maar de traditionele vestiging blijft ook bestaan. Sommige mensen zullen terugkeren naar kantoor, zodat er een nieuwe verschuiving in de verspreiding van medewerkers ontstaat. 82% van de respondenten van een recent Gartner-onderzoek wil werken op afstand deels toestaan wanneer medewerkers weer terugkeren naar werklocaties.[1] Ondanks deze aanhoudende veranderingen verwachten gebruikers een naadloze verbinding met de toepassingen die ze nodig hebben.

SASE is gebaseerd op cloud-native mogelijkheden die de IT-omgeving vereenvoudigen door networking en security teams dichter bij elkaar te brengen voor betere samenwerking en kortere responstijden. Voor het beste resultaat raadt Gartner organisaties aan om één SASE-leverancier te kiezen die een uitgebreide set security functies en flexibele, hoogwaardige networking kan leveren en een betrouwbare staat van dienst heeft.

Onze benadering

Cisco's SASE-architectuur combineert networking, clientconnectiviteit, security en mogelijkheden voor waarneembaarheid in één aanbieding. Onze benadering helpt organisaties om:

- Medewerkers op afstand, vaste locaties, via internet beschikbare apparaten en workloads te verbinden met en veilige toegang te verlenen tot toepassingen, data en het internet
- End-to-end waarneembaarheid te krijgen van gebruikers tot toepassingen op elk netwerk en in elke cloud
- Prestaties te optimaliseren door het snelste, betrouwbaarste en veiligste pad naar de cloud te garanderen
- Zero-trust netwerktoegang te adopteren door per sessie de identiteit van gebruikers en de status van hun apparaten te verifiëren voor veilige toegang tot toepassingen
- Hun bedrijfsvoering flexibeler te maken door de cloud te benutten, hun infrastructuur minder complex te maken en directe schaalbaarheid te bieden

Cisco's SASE-benadering biedt eenvoud, zichtbaarheid en efficiëntie. Organisaties kunnen verder bouwen op wat ze al hebben en hun investeringen op kantoor en in de cloud beschermen en toch de flexibiliteit hebben om de infrastructuur in de toekomst verder te ontwikkelen. Terwijl u services vanaf kantoor overbrengt naar de cloud, kunt u uw beleid in alle omgevingen consistent handhaven. Met open API's voor zowel networking als security kunt u snel de beste optie kiezen door eenvoudige integratie met favoriete producten of ons brede, open ecosysteem.

SASE in cijfers

40%

van de ondernemingen heeft tegen 2024 duidelijke strategieën om SASE te adopteren[2]

64%

meent dat netwerk security complexer is dan twee jaar geleden[3]

45%

van de verzoeken voor toegang tot beschermde apps komt van buiten het bedrijf[4]

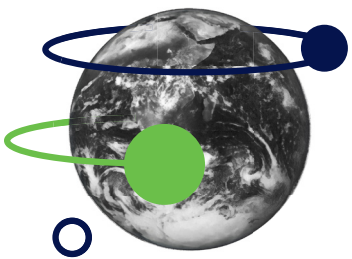
80%

van de organisaties gebruikt of overweegt het gebruik van SD-WAN[3]

20%

van de ondernemingen verwacht in 2023 SWG, CASB, ZTNA en FWaaS van dezelfde leverancier te gebruiken[2]

Componenten van Cisco's SASE-architectuur



Grootste leverancier van SD-WAN oplossingen

Cisco is 's werelds grootste leverancier van SD-WAN oplossingen met het grootste marktaandeel en meer dan 30.000 klanten

Verbinding via SD-WAN: Cisco SD-WAN ondersteund door Viptela en Meraki

Cisco SD-WAN is een cloudgebaseerde overlay WAN-architectuur die nevenvestigingen met het hoofdkantoor, datacenters en multi-cloud omgevingen verbindt en daarbij een voorspelbare toepassingservaring biedt. Dankzij de flexibiliteit van geïntegreerde security op kantoor en/of in de cloud kan IT het SASE-traject stimuleren. Uitgebreide integraties met meerdere cloudproviders die Cloud OnRamp gebruiken maken een einde aan complexiteit. U profiteert hierdoor van een echte zero-touch en meer automated ervaring. De analysemogelijkheden bieden zichtbaarheid en inzichten voor het snel isoleren en oplossen van problemen en verbeterde netwerkintelligentie. Alles wordt beheerd via een gecentraliseerd dashboard dat IT-processen vereenvoudigt met mogelijkheden als automated provisioning, unified beleid en geïntegreerde workflows. IT kan met een Cisco SD-WAN cloud-first architectuur flexibiliteit garanderen om elke gebruiker via de cloud te verbinden met elke gewenste toepassing.

Voordelen

- Verbind elke gebruiker met elke toepassing dankzij geïntegreerde mogelijkheden voor multicloud, security, unified communications en toepassingsoptimalisatie
- Benut uitgebreide security op kantoor en in de cloud (met Cisco Umbrella-integraties) om de overstap naar een SASE-architectuur te versnellen met behoud van compliance
- Bied een verbeterde toepassingservaring en voldoe aan serviceovereenkomsten (SLA's) met realtime analyses, zichtbaarheid en controle van bedrijfskritische toepassingen
- Breid SD-WAN fabric uit naar openbare clouds met Cloud OnRamp voor IaaS, voor automation van toegang tot workloads en voor consistent beleid
- Gebruik realtime analyses om gebruikers het beste pad te bieden voor optimale application performance met Cloud OnRamp voor SaaS
- Bied gecentraliseerde controle voor handhaving van intent-based beleid en security op het hele netwerk voor operationele eenvoud

Componenten van Cisco's SASE-architectuur

Verbinding via externe toegang: AnyConnect

Cisco AnyConnect is een security endpointagent die medewerkers op afstand probleemloze, zeer veilige toegang biedt tot het internet of het bedrijfsnetwerk vanaf elk apparaat, op elk moment en op elke locatie en tegelijk de organisatie beschermt. Het biedt ook de zichtbaarheid en controle die u nodig heeft om te identificeren wie en welke apparaten toegang zoeken tot uw uitgebreide onderneming. De brede reeks security services van Cisco AnyConnect omvatten functies als externe toegang, postuurhandhaving, web security functies en bescherming bij roaming. Cisco AnyConnect geeft uw IT-afdeling alle security functies om medewerkers op afstand een robuuste, gebruiksvriendelijke en zeer veilige gebruikerservaring te bieden.

Voordelen

- Stroomlijn gebruikerstoegang tot het internet en interne bronnen of toepassingen
- Krijg diepgaandere zichtbaarheid van gebruikers die toegang zoeken tot het netwerk, al dan niet op locatie
- Garandeer beleidshandhaving en apparaatpostuur voor alle gebruikers
- Bied flexibiliteit met ondersteuning van meerdere apparaten en platforms
- Vereenvoudig de infrastructuur met één client die cloud security, endpoint security en toegangsfuncties mogelijk maakt

Componenten van Cisco's SASE-architectuur

Leider in zero trust

In de Forrester Wave: Zero Trust is Cisco twee jaar op rij als leider benoemd

Zero-trust netwerktoegang: Cisco Secure Access by Duo

Cisco Secure Access by Duo biedt een uitgebreide ZTNA-oplossing voor veilige toegang tot uw toepassingen en omgeving voor elke gebruiker, via elk apparaat en vanaf elke locatie. ZTNA is een strategische benadering van security waarbij niets in de netwerkarchitectuur van een organisatie gewoonweg wordt vertrouwd. Een ZTNA-model behandelt alle resources als extern en controleert doorlopend het vertrouwen voordat toegang wordt verleend.

Met Duo kunt u zero trust implementeren door de identiteit van gebruikers en de status van apparaten bij elke toegangspoging te identificeren, met aangepast security beleid dat elke toepassing beschermt. Op die manier voorkomt u onbevoegde laterale beweging door een omgeving en wordt u beschermd tegen gekraakte inloggegevens, risicovolle apparaten en ongewenste toegang tot uw toepassingen en data. Duo omvat functies zoals eenvoudige en effectieve multi-factor authentication (MFA), volledige apparaatzichtbaarheid, adaptief beleid, externe toegang met of zonder VPN en eenmalige aanmelding (SSO) voor elke toepassing.

Voordelen

- Breng gebruikers- en apparaatvertrouwen tot stand bij elk toegangsverzoek, ongeacht waar dit vandaan komt
- Beveilig de toegang tot uw toepassingen en netwerk
- Breid vertrouwen uit om een moderne onderneming met een gedistribueerd netwerk te ondersteunen
- Implementeer security voor op kantoor, in de cloud, externe toegang en VPN in slechts enkele uren of dagen in plaats van weken
- Bespaar tijd en kosten door de security voor toegang te centraliseren en beheersinspanningen en het aantal helpdesk-tickets te verminderen

Componenten van Cisco's SASE-architectuur

Pionier in cloud security

Cisco Umbrella biedt sneller volledige bescherming met toonaangevende security effectiviteit en prestaties

Controle via cloud security: Cisco Umbrella

Cisco Umbrella is de cloud-native, multifunctionele security service die de kern vormt van Cisco's SASE-architectuur. Cisco Umbrella brengt functies als firewall, veilige webgateway, security op de DNS-laag, Cloud Access Security Broker (CASB) en threat intelligence samen in één cloudservice om grote en kleine bedrijven te helpen hun gebruikers, toepassingen en data te beveiligen. Naarmate meer organisaties directe internettoegang omarmen, wordt het uitbreiden van de bescherming naar roaming gebruikers en nevenvestigingen eenvoudig met Umbrella. Umbrella biedt wereldwijde dekking met een uitgebreid netwerk van snelle datacenters met peering naar meer dan 1.000 van 's werelds beste internetproviders (ISP's), netwerken voor contentlevering (CDN's) en SaaS-platforms die voor elk verzoek de snelste route bieden. Dit resulteert in superieure snelheid, effectieve security en gebruikerstevredenheid.

Umbrella gebruikt security op de DNS-laag om verzoeken van malware, ransomware, phishing en botnets te blokkeren voordat er een verbinding tot stand komt. De veilige webgateway biedt logboekregistratie en diepgaandere inspectie van al het webverkeer voor grotere transparantie, beheersing en bescherming. De cloudgebaseerde firewall registreert en blokkeert al het verkeer door gebruik te maken van IP-, poort- en protocolregels voor een consistente handhaving in uw gehele omgeving. CASB-functionaliteit is geïntegreerd om het gebruik van cloudtoepassingen te detecteren en te beheren. Met Cisco SecureX (bij alle Umbrella-abonnementen inbegrepen) kunt u bedreigingen sneller onderzoeken en herstellen.

Voordelen

- Stop bedreigingen voordat deze uw netwerk of endpoints bereiken
- Handhaaf brede, betrouwbare security voor alle poorten en protocollen
- Lever snelle, schaalbare security op en buiten uw netwerk
- Versnel detectie en herstel van bedreigingen met contextuele intelligentie
- Gebruik één security dashboard voor efficiënt beheer
- Profiteer van de betrouwbare prestaties van een wereldwijde cloudarchitectuur met 100% uptime sinds 2006

Componenten van Cisco's SASE-architectuur

Waarneembaarheid: ThousandEyes

Door het toenemend gebruik van het internet en cloudservices vallen meer netwerken buiten uw eigendom of directe controle. Organisaties moeten de prestaties en de integriteit van het onderliggende transport waarborgen, ook wanneer zij de infrastructuur niet in eigendom hebben of niet kunnen bepalen hoe serviceproviders het verkeer routeren.

ThousandEyes biedt niet alleen volledige zichtbaarheid van gebruikers en toepassingen op elk netwerk, maar ook praktisch bruikbaar inzicht in prestatieproblemen. Hierdoor kunt u snel incidenten oplossen om betrouwbare connectiviteit en een optimale toepassingservaring te waarborgen.

Voordelen

- Verminder de benodigde tijd om problemen te identificeren en op te lossen (MTTI/MTTR) door direct de bron ervan te bepalen op het interne netwerk, bij ISP's en providers van clouds en toepassingen
- Profiteer van succesvolle escalaties bij serviceproviders op basis van data die eenvoudig kan worden gedeeld met interne en externe belanghebbenden
- Maak een einde aan nutteloos vingerwijzen en beheer OLA's/SLA's effectief bij interne teams en externe providers

Waarom partner worden van Cisco

De implementatie van een volledige SASE-architectuur is een stapsgewijs traject dat voor elke organisatie anders is. Cisco biedt oplossingen met de consolidatie en het implementatie- en beheergemak die u nodig heeft om uw bedrijf te laten groeien en effectieve security te bieden voor gebruikers waar ze ook werken – zonder dat de snelheid, prestaties en gebruikerservaring achteruitgaan.

Prestaties van een leider in networking, security en waarneembaarheid waarop u kunt vertrouwen

Dankzij Cisco's streven naar operationele perfectie en onze geïntegreerde architectuur kunnen we in enkele minuten beveiligde verbindingen tot stand brengen. Klanten van Cisco profiteren van een uitgebreid netwerk van datacenters met directe peering naar duizenden serviceproviders en IaaS- en SaaS-leveranciers voor unified controle en orkestratie. In tegenstelling tot concurrenten kunnen we optimalisatie van ondernemingssegmentatie en toepassingservaring implementeren met voorspelbare prestatie- en latentiecontroles voor onze wereldwijde diensten.

Vereenvoudigde aankoop en snelle implementatie

Cisco vereenvoudigt de aanschaf met één SASE-aanbieding zodat u alle kerncomponenten kunt kopen – cloud security, zero-trust netwerktoegang, SD-WAN en waarneembaarheid – en zorgt voor een probleemloze toekomstige overgang naar één abonnementsservice. Of u nu alle componenten in één keer of in de loop van de tijd wilt kopen: met Cisco kunt u een SASE-architectuur bouwen zoals u dat wilt. Met automated implementatieopties en veel productintegraties kunt u honderden locaties snel en eenvoudig verbinden dankzij vereenvoudigd doorlopend beheer.

Uitgebreide controle voorbij de buitengrens met een leider in zero trust

Cisco heeft het hoogst mogelijke aantal punten behaald in de Forrester Wave: Zero Trust 2020 bij criteria zoals marktbenadering, pleitbezorging, visie en strategie, apparaat security en de toekomstige status van de zero-trust infrastructuur. Secure Access by Duo biedt controles op gebruikers- en apparaatniveau om de gebruikersidentiteit en de status van het apparaat te verifiëren. Duo stelt gebruikers- en apparaatvertrouwen vast en biedt doorlopende zichtbaarheid om het vertrouwen uit te breiden per sessie, zowel binnen als buiten het bedrijfsnetwerk. Door een consistent gebruikers- en apparaatgebaseerd toegangsbeleid te handhaven kunt u het risico op datalekken verminderen en voldoen aan compliancevereisten.

Kortere responstijd bij incidenten en hogere security effectiviteit

Cisco Umbrella gebruikt de inzichten van Cisco Talos, een van 's werelds grootste commerciële threat intelligence teams met meer dan 300 onderzoekers, om vele schadelijke domeinen, IP-adressen, URL's en bij aanvallen gebruikte bestanden te ontdekken en te blokkeren. Ook voeden we een combinatie van statistische en machine learning-modellen met grote hoeveelheden wereldwijde internetactiviteiten voor de identificatie van nieuwe aanvallen op het internet. Met Cisco SecureX kunt u bedreigingsonderzoeken versnellen en hersteltijden verkorten met automated responsacties voor meerdere security producten. Vereenvoudig uw security door een einde te maken aan handmatige taken en aanvallen eerder te stoppen.

Begin vandaag nog

Ontdek waarom Cisco 100% van de Fortune 100-bedrijven beschermt. Neem contact op met uw Cisco-verkoopvertegenwoordiger of partner om te starten met uw SASE-traject.

1. https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82 percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time
2. Gartner, The Future of Network Security Is in the Cloud, augustus 2019
3. Enterprise Strategy Group, Transitioning Network Security Controls to the Cloud, mei 2020
4. Cisco, Duo Trusted Access Report 2019