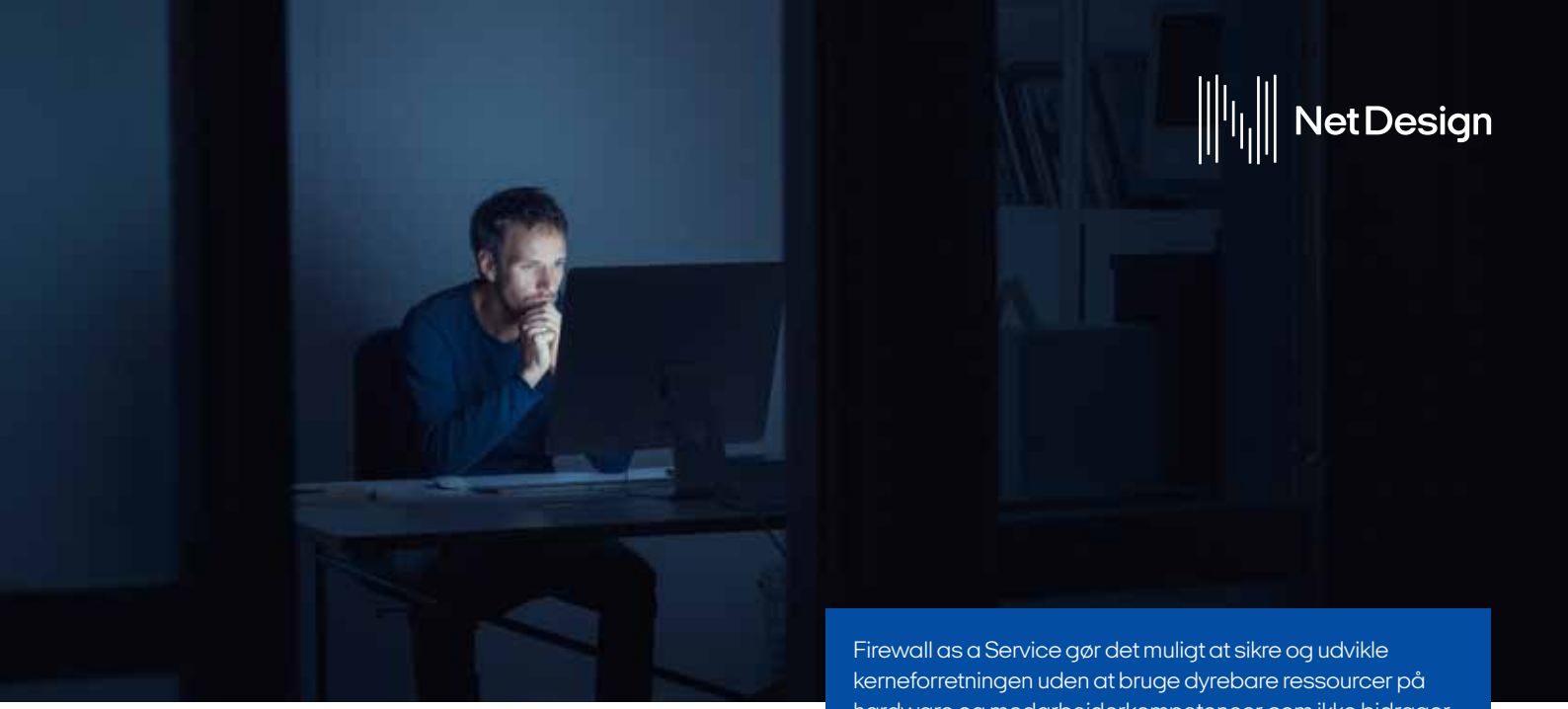


NetDesign

Firewall as a Service gør det muligt at sikre og udvikle kerneforretningen uden at bruge dyrebare ressourcer på hardware og medarbejderkompetencer, som ikke bidrager aktivt til at skabe værdi.

Firewall as a Service

Virksomhedens værn mod internettets trusler

Med Firewall as a Service kan din virksomhed etablere et værn mod internettets trusler uden at bruge ressourcer på interne kompetencer hos medarbejderne.

Internettet er i dag en forudsætning for virksomheders forretningsprocesser, salgs- og bestillingsprocedurer samt vidensdeling. Det gør virksomhederne sårbare over for IT-kriminalitet og systemnedbrud, hvad der igen stiller krav til sikkerhedsløsningerne. Vi hoster din firewall og holder den opdateret, så du og dine medarbejdere kan kommunikere, udveksle filer og holde sikre telefonmøder og videokonferencer.

Hvilke fordele giver det?

Med Firewall as a Service skal du og din virksomhed ikke sørge for indkøb og drift af dyrt hardware samt opkvalificering af medarbejdere. Vi står for alt det praktiske: Vi driver, vedligeholder og opdaterer den centralt placerede firewall i vores driftscenter. Med Firewall as a Service kan du løbende tilpasse din virksomheds behov for båndbredde, og det er derfor en fleksibel og fremtidssikker løsning. Firewall as a Service giver dig også adgang til VPN-klienter, så alle de mobile enheder (telefoner, tablets og bærbare PC'er) kan forbinde sig sikkert til det interne firmanetværk. Derfor er løsningen en investering i frihed og mobilitet – uden at kompromittere sikkerheden.

Er det aktuelt for dig?

Firewall as a Service er for virksomheder, der vil oprioritere arbejdsglæde, mobilitet, vidensdeling og produktivitet på nettet, og som samtidig ønsker et sikkert værn mod de mange trusler på nettet, der kan ende med ransomware, nedbrud og tab af vitale data.

Værd at vide før du vælger

Firewall as a Service kan hurtigt tilpasses din virksomheds behov for beskyttelse af din perimeter. Du kan vælge de services, der passer bedst til din virksomhed og det aktuelle behov for beskyttelse. Det er nemt at skalere løsningen, efterhånden som forretningen udvikler sig. Og du kan tilkøbe VPN-pakker á 100 brugere.

Funktionalitet	Basic	Add-on 1	Add-on 2	Add-on 3	Add-on 4	Add-on 5
Firewall	✓	✓	✓	✓	✓	✓
AVC	✓	✓	✓	✓	✓	✓
URL		✓		✓		✓
NGIPS			✓	✓	✓	✓
AntiBOT			✓	✓	✓	✓
AMP					✓	✓

Service	Bronze	Sølv	Guld
Månedlig rapport			✓
Læseadgang til management platform		✓	✓
5 timers hjælp pr. md.		✓	✓
Mulighed for tilkøb af ekstra hjælp	✓	✓	✓

Sådan fungerer løsningen

Firewall as a Service er baseret på Cisco Firepower, som tilbyder en lang række Next Generation Firewall-funktioner, inkl. muligheden for at tilbyde Client VPN (Cisco AnyConnect).

AVC – Application Visibility Control

AVC giver et nyttigt indblik i, hvad der rent faktisk passerer gennem virksomhedens firewall. Dette indblik kan ske helt ned på applikationsniveau, og det fungerer derfor også som et management-værktøj, der kan bidrage til ledelsens beslutningsgrundlag, når det gælder brugen af netværksressourcerne.

URL-filter

Et URL-filter kan bruges til virksomhedspolitiske begrænsninger i adgangen til bestemte sider – det kan være onlinespil i arbejdstiden, søgning på terrorrelaterede emner o.lign.
Det kan også anvendes til at begrænse adgangen til sider, der ifølge Cisco har et dårligt omdømme, når det gælder sikkerhed. Filtret er designet, så det ikke nødvendigvis blokerer alt skadeligt indhold på en hjemmeside, men kun elementer, hvor truslen er identificeret. URL-filtret kan genkende mere end 280 millioner hjemmesider, som alle er kategoriseret i 80 grupper, så det er nemt at opstille brugbare politikker.

NGIPS

NGIPS – Cisco Next Generation Intrusion Prevention System – gør det muligt at detektere og forhindre angreb, som udnytter kendte sårbarheder i enheder på indersiden af netværket. Det betyder, at man ikke nødvendigvis skal kende den enkelte malware eller lignende, som angriber, men hvis NGIPS kender til sårbarheden på f.eks. Microsoft serveren, vil alle angreb imod denne sårbarhed blive standset. Det er muligt selv at lave regler, for hvordan NGIPS skal beskytte ved hjælp af Snort, der er Open Source.

AMP – Advanced Malware Protection

AMP er installeret i selve firewall'en og vurderer alle filer i forhold til deres sikkerhedsomdømme. Får en fil for lav en sikkerhedsscore, bliver den sendt til emulering i en lukket 'sandkasse' og er i karantæne imens. Hvis filen vurderes som sikker, bliver den frigivet til modtageren.

Alle filer, som håndteres af Firewall as a Service, bliver registreret på firewall'en, hvad enten de er omkring den lukkede 'sandkasse' eller ej. Hvis det senere viser sig, at filen kan udgøre en sikkerhedstrussel, udløser det en alarm og en beskrivelse af, hvem der har modtaget filen. Så kan den hurtigt standses.

Services på tre niveauer

Bronze Service

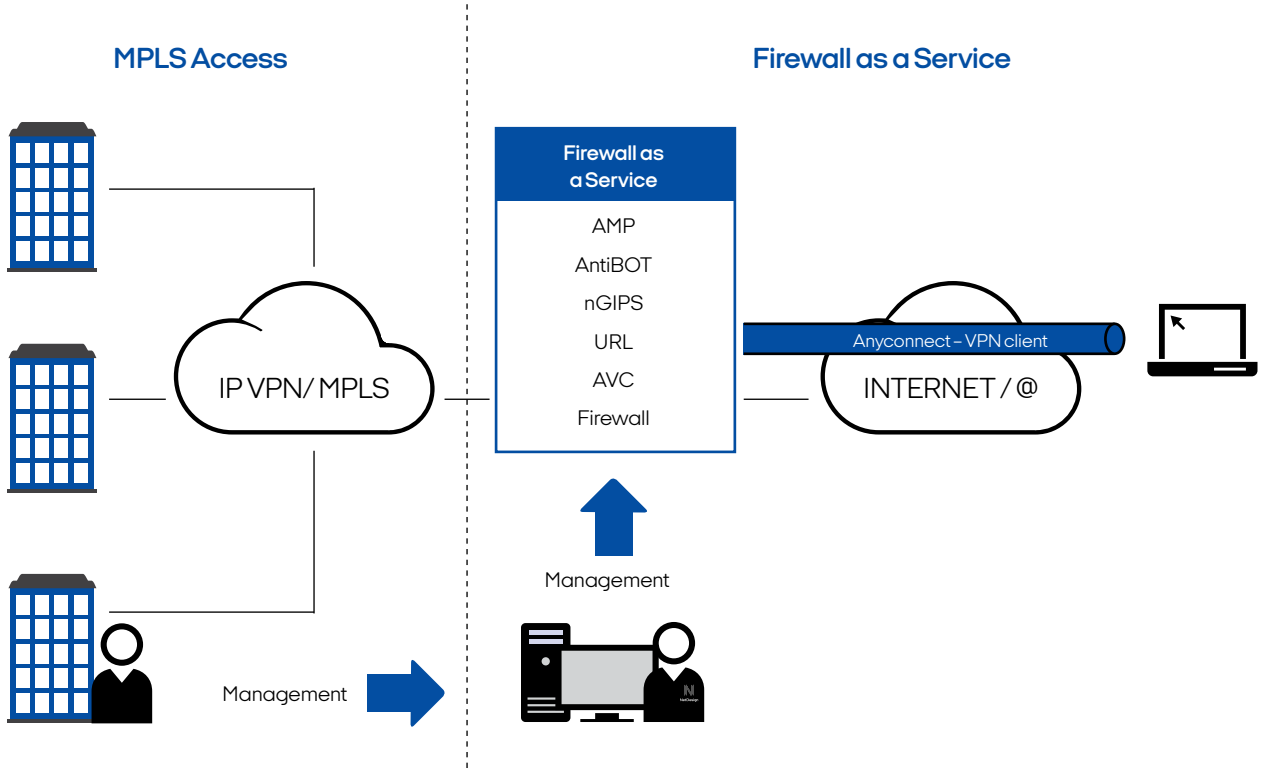
Denne service er som standard med i vores ydelse. Her afregner du ændringerne på timebasis. Vi sørger for at din firewall kørende og opdateret. Vi har det fulde ansvar for din firewall.

Sølv Service

Vi står for alle opgaver på din firewall. Din månedlige pris indbefatter et fast antal timer til ændringer, og du kan få lavet flere ændringer mod betaling. Du har ligeledes læseadgang til vores dashboard, så du kan se firewall regler mv. Vi har det fulde ansvar for din firewall. Med Sølv Service har du inkluderet 5 timers hjælp hver måned.

Guld Service

Vi står for alle opgaver på din firewall. Din månedlige pris indbefatter et fast antal timer til ændringer, og du kan få lavet flere ændringer mod betaling. Du har ligeledes læseadgang til vores dashboard, så du kan se firewall regler mv. og du modtager hver måned en rapport med trafik info. mv. Vi har det fulde ansvar for din firewall. Med Guld Service har du inkluderet 5 timers hjælp hver måned.



NetDesign, København, CVR 14 77 39 08 Communication/MC 2010.1914

For flere informationer, kontakt din NetDesign sælger, eller kontakt os på 44 35 80 00.

NetDesign