Tjenestebeskrivelse Brannmur

eviny

Innhold

Brannmur fra Eviny

Brannmur fra Eviny gir Kunden et sikkerhetsprodukt av høy kvalitet som beskytter bedriften mot trusler fra internett. Eviny drifter brannmuren, tar daglig backup av konfigurasjon, oppgraderer software ved behov, og tilpasser brannmurens konfigurasjon etter ønsker og behov. Eviny benytter kvalitetsprodukter fra Fortinet.

Standard regelsett

Brannmuren konfigureres som standard med et regelsett som tillater all trafikk initiert fra LAN mot internett, og blokkerer all trafikk initiert fra internett mot LAN. Dette sørger for at Kunde kan nå alle ressurser på internett, samtidig som bedriftens LAN har en enkel beskyttelse mot eksterne trusler. Brannmuren kan konfigureres med et mer restriktivt regelsett ved behov. For eksempel kan man blokkere all trafikk fra LAN mot internett som utgangspunkt, og kun tillate spesifisert trafikk. Dette øker sikkerheten, men medfører også økt administrasjon.

Dual-stack IPv4 og IPv6

Brannmuren leveres med dual-stack IPv4 og IPv6. Alle Evinys internettlinjer har støtte for native IPv6. Man tildeles et offisielt /48 IPv6 subnett.
Som standard konfigureres første /64 IPv6 subnett i denne rekkevidden i LANet. IPv6-trafikk blir ikke NATet. IPv6-trafikk sikres på tilsvarende måte som IPv4-trafikk.

IPv4 NAT

Brannmur konfigureres med 1 fast offisiell IP-adresse på WAN-interfacet. Som standard konfigureres «many-to-one» NAT (også kalt Port Address Translation - PAT) fra private IP-adresser i LANet til denne offisielle IP-adressen. Som standard konfigureres privat IP subnett 192.168.1.0/24 i LANet, med 192.168.1.1 som default gateway på brannmur. Brannmuren kan konfigureres med et annet privat subnett i LANet i hvis ønskelig.

DHCP tildeling av IPv4 adresser i LAN

Brannmur konfigureres som standard som DHCP-server, og deler ut IP-adresser til noder i LANet. DHCP-serveren deler som standard ut IP-adresser fra 192.168.1.100 og oppover. Det anbefales at utstyr med fast IP-adresse i LAN konfigureres med IP-adresse mellom 192.168.1.2 og 192.168.1.99. DHCP-server kan settes opp etter ønske.

SLAAC tildeling av IPv6 adresser i LAN

IPv6 noder i LANet benytter Stateless Address Autoconfigation (SLAAC) for automatisk IPv6 konfigurasjon.

Soner

Brannmuren kan konfigureres med ulike soner med forskjellige sikkerhetsbehov, og man kan konfigurere regler for å styre hvilken trafikk som tillates og blokkeres mellom de ulike sonene. Det kan for eksempel konfigureres en DMZ (DeMilitarized Zone) der man kan plassere servere med tjenester som skal nås fra internett.

Subnett

Man kan konfigurere ulike subnett, for å segmentere nettverket. Disse subnettene kan tilknyttes samme sone, eller ulike soner. Subnettene kan konfigureres med IPv4 og/eller IPv6 adresser. De ulike subnettene kan konfigureres på separate fysiske porter på brannmuren, eller på en 802.1Q trunk som kobles mot Kundens svitsj.

Ekstra sikkerhet

Ekstra Sikkerhet benytter Web Filter, DNS Filter og Application Control for å beskytte mot trusler på internett, og gir både brukere og data god sikkerhet. Eviny benytter FortiGate brannmurer fra Fortinet. Dette er Next-Generation Firewall (NGFW) med spesialiserte brikkesett som gir mulighet for applikasjonsgjenkjenning og sikkerhetsmekanismer med høy kapasitet.
Brannmurene fra FortiGate kan konfigureres til å benytte sikkerhetstjenester som leveres av FortiGuard Labs, som er en del av Fortinet.

FortiGuard Labs tilbyr sikkerhetstjenester ved hjelp av en global infrastruktur som kontinuerlig analyserer sikkerhetstrusler på internett. Databaser over sikkerhetstrusler oppdateres mange ganger for dagen. FortiGate brannmurer med lisens kan benytte disse sikkerhetstjenestene blant annet for å stanse trafikk mot nettsteder som inneholder skadelig eller uønsket innhold.

Les mer om FortiGuard Labs på: https://fortiguard.com.

Webfilter

Web Filter gir beskyttelse mot malware, spyware og andre trusler, og beskytter bedriften ved å blokkere tilgang til nettsider med skadelig innhold. FortiGuard vedlikeholder en global database over flere hundre millioner nettsider og rangerer disse blant annet utfra om de inneholder malware eller andre trusler. Denne globale databasen oppdateres kontinuerlig og reflekterer til enhver tid det gjeldende digitale trusselbildet. Når en klient i nettverket prøver å laste en URL (adresse til en nettside), sjekker brannmuren denne URLen mot FortiGuards globale database, og tilgangen blir blokkert hvis URLen er rangert som skadelig.

Web Filter kan også konfigureres til å blokkere kategorier av URLer i henhold til bedriftens ønsker. For eksempel kan brannmuren konfigureres til å blokkere tilgang til URLer med innhold som er rangert som uetisk, voldelig, pornografisk, osv. Send Eviny en forespørsel for å få en fullstendig oversikt over de URL kategoriene man kan bruke for å filtrere trafikk.

Web Filter konfigureres som standard med blokkering av følgende URL-kategorier:

- Dynamic DNS
- Malicious Websites
- Phishing
- Spam URLs
- Pornography
- Child Abuse
- Explicit Violence
- Illegal or Unethical

Web Filter fungerer også for URLer som benytter HTTPS.

DNS filter

DNS Filter fungerer på lignende måte som Web Filter, og benytter de samme globale databasene for å vurdere om klienter prøver å nå mål på internett som inneholder malware eller annet skadelig innhold. Mens Web Filter analyserer web-trafikk som går gjennom brannmuren, analyserer DNS Filter DNS trafikk som går gjennom brannmuren.

Brannmuren konfigureres til å benytte Quad9 DNS (IP-adresse 9.9.9.9), som gir malwarebeskyttelse for klienter bak brannmuren. Quad9 er en gratis DNS-tjeneste som gir malwarebeskyttelse ved å blokkere DNS-forespørsler mot domener som inneholder virus og annen malware.

Quad9 har et globalt nettverk av DNS-servere som blokkerer millioner av DNS-forespørsler mot malware-infiserte domener hver eneste dag. Quad9 vedlikeholder en omfattende database over domener med malware, og mottar informasjon om sikkerhetstrusler fra mange ledende sikkerhetsselskaper.

Quad9 er en ikke-kommersiell tjeneste som er etablert av IBM, Packet Clearing House og Global Cyber Alliance. Les mer om Quad9 på https://quad9.net.

Mens Web Filter beskytter bedriftens nettrafikk (HTTP og HTTPS), beskytter DNS Filter alle applikasjoner og protokoller. DNS Filter er imidlertid ikke like spesifikk som Web Filter – der Web Filter kan blokkere trafikk mot en spesifikk URL (f.eks http://www.domene-xxx.no/abc), vil DNS Filter blokkere all trafikk mot domene-xxx.no.

Application control

FortiGate brannmurene som Eviny leverer er Next-Generation Firewall (NGFW), med mulighet for applikasjonsgjenkjenning. Standard konfigurasjon er at brannmuren ikke blokkerer noen applikasjoner, men den kan konfigureres til å blokkere utvalgte applikasjoner i henhold til Kundens ønsker.
For eksempel kan brannmuren blokkere P2P-fildelingsapplikasjoner hvis dette er trafikk som Kunde ikke ønsker å ha i nettverket.

Tilleggstjenester og konfigurasjon

Port forwarding

Port forwarding kan benyttes hvis bedriften har tjenesteservere som skal nås fra internett. Trafikk mot brannmurens offisielle IPv4-adresse, med et spesifikt portnummer, blir forwardet til en node med privat IP-adresse i LANet. Hvert enkelt portnummer kan forwardes til én privat IP-adresse i LANet.

Ved konfigurasjon av port forwarding, legges det også inn en brannmurregel som slipper inn trafikk fra internett til det spesifiserte portnummeret.

IPv6 trafikk blir ikke NATet gjennom ruteren, men blir rutet helt frem. Port forwarding er derfor ikke nødvendig for IPv6. For IPv6 er det kun nødvendig å legge inn en brannmurregel som slipper inn trafikk fra internett til det spesifiserte portnummeret.

1:1 NAT

1:1 NAT kan benyttes hvis Kunde har flere tjenesteservere som skal nås fra internett på samme portnummer, for eksempel hvis bedriften har to webservere som skal nås på port 80. Med 1:1 NAT blir trafikk fra internett mot en gitt offisiell IPv4-adresse NATet og videresendt til en privat IPv4-adresse på innsiden av brannmuren.

1:1 NAT forutsetter at Kunde også har bestilt offisielle IPv4-adresser fra Eviny. Alle IP-adresser i et offisielt IPv4 subnett kan 1:1 NATes mot hver sin private IP-adresse i LAN eller DMZ. Det kan ikke konfigureres 1:1 NAT for den offisielle IPv4-adressen på brannmurens WAN-interface.

Ved konfigurasjon av 1:1 NAT, legges det også inn brannmurregler som slipper inn trafikk fra internett til et eller flere spesifisert(e) portnummer.

IPv6 trafikk blir ikke NATet gjennom brannmuren, men blir rutet helt frem. 1:1 NAT er derfor ikke nødvendig for IPv6. For IPv6 er det kun nødvendig å legge inn en brannmurregel som slipper inn trafikk fra internett til det spesifiserte portnummeret.

Klient VPN

Klient VPN kan benyttes hvis bedriften har behov for å nå noder i eget LAN eller DMZ via en sikker tilkobling fra internett. Dette kan være nyttig hvis bedriftens ansatte har behov for å nå ressurser når de benytter hjemmekontor. All trafikk er kryptert ved hjelp av IPsec.

Eviny legger inn på brannmuren de brukerne som skal ha tilgang til Klient VPN, med et personlig passord. Det legges også inn et felles passord (pre-shared key).

Disse brukerne installerer FortiClient VPN på sin PC, MAC, nettbrett eller mobiltelefon, og legger inn en enkel konfigurasjon for å få tilgang til bedriftens ressurser via Klient VPN. Eviny sender en enkel veiledning for å sette opp FortiClient VPN.

Når man er tilkoblet Klient VPN med FortiClient VPN, vil all internettrafikk fra klienten gå via brannmuren. Det betyr at klienten er sikret mot trusler fra internett på samme måte som når klienten er tilkoblet direkte i bedriftens nettverk.

VPN Site-to-Site

VPN Site-to-Site brukes for å etablere kommunikasjon mellom bedriftens LAN og et nettverk på en annen lokasjon. VPN Site-to-Site kan etableres mot brannmur driftet av Eviny på en annen lokasjon, eller mot brannmur driftet av Kunde eller en tredjepart. All trafikk er kryptert ved hjelp av IPsec.

VPN Site-to-Service

VPN Site-to-Service brukes for å etablere kommunikasjon mellom bedriftens LAN og tjenester hos en leverandør av skytjenester. All trafikk er kryptert ved hjelp av IPsec.

Tidsstyring av brannmurregler

Det kan legges inn tidsstyring av brannmurregler i henhold til Kundens ønsker. For eksempel kan man konfigurere tilgang til et gjestenett slik at det kun er tilgjengelig for bruk innenfor et angitt tidsrom.

Brukertilgang

Brukertilgang åpner for at kunden eller en tredjepart som kunden gir tilgang, selv ved behov kan foreta ønskede endringer på konfigurasjonen på brannmuren uten at Eviny engasjerer seg i endringen.

Etter at kunden er gitt tilgangen er Eviny ikke ansvarlig dersom det eventuelt oppstår feil som følge av at kunden eller tredjeparten har foretatt endringer, men Eviny vil ha backup av brannmur-innstillingene slik at den kan tilbakestilles til siste backup før endringene ble foretatt, mot at kunden dekker Evinys administrasjonskostnad med dette

Konfigurasjonsendring

Konfigurasjonsendringer vil bli fakturert i henhold til den enhver tid gjeldende prisliste. Funksjonalitet og konfigurasjonsendringer er begrenset til de tjenester som er beskrevet i denne tjenestebeskrivelsen.

HA-cluster

HA-cluster står for High Availability Cluster, og sikrer at Kunden har redundante brannmurer dersom brannmurene skulle ryke. Det er automatisk failover ved feil på aktiv brannmur når et brudd oppstår. Dette sikrer at nedetiden er minimal samtidig som Kundens sikkerhet ivaretas kontinuerlig.

Eviny tilbyr allerede redundante linjer for å sikre maksimal oppetid hos Kunde, og Evinys HA-cluster utvider Kundens mulighet til å sikre tilgang til tjenesten.

HA-cluster forutsetter at kunde har to internettlinjer og to brannmurer, hvor minste størrelse er 60F.

Begrensninger og kundens ansvar

Selv om Brannmur fra Eviny med Ekstra Sikkerhet gir god beskyttelse mot ulike trusler, gir det ikke en komplett beskyttelse, og det er viktig å være klar over hvilke begrensninger som ligger i produktet, og hvilke ekstra tiltak som er viktig at Kunde iverksetter for å oppnå best mulig sikkerhet.

Eviny gir ingen garantier for at man ikke blir utsatt for virus, malware, phishing, og andre typer dataangrep. Dette kan man dessverre bli utsatt for uansett hvor godt man sikrer seg. Eviny kan ikke holdes økonomisk ansvarlig for skader og tap som bedrfiten blir påført som følge av dataangrep.

Opplæring av brukere

Det er viktig å lære opp egne brukere og bevisstgjøre dem på hvilke trusler man kan utsettes for, og hvordan man best mulig kan beskytte seg og bedriftens data. Det anbefales å lære opp egne brukere til å:

- Ikke ukritisk klikke på linker i e-poster man mottar
- Unngå å laste ned programvare som ikke er godkjent av bedriften
- Unngå å besøke tvilsomme nettsteder som kan inneholde malware
- Unngå å sette inn minnepinner som kan være infisert av malware i datamaskinen

Endepunktssikkerhet

Det er viktig at brukerne installerer og vedlikeholder sikkerhetsprogramvare/antivirus på sine klienter. Dette for å sikre at klientene ikke blir infisert med malware og utsatt for andre sikkerhetstrusler når de er tilknyttet nettverk utenom egen brannmur.

Oppdatering av programvare

Det er viktig at Kunde kontinuerlig oppdaterer all programvare som benyttes. Det oppdages stadig nye sikkerhetshull i ulike typer programvare, både i operativsystemer og applikasjoner. For å unngå risiko forbundet med slike sikkerhetshull, må all programvare oppdateres jevnlig med de oppdateringer som programvareselskapene tilbyr.

Service Level Agreement (SLA)

Eviny tilbyr tre servicenivåer Gull, Sølv og Bronse for alle tjenester. Bronse leveres som standard. For tjenester man ønsker et høyere servicenivå for, kan man velge enten servicenivå Sølv eller Gull.

Høyere servicenivå gir en bedre garanti for oppetid, raskere respons i feilsituasjoner, samt mulighet for feilhåndtering utover det som er normal åpningstid.

Tjenestebeskrivelse Brannmur

Eviny AS
Postboks 7050,
5020 Bergen

Telefon: 55 57 00 00
E-post: hei@eviny.no

eviny.no