PALVELUKUVAUS - PFSENSE PALOMUURIPALVELU

SISÄLLYS

Palomuuripalvelu yleisesti

TNNet Oy:n tuottama pfSense-palomuuripalvelu parantaa yritysverkon tietoturvaa ja tarjoaa monipuolisuutta tietoliikennepalveluihin. Palomuuripalvelu tuotetaan Datavault Kanavuoresta Datacenter-ajattelumallia hyödyntäen. Tämä tarkoittaa sitä, että jokaista toimipistettä tai muuta tietoliikennepalvelua varten ei tarvitse ostaa uutta palomuuria, vaan kaikki tietoliikennepalvelut voidaan terminoida yhdelle muurille. Palomuuripalvelu tuotetaan virtualisoituna korkealaatuisessa palvelinympäristössä, jolloin palvelulle voidaan allokoida juuri oikea määrä palomuurikapasiteettia, eikä asiakkaan tarvitse maksaa käyttämättömistä resursseista tai lisensseistä.

Palomuuripalvelussa lähtökohtaisesti ylläpitovastuu on TNNetillä, ja muutokset toteutetaan TNNetin toimesta. Asiakkaalle voidaan tarvittaessa myöntää tunnukset palveluun, mutta tällöin vastuu siirtyy asiakkaalle. TNNet säilyttää palomuureista varmuuskopiota kahden viikon ajan, jolloin palomuuri voidaan tarvittaessa palauttaa aiempaan konfiguraatioon esimerkiksi virheellisten sääntömuutosten tai muun vikatilanteen jälkeen.

Muiden palvelujen liittäminen palomuuriin

Palomuuripalveluun on mahdollista liittää useita eri järjestelmiä ja palveluita. Näitä ovat esimerkiksi TNNetin tietoliikenne- ja laitesalipalvelut, jotka ovat samassa laitetilassa tai yhteensopivan tietoliikenneyhteyden perässä.

Eri järjestelmät voidaan liittää palveluun L2-tason yhteydellä. Tällöin yhteys eristetään muista joko loogisesti omalla VLAN-tunnisteella tai käyttämällä täysin muista asiakkaista eriytettyjä fyysisiä laitteita. Tämä mahdollistaa täysin eristetyn LAN-ympäristön jopa eri kaupungeissa sijaitsevien toimipisteiden välille. On kuitenkin aina suositeltavaa käyttää lähde- ja kohdejärjestelmien välistä salausta, kun käsitellään arkaluontoista dataa (esimerkiksi HTTPS-yhteyttä HTTP-yhteyden sijasta).

Tapauksissa, joissa kaikki liitettävät palvelut eivät sijaitse TNNetin verkon alueella, voidaan käyttää VPN-tunnelointi ja SD-WAN-ratkaisuja julkisen Internetin ylitse. Nämä ratkaisut ovat salattuja yhteyksiä kohdeympäristön sekä palomuuripalvelun välillä. Yleisimmin käytössä olevat tunnelointiprotokollat ovat SSL-VPN:t sekä IPSec-tunnelit.

Perusominaisuudet

pfSense on avoimeen lähdekoodiin perustuva palomuuriohjelmisto, joka on hyvin räätälöitävissä tarjoten jokaisen asiakkaan tarpeisiin soveltuvat ratkaisut. pfSense on kasvanut yhdeksi maailman käytetyimmistä palomuuriratkaisuista kustomoitavuutensa ja skaalautuvuutensa ansiosta.

pfSense on tilallinen palomuuri. Tilallinen palomuuri pitää pakettien tilatiedoista kirjaa, jonka perusteella voidaan tunnistaa esimerkiksi, onko ulkoverkosta tuleva paketti vastaus sisäverkosta aloitettuun yhteyteen, vai ulkoverkosta tuleva uusi yhteysyritys.

Oletuksena palomuurille on määritelty säännöstö siten, että kaikki ulkoapäin saapuva liikenne palomuurin läpi asiakkaan sisäverkkoon on kielletty (pl. tilalliset paluuyhteydet), ja kaikki liikenne sisäverkosta ulospäin sekä eri sisäverkkojen välillä on sallittu. Useimmissa tapauksissa ulkoverkosta sisäänpäin sallitaan ainoastaan muutama yksittäinen portti tai kohdeosoite. Yleisimpiä sallintakohteita ovat esimerkiksi

sisäverkosta löytyvät web-palvelut. Myös mahdollinen vierasverkko yleensä eristetään palomuurilla muista LAN-verkoista erillisillä kieltosäännöillä.

Asiakkaalla on mahdollisuus tilata kirjallisesti omia sääntöjä muurille, mutta TNNet ei ota vastuusta asiakkaan sääntömuutoksien turvallisuudesta. Kaikki muutospyynnöt on tehtävä sähköpostilla, ja niiden on tultava valtuutetulta henkilöltä. Jos pyyntö tulee henkilöltä, jolla ei ole oikeutta pyytää muutoksia, viesti välitetään valtuutetulle henkilölle luvan saamista varten.

Kaikki palomuurille tulevat yhteydet ja palvelut ovat täysin eristettävissä toisistaan. Verkon kompleksisuus ja segmentointi ovat täysin asiakkaan omasta toiveesta riippuvaisia. Olemme kuitenkin valmiita konsultoimaan asiakasta palomuurisäännöstöjen luomisessa.

Oletuksena palomuuripalveluun allokoidaan aina yksi kiinteä IP-osoite, joka annetaan palomuurille. Palomuuripalveluun liitettävät toimipisteet ja palvelimet käyttävät lähtökohtaisesti aina TNNetin määrittämiä sisäverkon osoitteita. Jos asiakkaan toimipisteeseen tai laitteeseen halutaan osoittaa julkisella IP-osoitteella, niin tämä toteutetaan NAT-säännöllä käyttäen palomuurin julkista IP-osoitetta tai palvelulle allokoitua omaa IP-osoitetta. Mikäli tarvitaan toimipiste- tai palvelukohtaisia julkisia IP-osoitteita, niin ne allokoidaan sovitun hinnaston ja tarpeen mukaisesti. Julkisia IP-osoitteita ei kuitenkaan allokoida ilman perusteltua tarvetta.

IPv6-osoitteita allokoidaan käyttöön ilman lisäveloitusta perustellun tarpeen mukaan. Palvelussa voidaan käyttää IPv4- ja IPv6-osoitteita rinnakkain. Asiakkaan omien IP-osoitteiden käyttö on myös mahdollista, jos asiakkaalla on oma IP-allokaatio alueelliselta IP-rekisteriylläpitäjältä. (RIPE NCC, ARIN, APNIC, LACNIC, AfriNIC)

Lisäominaisuudet

pfSensen monimuotoiset laajennukset ovat asiakkaan käytössä, mutta jokaisesta laajennuksesta on sovittava projektiluontoisesti TNNetin kanssa. Laajennukset mahdollistavat mm. kuormantasauksen, tunkeutumisen havaitsemisjärjestelmän ja dynaamisen reitityksen ynnä paljon muuta. Laajennuksia käyttöönotettaessa on huomioitava palomuuripalvelun suorituskyky. Mikäli asiantuntijamme arvioivat, että palomuuripalvelun olemassa oleva suorituskyky ei riitä, konsultoimme asiakasta ennen lisäpalvelun toteuttamista. Lisäominaisuudet ovat maksuttomia, mutta vaativat tietyn määrän palomuurikapasiteettia, joka itsessään nostaa muurin kokonaishintaa. Lisäominaisuuksien viemät lisäresurssit ovat listattu palvelukuvauksen lopussa lisäominaisuuskohtaisesti.

SD-WAN-toimipiste

pfSense-palomuuripalveluun voidaan liittää lisäpalveluna SD-WAN. Palvelussa yrityksen sisäverkkoon liitetään kiinteästi toinen toimipiste tietoturvallisesti (VPN) hyödyntämällä käytettävissä olevia internetyhteyksiä. Palvelu vaatii toimiakseen riittävän nopean ja laadukkaan internetyhteyden. Yhteys voi kuitenkin olla joko perinteinen lankayhteys tai mobiiliyhteys (4G). TNNet ei ota vastuuta palvelun toimivuudesta, mikäli epäkäytettävyys johtuu kolmannen osapuolen yhteyksistä.

SD-WAN palvelussa toimitamme soveltuvan päätelaitteen, joka tulee liittää paikalliseen yhteyteen. Päätelaitteen maksimiläpäisykyky on noin 100mbps/100mbps. Päätelaite huolehtii yhteyden muodostamisesta ja salauksesta. Palvelu ei vaadi kiinteää IP-osoitetta, mutta se on silti suositeltava, sillä se nopeuttaa mahdollisten ongelmatilanteiden ratkaisua huomattavasti.

Mikäli käytössä on mobiiliyhteydet, tulee operaattoreiden kanssa huomioida seuraavat erityisehdot:

Elisa: Poikkeuksellisesti vaatii julkisen IP-osoitteen päällä olon. Tämä pitää asiakkaan pyytää Elisan asiakaspalvelusta tai laittaa itse päälle heidän portaalistaan.

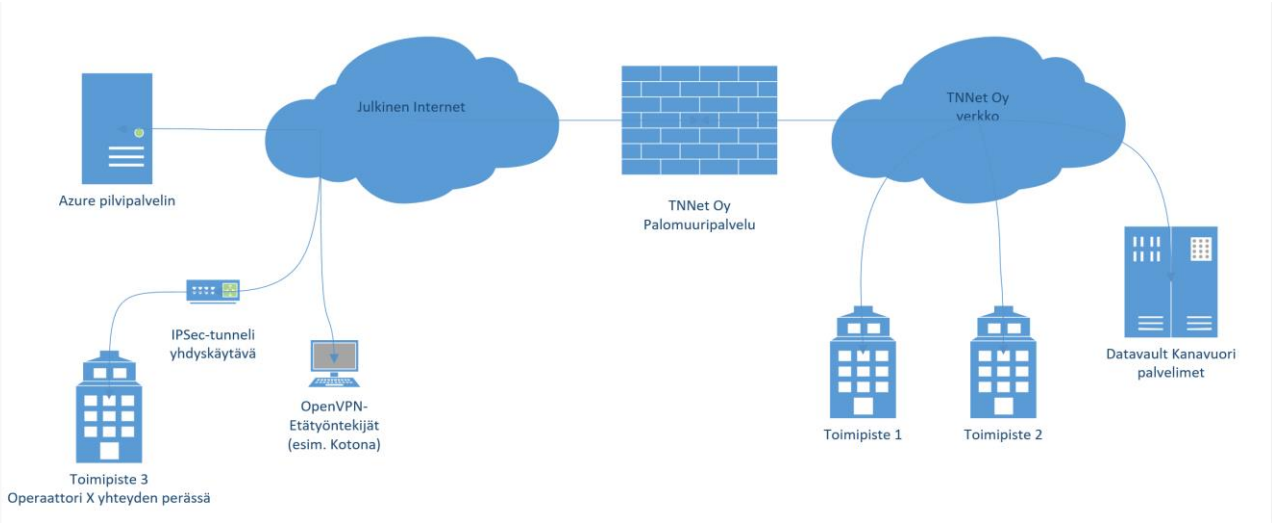
DNA: Ei erityisvaateita, eli mikä vain SIM käy.

Telia: Vaatii Opengate-lisäpalvelun. Asiakkaan on tilattava tämä Telian asiakaspalvelusta tai itsepalveluportaalista.

IPSec

IPsec mahdollistaa kiinteät VPN-yhteydet toimistojen välille tilanteessa, jossa toimipisteissä on eri palveluntarjoajien tietoliikenneyhteydet ja palomuuripalvelut. IPSec siis tavallaan yhdistää eri palomuurit toisiinsa. Konsultoimme asiakasta tai asiakkaan muita IT-kumppaneita IPSec-yhteyden käyttöönotossa tarvittaessa. IPSec vaatii aina olemassa olevan toisen palveluntarjoajan palomuuripalvelun yhdistettävässä toimipisteessä.

IPSeciä voidaan käyttää myös suurten, tunnettujen pilvipalvelutarjoajien palveluiden yhdistämiseen asiakkaan yritysverkkoon. Näitä ovat esimerkiksi Amazon ja Azure. Tarkista aina kolmannen osapuolen mahdollisuus IPSec tunnelointiin tai kysy TNNetin asiantuntijoilta.



Kuva 1 Esimerkki VPN- ja IPSec-tekniikoita hyödyntävästä yritysverkosta.

OpenVPN

OpenVPN on yksittäisten laitteiden tietoturvaratkaisu. Laitekohtaiselle VPN-yhteydelle on käytännössä kaksi käyttökohdetta: Verkkoliikenteen salaus siten, että liikennettä ei voida kaapata esimerkiksi julkisissa langattomissa verkoissa ja etätyöskentelyn mahdollistaminen siten, että VPN-yhteyttä käyttävä laite pääsee yrityksen sisäverkon palveluihin kiinni. VPN-yhteydelle voidaan luoda omat muurisäännöt, jolloin VPN-yhteyksille voidaan määritellä tarkasti, mihin verkkoihin etätyöntekijät voivat päästä. OpenVPN:lle on olemassa ilmaiset sovellukset mm. Windows-, Mac- ja Linux-koneille, sekä Android- ja IPhone-puhelimille.

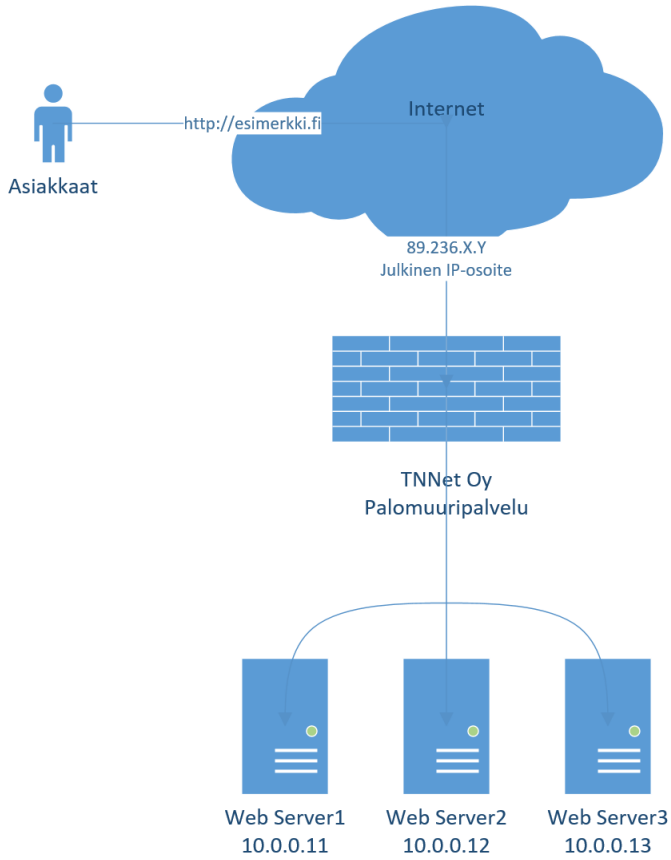
AD-kirjautuminen

Tyypillisesti palomuuripalveluun kirjautuessa käytetään palomuurin omaa, lokaalia käyttäjätietokantaa. Palomuurille kirjaudutaan esimerkiksi OpenVPN-yhteyksiä käytettäessä. Palomuuripalvelu on kuitenkin mahdollista liittää suoraan osaksi asiakkaan olemassa olevaa AD-ympäristöä siten, että VPN-käyttäjien ei

tarvitse muistaa useita tunnuksia, vaan he pääsevät kirjautumaan omilla Windows AD -tunnuksillaan. Samaan tapaan palomuuripalvelu voidaan liittää asiakkaan omaan Radius-ympäristöön.

Kuormantasaus

Palomuuripalvelu voi toimia myös kuormantasaajana sisäverkon palveluille. Kuormantasaus tukee hyvin esimerkiksi web-palvelimia, jotka sijaitsevat palveluntarjoajan virtuaalipalvelinalustalla. Palomuurin kuormantasaus tukee useita eri tekniikoita, joista yleisimmät ovat perinteinen aktiivinen/epäaktiivinen laitepari ja skaalautuvampi DNS round-robin. Palomuuripalvelun kuormantasaaja tekee myös tarvittavat health-checkit sille määritellyille laitteille, jotta yhden laitteen vikaantuessa kuormantasausta ei jatketa vikaantuneille laitteille.



Kuva 2 Verkkokuva tyypillisestä kuormantasauksesta.

Kahdennettu palomuuri

pfSense-palomuuripalvelu on kahdennettavissa siten, että mahdollisen vikatilanteen sattuessa liikenne ohjataan toisen täysin vastaavan palomuurin kautta. Kahdennetussa palomuuriratkaisussa on sekä Primary- että Secondary-rooleissa toimivat muurit. Muurit tietävät toistensa tilan VRRP-protokollaa hyödyntämällä. Muurien tilataulut ja konfiguraatiot taas kopioituvat reaaliajassa CARP-protokollaa käyttäen. Näin asiakkaan tietoliikenneyhteydet eivät katkea, vaikka toinen muureista vikaantuisi tai muurille tehtäisiin muutostöitä.

Tietoturva

TNNet takaa palvelun tietoturvallisuuden koko palvelun elinkaaren ajan. Virtuaalipalomuurit ovat jaetulla virtuaalialustalla eriytettynä täysin toisista virtuaalimuureista KVM-hypervisoria käyttäen. Liikenne muurille kuljetetaan täysin asiakas- ja lisäpalvelukohtaisilla VLANeilla siten, että liikenne ei vuoda sille tarkoittamattomaan paikkaan.

Palveluiden tunnuksiin ja muihin pääsyihin noudatetaan niin sanottua ”need-to-know” -periaatetta. TNNetin henkilökunnasta pääsy palomuureille on vain ylläpitohenkilöillä, jotka ovat koulutettu ylläpitämään kyseisiä järjestelmiä. Näistä henkilöistä pidetään myös säännönmukaisia katselmuksia ja palveluiden käyttöoikeudet tarkistetaan säännönmukaisesti. Virtualisointialustat sijaitsevat Datavault Kanavuoressa palveluntarjoajan omassa kaapissa. Laitetilaan sekä laitekaapille on tarkka kulunvalvonta, ja laitteille pääsevät myös fyysisesti käsiksi ainoastaan koulutetut TNNetin työntekijät. Ulkopuolisilla henkilöillä ei ole pääsyä palvelussa käytettäville komponenteille.

TNNetillä on pitkään kehitetty ja käytössä ollut ITIL-prosessi palomuuriin liittyviin muutos- ja palvelupyyntöihin siten, että ainoastaan oikeutetut henkilöt asiakkaalta voi pyytää muutoksia. Jos pyyntö tulee joltakin muulta, esimerkiksi uudelta työntekijältä tai IT-kumppanilta, kysymme aina luvan pyynnön suorittamiselle TNNetillä dokumentoidulta henkilöltä.

Lähetämme kaikki palveluun liittyvät tunnukset asiakkaalle asiakkaan haluamalla tavalla tarvittaessa salattuna. Lähetämme tunnukset oletusarvoisesti joko pelkällä sähköpostilla. Arkaluontoisempien tunnusten kohdalla käyttäjätunnus lähetetään sähköpostilla ja salasana esimerkiksi tekstiviestillä. Myös salatut sähköpostiviestit ovat mahdollisia.

Lisätietoja

Lue myös TNNet yleinen palvelukuvaus sekä SLA-palvelukuvaus.

pfSense palomuuripalvelu on liitettävissä laajalle kirjolle muita palveluita. Liitettävistä palveluista lisätietoa löytyy ainakin seuraavista palvelukuvauksista:

- Openstack virtuaalipalvelimet
- Tietoliikenne
- Yksityinen pilvi