PALVELUKUVAUS – SOPHOS (SD-WAN)

SISÄLLYS

Yleistä

Tämä palvelukuvaus olettaa, että SD-WAN-ympäristön keskusmuurit ovat sijoitettuna TNNetin laitesaliin Datavault Kanavuoreen. Jos keskusmuurit sijaitsevat jossain muualla, voidaan tätä palvelukuvausta soveltaa todellisen ympäristön mukaan. Tämä palvelukuvaus on tarkoitettu ainoastaan Sophoksen laitteilla toteutettuun SD-WAN-ratkaisuun. Mikäli käytössä on muita muurivalmistajia tai muita SD-WAN-ratkaisuja, niille on omat palvelukuvauksensa.

Sophos on englantilainen yksityisomisteinen tietoturvayritys. Sophoksen käyttämät pilvipalvelut ja toimintamallit ovat todettu tietoturvallisiksi TNNetin tietoturvaprosessien mukaisesti. Sophoksella on useita eri tietoturvasertifikaatteja, kuten muun muassa sama ISO27001 -sertifiointi kuin TNNetilläkin. Lisää Sophoksesta ja heidän tietoturvapolitiikoistaan voi lukea Sophoksen sivuilta: https://www.sophos.com/en-us/trust/privacy

Datan sijainti

Palomuuri ja SD-WAN-verkko käyttävät hyödykseen Sophoksen omaa pilvialustaa, jota toteutetaan AWS:n kapasiteetista. Pilvialustan fyysinen lokaatio voidaan kuitenkin valita vapaasti, ja ellei toisin sovita, sijainniksi valitaan aina Saksa. Tarkat tiedot pilveen kerätystä datasta voi tarkastella Sophoksen omilta sivuilta, https://www.sophos.com/en-us/legal/sophos-firewall

Asiakasliikenne ei kierrä Sophoksen pilven kautta, vaan kaikki liikenne kulkee aidosti ainoastaan palomuurin läpi. Liikenteen todellinen reitti riippuu luonnollisesti käytetyistä tietoliikenneoperaattoreista, joihin TNNet ei voi vaikuttaa.

Fyysinen turvallisuus

Keskusmuurit ovat sijoitettuna Datavault Kanavuoreen, joka itsessään on hyvin tietoturvallinen ja korkean saavutettavuuden laitesali. Datavault Kanavuoresta voi lukea lisää omasta palvelukuvauksestaan. Laitesalissa palomuurien redundanttisuudesta on pidetty erityistä huolta. Kaikki tietoliikennelaitteet ja yhteydet ovat vähintään kahdennettuja koko matkalta, palomuurin portista internettiin reitittävälle laitteelle asti.

Palomuurit toteutetaan oletusarvoisesti kahdennettuna siten, että yhden fyysisen laitteen hajoaminen ei aiheuta tietoliikennekatkosta. Lisäksi yksittäisessä palomuurissakin on kaksi redundanttista virtalähdettä, joten virran menetys yhdeltä kiskolta ei aiheuta katkosta muuriklusterin kumpaankaan laitteeseen. Virtualisoidut keskusmuurit eivät ole kahdennettuja, mutta ne on toteutettu vikasietoisella alustaraudalla.

Hätätilanteita varten muurit ovat kytketty konsoliserveriin, jolla mahdollisestaan TNNetin ylläpitäjille pääsy palomuurien konsoliin, vaikka palomuurit putoaisivat kokonaan verkosta.

Varmuuskopiointi

Palomuurien konfiguraatio varmuuskopioidaan kerran viikossa Sophoksen omaan pilvijärjestelmään. Backup on kuitenkin salasanasuojattu, eli se ei ole luettavissa, jos salasanaa ei ole tiedossa. Tarvittaessa backup voidaan disabloida pilveen, ja laittaa se sähköpostilla haluttuun sähköpostiosoitteeseen. Tällöin asiakas vastaa sähköpostiin tulevien backupien säilytyksestä.

Lisenssit

Sophoksen palomuureja on saatavilla kolmella eri lisenssitasolla: Standard, Xstream ja Xstream + WAF. Palomuurissa on vakiona Standard protection -lisenssi, mutta erikseen sovittuna voidaan käyttää myös korkeampaa lisenssitasoa. Lisenssitaso katsotaan aina asiakkaan kanssa yhdessä, jolloin saadaan haluttuihin ominaisuuksiin nähden paras kokonaisratkaisu. Jos palomuurin haluaa liittää SOC-palvelun piiriin, tulee palomuurilla olla vähintään Xstream lisenssi.

Mikäli muurilla ei ole lainkaan lisenssiä, sen ominaisuudet ovat huomattavan rajatut, eikä tietoturvapäivityksiä voida asentaa. TNNet huolehtii siitä, että muurilla on oikea lisenssi ja lisenssit ovat voimassa.

Lisenssien tarkemmat ja ajantasaiset ominaisuudet ovat luettavissa Sophoksen omilta sivuilta.

Laitteiston päivitys

TNNet huolehtii siitä, että laitteilla on aina ajantasaiset tietoturvapäivitykset haavoittuvuuksien ilmenemisen varalta. Useimmat tietoturvapäivitykset saadaan toteutettua ns. hotfixeinä, jotka eivät aiheuta käyttökatkosta laitteissa. Softaversiot päivitetään tarpeen mukaan, kun ne on todettu omissa labralaitteissa toimiviksi versioiksi. Laitteistoa ei päivitetä jokaiseen softaversioon, jos versiossa ei tule merkittäviä parannuksia tai korjauksia käytössä oleviin komponentteihin. Laitteiston päivitykset kuuluvat palvelun hintaan palomuurin SLA-tason mukaisesti, eikä niistä veloiteta erikseen. Jos päivitykset tehdään SLA-sopimuksen ulkopuolisilla ajoilla, sovitaan työkustannuksista erikseen.

Kahdennetut keskusmuurit voidaan päivittää lähes katkoitta, mutta lyhyitä katkoksia voi esiintyä. Päivitykset voidaan kuitenkin suorittaa virka-ajan ulkopuolella erikseen sovittuna ajankohtana. Jos päivitettävä muuri ei ole kahdennettu, tulee päivityksestä käyttökatkos muurin uudelleenkäynnistyksen ajaksi.

SD-RED laitteiden päivitykset vaativat tyypillisesti laitteille uudelleenkäynnistyksen, joka luonnollisesti myös aiheuttaa toimipistekohtaisen katkoksen päivityksen ajaksi. Kaikki SD-RED-laitteet on päivitettävä samanaikaisesti, jotta kaikilla laitteilla on aina sama softaversio. Keskusmuurit ja SD-RED-laitteet voidaan kuitenkin päivittää eri aikaan.

Palvelun sisältö

SD-WAN yleiskuvaus

SD-WAN verkko toteutetaan tyypillisimmin siten, että kaikki liikenne tunneloidaan keskusmuurin kautta. Näin liikennettä voidaan suodattaa ja palomuurin edistyneitä NGFW-ominaisuuksia voidaan hyödyntää kaikkeen liikenteeseen. SD-WAN-topologioita ja erilaisia yhdistelmiä ratkaisuista voi olla lähes yhtä monta, kuin on SD-WANin käyttäjiäkin. Tämä palvelukuvaus kuitenkin keskittyy TNNetin kokemuksen mukaan asiakkaiden käytetyimpään toplogiaan (hub and spoke).

SD-WAN liikenne tunneloidaan Sophoksen omaa RED (Remote Ethernet Device) -protokollaa hyödyntäen. Käytännössä RED on VPN-liikennettä AES256 salauksella. Protokolla kuitenkin poikkeaa tyypillisistä VPN- ja IPSec-ratkaisuista siten, että se on palomuurin näkökulmasta L2-liikennettä, eli tunnelin yli voidaan ajaa myös VLAN-liikennettä.

SD-WAN-toimipisteellä voi olla mikä internetyhteys tahansa. Yhteys voi olla niin kiinteästä kuin mobiiliverkostakin. Vaikka pakottavia vaatimuksia ei ole, parhaan lopputuloksen saa, kun SD-WAN-laite on

suoraan internetissä (eli ei NATaavan tai palomuuraavan laitteen takana), ja se saa tarvittavat verkkomääreet DHCP:lta. Jos IP-osoitteet eivät tule DHCP:lta, tulee kiinteät osoitukset määrittää ennen laitteen lähettämistä asiakkaalle. Jos laite on palomuurin takana, tulee RED-laitteelle sallia molempiin suuntiin TCP/UDP 3400 ja 3410.

SD-RED-laitteet

SD-RED laitteita on kahta mallia, SD-RED 20 ja SD-RED 60. SD-RED 20 on tarkoitettu hyvin pieniin ja yksinkertaistettuihin sisäverkkoihin tai yksittäisen käyttäjän etätyöpisteelle. SD-RED 60 taas voi toimia isonkin verkon päätelaitteena.

SD-RED-laitteet voivat soittaa vain tunnelin yhdelle muurille kerrallaan. RED-laitteet eivät siis juttele suoraan keskenään, eli niillä ei saa tehtyä full-mesh verkkoa, vaan kyseessä on hub- and spoke-topologia. Yleisimmässä topologiassa SD-RED-laitteet soittavat aina keskusmuureille, jotka reitittävät liikenteen eteenpäin. On myös mahdollista asettaa SD-RED-laite tunneloimaan ainoastaan haluttu sisäverkon liikenne, jolloin laite suorittaa NAT:n internetiin lähtevälle liikenteelle. Split tunneling -asennossa laite sallii aina kaiken liikenteen internetiin, eikä päästä mitään internetistä sisäänpäin. SD-RED-laitteella ei voi myöskään käyttää edistyneitä muurin ominaisuuksia, kuten IPS tai Heartbeat, internetliikenteelle. Jos halutaan toteuttaa kuvattua split tunnelingia, suositellaan valitsemaan toimipisteen laitteeksi aito palomuurilaite (XGS 1xx).

SD-RED-laite ei tee liikenteen suodatusta, eikä sillä ole juuri mitään palomuurin ominaisuuksia. Esimerkiksi palomuurisäännöt ja DHCP määritellään keskusmuurilla, ei SD-RED-laitteella itsellään. SD-RED-laitteen ainoa tehtävä on muodostaa sille määritelty tunneli keskusmuurin kanssa. Jos SD-RED-laite ei saa vastausta sille määrätyltä keskusmuurilta, laite yrittää tavoittaa Sophoksen pilven selvittääkseen, onko laitteen konfiguraatio mahdollisesti muuttunut. Jos konfiguraatio ei ole muuttunut, tai laite ei saa yhteyttä pilveen, laite käynnistää itsensä ja lähtee yrittämään yhteyttä keskusmuurille uudestaan toistaen tätä toimintamallia, kunnes yhteys muodostuu.

Alla listattuna tärkeimmät ominaisuudet SD-RED-laitteiden välillä. Jos ominaisuudet eivät ole riittävät, voidaan SD-RED-laite korvata palomuurilaitteella (*kts. seuraava kappale*).

Ominaisuus	**SD-RED 20**	**SD-RED 60**
Maksiminopeus	250 Mbps	850 Mbps
LAN Portit	4 x 1000 Base-TX (1 GbE Copper)	4 1000 Base-TX (1 GbE Copper)
WAN Portit	1 x 10/100/1000 Base-TX (jaettu SFP portin kanssa)	2 x 10/100/1000 Base-TX (WAN1 jaettu SFP portin kanssa)
Kahdennettu internetyhteys	1 kiinteä WAN-yhteys ja 4G moduulilla	Kaksi kiinteää WAN-yhteyttä ja/tai 4G moduuli. WAN-yhteydet voivat toimia load-balancing moodissa.
VLAN tuki	Ei ole	Max 64 VLANia
PoE virransyöttö	Ei ole	2 PoE -porttia (yhteensä 30W)
4G TAI WiFi moduuli	Saatavilla lisäosana	Saatavilla lisäosana

Kahdennettu SD-RED-laite	Ei mahdollista	Ei mahdollista
Kahdennettu virransyöttö	Saatavilla lisäosana	Saatavilla lisäosana

Palomuuri SD-WAN-laitteena

Jos toimipisteellä on edistyneitä tarpeita liikenteen suodatukselle, voidaan RED-tunneli toteuttaa myös esimerkiksi Desktop-mallin täysverisellä palomuurilla (esim. XGS106 tai XGS 126). Tällaisessa ratkaisussa on mahdollista hyödyntää kaikkia mahdollisia palomuurin ominaisuuksia, lisenssitason mukaan, ja tunneloida haluttu liikenne keskusmuurille RED-protokollaa hyödyntäen. Myös virtuaalista palomuuria esimerkiksi Azuresta tai AWS:n pilvestä voidaan käyttää SD-WAN-päätteenä.

Palomuurit voivat soittaa useita tunneleita eri muureille, jolloin myös full-mesh-verkko on mahdollinen. Full-mesh-verkon toteutus voidaan tehdä keskitetyllä hallinnalla, joka poikkeuksellisesti vaatii jokaisella laitteelle vähintään Xstream tason -lisenssin. Ilman lisenssiä tulee tunnelimuutokset ja reititykset tehdä laite kerrallaan, joka isossa verkossa vie paljon aikaa ja on herkkä inhimillisille virheille.

TNNetin toimittama internetyhteys

TNNet toimii myös tietoliikenneoperaattorina, jolloin SD-WAN-toimipisteen tietoliikenteen voi tilata myös suoraan TNNetiltä. Mikäli kohteessa on TNNetin toimittama tietoliikenneyhteys, voidaan se tuoda TNNetin runkoverkossa suoraan L2-tasolla keskusmuureille. Jos yhteys voidaan tuoda suoraan L2-tasolla palomuurille, ei tarvita erillistä SD-WAN-laitetta ja tunnelointia.

TNNetin toimittama tietoliikenneyhteys voidaan kuitenkin kahdentaa hyödyntäen SD-WAN-laitteistoa. Tällaisessa tapauksessa tietoliikennettä ei tuoda ollenkaan L2-tasolla palomuureille, vaan kaikki liikenne tunneloidaan SD-WAN-laitteen muodostaman RED-tunnelin läpi. Vaihtoehtoinen tapa kahdentaa TNNetin toimittama internetyhteys on tilata tietoliikenne kahdennettuna, jolloin liittymä toimii edelleen L2-tasolla palomuurille asti. Jos varmentavaksi tietoliikenneyhteydeksi halutaan mobiiliyhteys, tulee toimipiste liittää aina SD-WAN-laitteella verkkoon.

Palomuuri

Liikenteen suodatus

Sophoksen palomuurit ovat Zone-pohjaisia palomuureja. Toisin sanoen monta interfacea (VLANia) voivat olla samassa Zonessa, jolloin yhdellä säännöllä voidaan tehdä montaa VLANia koskeva sääntö. Tyypillisiä zoneja voisivat olla esimerkiksi Sisäverkot, Vierasverkot, Internet ja VPN. Muurit ovat täysiverisiä NGFW-palomuureja, joilla on kattavasti eri ominaisuuksia liikenteen suodatukselle. Käytettävät ominaisuudet riippuvat aina palomuurin valitusta lisenssitasosta sekä palomuurin suorituskyvystä suodatettavaan liikenteeseen nähden. Standard-ominaisuuksiin kykenevällä muurilla ei aina voi käyttää kaikkia Xstream-ominaisuuksia samassa ympäristössä. Tarkat saatavilla olevat ominaisuudet ovat luettavissa valmistajan omilta sivuilta, kun taas suositelluista ominaisuuksista kannattaa kysyä TNNetin asiantuntijoilta.

Oletuksena palveluntarjoaja määrittelee säännöstön 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 tai VPN-, IPSec- ja RED-tunneleihin vaaditut portit. Myös mahdollinen vierasverkko yleensä eristetään palomuurilla muista LAN-verkoista erillisillä kieltosäännöillä.

Palomuureille tulee Sophoksen pilven kautta TNNetin luomat vakiopolitiikat, joita asiakas ei itsenäisesti voi muokata. Politiikoissa on TNNetin ylläpidon toimesta tehdyt turvalliset asetukset mm. IPS:n ja VPN:n oletusarvoihin. Jos muurille tehdään paikallisia muutoksia, jotka ovat ristiriidassa pilvestä tulevan politiikan kanssa, pilvi yliajaa muutokset säännöllisin väliajoin. Pilvestä tulevia politiikkoja voidaan kuitenkin muokata oletusarvoista asiakkaan haluamiksi. TNNetin tuottamassa oletuspolitiikassa tulee muun muassa seuraavat asetukset:

- Kaikki liikenne sallittu internetiin. Kaikki liikenne NATataan internetiin palomuurin oman julkisen IP:n taakse (muokattavissa).
- Kaikki liikenne estetty Internetistä sisäverkkoon (muokattavissa).
- TNNetin ylläpidolliset pääsyt ja tunnukset palomuurille.
- Palomuurikonfiguraation backup.
- Turvalliset (löyhät) IPS-asetukset. IPS päällä vakiona säännöissä.
- Tietoturvalliset VPN-asetukset käyttäjille.
- Ilmoitukset TNNetin ylläpidolle mahdollisista tietoturvapäivityksistä.
- Erikseen sovittaessa URL-filteröinti (suositellaan tehtävän päätelaitteella itsellään, ei palomuurilla).

Asiakkaalla on mahdollisuus tilata kirjallisesti omia sääntöjä muurille, mutta TNNet ei ota vastuusta asiakkaan sääntömuutoksien turvallisuudesta. Jos tilattu sääntö vaikuttaa tietoturvattomalta, kysymme asiakkaalta vielä varmistuksen erikseen. 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. Puhelimitse tulleita muutospyyntöjä ei toteuteta, vaan ne on aina laitettava puhelun jälkeen kirjallisesti. Puhelimessa voidaan kuitenkin konsultoida asiakasta, mitä viestiin pitää kirjoittaa.

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.

Keskusmuurien tietoliikenne ja IP-osoitteet

Oletuksena keskuspalomuureille allokoidaan aina yksi julkiverkko (/29 mask), josta yksi osoite menee verkon gatewaylle ja yksi palomuurin julkiseksi IP:ksi. Loppuja verkon osoitteita voidaan käyttää tarpeen mukaan, esimerkiksi palveluiden julkaisuun internetin suuntaan. Virtualisoidut keskusmuurit sisältävät ainoastaan yhden julkisen IP-osoitteen. Lisää IP-osoitteita on saatavilla erillisenä lisäpalveluna.

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)

Keskusmuurien palveluhintaan sisältyy symmetrinen 1Gbps tietoliikenneyhteys internetiin. Internet liityntää pitkin kulkee kaikki TNNetin toimittamien L2-yhteyksien ulkopuolinen liikenne, kuten esimerkiksi SD-WAN-liikenne, VPN-käyttäjät, IPSec-yhteydet ja liikenne internetiin. Palomuureilla on myös toinen symmetrinen 1Gbps LAN -kytkentä, jota pitkin TNNetin toimittamat L2 liittymät toimitetaan. Lisäpalveluna on saatavilla lisää 1Gbps tai 10Gbps tietoliikenneportteja tai yhteyksiä.

Tunnuspolitiikka

Palomuurin admin-tunnukset luovutetaan TNNetillä vain henkilöille, joilla on vähintään Sophoksen Engineer -tason sertifikaatti palomuureista. Muulla TNNetin henkilöstöllä ei ole tunnuksia palomuureille. Tunnuksien salasanat vaihdetaan säännöllisesti TNNetin salasanapolitiikan mukaisesti.

Asiakkaalle on mahdollista luovuttaa omat tunnukset palomuurille. Tunnukset voivat olla joko ReadOnly, rajatut adminit tai täydet adminit. TNNet ei kuitenkaan vastaa asiakkaan tekemistä muutoksista palomuureilla.

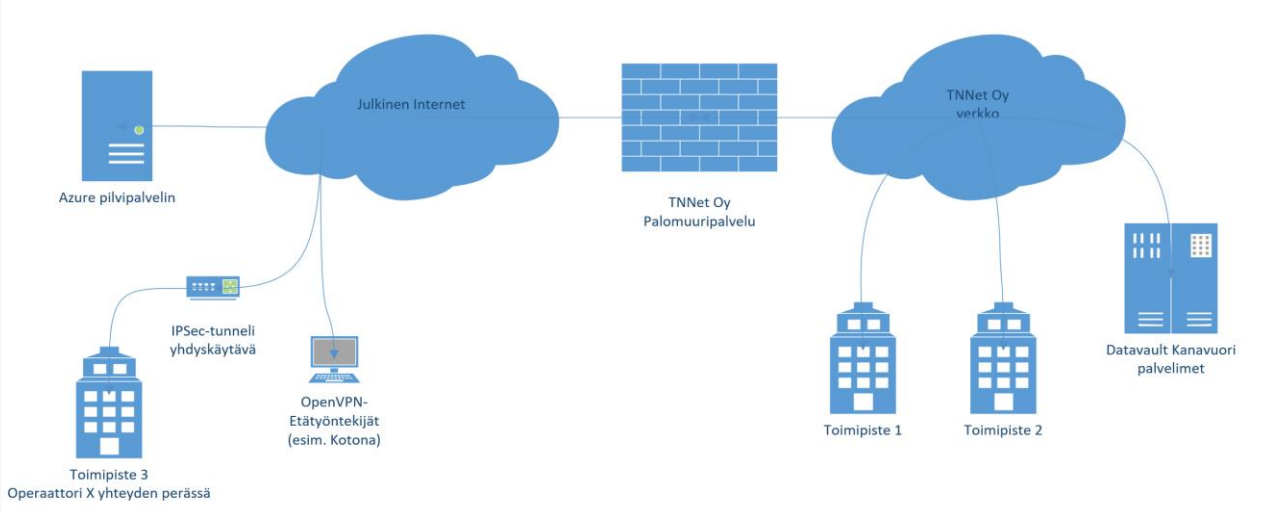
Yleisimmät lisäominaisuudet

Sophoksen muurilaitteissa on kattava valikoima eri lisäominaisuuksia, joista ajankohtaiset ja tarkat tiedot löytyvät aina laitevalmistajan sivuilta. Alla on listattu TNNetin kokemuksen mukaan yleisimpiä lisäominaisuuksia, sekä kuvaus niiden käyttötarpeista. Suurin osa lisäominaisuuksista toimii jo Standard lisenssillä, mutta eivät sisälly TNNetin tekemään peruskonfiguraatioon, vaan on erikseen tilattavia lisätöitä. Jos lisenssikuluja ei tule ominaisuuden käyttöönotosta, ei lisäominaisuudet aiheuta kertaluontoista työkustannusta lukuun ottamatta muita lisäkuluja.

IPSec

IPsec mahdollistaa kiinteät VPN-yhteydet toimistojen välille, jos toimipisteissä on eri palveluntarjoajien tietoliikenneyhteydet ja palomuuripalvelut. IPSec siis tavallaan yhdistää eri palomuurit toisiinsa. Palveluntarjoaja konsultoi 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 yritsverkkoon. Näitä ovat esimerkiksi Amazon AWS ja Azure (Entra). Tarkista aina kolmannen osapuolen mahdollisuus IPSec-tunnelointiin tai kysy palveluntarjoajan asiantuntijoilta.



Kuva 1 Esimerkki VPN ja IPSec tekniikoita hyödyntävästä yritysverkosta.

Käyttäjän VPN-yhteys (OpenVPN)

OpenVPN on yksittäisten laitteiden etätyöratkaisu. 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.

VPN yhteys on käyttäjäkohtainen. Jokainen käyttäjä voi itse ladata konfiguraationsa TNNetin toimittamilla tunnuksilla ja samassa yhteydessä vaihtaa oman salasanansa. Oletuksena portaali, josta VPN-konfiguraatiot voi ladata, on auki ainoastaan sisäverkoista. Joissakin tapauksissa käyttäjien ei ole mahdollista ladata tiedostoja sisäverkosta, jolloin käyttäjäportaali voidaan avata internetistä joko väliaikaisesti tai erikseen sovittuna pidemmäksi aikaa.

Captive Portal

Captive Portal on nettisivu, joka esitetään käyttäjälle hänen kirjautuessa verkkoon. Captive Portalia voidaan käyttää esimerkiksi asiakkaan langattoman vierasverkon tervetuloa-viestinä, autentikaatiokanavana tai tärkeiden tiedotteiden välittämisen kanavana. Captive Portal tavoittaa kaikki käyttäjät, jotka kirjautuvat määriteltyyn verkkoon. Jokaiselle palomuurin eri verkolle voidaan määritellä oma Captive Portal.

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, tai Azure AD:n, jos Azureen on konfiguroitu nk. Legacy AD -ominaisuus.

Palvelukohtaiset muurisäännöt

Palvelukohtaiset muurisäännöt mahdollistavat tavanomaisten IP-osoitteiden ja porttinumeroiden perusteella tehtävien sääntöjen lisäksi myös erilaisten palveluiden, kuten Facebook, Whatsapp ja Spotify, tunnistamisen. Palvelukohtaisilla muurisäännöillä voidaan siis joko estää kokonaan, tai jopa priorisoida tiettyihin palveluihin kohdistuvaa liikennettä muuhun liikenteeseen verrattuna. Palvelukohtaisia muurisääntöjä käyttöönottaessa tulee varmistaa palveluntarjoajan asiantuntijoilta halutun palvelun saatavuus, sillä kaikkiin palveluihin ei ole vielä olemassa palvelukohtaisia muurisääntöjä.

Palvelukohtaisesti voidaan myös suorittaa liikenteen reititystä. Esimerkkitilanteessa toimipisteellä voi olla kaksi internetyhteyttä; kiinteä kuituyhteys ja mobiiliyhteys. SD-WAN reitityksellä voidaan tehdä määritys, että työhön liittyvät tärkeät sovellukset menevät aina kuitua pitkin, kun taas viihdekäyttö (Youtube, Facebook) menee mobiiliyhteyttä pitkin.

URL-suodatus

Palomuurilla on mahdollista “kaapata” web-liikenteen URL-osoitteet ja suodattaa niitä osoitteiden perusteella. Näin paketista ei pureta kaikkea dataa, esimerkiksi mahdollista salasanasisältöä, vaan ainoastaan suodatukseen tarvittava nettiosoitteen nimi. URL-suodatuksella on mahdollista estää liikenne ennalta määriteltyihin selainosoitteisiin, kuten esimerkiksi youtube.com tai facebook.com.

Salauksen purku

Lähes kaikki TCP-liikenne on nykyään salattua, joten palomuurin suojausominaisuudet, kuten IPS, ei voi havainnoida uhkia liikenteestä, ellei salauksen purku ole päällä. Salauksen purku vaatii Xstream lisenssin ja huomattavan määrän laskentatehoa palomuurilta, joten tämä kannattaa huomioida jo palvelua tilattaessa.

Salauksen purussa palomuuri purkaa liikenteen salauksen, tutkii sisällön, ja lisää oman salauksen takaisin päälle. Näin liikenne kulkee palomuurin ulkopuolella kokoajan salattuna. Osa sovelluksista ei toimi, jos salauksen purkua tehdään, ja sellaiset sovellukset voidaan erikseen määrittää salauksen purun ulkopuolelle. Palomuuri myös tunnistaa muut hyvin arkaluontoiset sovellukset, kuten esimerkiksi pankkiliikenteen, jonka salausta ei pureta.

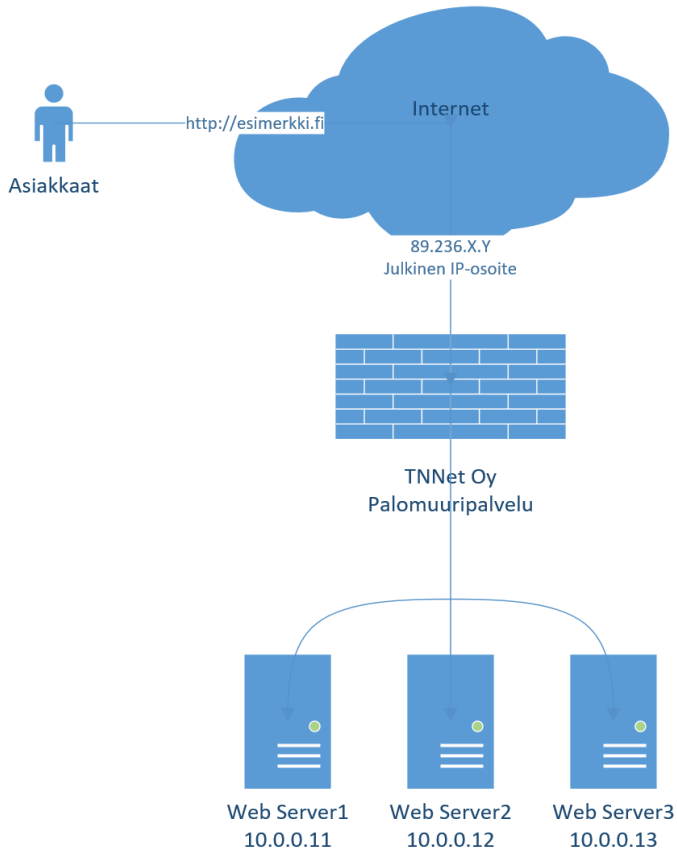
WAF (Web Application Firewall)

WAF on Xstream + WAF lisenssin mukana tuleva lisätuote. WAF tarkoittaa selainliikenteelle edistynyttä palomuuria, jossa käyttäjien lähettämistä HTTP-metodeista voidaan tulkita haitallisia pyyntöjä. Haitallinen pyyntö voisi olla esimerkiksi SQL-injektioyritys, jonka muuri osaa tunnistaa ja blokata, ennen kuin pyyntö menee sovelluspalvelimelle asti.

WAF:lla voidaan myös tarkkaan määritellä, mitä pyyntöjä tietylle verkkosivulle voidaan lähettää. On mahdollista esimerkiksi estää kaikki HTTP POST metodit ja sallia ainoastaan HTTP GET liikenne.

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. Kuormantasaus on tehtävissä Standard lisenssillä.



Kuva 2 Verkkokuva tyypillisestä kuormantasauksesta.

MFA

Palomuurin tunnuksille on mahdollista pakottaa MFA päälle. Palomuurilla generoidaan OTP-koodi, joka luetaan puhelimeen jollakin autentikaattorisovelluksella (esim Google Authenticator). Jos MFA-ominaisuus on asetettu päälle, tulee jokaisen käyttäjän aina syöttää autentikaattorin tarjoama numerosarja oman salasanansa perään, jotta kirjautuminen onnistuu.

Heartbeat, ”liikennevalot”

Jos palomuurin takana on laitteita, joilla on myös Sophoksen XDR-ratkaisut käytössä, voidaan päätelaitteen tietoturvan tasoa käyttää hyväksi palomuurisäännöissä. Voidaan tehdä sääntö, joka esimerkiksi sallii liikenteen palvelimille ainoastaan, mikäli XDR-tuotteen mukaan laitteella ei ole mitään epäilyttävää. Jos laitteella on haittatiedosto edes karanteenissa, tai XDR-tuotetta ei ole ollenkaan, liikenne estetään.

Samaa heartbeatiä hyödyntäen muuri osaa viestiä muille XDR-tuotteen omaaville laitteille, jos jokin laite verkossa saastuu. Näin saastunut laite saadaan eristettyä täysin muista verkon laitteista, eikä haittaohjelma pääse leviämään edes sisäverkossa.

Lisätietoja

Tämä palvelukuvaus pohjautuu TNNetin yleiseen palvelukuvaukseen. Lue myös TNNet yleinen palvelukuvaus.

Lisäpalveluista löytyy lisätietoja ainakin seuraavista palvelukuvauksista:

- SLA
- Tietoliikenne
- Sisäverkon palvelut
- Tietoturvapalvelut
- Datavault Kanavuori