Patrik Santasalo

Hallinta- ja valvontaverkon suunnittelu ja toteutus

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja viestintäteknologia

Insinöörityö

23.3.2022

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Patrik Santasalo Hallinta- ja valvontaverkon suunnittelu ja toteutus 20 sivua 23.3.2022
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tieto- ja viestintäteknologia
Suuntautumisvaihtoehto	Tietoliikenne ja tietoturva
Ohjaaja	Service Transition Team Leader Jyri Lappalainen

Opinnäytetyössä sovelletaan verkkoarkkitehtuurin määrityksiä ja luodaan uuteen palvelutuotantojärjestelmään hallinta- ja valvontaverkko olemassa oleville verkkolaitepalveluasiakkaille. Opinnäytetyö tehdään työnantajani käyttöön, joten tietyt tunnistetiedot on piiloitettu. Työnantajani käyttöön olen tehnyt vielä yksityiskohtaisemman ohjeen.

Avainsanat	

Author(s) Title Number of Pages Date	Patrik Santasalo Planning and implementation of new management network 20 pages 23 March 2022
Degree	Bachelor of Engineering
Degree Programme	Information and Computing Technology
Specialisation option	Networking
Instructor	Jyri Lappalainen Service Transition Team Leader

Goal for this Theses was to plan and implement new management network for my employer's new service platform. This management network is only for network service customers. This theses is only for my employer's use and more detailed instructions has been left for internal use only.

Keywords	

Sisällys

Lyhenteet

VLAN	Virtuaalinen lähiverkko. Mahdollistaa useamman verkon toimivuuden samassa fyysisessä portissa
IPAM	IP Address Management. IP osoitteiden hallintaan ja ylläpitoon käytetty ohjelmisto.
MPLS	Multiprotocol Label Switching. Menetelmä jolla kuljetetaan IP-paketteja ennalta määriteltyjen yhteyksien ylitse ilman että tarvitsee tehdä reititystä.
DWDM	Dense Wavelength-Division Multiplexing. Kuituoptiikan teknologia joka mahdollistaa usean data signaalin lähetyksen yhdessä optisessa kuitukaapelissa samalla pitäen data virrat erillään.

1 Johdanto

Opinnäytetyössä suunnitellaan ja toteutetaan työnantajani uuteen palvelutuotantojärjestelmään hallinta- ja valvontayhteys verkkolaitepalveluasiakkaille. Opinnäytetyössä luodaan toimintaohjeet standartoidun mallin toteutukseen sekä luodaan itse hallinta- ja valvontayhteys testiasiakkaalle. Testiasiakkaan avulla testataan asiakasmigraatioprosessia ennen kuin verkkolaitepalveluasiakas siirretään uuden palvelutuotannon piiriin. Jotta asiakkaille pystytään tuottamaan palvelua, tarvitaan myös hallinta- ja valvontakomponentteja. Näiden komponenttien asennukseen ja käyttöönottoon ei tässä opinnäytetyössä oteta kantaa. Itse verkkoyhteyden suunnittellussa ja toteutuksessa hyödynnetään työnantajan arkkitehtien määrittelemiä reunaehtoja.

2 Verkkoyhteyden suunnittelu

Verkkoyhteyden suunnittelussa tulee ottaa huomioon asiakkaalle tarjottava palvelu sekä asiakkaan sopimuksissa määräämät ehdot. Myös asiakkaan kanssa tulee keskustella verkkosegmenttien valinnoista, jotta vältetään päällekkäisten osoitteiden varmaamiselta sekä mahdollisilta reititys ongelmilta. Tietoliikenneyhteys asiakkaan ja konesalin välillä voidaan toteuttaa eri operaattorien MPLS yhteyksillä, DWDM tai IPSec VPN over internet ratkaisulla.

2.1 Hallintayhteys toteutustavan valinta

Hallintayhteyden toteutustapa riippuu asiakkaan verkkolaitemäärästä sekä palvelusopimuksesta. Asiakkaan palvelusopimuksessa voi olla vaatimuksena tiettyjä ehtoja, jotka estävät tavanomaisen hallinta- ja valvontayhteyden toteutuksen. Näitä ehtoja voivat olla mm. tietoturva vaatimukset. Näitä poikkeuksia varten työnantajani arkkitehdit ovat määrittäneet muutamia erinlaisia toteutustapoja. Verkkolaitemäärä vaikuttaa myös toteutustavan valintaan rahallisessa näkökulmassa. Toteutustavasta riippumatta, kaikki hallintayhteydet terminoidaan työnantajani konesaliin.

Hallintayhteys muodostetaan palomuurien välille. Toinen palomuuri sijaitsee työnantajani konesalissa ja toinen joko asiakkaan oma tai sitten asiakkaan laitetilaan toimitetaan uusi palomuuri pelkästään haliintayhteyttä varten.

2.2 Verkkojen suunnittelu

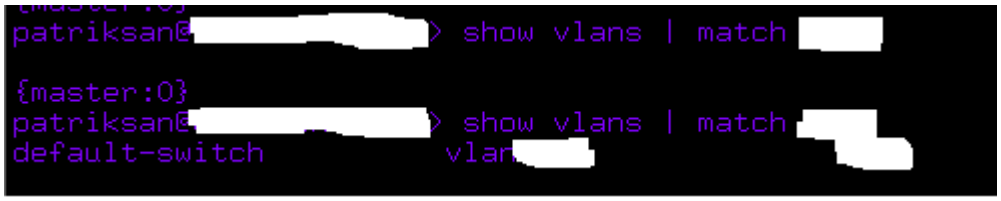
Hallinta- ja valvontayhteyksiä varten tulee jokaista asiakkuutta kohtaan luoda kaksi erillistä verkkoa. Nämä verkot nimetään ’XXXXXX1-transit’ ja ’XXXXXX2-transit’. XXXXXX1 verkkoon asennetaan hallintaa ja valvontaa tuottavat komponentit kun taas XXXXXX2 verkon avulla yhdistämme asiakkaan verkkolaitteiden hallintaosoitteet tähän XXXXXX1verkkoon.

2.2.1 VLAN varaukset

VLAN varaukset tulee tehdä ennen verkkojen luontia. VLAN avulla voimme määrittää useamman verkon toimivuuden samassa kytkin portissa. Varauksien avulla pystymme välttämään päällekkäisten verkkojen luomista konesaliin.

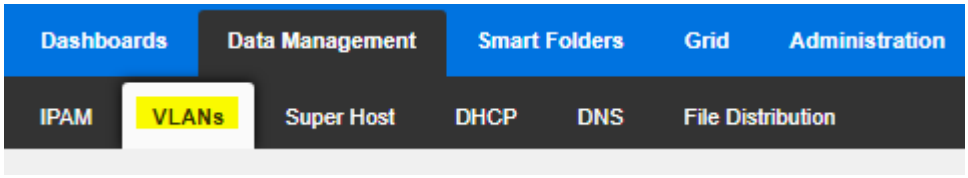
VLAN varaukset tehdään työnantajani IPAM järjestelmään. Kyseiseen järjestelmään on merkitty VLAN alue, josta varaukset tulee tehdä.

Varmistetaan asiakkaalta ettei heillä ole esteitä uuden VLAN lisäykselle. Tämän jälkeen varmistetaan että haluttu VLAN on varmasti vapaana konesalin kytkimeltä.



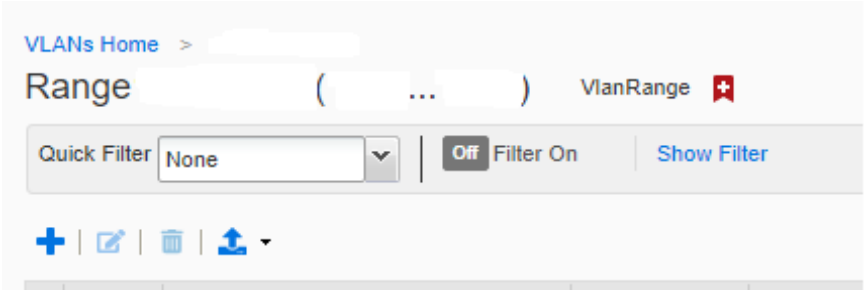
Kuva 1. Konesalikytkimeltä käyty tarkistamassa seuraava vapaa VLAN

Tämän jälkeen tehdään varaus IPAM-järjestelmään. IPAM-järjestelmässä siirrytään VLAN näkymään



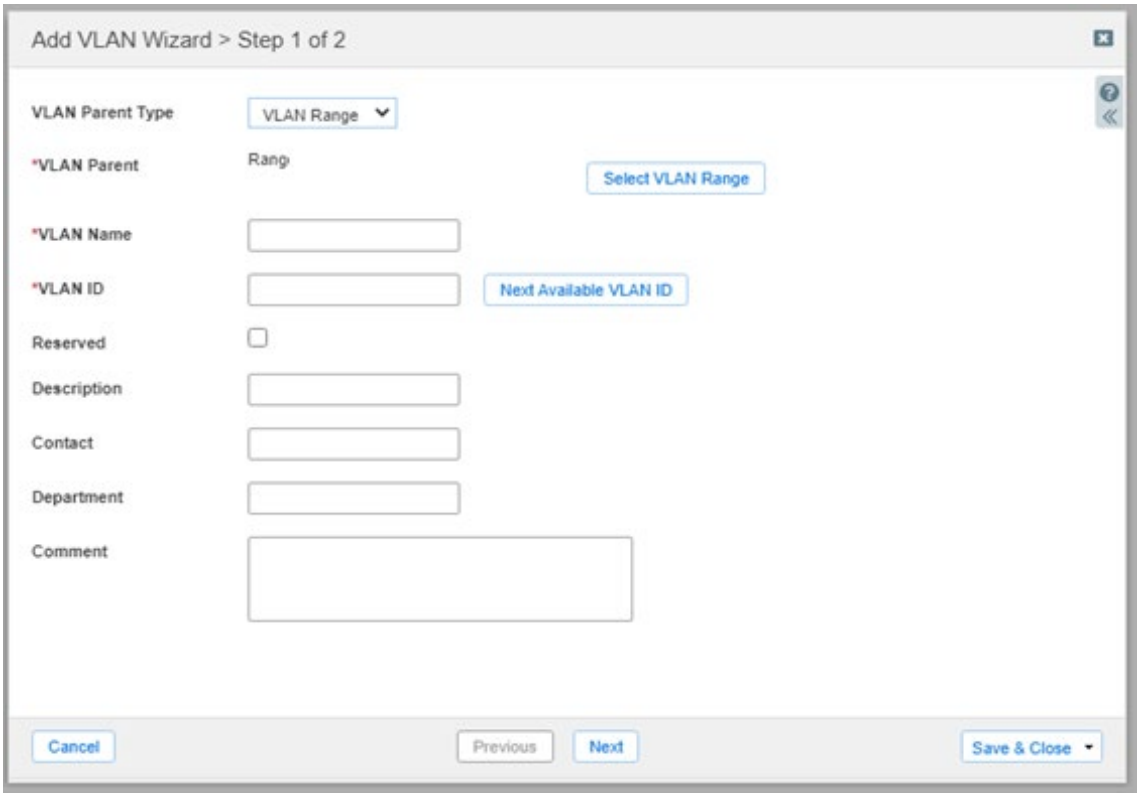
Kuva 2. IPAM käyttöjärjestelmän päänäkymä

jonka jälkeen valitaan haluttu range



Kuva 3. IPAM järjestelmän VLAN varaus näkymä

ja mennään viimeiselle sivulle ja painetaan yllä olevassa kuvassa näkyvää '+' merkkiä. Tästä avautuu VLAN lisäystä varten 'Wizard' työkalu. Tähän täydennetään tässä kohtaa 'VLAN Name', 'VLAN ID' ja 'Comment' kentät ja painetaan oikeassa alakulmassa olevaa 'Save & Close' painiketta.



Kuva 4. VLAN luontiin tarkoitettu alustusohjelma

2.2.2 Verkkojen varaukset

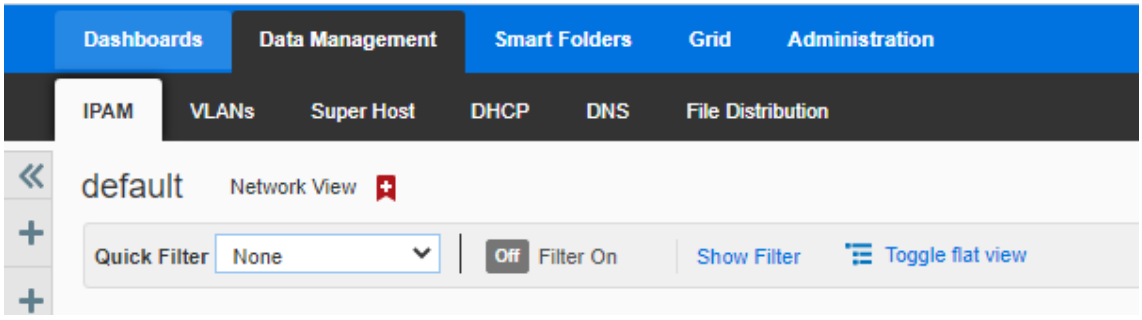
VLAN varauksen jälkeen tehdään hallintaverkkojen varaukset. Verkot varataan myös IPAM:sta. Verkkojen varauksissa tulee ottaa huomioon asiakkaan private-verkkojen

päällekkäisyydet sekä arkkitehtuurin määrittämät IP-alueet. XXXXXX1-transit verkkosegmentin varaamiseen on arkkitehtuuri määrittänyt seuraavat ehdot:

> ”Mikäli on mahdollista, käytetään asiakkaan julkisesta verkosta olevia osoitteita /28 maskilla. Mikäli joudutaan käyttäämään privaatteja osoitteita varataan verkko /27 maskilla näistä pooleista: xxx.xxx.xxx.xxx /19, xxx.xxx.xxx.xxx /21, xxx.xxx.xxx.xxx /21. Jos edellä mainituista osoite pooleista mikään ei sovellu, asiakas ehdottaa omia privaatteja osoitteita mitkä tarkistetaan IPAM:sta päällekkäisyyksien välttämiseksi.”

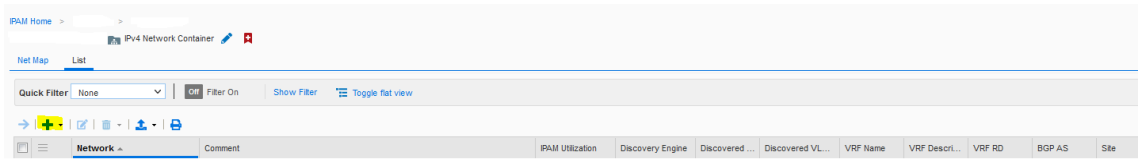
XXXXXX2-transit verkon varataan verkko poolista xxx.xxx.xxx.xxx /23. Varattavan verkko segmentin koko on /29.

Verkkojen varausta varten mennään IPAM:n ja haetaan haluttu pooli. Jos haluttua IP blokkia ei heti löydy hausta, niin kyseinen blokki kuuluu todennäköisesti osaksi isompaa blokkia (esim. verkkoa xxx.xxx.xxx.xxx /19 ei löydy suoraan haun avulla, koska kyseinen verkko on osa isompaa kokonaisuutta xxx.xxx.xxx.xxx/8). Kun kyseinen verkko on löytynyt, avaa se.



Kuva 5. IPAM päänäkymä

Tämän jälkeen luodaan valittuun IP blokkiin uusi verkko. Luodaan halutun kokoinen verkko (mikäli asiakkaan kanssa ei ole sovittu mitään poikkeuksia transit verkkoihin liittyen niin varataan seuraava vapaa verkko yllämainittujen ehtojen mukaisesti). Verkon luonnin yhteydessä tulee määrittää ”Extensible Attributes” kohtaan määritetään varattu VLAN ja lisätä se VLAN ID:n value kenttään.



3 Hallintaverkon toteutus

Kun IP-verkot on varattu IPAM:sta, tulee kyseiset verkot levittää kaikille konesalikytkimille sekä UCS-podeille. Näin luodaan kyvykkyydet luoda hallinta- ja valvontakomponentteja työnantajani konesaliin. Verkkojen levitys tapahtuu lisäämällä IP-uid dokumentissa varattu VLAN konesalikytkimille sekä UCS-podeille. Hallintaverkon gatewaynä tulee toimimaan konesalin palomuuri.

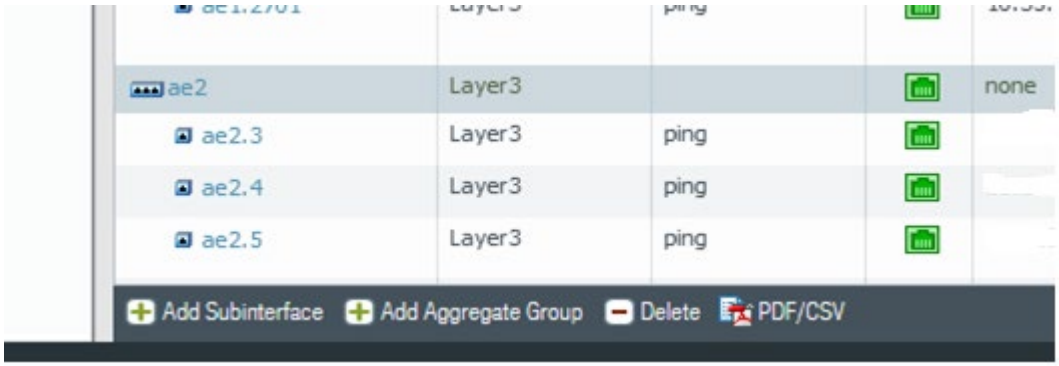
3.1 Hallintaverkon luonti konesalipalomuurille

Konesalipalomuurille luodaan uusi subinterface hallintaverkkoa varten. Subinterfacen avulla verkkolaitteen fyysisten portteihin voidaan liittää useampi verkko. Konesalipalomuurin aggregate-ethernet AE2 alle luodaan nämä subinterfacet.

Kirjaudutaan palomuurille ja mennään ’Network’ -> ’Interfaces’ valikon alle.

Kuva 6. Palomuurin hallintasivu

Valitaan kyseinen Interface ja painetaan alalaidassa olevaa ’Add Subinterface’ painiketta.



Kuva 7. Aliverkot palomuurilla

Add Subinterface valikkoon tulee täyttää seuraavat tiedot:

Interface Name	Verkon VLAN numero
Comment	Asiakastunniste
Tag	VLAN numero
Virtual Router	Asiakkaalle määritetty virtuaali reititin
Virtual System	Asiakkaalle määritetty virtuaali palomuuri
Security Zone	Luotavat verkon transit zone (joko XXXXXX1-transit tai XXXXXX2-transit)
Ipv4	Määritetty transit verkko, niin että verkon default-gateway osoite tulee palomuurille

XXXXXX1-transit verkko luodaan niin että siihen voidaan asentaa hallinta- ja valvontakomponentit. XXXXXX2-transit verkko luodaan kahden konesali palomuuriklusterin välille.

3.2 Hallintaverkon lisäys konesalikytkimille sekä UCS-podeille

Edellä luotujen verkkojen VLAN:t lisätään konesalikytkimille sekä XXXXXX1-transit verkot lisätään myös UCS-podeille. VLAN lisäyksiä varten on olemassa jo erillinen ansiblellä tehty skripti jolla saadaan kaikille kytkimille lisättyä uudet VLAN:t ilman että jokaiselle kytkimelle tarvitsee mennä erikseen.

Skripti käy määrittämässä kytkimille konfiguraatioksi:

’Set vlans vlanXXXX description “XXXXXXX”’

‘Set vlans vlanXXXX vlan-id XXXX’

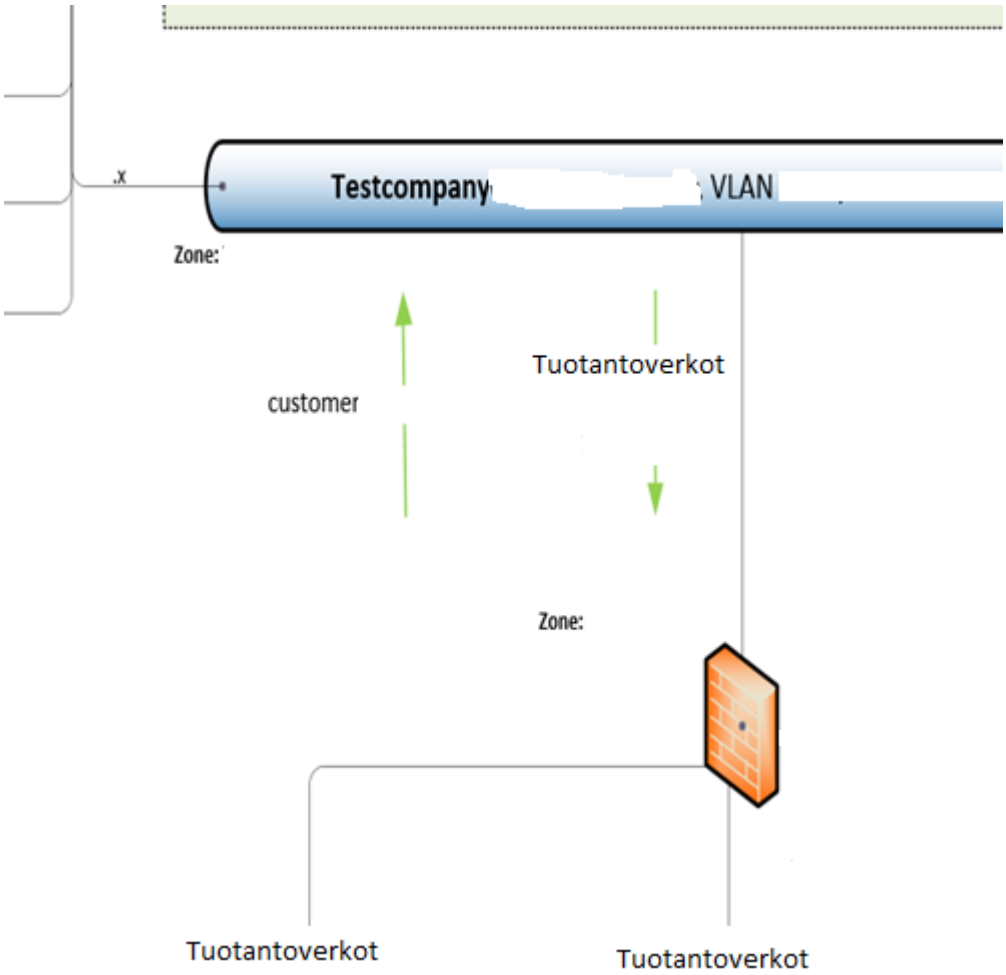
UCS-podeille VLAN lisäys tapahtuu joko olemassa olevalla skriptillä tai suoraan UCS POD web gui:n kautta. VLAN lisäyksistä UCS-podeille on olemassa erillinen ohjeistus mitä ei käydä tässä työssä läpi.

3.3 Hallintaverkon reititykset

Arkkitehtuuri on määrittänyt seuraavat ehdot reititysten osalta:

> *Asiakkaan suuntaan reititetään palvelutarjoajan Palvelutuotannosta ainoastaan* XXXXXX1 *transit segmentti. Asiakkaalta reititetään palvelutarjoajan suuntaan uuden palvelutuotannon palveluiden segmentti XXX.XXX.XXX.XXX/24 sekä varmistuspalveluiden-verkko XXX.XXX.XXX.XXX/24*

Kyseiset reitit tullaan tekemään konesali palomuuriklusterien välille. Transitio vaiheessa uuteen hallintayhteyteen halutaan reitittää sekä vanha tuotantoverkko että uusi. Testi asiakkaan verkkokuva jonka mukaan reitit tehdään:

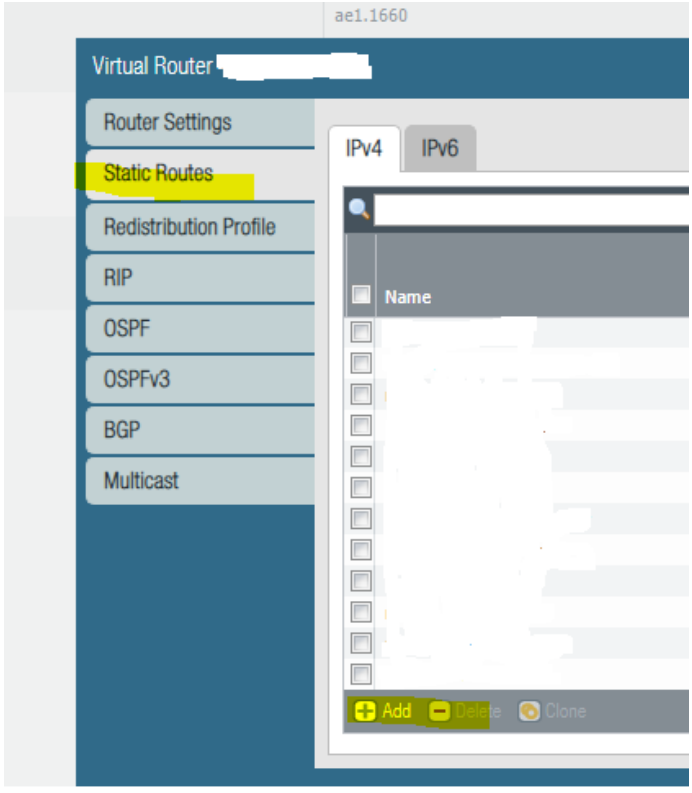


Kuva 8. Hallintaverkko kuva

Kirjautudutaan palomuureille, joka palomuurien hallintakomponentin Panoraman kautta tai suoraan palomuurin hallintaosoitteen kautta. Kun olet kirjautunut palomuurille, mene Network valikkoon ja avaa Virtual Routers näkymä.

Kuva 9. Palomuurin Network valikko

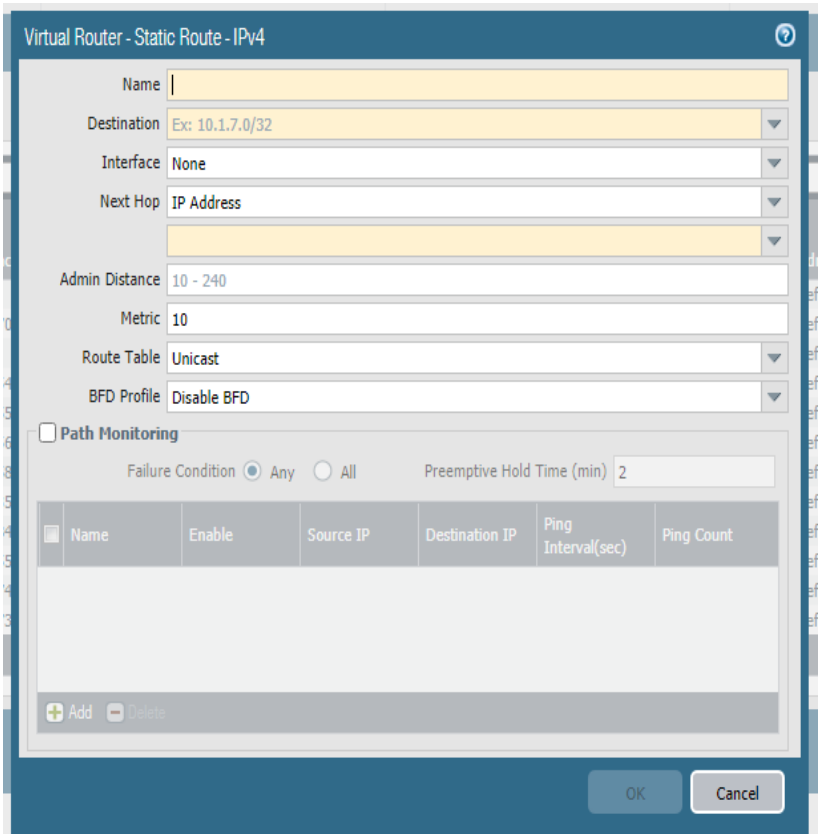
Hallintayhteys toteutustavaksi on valittu suunnittelu vaiheessa numero 1, joka myös määrittää mihin palomuurin virtuaalireitittimistä kyseiset reititykset tehdään. Verkkokuvan mukaisesti tuotantoverkkojen läpi menevälle palomuurilta tulee mainostaa tuotantoverkoille asiakkaan XXXXXX1-transit verkko, tehdään staattinen reitti XXXXXX2-transit verkkoa kohti. Avataan haluttu virtuaalireititin ja valitaan Static Routes ja painetaan alhaalla olevasta Add painikkeesta.



Kuva 10. Palomuurin virtuaalireititin

Add painikkeesta avautuu valikko, johon täytetään seuraavat kohdat.

Name	Nimeksi tulee standardien mukainen nimi kuvaamaan reittiä
Destination	Asiakkaalle määritetty XXXXXX1-transit verkko
Interface	Palomuurille määritetty XXXXXX2-transit verkon subinterface
Next Hop	IP address ja toiselle palomuurille määritetty IP osoite



Kuva 11. Staattisen reitin luonti palomuurin virtuaalireitittimelle

Kun reitit ykset on tehty tuotantoverkon puoleiselle palomuurille, tulee tehdä edellä mainittujen ehtojen mukaisesti vastaavanlaiset reitit ykset konesalin toiselle palomuuriklusterille.

4 Hallintayhteys palomuurin konfigurointi

Jotta tuotantoverkosta saa yhteyden asiakkaan tilassa oleviin verkkolaitteisiin tulee asiakkaan tilassa olevaan palomuuriin rakentaa VPN tunneli. Toinen vaihtoehto, jota sovelletaan tässä ohjeessa, on toimittaa asiakkaan tilaan erillinen palomuuri hallintayhteyttä varten. Tämä jälkimmäinen tapa on vastaavanlainen kuin vanhassa tuotannossa toteutettu hallintayhteys. Näin ollen hallintayhteyden yliheitosta tulee helpompaa kun asiakkaan tilassa tarvitsee vain vaihtaa yksi laite. Tässä työssä VPN-tunneli perustetaan kahden julkisen IP-osoitteen välille.

4.1 Palomuurin esikonfigurointi

Uuteen palomuurin saa yhteyden joko erillisen konsoliportin avulla tai sitten erillisen management-portin avulla. Erona näissä on se, että konsoliportin kautta avautuu konsolinäkymä ja management-portin kautta saadaan palomuurin web-hallinta auki. Tässä työssä hyödynnetään jälkimmäistä tapaa.

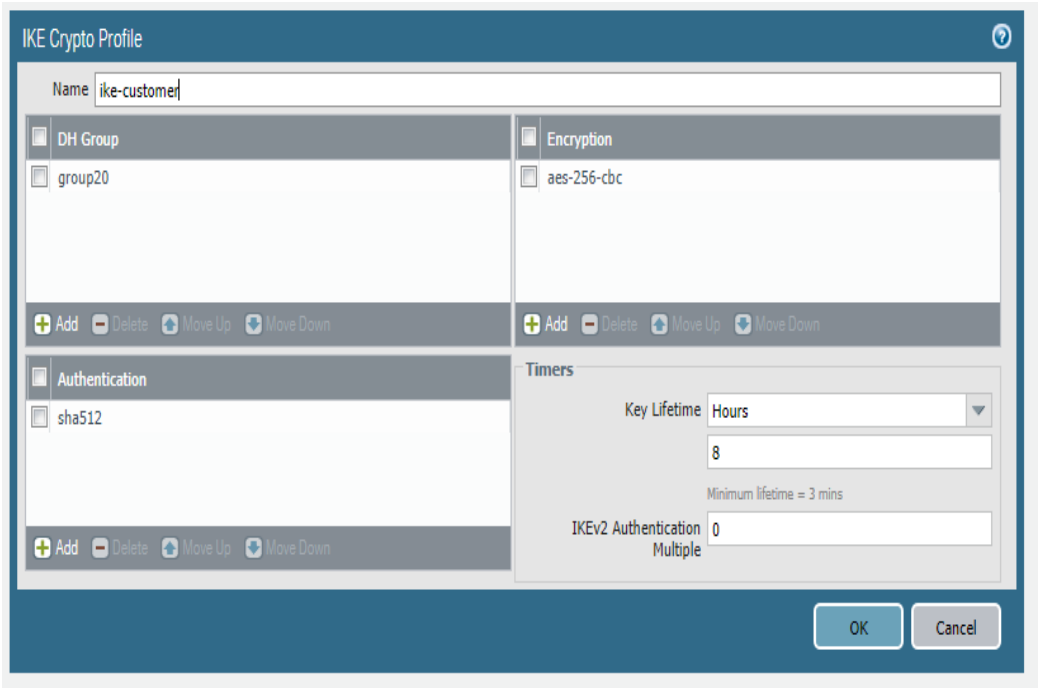
Palomuurille tulee laittaa laitevalmistajalta saatu lisenssi avain, jotta laite saa versio päivityksiä ja pysyy näin tietoturvallisena. Laitevalmistajan verkkosivuille tulee määrittää tämän uuden laitteen serial-tunniste ja liittää se lisenssi avaimen kanssa. Kun tämä toimenpide on tehty, tulee tämä lisenssi avain määrittää palomuurille joko manuaalisesti tai sitten automaattisesti kun verkkoyhteys on saatu toimimaan. Tämän jälkeen palomuurille on hyvä vaihtaa vakio admin-tason käyttäjätunnus ja salasana. Muiden tietojen, kuten laitteen nimen vaihtaminen, on tässä vaiheessa valinnaista.

Hallintayhteyttä varten tärkein konfigurointi tässä vaiheessa on Interfacen luonti julkista IP-osoitetta varten. Mennään siis palomuurilla Network näkymään ja valitaan Interfaces valinta. Avataan tässä tapauksessa Ethernet1/1 ja määritetään siihen operaattorilta saatu julkinen IP-osoite.

4.2 VPN-tunnelin luominen

VPN-tunnelin luomista varten käytetään pre-shared-key avainta, joka tulee olla identtinen tunnelin molemmissa päissä. Myös muut salaus parametrit tulee olla identtiset tunnelin molemmissa päissä. Mennään Network näkymän alla olevaan Network Profiles valikkoon luomaan IKE ja IPSEC salausprofiilit.

Valitaan ensimmäiseksi IKE salaus valitsemalla IKE Crypto palomuurilla. Painetaan +Add painiketta ja määritetään seuraavat arvot: DH Group, Encryption ja Authentication. Alla esimerkki



Kuva 12. IKE profiilin luonti palomuurilla

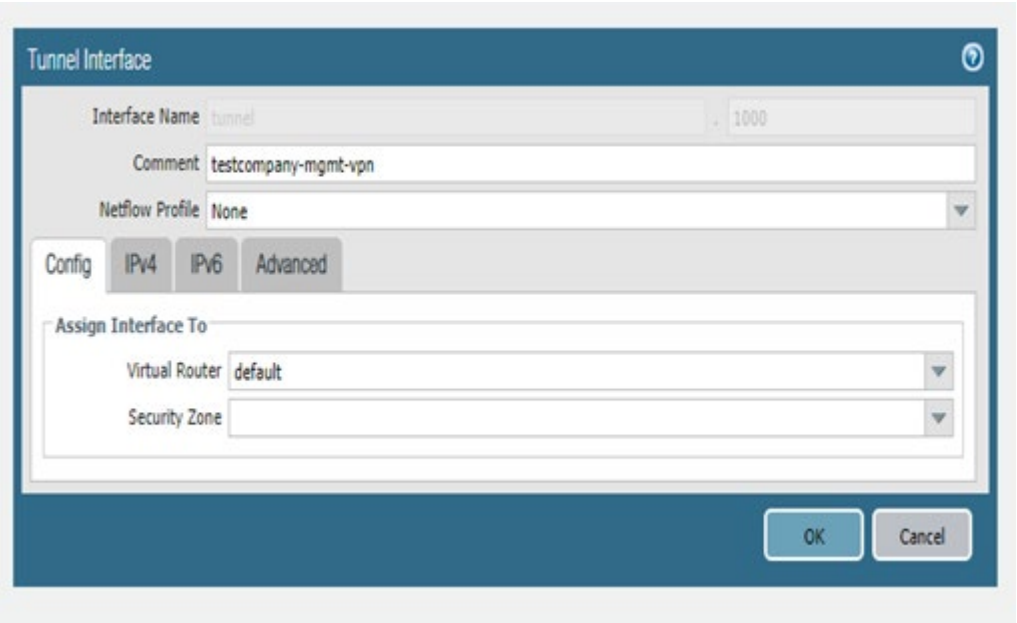
Tämän jälkeen tulee määrittää IKE Gateway.

Name	Gatewayta kuvaava nimi

Version	IKE:n versio, version tulee olla identtinen molemmissa päissä
Address Type	Valitaan Ipv4
Interface	Ulospäin liikennöivä ethernet portti
Local IP Address	Aikaisemmassa kohdassa määritetyn portin IP osoite
Peer IP Address Type	IP
Peer Address	Vastapuolen julkinen IP osoite
Authentication	Pre-Shared Key
Pre-Shared Key	Ennalta määritetty salausavain joka on identtinen molemmissa päissä

Tämän jälkeen luodaan vielä IPSec Crypto Profile. Profiiliin tulee määrittää: DH Group, Encryption ja Authentication. Kun salaus profiilit on luotu voidaan tehdä itse tunneli.

Mennään Interface näkymään ja avataan valikko Tunnel. Painetaan +Add painiketta ja lisätään seuraavat tiedot: Interface numero, Comment kohtaan tunnelin käyttötarkoitus, Virtual Router sekä Security Zone. Alla esimerkki



Kuva 13. Tunnelin luonti palomuurille

Tunnelin luonnin jälkeen mennään IPSec Tunnels näkymään ja luodaan uusi IPSec tunneli painamalla +Add painiketta. Tunnelia varten tulee täyttää seuraavat tiedot

Name	Tunnelille kuvaava nimi
Tunnel Interface	Aikaisemmassa kohdassa luotu tunneli
Type	Auto Key
Address Type	Ipv4

IKE Gateway	Aikaisemmin luotu IKE Gateway
IPSec Crypto Profile	Aikaisemmin luotu IPSec Crypto profiili

Kun sekä asiakkaan tilaan että työnantajani tilassa olevaan palomuuriin on määritetty edellä mainitut kohdat, tunnelin pitäisi nousta automaattisesti ylös.

4.3 VPN-tunnelin reitit ykset ja palomuurisäännöt

Asiakkaan tiloissa olevaan hallintayhteys palomuuriin tulee tehdä samanlaiset reititykset kuin konesalissa tehtiin. Konesalista reititetään pelkästään asiakkaan XXXXXX1-transit verkko asiakkaan tiloissa olevaa hallintayheys palomuurin suuntaan. Hallintayhteys palomuurilta reititetään asiakkaan hallintaverkko konesalia kohti.

Mennään palomuurin Network näkymään ja valitaan Virtual Routers valikko. Avataan haluttu virtuaali reititin ja luodaan sinne uusi staattinen reitti valitsemalla Static Routes ja painamalla +Add painiketta. Staattiseen reittiin tulee täyttää seuraavat tiedot.

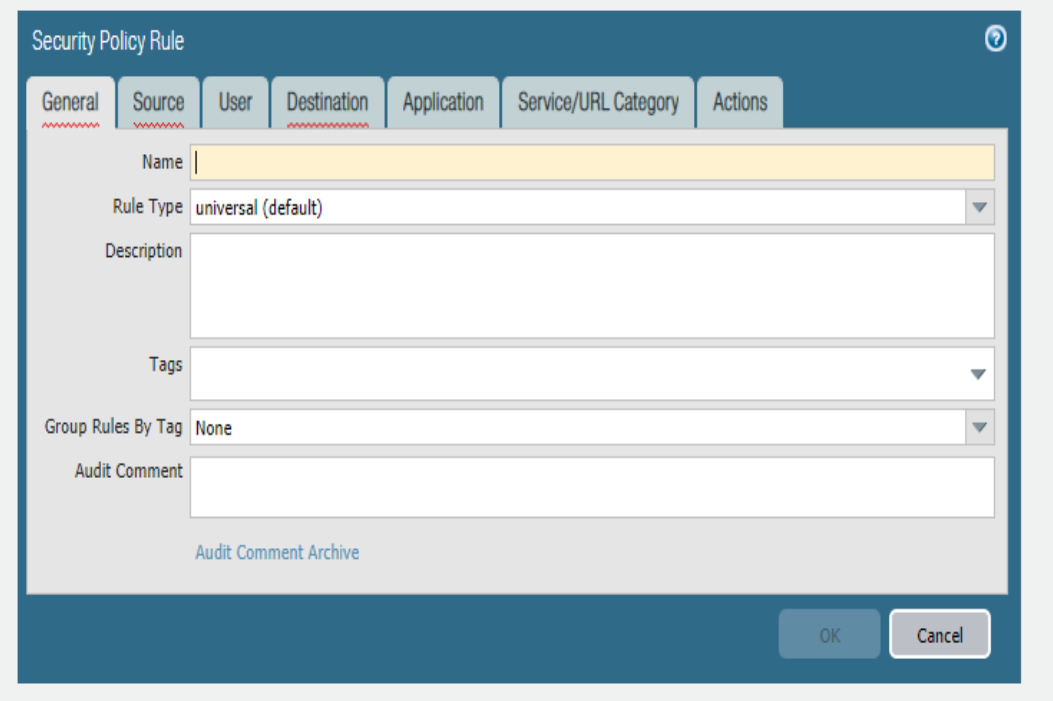
Name	Nimetään standardien mukaisesti
Destination	Asiakkaan hallintaverkko
Interface	Hallintayhteyttä varten luotu tunnel interface

Next-Hop	None

Asiakkaan laitetilassa olevaan hallintayhteys palomuuriin luodaan myös staattinen reitti joka reititetään myös luotuun tunneliin. Tämän tunnelin kohteena on konesaliin luotu XXXXXX1-transit verkko.

Hallintayhteyspalomuurilla tulee myös sallia haluttu liikenne palomuurisäännöillä. Hallintayhteys palomuurilla en näe tarpeelliseksi rajoittaa liikennöintiä asiakkaan XXXXXX1-transit ja hallintaverkon välillä. Näin ollen sallitaan kaikki liikennöinti kyseisten verkkojen välillä. Tämä ei ole tietoturvallisin vaihtoehto, joten palomuurisääntöä tullaan muokkaamaan tietoturvallisemmaksi kun tiedetään tarkkaan mitä protokkollia halutaan sallia.

Mennään palomuurilla Policies näkymään ja valitaan Security valikko. Painetaan alhaalla olevasta +Add painikkeesta, jolloin avautuu Security Policy Rule ikkuna. Täytä kyseiseen ikkunaan kaikki tarpeellinen tieto, keltaiset kohdat ovat pakollisia.



Kuva 14. Palomuurisäännön teko

Luodaan palomuurisäännölle sääntöä kuvaava nimi ja lisätään se kohtaan Name. Tämän jälkeen siirrytään Source valikkoon määrittämään mistä liikennöinti on salittua. Tässä tapauksessa halutaan sallia liikennöinti testi asiakkaan XXXXXX1-transit verkosta (xxx.xxx.xxx.xxx/27). Lisätään siis kyseinen verkko ’Source Address’ kohtaan painamalla alhaalta olevasta ’+Add’ painikkeesta. Samalla tarvitsee määrittää kyseisen verkon ’Zone’. Zone tiedot löytyvät Network asetusten alta. Tässä tapauksessa Zone tulee olemaan VPN-tunnelin Zone. Alla täytetty esimerkki Test Companyn säännöstä.

Tämän jälkeen mennään Destination valikkoon ja listäään kohdeverkko kyseiselle säännölle. Tässä tapauksessa täytyy sallia liikennöinti asiakkaan hallintaverkkoa kohti. Lisätään siis asiakkaan verkon ’Destination Zone’ ja asiakkaan hallintaverkko ’Destination Address’ kenttiin alhaalla olevan ’+Add’ painikkeen avulla.

Tämän jälkeen tulee määrittää haluttu liikenne näiden kahden verkon välille. Mennään siis seuraavaksi Application valikkoon ja laitetaan ruksi Any laatikkoon. Tämä ei ole tietoturvallisin vaihtoehto, mutta tässä vaiheessa haluamme vain liikenteen toimivan asiakkaan verkkolaitteiden ja uusien hallinta- ja valvontakomponenttien välillä.

Liikennöinti tulee sallia molempiin suuntiin. Asiakkaan hallintaverkosta konesaliin tuleva liikennöinti sallitaan muuten samalla tavalla kuin aikaisempi sääntö, erona vain ’Source’ ja ’Destination’ kenttien tiedot tulee olla toistepäin. On myös hyvä varmistaa, että kyseiset säännöt ovat Deny sääntöjen yläpuolella. Palomuurisäännöt tulee tehdä sekä konesalin palomuurille että asiakkaan laitetilassa olevaan hallintapalomuuriin.

5 Yhteenveto

Ohjeen avulla pysytytään luomaan hallinta- ja valvontayhteys tuotantoverkon ja asiakkaan verkkolaitteiden välille. Hallintayhteys toteutustapoja on muutamia, mutta kaikkien niiden tekemiseen pystytään soveltamaan tätä. Vaikka itse verkko on kunnossa ja yhteys toimii toimipisteiden välillä, tulee vielä asentaa itse hallinta- ja valvontakomponentit. Myös asiakkaan verkkolaitteille tulee tehdä tarvittavat muutokset jotta uudet hallinta- ja valvontakomponentit toimivat. Näitä muutoksia ovat mm. palomuurisääntöjen muokkaukset, verkkolaitteilla olevat snmp-asetukset sekä access-listojen muutokset. Hallintayhteyden yliheitto vaiheessa tulee ottaa huomioon uuden sekä vanhan yhteyden yhtäaikainen toimiminen. Näin vältetään mahdolliset hallintayhteys katkokset mikäli on tullut konfiguraatio virheitä.

Lähteet

Sisäinen dokumentaatio