KYMENLAAKSON AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma / Tietoverkkotekniikka

Erna Komulainen & Juuso Wägar

MONIPISTEYHTEYKSINEN VIRTUAALINEN YKSITYISVERKKORATKAISU

Opinnäytetyö 2012

TIIVISTELMÄ

KYMENLAAKSON AMMATTIKORKEAKOULU
Tietotekniikka

KOMULAINEN, ERNA
WÄGAR, JUUSO

MONIPISTEYHTEYKSINEN VIRTUAALINEN YKSITYISVERKKORATKAISU

Opinnäytetyö 34 sivua + 16 liitesivua
Työn ohjaaja Yliopettaja Martti Kettunen
Toimeksiantaja Profimill Engineering Oy
Toukokuu 2012
Avainsanat 3G, VPN, DMVPN, IPSec, GRE

Opinnäytetyön tavoitteena oli rakentaa dynaaminen ja skaalautuva virtuaalinen yksityisverkko keskusreitittimen ja usean etäpäädyn välille käyttäen matkapuhelinverkkoyhteyttä. Testiverkko rakennettiin Kymenlaakson ammattikorkeakoulun ICT-laboratorioon. Opinnäytetyö on osa laajempaa Profimill Engineering Oy:n projektia.

Siirrettävän automaatiodatan tuli kulkea Internetin yli suojatusti ja luotettavasti. Dynaamisuuden takaamiseksi päätelaitteiden lisäämisen tuli olla mahdollisimman yksinkertaista.

Testiverkko toteutettiin kahdella Cisco Integrated Services-reitittimellä, joista toisessa oli sisäänrakennettu 3G-moduuli. 3G-reititin toimi etäpäädyn reitittimenä ja toinen hieman tehokkaampi reititin keskuspäädyn laitteena. Ratkaisuun valittu GRE over IPSec-tunneli muodostui laitteiden välille 3G-reitittittimen toimiessa aktiivisena osapuolena yhteyttä muodostettaessa. Lisäksi verkon etähallinta toteutettiin Ciscon palomuurilaitteella.

Lopullinen ratkaisu saavutettiin käyttämällä Dynamic Multipoint VPN ratkaisua, joka koostuu useista protokollista ja salaustekniikoista. Tämä ratkaisu takasi erinomaisen palautumisen vikatilanteista sekä vaivattoman tavan lisätä etälaitteita verkkoon. Työlle jäi useita jatkokehitysmahdollisuuksia, kuten esimerkiksi verkonhallinta.

ABSTRACT

KYMENLAAKSON AMMATTIKORKEAKOULU
University of Applied Sciences
Information Technology

KOMULAINEN, ERNA &
WÄGAR, JUUSO

Bachelor's Thesis	Point-to-multipoint Virtual Private Network Solution
Supervisor	34 pages + 16 pages of appendices
Commissioned by	Martti Kettunen, Principal Lecturer
May 2012	Profimill Engineering Oy
Keywords	3G, VPN, DMVPN, IPSec, GRE

The objective of this thesis work was to build a dynamic and scalable point-to-multipoint virtual private network using mobile communication network connections. The test network was built in Kymenlaakso University of Applied Sciences' networking laboratory.

The main goal was to build a reliable solution for transferring automation data securely through the Internet. Attention was especially paid eliminating the need for end user's action to initiate and restore connectivity.

The network was built using two Cisco Integrated Services routers, where one had an integrated 3G module. The other router stood as a central hub router and the 3G router was a client end router. An IPsec tunnel within GRE tunnel was formed between the two when the 3G router initiated traffic. Remote management connections were made using a firewall.

The goal was achieved using a Dynamic Multipoint VPN solution which uses several protocols and encryption techniques. This solution guaranteed excellent recovery from malfunctions and a dynamic way to add clients to the network. Some development issues, such as the management of the network, remained to be solved.

SISÄLLYS

LYHENTEITÄ JA KÄSITTEITÄ

3G, yleinen lyhenne kolmannen sukupolven matkapuhelinteknologioille

ASA*, Adaptive Security Appliance,* Cisco Systemsin palomuurilaite

ASDM, *Adaptive Security Device Manager*, graafinen käyttöliittymä palomuurilaitteille

DMVPN, *Dynamic Multipoint Virtual Private Network*

DMZ, *demilitarized zone*, eteisalue, jolla on alempi tietoturvataso kuin sisäverkolla

EEM, *Embedded Event Manager,*Cisco IOS:n ominaisuus, jolla voi automatisoida erilaisia toimintoja

EIGRP, *Enhanced Interior Gateway Routing Protocol,* reititysprotokolla

GRE, *Generic Routing Encapsulation*, Ciscon kehittämä tunnelointiprotokolla

IOS, *Internetwork Operating System*, Ciscon laitteiden käyttämä käyttöjärjestelmä

IP, *Internet Protocol,* Internet-protokolla

IPSEC, *IP security architecture*, joukko TCP/IP tietoliikenneyhteyskäytäntöjä yhteyksien suojaamiseen

IP SLA, *IP Service Level Agreements*, ominaisuus, jolla voi tarkkailla esimerkiksi yhteyden laatua

LAN*, Local Area Network,* paikallinen lähiverkko

NAT, *Network Address Translation*, IP-osoitteen muunnos, joka tarvitaan liikennöidessä yksityisillä osoitteilla

OSI, *Open Systems Interconnection Reference Model*, seitsemänkerroksinen tiedonsiirtoprotokollamalli

Point-to-multipoint, topologiamalli

Telnet, yhteysprotokolla pääteyhteyksiin

Trunk, linkki, jossa kuljetaan usean VLAN:n tiedot

VLAN, *Virtual Local Area Network*, virtuaalilähiverkko

VPN, *Virtual Private Network*, tapa yhdistää kaksi tai useampi lähiverkko toisiinsa julkisen verkon yli

VRF, *Virtual Routing and Forwarding*, tapa jakaa reititin useaan virtuaaliseen reititys-tauluun

1 JOHDANTO

Lähiverkkojen määrän kasvaessa on syntynyt tarve yhdistää näitä maantieteellisesti kaukana toisistaan olevia verkkoja toisiinsa. Vielä 1990-luvulla käytettiin kalliita suljettuja verkkoja. Nykyään suosittu tapa on yhdistää verkot toisiinsa erilaisilla virtuaaliyksityisverkoilla eli VPN-tekniikoilla. VPN-yhteyksien suosio on kasvanut paljon viime vuosina niiden halvan hinnan takia. Tästä syystä eri organisaatiot ovat kehittäneet paljon uusia ja tehokkaita protokollia näiden yhteyksien tueksi. VPN-yhteyden avulla voidaan turvallisesti yhdistää verkkoja Internetin yli salaten data erilaisilla kryptografisilla menetelmillä.

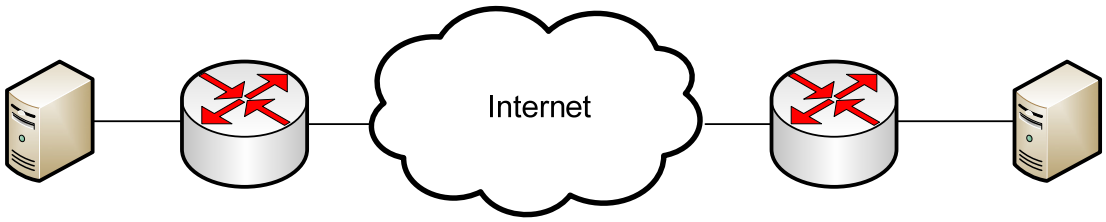
Tämä työ toteutettiin Profimill Engineering Oy:n toimeksiantona ja se on osa laajempaa projektia. Varsinaista työtä edeltävä testi- ja suunnitteluympäristö rakennettiin Kymenlaakson ammattikorkeakoulun tietoliikennelaboratorioon hyödyntäen joitakin laboratorion SimuNet-hankkeen laitteita.

Pähkinänkuoressa työn päämääränä oli rakentaa tiedonkeruuverkko, joka nimensä mukaisesti kerää tietoa maantieteellisesti toisistaan kaukana olevista lähteistä yhteen keskitettyyn palvelimeen, jossa tieto käsitellään ja jalostetaan haluttuun muotoon. Koska siirretty data kulki julkisen Internetin yli, se tuli suojata vääriltä tahoilta. Käyttämällä matkapuhelinverkkoa reunalaitteiden yhteytenä julkiseen Internetiin, saavutettiin riippumattomuus paikallisista verkoista ja palveluntarjoajista. 3G-yhteys toimi reunalaiteissa joko ensisijaisena yhteytenä tai varayhteytenä. Verkkoon toteutettiin myös etähallinta erillisellä palomuurilaitteella. Etähallinnan avulla reitittimiä ja palvelimia voitiin hallinnoida mistä vain. Tässä työssä keskityttiin verkkolaitteiden valintaan sekä niiden väliseen kommunikointiin.

2 VIRTUAALISET YKSITYISVERKOT

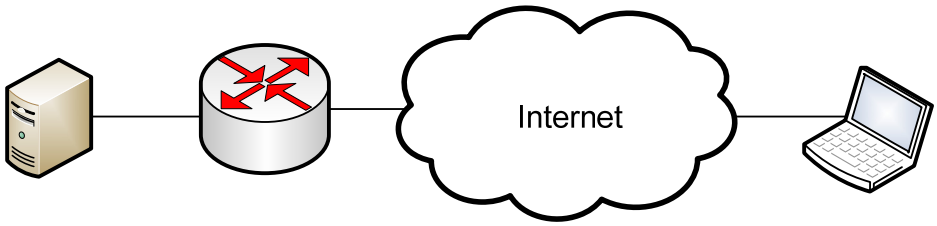
VPN eli Virtual Private Network on virtuaalinen yksityisverkko, jolla voidaan yhdistää usea lähiverkko toisiinsa julkisen Internetin yli. VPN luo virtuaalisen tunnelin, jossa data paketoidaan ja salataan käyttäen erilaisia menetelmiä. VPN-yhteyskäytännöt voidaan jakaa karkeasti kahteen luokaan: site-to-site ja remote access.

Site-to-site yhdistää yleisesti kahden tai useamman staattisen verkon toisiinsa. Näitä yhteyksiä voidaan myös käyttää yksityisten tai osittain yksityisten verkkojen yhdistämiseen eri organisaatioiden välillä. Yleisimpiä site-to-site-yhteyskäytäntöjä ovat IPSec, GRE sekä MPLS VPN. (1)



Kuva 1. Site-to-site VPN

Tämän lisäksi voidaan muodostaa yksittäinen etäyhteys julkisen verkon yli etäällä sijaitsevaan verkkoon, jota kutsutaan remote access-yhteydeksi. Tällaista yhteyttä tarvitaan esimerkiksi silloin, kun työntekijän täytyy päästä käsiksi yrityksen resursseihin etäältä, kuten kotoa tai matkoilta. Yleisemmin käytetyt remote access VPN-yhteyskäytännöt ovat SSL VPN, IPsec, L2TP, L2TP over IPsec ja PPTP. (1)



Kuva 2. Remote access VPN

VPN yhteydet toteutetaan joko laitteistolla tai ohjelmistolla. Usein site-to-site-yhteydet aloitetaan ja päätetään laitteistolla esimerkiksi reitittimellä tai palomuurilla. Remote access -yhteydet yleensä muodostetaan käyttäen erillistä VPN client ohjelmistoa, jossa salaamisesta ja salauksen purkamisesta vastaa isäntäkoneen laitteisto.

2.1 Dynamic Multipoint VPN

Dynamic Multipoint VPN (DMVPN) on eräänlainen site-to-site- ja remote access-yhteyksien välimuoto. Toisaalta se käyttää site-to-sitelle ominaista GRE-tunnelointia, mutta koska yhdellä tunnelilla voi olla useita päätyjä, voidaan DMVPN mieltää remote access -tyyppiseksi yhteydeksi. DMVPN toimii käyttäen useita yhteyskäytäntöjä ja protokollia, jotka tekevät ratkaisusta dynaamisen ja skaalautuvan. Se muun muassa poistaa tarpeen käyttää etälaitteissa kiinteitä IP-osoitteita. Voidaan ajatella, että DMPVN koostuu seuraavista elementeistä:

- Multipoint Generic Routing Encapsulation (mGRE)
- Next-Hop Resolution Protocol (NHRP)
- Internet Protocol Security (IPSec)
- Dynaaminen reititysprotokolla (EIGRP, OSPF, RIP, BGP, ODR, IS-IS)(2, 3)

2.1.1 Generic Routing Encapsulation

Generic Routing Encapsulation (GRE) on Cisco Systemsin kehittämä tunnelointiprotokolla, joka määritellään RFC 2784 dokumentissa. GRE tukee useita verkkokerroksen protokollia, kuten esimerkiksi IP ja IPv6. Tämän lisäksi sillä voidaan siirtää multicast-liikennettä, joka mahdollistaa reititystiedon kulun tunnelissa. GRE-tunnelit ovat point-to-point-yhteyksiä. Multipoint GRE (mGRE) mahdollistaa monipistetopologian, jota DMVPN käyttää. (4)

Kuva 3. GRE kapselointi.

2.1.2 Next-Hop Resolution Protocol

Next-Hop Resolution Protocol (NHRP) on protokolla, jota käytetään Non-Broadcast Multiple Access eli NBMA-verkoissa löytämään lyhin reitti lähteestä kohde osoitteeseen. NHRP on määritelty RFC 2332 dokumentissa.(2, 5)

2.1.3 Internet Protocol Security

Internet Protocol Security (IPSec) on joukko tietoliikenneprotokollia yhteyksien turvaamiseen. Nämä protokollat tarjoavat salauksen, tiedon eheyden varmistuksen ja osapuolten todennuksen. IPSec on yleisin OSI-mallin verkkokerroksella toimiva VPN teknologia.(6)

2.1.4 Reititysprotokolla

DMVPN tarvitsee reititystietojen välitykseen reititysprotokollan. Reititysprotokollan avulla reitittimet vaihtavat tietoa verkon rakenteesta. Tällaisia ovat esimerkiksi EIGRP, OSPF, RIP sekä BGP. (7)

3 3G-VERKKO

3G-lyhenteellä tarkoitetaan niin sanottuja kolmannen sukupolven matkapuhelinverkkoteknologioita. Euroopassa yleisin käytössä oleva teknologia on UMTS (Universal Mobile Telecommunications System), jonka teoreettinen maksiminopeus on 2Mbps. Näiden verkkojen yleistyminen ja niiden tarjoama nopeus on kasvattanut pakettipohjaisen datan siirtämistä matkapuhelinverkossa. Tämä on johtanut 3G-modeemien määrän suureen kasvuun. Kotikäyttöön suunnatut USB-väylää käyttävät modeemit ovat yleistyneet ensisijaisena yhteytenä Internetiin niiden helppouden ja liikkuvuuden takia. Verkkolaitepuolella laitevalmistajat ovat tuoneet markkinoille useita laitteita, jotka hyödyntävät 3G-verkkoa, kuten reitittimiä sekä erillisiä moduuleita. (8, 9)

3G-ominaisuuden lisääminen reititinlaitteisiin tuo mukanaan helpon tavan liittyä Internetiin. Kotikäyttöön tarkoitetuissa laitteissa tämä ominaisuus on monesti integroituna tai vaihtoehtoisesti käytössä on USB-väylään sijoitettava liitännäinen eli mokkula. Ammattikäyttöön tarkoitetuissa laitteissa 3G-mahdollisuus tuodaan yleensä irrallisena moduulina, missä sitä käytetään useasti varayhteytenä lankayhteyden rinnalla. Langattoman verkon käyttö varayhteytenä onkin kannattavaa, koska se ei ole sidoksissa paikallisiin lankaverkkoihin.

4 TIEDONKERUUVERKON TEKNINEN MÄÄRITELMÄ

Työn lopputuloksena tuli olla tiedonkeruuverkko, jossa yksi keskusreititin muodostaa salatun ja luotettavan yhteyden kaikkiin etäällä oleviin reunalaitteisiin. Etäpäädyistä kerätty data tallennettiin keskusreitittimen takana sijaitsevaan keskitettyyn palvelimeen.

Verkon keskeisiä vaatimuksia olivat sen dynaamisuus ja laajennettavuus tulevaisuuden kasvua varten. Huomioon tuli ottaa myös reunareitittimien lisäyksen helppous keskusreitittimen kannalta eli minimoida lisäkonfiguraation tarve. Koska verkon tarkoituksena oli, että kommunikointi tapahtui keskuslaitteen ja etälaitteiden välillä, tuli etälaitteiden olla näkymättömiä toisilleen. Reunareitittimien takana sijaitseviin paikallisiin verkkoihin ei pystytty vaikuttamaan, joten tuli varmistaa, että niissä olevat mahdollisesti päällekkäin menevät yksityiset IP-osoitteet, eivät aiheuta ongelmaa keskusreitittimessä. Oli tärkeää, että reunalaitteet ja niiden takana sijaitsevat verkot olivat jatkuvasti saatavilla eikä yhteys katkennut.

Valmiilla verkolla tuli olla myös etähallinta, jonka avulla voitiin hallinnoida keskusreititintä, reunareitittimiä ja palvelimia mistä vain. Tässä työssä keskityttiin lähinnä eri verkkolaitteiden valintaan sekä niiden väliseen kommunikointiin.

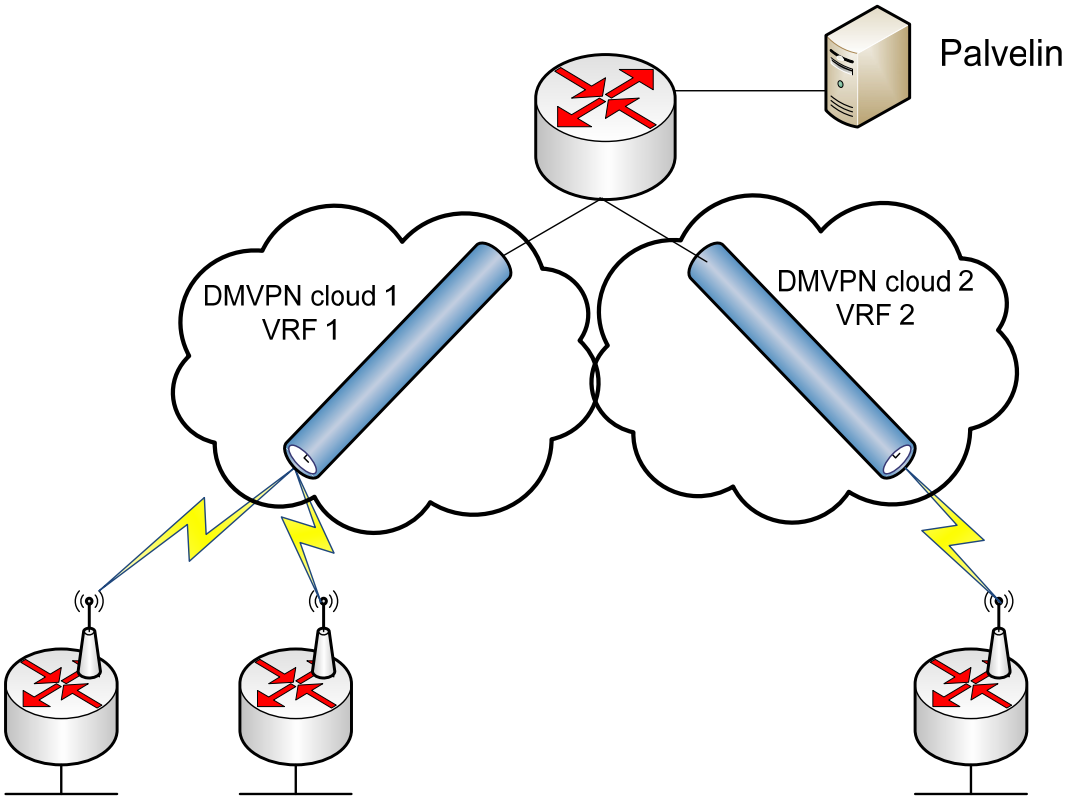
5 TIEDONKERUUVERKON TOTEUTUKSEN VALINTA

Työssä päädyttiin käyttämään Dynamic Multipoint VPN -ratkaisua, koska se tarjosi optimaalisen monipisteyhteys-topologian. Etuna oli myös se, että yhteen IPSec salattuun multipoint GRE-tunneliin voitiin liittää useita reunalaitteita, ilman että se vaati erillistä konfigurointia keskusreitittimeen. Päällekkäisten yksityisten IP-osoitteiden ongelma ratkaistiin siirtämällä jokainen DMVPN pilvi omaan virtuaaliseen reititystauluunsa (Virtual Routing and Forwarding).

Jotta reunareitittimien saatavuus pysyi korkeana, oli mahdollista käyttää Internetyhteytenä kiinteää lankaverkkoa, matkapuhelinverkkoa tai niitä molempia, jolloin 3G-yhteys toimi varayhteytenä. Tämänkaltainen ratkaisu takasi paremman luotettavuuden, mikä tarjosi mahdollisuuden tulevaisuudessa hyödyntää verkkoa myös kriittisempiin toimintoihin, kuten esimerkiksi ohjauskäskyihin.

5.1 DMVPN-pilvien toteutus

Jokaista DMVPN-pilveä kohden luotiin uusi mGRE/IPSec-tunneli sekä virtuaalinen reititystaulu (VRF) keskusreitittimeen, johon pystyi liittymään yksi tai useampi reunareititin. Näin tekemällä pystyttiin jaottelemaan reunareitittimet tilanteen mukaan sopiviin kokonaisuuksiin. Tämä mahdollisti eri DMVPN-pilvissä päällekkäiset IP-osoitteet. Jokaista virtuaalista reititystaulua kohden luotiin myös oma virtuaalilähiverkko (VLAN), jotka kuljetettiin runkolinjaa pitkin palvelimelle.



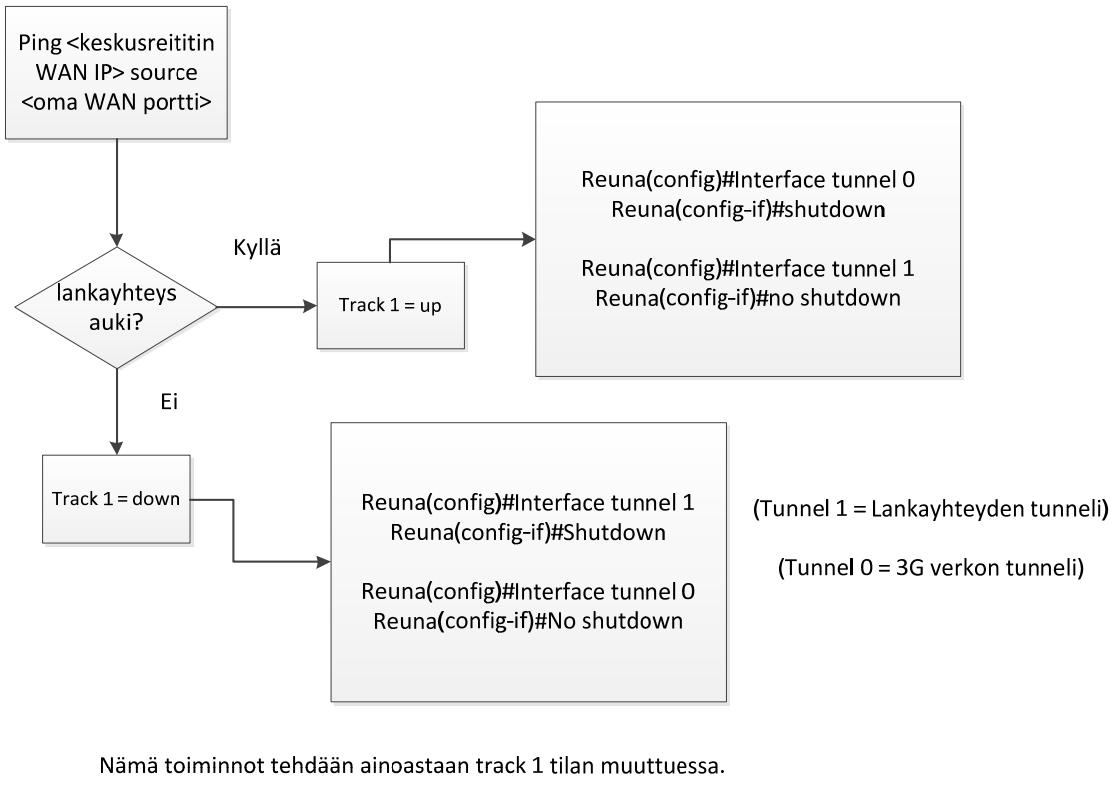
Kuva 4. Verkon rakenne.

5.2 Varayhteyden toteutus

Reunareitittimen käyttäessä ensisijaisesti lankayhteyttä, toimi 3G-yhteys toissijaisena varayhteytenä Internetiin. Varayhteys toteutettiin käyttämällä kahta tunneliliityntäporttia, toinen lankayhteydelle ja toinen 3G-yhteydelle sekä Cisco Embedded Event Manageria (EEM). Tunneliliityntäportit olivat keskenään lähes identtiset, sillä vain niiden lähdeliityntäportit erosivat toisistaan. Tästä päällekkäisyydestä johtuen vain yksi tunneliliityntäportti oli kerrallaan päällä.

Kiinteän yhteyden tilaa tarkkailtiin IP SLA (Service Level Agreements) määrityksellä, joka lähetti ICMP ECHO- paketteja keskusreitittimen julkiseen IP-osoitteeseen kymmenen sekunnin välein lähdeporttinaan lankayhteyden käyttämä liityntäportti. Tehdyn määrityksen saavutettavuutta tarkkailtiin track 1 -muuttujalla, jonka tila kiinteän yhteyden toimiessa oli UP ja vastaavasti lankayhteyden katketessa DOWN.

Cisco Embedded Event Managerin avulla reititin voi tehdä automaattisia toimintoja jonkun tietyn ehdon täyttyessä. Tässä tapauksessa EEM suoritti komentorivikäskyjä. Ehtona toimi track 1 muuttujan arvo, jonka perusteella EEM valitsi oikean tunnelliliityntäportin, jota pitää ylhäällä.

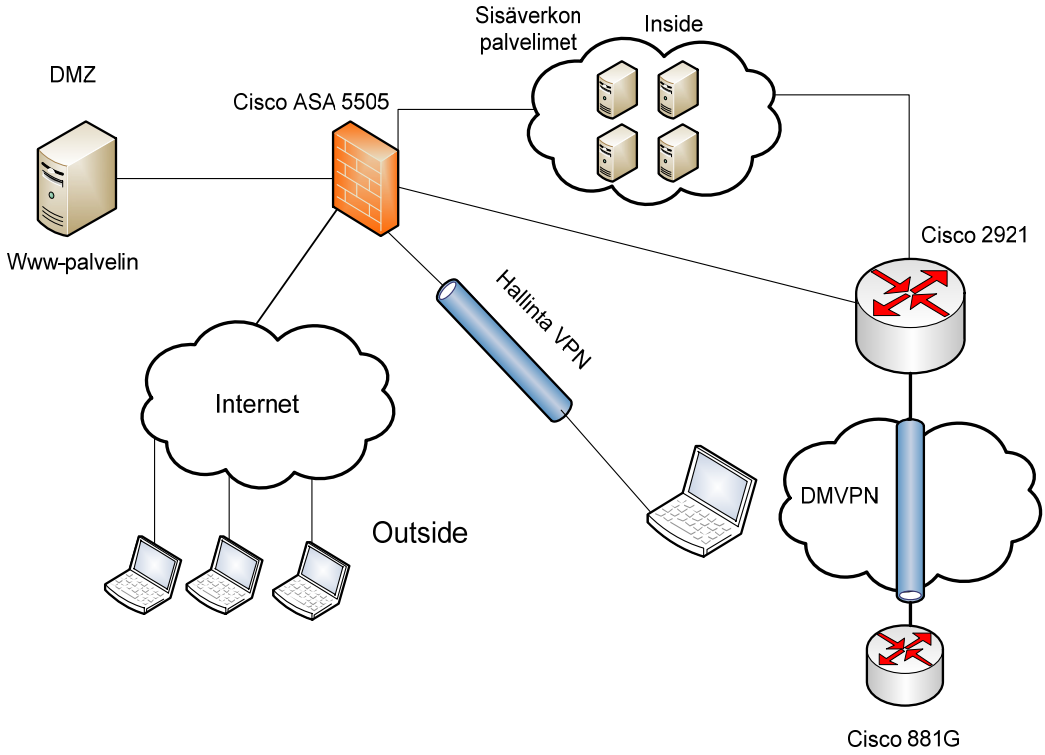


Kuva 5. Vuokaavio EEM toiminnasta

5.3 Palomuurin lisääminen verkkoon

Valmiille verkolle suunniteltiin etähallinta, jonka avulla päästiin hallinnoimaan reitittimiä ja palvelimia mistä tahansa. Verkko jaettiin kolmeen alueeseen: sisä-, ulko- ja eteisverkkoon. Näillä kolmella alueella oli toisistaan eroavat turvallisuustasot: 100 (inside), 50 (DMZ) ja 0 (outside). Suuremman turvallisuustason omaava alue pystyi kommunikoimaan pienemmän tason alueen kanssa. Mikäli haluttiin liikennöidä toiseen suuntaa, tuli kyseinen liikenne sallia pääsylistalla. Verkon julkinen www-

palvelin sijoitettiin eteisalueelle eli DMZ-alueelle (demilitarized zone). Tämän toteutukseen käytettiin Cisco Systemsin Adaptive Security Appliance ASA -palomuurilaitetta.



Kuva 6. Palomuurin lisääminen verkkoon

Etähallinta toteutettiin remote access -tyypisellä IPSec VPN-ratkaisulla. Etätietokone tarvitsi VPN-yhteyden muodostamiseen erikseen asennetun IPSec-asiakasohjelmiston, joka tässä tapauksessa oli Cisco VPN Client. Kun VPN-yhteys oli muodostettu, etäkäyttäjä sai palomuurilta yksityisen IP-osoitteen, jolla oli oikeudet liikennöidä sisä- ja eteisverkkoon. Käyttäjien tunnistukseen käytettiin palomuuriin luotuja paikallisia käyttäjätunnuksia.

5.4 Laitteiston valinta

Laitteistoa valittaessa tuli huomioida resurssien riittävyys, luotettavuus, hinta, ominaisuudet, skaalautuvuus sekä 3G-tuki. Laitteistoa valittaessa päädyttiin käyttämään Cisco Systemsin reititin-laitteita, koska testiympäristössä käytetyt laitteet olivat myös Ciscon reitittimiä ja niiden käyttämä Cisco IOS-käyttöjärjestelmä oli entuudestaan tuttu. VPN-ratkaisuja tehdään perinteisesti palomuurilaitteilla. Työssä tutkittiin tätäkin

mahdollisuutta, mutta päädyttiin reitittimiin niiden parempien reititysominaisuuksien, sekä DMVPN tuen takia, mitä ei palomuureista löytynyt.

5.4.1 Keskusreititin

Keskusreitittimeksi valittiin Cisco Systemsin 2921 Integrated Services Router Generation 2 (ISR G2) reititin securitylisenssillä. Laitteeseen lisättiin 512 Mt muistia, jolloin muistin määrä oli yhteensä 1 Gt. Gigabit Ethernet -portteja reitittimessä oli kolme ja siinä oli sisäänrakennettu VPN-moduuli.

Kuva 7. Cisco 2921 ISR –reititin (10)

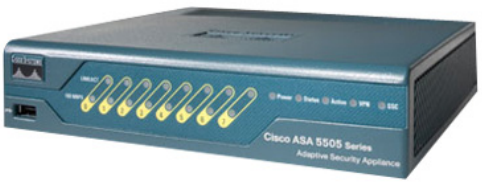
5.4.2 Reunareititin

Reunareitittimen tärkein ominaisuus oli 3G-tuki, joka rajoitti vaihtoehtoja huomattavasti. Valinnassa päädyttiin Cisco Systemsin 881G ISR reitittimeen, johon sisältyi erillinen 3G moduuli. FastEthernet -portteja laitteessa oli viisi, joista yksi oli WAN -portti.

Kuva 8. Cisco 881G ISR –reititin (11)

5.4.3 Palomuuri

Palomuuria valittaessa tuli ottaa huomioon käytettävä VPN-yhteyskäytäntö sekä aktiivisten yhteyksien yhtäaikainen määrä. Koska VPN-yhteyksien lukumäärä oli pieni eikä liikenteen määrä ollut muutenkaan suuri, päädyttiin Cisco ASA 5505-malliin. Palomuuriin oli saatavilla kaksi lisenssiä: basic ja security plus. Basic-lisenssissä oli monia rajoituksia. Se esimerkiksi tuki vain kolmea aktiivista virtuaalista lähiverkkoa, jolloin eteisalueelta ei voitu liikennöidä sisäverkkoon. Tästä johtuen lisenssiksi valittiin Security Plus, sillä se tuki maksimissaan kahtakymmentä virtuaalista lähiverkkoa (VLAN). Suurin yhtäaikaisten IPSec VPN-yhteyksien määrä oli 25. Ethernet –portteja palomuurissa oli kahdeksan. (12)



Kuva 9. Cisco ASA 5505-palomuuri (13)

6 LAITTEISTOJEN KONFIGURAATIOT

Tärkeimmät konfiguroitavat kokonaisuudet olivat keskusreitittimessä DMVPN-pilvi ja virtuaalinen reititystaulu (VRF), joita voitiin luoda lisää tarpeen mukaan. Reunalaitteessa huomiota vaati 3G-yhteyden konfigurointi. Lisäksi reunalaitteeseen lisättiin ominaisuus, jossa 3G-yhteyttä käytettiin varayhteytenä. Palomuuriin tehtiin IPSec VPN etähallintaa varten. Lisäksi pääsylistoilla sallittiin muun muassa www-palvelimen kommunikoida sisäverkon tietokantapalvelimen kanssa.

6.1 Keskusreititin

Uutta DMVPN-pilveä varten luotiin uusi virtuaalinen reititystaulu (VRF), johon myös mGRE-tunneli myöhemmin liitettiin. VRF:lle annettiin nimi Datariina.

```
keskus(config)#ip vrf Datariina
```

Määriteltiin IPSec:n käyttämä avaimenvaihtopolitiikka.

```
keskus(config)#crypto isakmp policy 1
keskus(config-isakmp)#encr 3des
keskus(config-isakmp)#authentication pre-share
keskus(config-isakmp)#group 2
```

Määritettiin IPSec:n käyttämä avain sekä hyväksyttävät IP-osoitteet. Avaimeksi laitettiin salasana ja hyväksyttäviksi IP-osoitteiksi kaikki osoitteet.

```
keskus(config)#crypto isakmp key salasana address 0.0.0.0 0.0.0.0
```

Määriteltiin IPSec:n käyttämä salausalgoritmit.

```
keskus(config)#crypto ipsec transform-set salaus esp-3des esp-sha-hmac
keskus(cfg-crypto-trans)#mode transport
```

Luotiin IPSec profiili, joka määritettiin käyttämään edellä luotua salausta

```
keskus(config)#crypto ipsec profile Profile1
```

```
keskus(ipsec-profile)#set transform-set salaus
```

Seuraavaksi luotiin mGRE-tunneli liityntäportti, joka liitettiin aiemmin luotuun VRF Datariinaan. Kyseiseen virtuaaliseen reititystauluun kuuluvat reunalaitteet liittyivät siis tähän tunneliin. Tunnelin aliverkko oli 1.1.1.0/24.

```
keskus(config)#interface Tunnel1
keskus(config-if)#ip vrf forwarding Datariina
keskus(config-if)#ip address 1.1.1.1 255.255.255.0
keskus(config-if)#no ip redirects
keskus(config-if)#ip mtu 1400
keskus(config-if)#ip hello-interval eigrp 1 30
keskus(config-if)#ip hold-time eigrp 1 90
keskus(config-if)#ip nhrp authentication datis
keskus(config-if)#ip nhrp map multicast dynamic
keskus(config-if)#ip nhrp network-id 1
keskus(config-if)#ip nhrp holdtime 360
keskus(config-if)#ip tcp adjust-mss 1360
keskus(config-if)#tunnel source GigabitEthernet0/1
keskus(config-if)#tunnel mode gre multipoint
keskus(config-if)#tunnel key 1
keskus(config-if)#tunnel protection ipsec profile Profile1 shared
```

Reititysprotokollaa valittaessa päädyttiin käyttämään EIGRP:tä sen split-horizon ominaisuuden takia. Tämän ominaisuuden ansiosta reunareitittimet eivät näkyneet toisilleen. Seuraavaksi määriteltiin, mitä verkkoja reititysprotokolla mainostaa VRF Datariinaan kuuluville reunalaitteille.

```
keskus(config)#router eigrp 1
keskus(config-router)#address-family ipv4 vrf Datariina
keskus(config-router-af)#network 1.1.1.0 0.0.0.255
keskus(config-router-af)#network 9.9.9.9 0.0.0.0
keskus(config-router-af)#network 192.168.100.0
keskus(config-router-af)#autonomous-system 10
keskus(config-router-af)#exit-address-family
```

Määritettiin sisäverkon liityntäportti, joka välitti liikenteen palvelimelle. Liityntäportti jaettiin aliliityntäportteihin, jotka kuuluivat eri VRF:iin ja niillä oli omat VLAN-numeronsa.

```
keskus(config)#interface GigabitEthernet0/0
keskus(config-if)#no shutdown
keskus(config-if)#interface GigabitEthernet0/0.1
keskus(config-subif)#encapsulation dot1Q 100
keskus(config-subif)#ip vrf forwarding Datariina
keskus(config-subif)#ip address 192.168.100.1 255.255.255.0
```

6.2 Reunareititin

Reunareitittimen konfiguraatio jaettiin kolmeen tärkeimpään kokonaisuuteen: 3G, VPN ja varayhteys. Käytössä oli Saunalahden 3G liittymä nopeudella 1Mb/s.

6.2.1 3G-modeemi

Ensimmäiseksi oli tarkoitus saada modeemi kommunikoimaan reitittimen kanssa. Tämä tapahtui telnet-yhteydellä reitittimen sisältä. Konfiguroitiin seuraavat komennot:

```
reuna(config)#interface Loopback0
reuna(config-if)#ip address 128.1.1.1 255.255.255.255

reuna(config)#line 3
reuna(config-line)#exec-timeout 0 0
reuna(config-line)#script dialer gsm
reuna(config-line)#modem InOut
reuna(config-line)#no exec
reuna(config-line)#transport input all
```

Seuraavaksi muodostettiin telnet-yhteys loopback0 liityntäporttiin komennolla:

```
reuna#telnet 128.1.1.1 2003
```

Komennon lopussa oleva ”2003” kuvasi linjanumeroa kolme.

Telnet-yhteyden avauduttua alettiin konfiguroida modeemia. Komennolla AT!CUSTOM? tarkastettiin modeemin olemassa olevat asetukset. Asetuksista muutettiin ainoastaan PRLREGION vastaamaan Euroopan arvoa 01. Oletuksena tämä oli 02, mikä on Pohjois-Amerikan maantieteellinen numero. Tämä komento määrittää modeemin käyttämään oikeita taajuusalueita. Tämän jälkeen asetukset olivat seuraavat:

```
AT!ENTERCND=”A710”
AT!SLEEP=1
AT!NVOEM=GMSCLASS,0C
AT!NVOEM=EMSCLASS,0C
AT!CUSTOM=”MEPCODE”,1
AT!CUSTOM=”MEPLOCK”,0
AT!NVPLMN=505,01
AT!SCDFTPROF=1
AT!CUSTOM=”PRLREGION”,01 (Maantieteellisen alueen numero)
AT!GBAND=0000000004000380
AT!BAND=03
AT!RESET
```

Ensin piti ottaa käyttöön sim-kortti. 0000 oli sim-kortin pin-koodi.

```
reuna(config)#cellular 0 gsm sim unlock 0000
```

Tämän jälkeen luotiin yhdistettäessä käytettävä profiili. Komennossa numero 1 kertoo luotavan profiilin numeron, ”internet.saunalahti” on Saunalahden tukiaseman nimi, chap kertoo autentikointimetodin sekä ”group” ja ”group” ovat autentikoinnin arvot eli username ja password, jotka voidaan valita mielivaltaisesti.

```
reuna(config)#cellular 0 gsm profile create 1 internet.saunalahti chap
group group
```

Chat scriptin luonti. Tämän avulla reititin ottaa yhteyden 3G verkkoon.

```
reuna(config)#chat-script gsm "" "ATDT*98*1#" TIMEOUT 60
"CONNECT"
```

Seuraava vaihe oli konfiguroida cellular liityntäportti, josta 3G yhteys muodostuu.

```
reuna(config)#interface Cellular0
reuna(config-if)#no ip address
reuna(config-if)#ip virtual-reassembly
reuna(config-if)#encapsulation ppp
reuna(config-if)#no ip route-cache cef
reuna(config-if)#load-interval 60
reuna(config-if)#dialer in-band
reuna(config-if)#dialer pool-member 1
reuna(config-if)#dialer idle-timeout 0
reuna(config-if)#dialer-group 1
reuna(config-if)#async mode interactive
reuna(config-if)#fair-queue 64 16 0
reuna(config-if)#ppp chap hostname group
reuna(config-if)#ppp chap password 0 group
reuna(config-if)#ppp ipcp dns request
reuna(config-if)#routing dynamic
```

Konfiguroitiin dialer liityntäportti, jota cellular liityntäportti kutsuu yhteyttä muodostaessa.

```
reuna(config)#interface Dialer1
reuna(config-if)#ip address negotiated
reuna(config-if)#ip virtual-reassembly
reuna(config-if)#no ip route-cache cef
reuna(config-if)#dialer pool 1
reuna(config-if)#dialer string gsm
reuna(config-if)#dialer-group 1
reuna(config-if)#no cdp enable
```

Kiinnostava liikenne määriteltiin pääsylistalla komennolla:

```
reuna(config)#access-list 1 permit any
reuna(config)#dialer-list 1 protocol ip permit
```

Jotta dialer liityntäportti säilyttäisi katkeamattoman yhteyden 3G-verkkoon, oli reitittimen luotava liikennettä tietyin väliajoin. Ratkaisuna toimi IP SLA, jonka avulla reititin lähetti ICMP Echo paketteja (ping) Googlen DNS-palvelimen osoitteeseen 15 sekunnin välein.

```
reuna(config)#ip sla 1
reuna(config-ip-sla)#icmp-echo 8.8.8.8
reuna(config-ip-sla)#frequency 15
reuna(config)#ip sla schedule 1 life forever start-time now
```

6.2.2 VPN-yhteys ja reititys

IPSec:n avaimenvaihtopolitiikka, suojausalgoritmit ja profiili määriteltiin vastaaviksi keskusreitittimen kanssa. Koska reunareititin muodostaa VPN-yhteyden vain keskusreitittimen kanssa, korvattiin neljä nollaa keskuslaitteen staattisella WAN IP-osoitteella.

```
reuna(config)#crypto isakmp key salasana address <keskus WAN IP-
osoite ja maski>
```

Luotiin 3G-yhteyden tunneliliityntäportti.

```
reuna(config)#interface Tunnel0
reuna(config-if)#description VPN via 3G
reuna(config-if)#ip address 1.1.1.2 255.255.255.0
reuna(config-if)#ip mtu 1400
reuna(config-if)#ip hello-interval eigrp 10 30
reuna(config-if)#ip hold-time eigrp 10 90
reuna(config-if)#ip nhrp authentication datis
reuna(config-if)#ip nhrp map multicast <keskus WAN IP-osoite>
reuna(config-if)#ip nhrp map 1.1.1.1 <keskus WAN IP-osoite>
reuna(config-if)#ip nhrp network-id 1
reuna(config-if)#ip nhrp holdtime 360
```

```
reuna(config-if)#ip nhrp nhs 1.1.1.1
reuna(config-if)#ip nhrp registration no-unique
reuna(config-if)#ip tcp adjust-mss 1360
reuna(config-if)#tunnel source Dialer1
reuna(config-if)#tunnel destination <keskus WAN IP-osoite>
reuna(config-if)#tunnel key 1
reuna(config-if)#tunnel protection ipsec profile Profile1 shared
```

Määriteltiin verkot, joita reititysprotokolla mainostaa.

```
reuna(config)#router eigrp 10
reuna(config-router)#network 1.1.1.0 0.0.0.255
reuna(config-router)#network 172.16.90.1 0.0.0.0
reuna(config-router)#network 172.16.100.0 0.0.0.255
```

6.2.3 Varayhteys

Kun varayhteys oli käytössä, tunneliliityntäportteja oli kaksi. Tunnelit olivat lähes identtiset, sillä ainoastaan tunnelin numero ja lähdeliityntäportit erosivat toisistaan. Luotiin toinen tunneli kiinteälle Internet-yhteydelle, joka tässä tapauksessa muodostui FastEthernet4- liityntäportista. Edellä luodusta tunnelista vain kaksi komentoa muutettiin. Kun uusi tunneli oli luotu, oli tärkeä huomioida, että vain yksi tunneli oli samanaikaisesti päällä.

```
reuna(config)#interface Tunnel1
reuna(config-if)#description VPN via lankayhteys
reuna(config-if)#tunnel source FastEthernet4
```

Luotiin IP SLA, joka tarkkaili kiinteän Internet yhteyden tilaa pingaamalla keskusreitittimen IP-osoitetta kymmenen sekunnin välein.

```
reuna(config)#ip sla 2
reuna(config-ip-sla)#icmp-echo <keskus WAN IP> source-interface
FastEthernet4
reuna(config-ip-sla)#frequency 10
reuna(config)#ip sla schedule 2 life forever start-time now
```

Luotiin track 1, jonka tehtävänä oli tarkkailla onnistuiko edellä määritellyn IP SLA 2 ping. Kun track 1 saavutettavuus oli tilassa UP, lankayhteys toimi, jolloin myös VPN-yhteys muodostui tunnel1 liityntäportista. Vastaavasti, kun tila oli DOWN, lankayhteys ei ollut toiminnassa ja VPN-yhteyden muodostamiseen käytettiin 3G-yhteyttä.

```
reuna(config)#track 1 ip sla 2 reachability
```

Ciscon Embedded Event Managerilla määriteltiin tietyn track 1 tilan mukaan suoritettavat komentorivikäskyt. Tunneliliityntäportin avaamisen ja sulkemisen lisäksi, EEM täytyi myös kertoa reitittimelle uusi oletusreitti Internetiin riippuen liityntäportista, josta liikennöitiin. Luotiin kaksi EEM appletia, jotka nimettiin kiinteän yhteyden tilan mukaan, kiintea_ei_toimi ja kiintea_toimii.

Kun kiinteä yhteys katkesi, sitä kautta muodostettu tunneli tunnel1 suljettiin ja 3G:n kautta muodostettu tunneli tunnel0 käynnistettiin. Lisäksi vanha lankayhteyden käyttämä oletusreitti poistettiin ja lisättiin uusi oletusreitti osoittamaan 3G-yhteyden liityntäporttia.

```
reuna(config)#event manager applet Kiintea_ei_toimi
reuna(config-applet)#event track 2 state down
reuna(config-applet)#action A1 cli command "enable"
reuna(config-applet)#action A2 cli command "configure terminal"
reuna(config-applet)#action A3 cli command "no ip route 0.0.0.0 0.0.0.0
FastEthernet4"
reuna(config-applet)#action A4 cli command "ip route 0.0.0.0 0.0.0.0
dialer1"
reuna(config-applet)#action A5 cli command "interface tunnel 1"
reuna(config-applet)#action A6 cli command "shutdown"
reuna(config-applet)#action A7 cli command "exit"
reuna(config-applet)#action A8 cli command "interface tunnel 0"
reuna(config-applet)#action A9 cli command "no shutdown"
```

Vastaavasti, kun kiinteä yhteys palautui, 3G liityntäporttiin ohjaava oletusreitti poistettiin ja uusi oletusreitti lisättiin. Lisäksi 3G VPN tunneli suljettiin ja kiinteän yhteyden VPN tunneli avattiin.

```
reuna(config)#event manager applet Kiintea_toimii
reuna(config-applet)#event track 2 state up
reuna(config-applet)#action A1 cli command "enable"
reuna(config-applet)#action A2 cli command "configure terminal"
reuna(config-applet)#action A3 cli command "no ip route 0.0.0.0 0.0.0.0
dialer1"
reuna(config-applet)#action A4 cli command "ip route 0.0.0.0 0.0.0.0
FastEthernet4"
reuna(config-applet)#action A5 cli command "interface tunnel 0"
reuna(config-applet)#action A6 cli command "shutdown"
reuna(config-applet)#action A7 cli command "exit"
reuna(config-applet)#action A8 cli command "interface tunnel 1"
reuna(config-applet)#action A9 cli command "no shutdown"
```

6.3 Palomuuri

Ensimmäisenä määriteltiin mitkä VLAN:t kuuluivat sisäverkkoon (inside), eteisalueeseen (DMZ) ja ulkoverkkoon (outside), luotiin niille SVI:t (Switched Virtual Interface) ja annettiin niille IP-osoitteet. Samalla määritellään verkoille turvallisuustasot, jotka olivat oletuksina sisäverkolle 100 ja ulkoverkolle 0. Eteisalueelle annettiin turvallisuustasoksi 50.

```
ciscoasa(config)#interface Vlan1
ciscoasa(config-if)#description INSIDE
ciscoasa(config-if)#nameif inside
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#ip address 192.168.1.1 255.255.255.0

ciscoasa(config)#interface Vlan2
ciscoasa(config-if)#description OUTSIDE
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)# ip address <WAN IP-osoite>
```

```
ciscoasa(config)#interface Vlan3
ciscoasa(config-if)#description DMZ
ciscoasa(config-if)#nameif dmz
ciscoasa(config-if)#security-level 50
ciscoasa(config-if)#ip address 192.168.2.1 255.255.255.0
```

Pääsylistoja tarvittiin NAT:in tekoon sekä SQL-kyselyiden sallimiseen eteisverkon www-palvelimelta sisäverkon tietokantapalvelimeen. Myös ICMP ECHO sallittiin.

```
ciscoasa(config)#access-list dmz-entry extended permit tcp host
192.168.2.52 host 192.168.1.52 eq 1433
ciscoasa(config)#access-list dmz-entry extended permit icmp host
192.168.2.52 host 192.168.1.52 echo-reply
ciscoasa(config)#access-group dmz-entry in interface dmz
```

Sallittiin ulkoa tuleva http ja https liikenne eteisalueen julkiseen palvelimeen.

```
ciscoasa(config)#access-list outside-entry extended permit tcp any host
<WAN IP> eq www
ciscoasa(config)#access-list outside-entry extended permit tcp any host
<WAN IP> eq https
ciscoasa(config)#access-group outside-entry in interface outside
```

Tehtiin http ja https liikenteelle porttiohjaus www-palvelimelle.

```
ciscoasa(config)#static (dmz,outside) tcp interface www 192.168.2.52
www netmask 255.255.255.255
ciscoasa(config)#static (dmz,outside) tcp interface https 192.168.2.52
https netmask 255.255.255.255
```

NAT poistettiin sisäverkon ja eteisverkon väliltä sekä VPN-yhteyksien käyttämästä 10.10.10.0/24 aliverkosta. Tätä varten luotiin pääsylistat.

```
ciscoasa(config)#access-list nat extended permit ip 192.168.1.0
255.255.255.0 192.168.2.0 255.255.255.0
```

```
ciscoasa(config)#access-list nat extended permit ip any 10.10.10.0
255.255.255.0
ciscoasa(config)#nat (inside) 0 access-list nat
ciscoasa(config)#access-list dmznat extended permit ip 192.168.2.0
255.255.255.0 192.168.1.0 255.255.255.0
ciscoasa(config)#access-list dmznat extended permit ip any 10.10.10.0
255.255.255.0
ciscoasa(config)#nat (dmz) 0 access-list dmznat
```

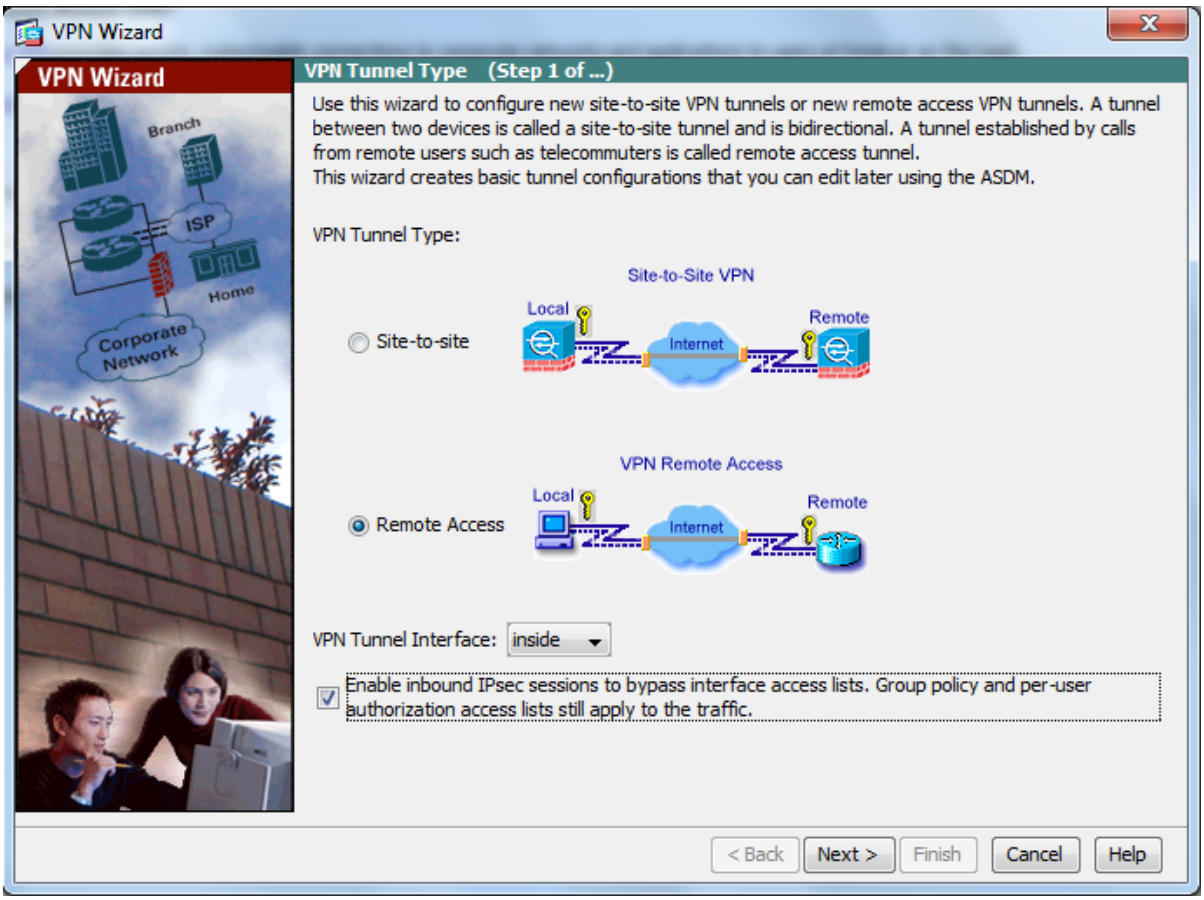
NAT suoritettiin muulle liikenteelle.

```
ciscoasa(config)#global (outside) 1 interface
ciscoasa(config)#nat (inside) 1 0.0.0.0 0.0.0.0
ciscoasa(config)#nat (dmz) 1 0.0.0.0 0.0.0.0
```

Hallinta VPN luotiin käyttäen Adaptive Security Device Manageria (ASDM). ASDM avattiin kirjoittamalla selaimen osoiteriville palomuurin hallinta IP-osoite eli https://192.168.1.1. Lisäksi palomuuriin tuli määritellä, mistä verkosta ASDM-yhteys sallittiin.

```
ciscoasa(config)#http server enable
ciscoasa(config)#http 192.168.1.0 255.255.255.0 inside
```

ASDM-käyttöliittymästä käynnistettiin VPN wizard, josta valittiin remote access-yhteystyyppi. Valittiin kohta, jossa sisääntulevat IPSec-istunnot määriteltiin ohittamaan pääsylistat.



Kuva 8. ASDM VPN wizard.

Määritettiin IP-osoitealue, josta etäkoneille jaettiin osoitteet. Lisäksi otettiin käyttöön split tunneling, jonka avulla etäkoneet pystyivät samanaikaisesti liikennöimään sekä Internetiin että VPN tunnelin kautta Asan inside ja DMZ verkkoihin, eli osoitealueisiin 192.168.1.0/24 ja 192.168.2.0/24 menevä liikenne ohjattiin VPN-tunneliin. Lisäksi luotiin ja nimettiin VPN-yhteyksien käyttämä ryhmä ja annettiin sille salasana.

VPN-yhteys muodostettiin käyttämällä Cisco VPN asiakasohjelmistoa. Yhteyttä muodostettaessa tarvittiin palomuurin julkinen IP-osoite sekä edellä luodun ryhmän nimi ja jaettu salasana. Lisäksi käyttäjä tunnistettiin palomuurin paikallisilla käyttäjätunnuksilla.

7 TESTITULOKSET JA YHTEENVETO

Tärkeimmät testit 3G-yhteyden kannalta olivat sen luotettavuus, nopeus ja palautuvuus. Luodun IP SLA:n avulla sekä dialerin timeout-arvoa muuttamalla (dialer idle-timeout 0) yhteys matkapuhelinverkkoon pysyi katkeamattomana. Palautuvuutta testattiin sulkemalla ja avaamalla dialer-liityntäportti. Yhteys palautui muutamassa se-

kunnissa. Yhteyden teoreettinen maksimi nopeus oli 1Mb/s, mutta todellinen nopeus oli keskimäärin 300kb/s.

Varayhteyden toimintaa testattiin yksinkertaisesti ottamalla lankayhteyden käyttämä kaapeli irti seinästä. Palautuminen tapahtui alle kymmenessä sekunnissa, riippuen siitä siirryttiinkö lankayhteydestä 3G-yhteyteen vai toisinpäin. Kuitenkin varayhteyden testaaminen jäi liian vähäiselle määrälle, ja esimerkiksi reitittimen uudelleen käynnistyminen virtojen katketessa tuotti välillä virhetilanteita. Tästä syystä varayhteyttä ei otettu vielä tuotantoon mukaan ja se jäi osittain kehitysasteelle.

Laitteiden lisäys samaan DMVPN-pilveen monistamalla reunalaitteen pohjakonfiguraatio oli yksinkertaista eikä vaatinut keskusreitittimen konfigurointia. Reunalaitteen lisääminen uuteen DMVPN-pilveen vaati myös keskusreitittimen konfigurointia. VRF:n toiminta varmistettiin käyttämällä päällekkäisiä IP-osoitteita eri pilvien päätelaitteissa onnistuneesti. Reititysprotokolla EIGRP:n osalta testattiin verkon konvergoitumista, joka tapahtui noin minuutissa.

Käytetyistä protokollista osa on tuettu ainoastaan Cisco Systemsin IOS käyttöjärjestelmän omaavissa laitteissa. Tämä tekee DMVPN-ratkaisusta toimivan ainoastaan Ciscon laitteilla. Huomioitavaa kuitenkin on, että Ciscon palomuurilaitteet eivät tue tätä ratkaisua niiden GRE-tuen puutteen takia.

VPN-nopeutta testattiin yhdistämällä keskusreititin ja reunareititin toisiinsa suoraan 100 Mb/s linkillä. Pullonkaulaksi muodostui 881G-reititin, joka pystyi parhaimmillaan 10Mb/s salausnopeuteen. Keskusreitittimelle tämä merkitsi 10 % prosessorin käyttöä.

Laboratorio-olosuhteissa saavutetut tulokset olivat järjestelmän kannalta hyvät. Kaikkia käytännön ongelmia ei kuitenkaan pienestä laitemäärästä johtuen pystytty testaamaan. Välityskyky sekä prosessorin ja muistin käyttö jäi siis vähäiselle testaukselle huomioiden, että laitteiden määrän kasvaessa resurssien käyttö ei välttämättä kasva lineaarisesti.

Palveluntarjoajat tarjoavat erilaisia liittymiä erilaisiin tarkoituksiin. 3G-liittymää valittaessa otettiin huomioon mahdolliset palomuurit tai muut estot, jotka voivat rajoittaa joitakin protokollia. Esimerkiksi laboratoriossa alkuun käytössä olleen Soneran 3G dataliittymän WAN IP-osoitteen pingaus oli estetty.

Kokonaisuudessaan järjestelmän palautuminen sähkökatkoista oli kiitettävä: virtojen palautumisesta kesti noin kolme minuuttia koko verkon konvergoitumiseen.

Vastaavanlaisia ratkaisuja tarjotaan myös operaattoreiden puolesta, mutta jos halutaan säilyttää kokonaisuuden hallinta, on itsenäinen VPN-verkko hyvä ratkaisu. Tämä ratkaisu vaatii erillistä ylläpitoa, mutta järjestelmän kasvaessa on se kuitenkin suhteellisen yksinkertaista, mikäli verkolle on luotu hyvä pohja.

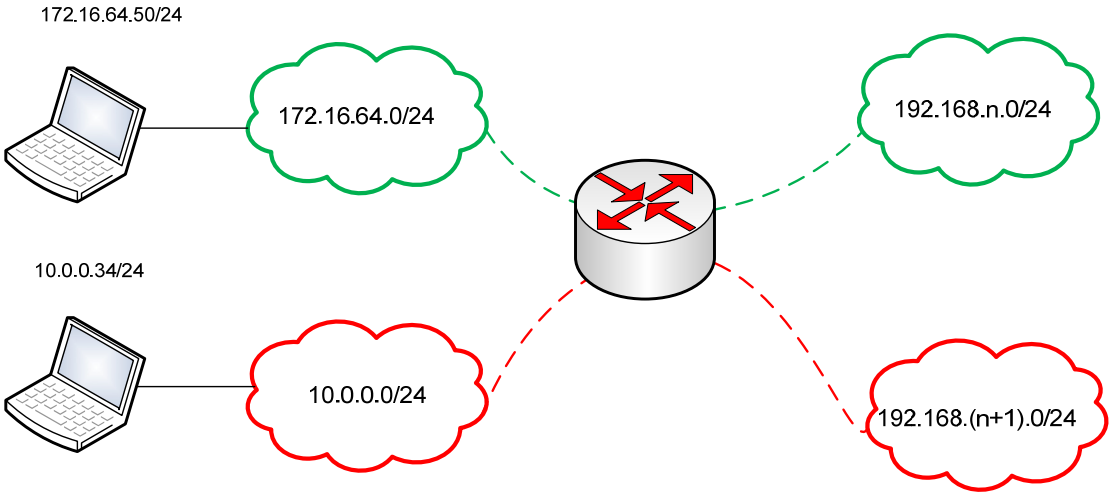
8 JATKOKEHITYS

Työssä tutkitulle ja rakennetulle verkolle jäi vielä jatkokehitystarpeita ja -mahdollisuuksia. Reunalaitteiden varayhteyden toimintaa kehitettiin sietämään reitittimen uudelleen käynnistymisen. Täysin valmiiksi varayhteyttä ei kuitenkaan saatu vähäisen testausajan vuoksi.

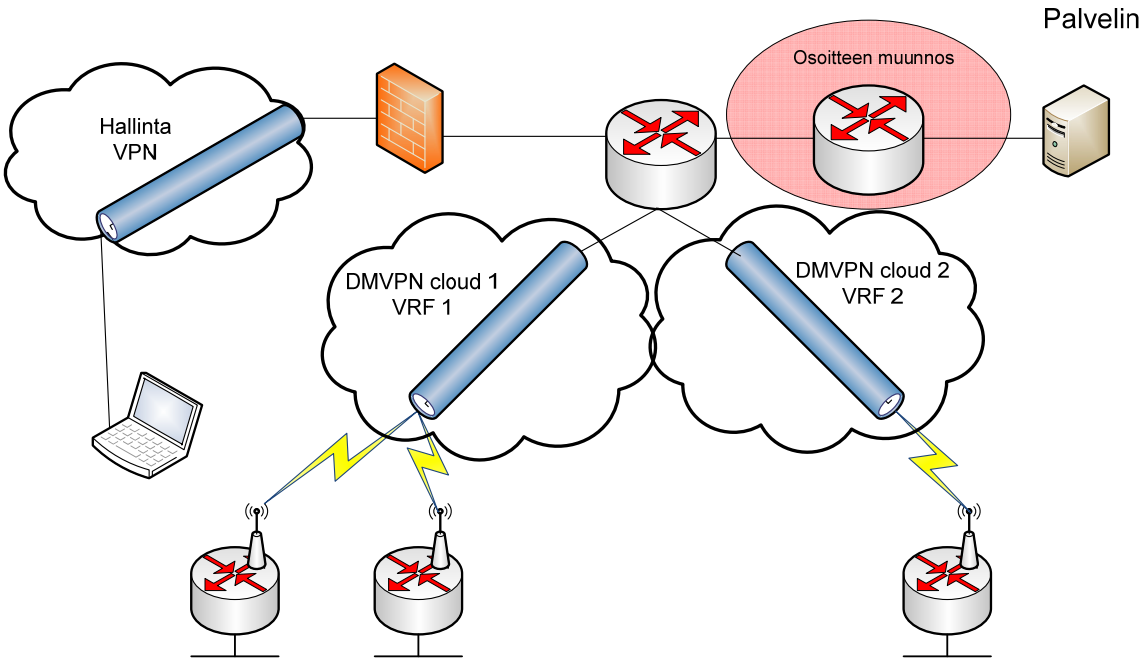
Tulevaisuutta ajatellen tämänkaltainen ratkaisu tarvitsee verkonhallintaa. Verkko nykyisessä muodossaan on helppo ylläpitää ja vikatilanteet löytyvät nopeasti. Laitemäärän kasvaessa tilanne mutkistuu. Keskitetty verkonvalvonta käyttäen Simple Network Management Protokollaa (SNMP) on seuraava tärkeä jatkokehityshanke.

Reunalaitteiden määrän kasvaessa verkon luotettavuuden ja saatavuuden tärkeys lisääntyy. Tästä syystä keskusreitittimen kahdennus on myös tärkeä kehitysaskel tulevaisuudessa.

Verkon mahdollista suurta kasvua varten on tärkeää luoda sille hyvä pohja. Verkon skaalautuvuuden kannalta olisi järkevä muuntaa kaikki reunaverkkojen osoitteet halutuiksi osoitteiksi. Tämän avulla myös osoitteiden ylläpidosta ja dokumentoinnista tulisi järkevä ja johdonmukainen. Muunnos voidaan toteuttaa joko pelkillä IPv4 osoitteilla, tai upottaen IPv4 osoitteet IPv6 osoitteisiin, mikä jouduttaisi palvelimien IPv6 migraatiota. Alla esimerkki siitä kuinka osoitteenmuunnos voitaisiin toteuttaa IPv4 osoitteilla.



Kuva 9. Osoitteenmuunnos 4to4.



Kuva 10. Valmis verkko ja tulevaisuus.

LÄHTEET

1. Frahim, J. & Huang, Q. 2008. SSL Remote Access VPNs. Indianapolis, USA: Cisco Press

2. Petr Lapukhov. DMVPN Explained. Saatavissa: http://blog.ine.com/2008/08/02/dmvpn-explained/ [viitattu 17.1.2012]

3. Cisco Systems: Dynamic Multipoint VPN (DMVPN). Saatavissa: http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftgreips.html [viitattu 17.1.2012]

4. Generic Routing Encapsulation (GRE). Saatavissa: http://tools.ietf.org/html/rfc1701 [viitattu 17.1.2012]

5. Cisco Systems: NHRP. Saatavissa: http://www.cisco.com/en/US/docs/ios/12_4/ip_addr/configuration/guide/hadnhrp.html [viitattu 18.1.2012]

6. Security Architecture for the Internet Protocol. Saatavissa: http://tools.ietf.org/html/rfc4301#page-4 [viitattu 18.1.2012]

7. Teare, D. 2010. Implementing Cisco IP Routing. Indianapolis: Cisco Press

8. Wikipedia: 3G. Saatavissa: http://en.wikipedia.org/wiki/3G [viitattu 18.1.2012]

9. Pietiläinen, J. 2011 Opinnäytetyö: Matkapuhelinverkon dataratkaisut ja niiden ongelmatilanteita. Savonia-ammattikorkeakoulu. Saatavissa: https://publications.theseus.fi/bitstream/handle/10024/33307/Pietilainen_Jussi.pdf?sequence=1 [viitattu 18.1.2012]

10. Cisco Systems tuote-esittely: http://www.cisco.com/en/US/products/ps10543/index.html

11. Cisco Systems: http://www.cisco.com/en/US/prod/collateral/routers/ps380/ps10082/data_sheet_c78_498096.html

12. Cisco ASA 5505 Vlans and Licensing. Saatavissa: http://www.networkstraining.com/cisco-asa-5505-vlans-and-licensing/ [viitattu 4.5.2012]

13. Cisco Systems: Tuotevertailu http://www.cisco.com/en/US/products/ps6120/prod_models_comparison.html

Keskusreititimen konfiguraatio Liite 1

```
Current configuration : 2812 bytes
!!
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname keskus
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$MFm5$xpBfvATo0k3eSkTLw3NTH15
!
aaa new-model
!
aaa session-id common
!
memory-size iomem 10
!
no ipv6 cef
ip source-route
ip cef
!
ip vrf datariina
 description Yritykset
!
multilink bundle-name authenticated
!
license udi pid CISCO2921/K9 sn FCZ1529709S
!
archive
 log config
```

```
 hidekeys
!
redundancy
!
ip ssh version 1
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp policy 2
crypto isakmp key salasana address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile Profile1
 set transform-set ESP-3DES-SHA
!
interface Loopback10
 description telnet source interface
 ip vrf forwarding datariina
 ip address 9.9.9.9 255.255.255.255
!
interface Tunnel0
 no ip address
!
interface Tunnel1
 ip vrf forwarding datariina
 ip address 1.1.1.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip hello-interval eigrp 1 30
 ip hold-time eigrp 1 90
```

```
 ip nhrp authentication salasana
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 ip nhrp holdtime 360
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
 tunnel key 1
 tunnel protection ipsec profile Profile1 shared
!
interface GigabitEthernet0/0
 description Fyysinen inside portti
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.1
 description Datariinan liityntaportti
 encapsulation dot1Q 100
 ip vrf forwarding datariina
 ip address 192.168.100.1 255.255.255.0
!
interface GigabitEthernet0/1
 description WAN
 ip address <WAN IP ja maski>
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 description To ASA
 ip address 192.168.1.2 255.255.255.0
 duplex auto
 speed auto
 !
router eigrp 1
```

```
 !
 address-family ipv4 vrf datariina
  network 1.1.1.0 0.0.0.255
  network 9.9.9.9 0.0.0.0
  network 192.168.100.0
  autonomous-system 10
 exit-address-family
!
ip forward-protocol nd
!
no ip http server
ip http authentication local
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/1
ip route 10.10.10.0 255.255.255.0 192.168.1.1
!
ip access-list extended telnet
 permit tcp 10.10.10.0 0.0.0.255 any eq telnet
 deny   tcp any any eq telnet
!
control-plane
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 access-class telnet in
 transport input telnet ssh
!
scheduler allocate 20000 1000
end
```

```
Current configuration : 5954 bytes
!
version 15.1
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname reuna
!
boot-start-marker
boot-end-marker
!
logging buffered 51200 warnings
enable secret 5 $1$g2gJ$9zJTIoMfFKqIaldevZ4BE0
!
no aaa new-model
!
memory-size iomem 10
!
crypto pki trustpoint TP-self-signed-2069101921
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2069101921
 revocation-check none
 rsakeypair TP-self-signed-2069101921
!
crypto pki certificate chain TP-self-signed-2069101921
 certificate self-signed 01
ip source-route
!
ip cef
no ip domain lookup
ip domain name yourdomain.com
```

```
no ipv6 cef
!
multilink bundle-name authenticated
chat-script gsm "" "ATDT*98*1#" TIMEOUT 60 "CONNECT"
license udi pid CISCO881G-G-K9 sn FCZ152392VW
!
no spanning-tree vlan 1
username admin privilege 15 password 0 salasana
!
controller Cellular 0
!
track 1 ip sla 1 reachability
!
track 2 ip sla 2 reachability
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key salasana address <WAN IP>
!
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile SDM_Profile1
 set transform-set ESP-3DES-SHA
!
interface Loopback0
 ip address 128.1.1.1 255.255.255.255
!
interface Loopback111
 ip address 172.16.90.1 255.255.255.0
!
interface Tunnel0
shutdown
```

```
 description VPN via 3G
 ip address 1.1.1.2 255.255.255.0
 ip mtu 1400
 ip hello-interval eigrp 10 30
 ip hold-time eigrp 10 90
 ip nhrp authentication salasana
 ip nhrp map multicast <WAN IP>
 ip nhrp map 1.1.1.1 <WAN IP>
 ip nhrp network-id 1
 ip nhrp holdtime 360
 ip nhrp nhs 1.1.1.1
 ip nhrp registration no-unique
 ip tcp adjust-mss 1360
 tunnel source Dialer 1
 tunnel destination <WAN IP>
 tunnel key 1
 tunnel protection ipsec profile Profile1 shared
!
interface Tunnel1
 description VPN via lankayhteys
 ip address 1.1.1.2 255.255.255.0
 ip mtu 1400
 ip hello-interval eigrp 10 30
 ip hold-time eigrp 10 90
 ip nhrp authentication salasana
 ip nhrp map multicast <WAN IP>
 ip nhrp map 1.1.1.1 <WAN IP>
 ip nhrp network-id 1
 ip nhrp holdtime 360
 ip nhrp nhs 1.1.1.1
 ip nhrp registration no-unique
 ip tcp adjust-mss 1360
 tunnel source FastEthernet4
 tunnel destination <WAN IP>
 tunnel key 1
```

```
 tunnel protection ipsec profile Profile1 shared
!
interface FastEthernet0
!
interface FastEthernet1
!
interface FastEthernet2
!
interface FastEthernet3
!
interface FastEthernet4
 ip address dhcp
 ip nat inside
 ip virtual-reassembly
 no ip route-cache cef
 no ip route-cache
 duplex auto
 speed auto
!
interface Cellular0
 no ip address
 ip nat outside
 ip virtual-reassembly
 encapsulation ppp
 no ip route-cache cef
 load-interval 60
 dialer in-band
 dialer pool-member 1
 dialer idle-timeout 0
 dialer-group 1
 async mode interactive
 fair-queue 64 16 0
 ppp chap hostname group
 ppp chap password 0 group
 ppp ipcp dns request
```

```
 routing dynamic
!
interface Vlan1
 ip address 172.16.100.1 255.255.255.0
 ip nat inside
 ip nat enable
 ip virtual-reassembly
 no ip route-cache cef
 no ip route-cache
 ip tcp adjust-mss 1452
!
interface Dialer1
 ip address negotiated
 ip nat outside
 ip virtual-reassembly
 no ip route-cache cef
 dialer pool 1
 dialer string gsm
 dialer-group 1
 no cdp enable
!
router eigrp 10
 network 1.1.1.0 0.0.0.255
 network 172.16.90.1 0.0.0.0
 network 172.16.100.0 0.0.0.255
!
router nhrp
!
ip forward-protocol nd
no ip http server
ip http authentication local
no ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip dns server
```

```
ip route 0.0.0.0 0.0.0.0 192.168.106.1
ip route 8.8.8.8 255.255.255.255 Dialer1
ip route <keskus WAN IP> 255.255.255.255 FastEthernet4
!
ip access-list extended telnet
 permit tcp host 9.9.9.9 any eq telnet
!
ip sla 1
 icmp-echo 8.8.8.8
 frequency 15
ip sla schedule 1 life forever start-time now
ip sla 2
 icmp-echo <keskus WAN IP> source-interface FastEthernet4
 frequency 10
ip sla schedule 2 life forever start-time now
access-list 1 permit any
dialer-list 1 protocol ip permit
no cdp run
!
control-plane
!
line con 0
 exec-timeout 0 0
 script dialer gsm
 login local
 no modem enable
line aux 0
 login local
 no exec
 transport input telnet
line 3
 exec-timeout 0 0
 script dialer gsm
 modem InOut
 no exec
```

```
 transport input all
 speed 237000
line vty 0 4
 access-class telnet in
 privilege level 15
 login local
 transport input telnet ssh
!
event manager applet Kiintea_ei_toimi
 event track 2 state down
 action A1 cli command "enable"
 action A2 cli command "configure terminal"
 action A3 cli command "no ip route 0.0.0.0 0.0.0.0 FastEthernet4"
 action A4 cli command "ip route 0.0.0.0 0.0.0.0 dialer1"
 action A5 cli command "interface tunnel 1"
 action A6 cli command "shutdown"
 action A7 cli command "exit"
 action A8 cli command "interface tunnel 0"
 action A9 cli command "no shutdown"
!
event manager applet Kiintea_toimii
 event track 2 state up
 action A1 cli command "enable"
 action A2 cli command "configure terminal"
 action A3 cli command "no ip route 0.0.0.0 0.0.0.0 dialer1"
 action A4 cli command "ip route 0.0.0.0 0.0.0.0 FastEthernet4"
 action A5 cli command "interface tunnel 0"
 action A6 cli command "shutdown"
 action A7 cli command "exit"
 action A8 cli command "interface tunnel 1"
 action A9 cli command "no shutdown"
end
```

```
ASA Version 8.2(5)
!
hostname ciscoasa
enable password OHnuCgWPzhB04re/Cut encrypted
passwd 2KFQnbNIdI.2KYOUe23 encrypted
names
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
 description DMZ interface
 switchport access vlan 3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
```

```
 security-level 0
 ip address <WAN IP> 255.255.255.0
!
interface Vlan3
 nameif dmz
 security-level 50
 ip address 192.168.2.1 255.255.255.0
!
ftp mode passive
access-list dmz-entry extended permit tcp host 192.168.2.52 host 192.168.1.52 eq
3306
access-list dmz-entry extended permit icmp host 192.168.2.52 host 192.168.1.52 echo
access-list dmz-entry extended permit icmp host 192.168.2.52 host 192.168.1.52
echo-reply
access-list dmz-entry extended permit tcp host 192.168.2.52 host 192.168.1.52 eq
www
access-list dmz-entry extended permit tcp host 192.168.2.52 host 192.168.1.52 eq ftp
access-list dmz-entry extended permit icmp host 192.168.2.52 10.10.10.0
255.255.255.0 echo-reply
access-list dmznat extended permit ip 192.168.2.0 255.255.255.0 192.168.1.0
255.255.255.0
access-list dmznat extended permit ip any 10.10.10.0 255.255.255.0
access-list nat extended permit ip 192.168.1.0 255.255.255.0 192.168.2.0
255.255.255.0
access-list nat extended permit ip any 10.10.10.0 255.255.255.0
access-list outside_access_in extended permit icmp any any echo-reply
access-list outside-entry extended permit tcp any host <WAN IP> eq www
access-list outside-entry extended permit tcp any host <WAN IP> eq https
access-list outside-entry extended permit icmp any any echo-reply
access-list inside standard permit 192.168.1.0 255.255.255.0
access-list inside standard permit 192.168.2.0 255.255.255.0
pager lines 24
logging asdm informational
mtu inside 1500
mtu outside 1500
```

mtu dmz 1500
ip local pool vpnpool 10.10.10.10-10.10.10.254 mask 255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list nat
nat (inside) 1 0.0.0.0 0.0.0.0
nat (dmz) 0 access-list dmznat
nat (dmz) 1 0.0.0.0 0.0.0.0
static (dmz,outside) tcp interface www 192.168.2.52 www netmask 255.255.255.255
access-group outside-entry in interface outside
access-group dmz-entry in interface dmz
route outside 0.0.0.0 0.0.0.0 <WAN IP> 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.1.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac

```
crypto ipsec transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set pfs group1
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set transform-set
ESP-AES-128-SHA ESP-AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5
ESP-AES-256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5 ESP-
DES-SHA ESP-DES-MD5
crypto map outside_map 65535 ipsec-isakmp dynamic SYS-
TEM_DEFAULT_CRYPTO_MAP
crypto map outside_map interface outside
crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd auto_config outside
!
dhcpd address 192.168.1.5-192.168.1.254 inside
dhcpd enable inside
!

threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
group-policy DfltGrpPolicy attributes
 dns-server value 8.8.8.8
```

```
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value inside
username PME_admin password HCo2BMADM/Q2Jarw3M encrypted
tunnel-group PME_group type remote-access
tunnel-group PME_group general-attributes
 address-pool vpnpool
tunnel-group PME_group ipsec-attributes
 pre-shared-key *****
!
!
prompt hostname context
no call-home reporting anonymous
Cryptochecksum:84b5d588f54f82873882f27ba3ecf84c
: end
```