Rafael Silvonen

# VPN-tekniikat ja IPSec-tunnelin vikatilanteet

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

15.4.2016

Metropolia

| | |
|---|---|
| Tekijä(t)<br>Otsikko<br><br>Sivumäärä<br>Aika | Rafael Silvonen<br>VPN-tekniikat ja IPSec-tunnelin vikatilanteet<br><br>30 sivua<br>20.4.2016 |
| Tutkinto | Insinööri (AMK) |
| Koulutusohjelma | Tietotekniikka |
| Suuntautumisvaihtoehto | Tietoverkot |
| Ohjaaja(t) | Lehtori Marko Uusitalo<br>Lehtori Jukka Louhelainen |

Tämän opinnäytetyön tarkoituksena on esitellä erilaisia VPN-tekniikoita ja antaa lukijalle avaimet vianetsinnän perusteisiin IPSec-tunneleissa. Teoriaosuudessa käydään läpi yleisiä VPN-tunnelointiprotokollia ja niiden käyttömahdollisuuksia. Työssä esitetään tarvittavat asennusvaiheet IPSec-tunnelin luomiseksi ja käydään läpi vianhaussa käytettäviä työkaluja. Työssä havainnollistetaan myös Ciscon käyttöliittymän lauseoppia sekä eri asetuksien vaikutusta palomuurin toimintaan.

Käytännön osuudessa luodaan toimiva IPSec Site-to-Site -tunneli kahden Cisco ASA-5505 -palomuurin välille. Implementointi on sovitettu osaksi Metropolian Bulevardin laboratorioverkkoa. Vikatilanteet käydään yksityiskohtaisesti läpi kuvien ja komentojen avulla.

Työn tavoitteena on vähentää vikatilanteiden aiheuttamaa työtaakkaa ja tarjota systemaattinen ongelmanratkaisumalli tulevaisuuden varalle.

| | |
|---|---|
| Avainsanat | VPN, IPSEC, vianetsintä |

| | |
|---|---|
| Author(s)<br>Title<br><br>Number of Pages<br>Date | Rafael Silvonen<br>VPN-technologies and IPSec-tunnel troubleshooting<br><br>30 pages<br>20 April 2016 |
| Degree | Bachelor of Engineering |
| Degree Programme | Communication Networks and Applications |
| Specialisation option | Networks |
| Instructor(s) | Jukka Louhelainen, Senior Lecturer<br>Marko Uusitalo, Senior Lecturer |

The purpose of this study is to present a variety of VPN technologies, and give the reader help for troubleshooting IPSec tunnels. The theoretical part deals with the general VPN tunneling protocols and their use. The work presents the necessary installation steps in the creation of an IPSec tunnel and go through the tools used in troubleshooting. The work is also illustrated by Cisco interface syntax as well as the effect of various settings for the firewall function.

In the practical part is shown how to create a working IPSec Site-to-Site tunnel between two Cisco ASA 5505 firewalls. Implementation is arranged as part of the boulevard Metropolia laboratory network. Problem solving takes place through images and commands.

The aim is to reduce the workload caused by faults and provide a systematic problem-solving model for the future.

| | |
|---|---|
| Keywords | VPN, IPSEC, troubleshooting |

## Sisällys

Lyhenteet

1 Johdanto 1

2 Virtual Private Network 1

2.1 Yksityisyyden suoja 1
2.2 Luottamus 2

3 VPN-markkinat 2

4 VPN-tunnelointiprotokollat 3

4.1 Yleistä VPN-tunnelointiprotokollista 3
4.1.1 Point to Point Tunneling Protocol 3
4.1.2 Layer Two Tunneling Protocol 4
4.1.3 IP Security Architecture 4
4.1.4 Secure Sockets Layer Virtual Private Network 5
4.1.5 Security Association (SA) 5
4.2 Internet Key Exchange 5
4.3 Päätila 5
4.4 Aggressiivinen tila 6

5 Testiympäristö 6

5.1 Missä vikatilanteita voi esiintyä 7
5.1.1 Pääsylistat 7
5.1.2 NAT 8
5.1.3 PSK 9
5.1.4 Diffie-Hellman 9
5.1.5 Kryptografinen tiivistefunktio 11
5.2 Asennus ja konfigurointi 12
5.3 Toiminnan testaus 16

6 Vikatilanteiden simulointi 20

6.1 Vikatilanteen selvittäminen 21
6.2 Pääsylistoista johtuvat vikatilanteet 23
6.3 Osoitteenmuunnoksesta johtuvat vikatilanteet 24
6.4 Esijaettujen avainten vikatilanteet 26
6.5 Diffie-Hellman ja tiivistefunktion vikatilanteet 27

7 Yhteenveto 29

Lähteet 30

## Lyhenteet

| | |
|---|---|
| AH | Authentication Header. Suojausprotokolla, joka vastaa IPSecin liikenteen eheydestä, autentikoinnista ja toteutuksesta. |
| ASA | Adaptive Security Appliance. Ciscon verkon turvalaitteiden tuotesarja. |
| DH | Diffie-Hellman. Julkiseen avaimeen perustuva algoritmi. Käytetään usein VPN-tunnelin luontivaiheessa kun sovitaan yhteisestä salauksesta. |
| ESP | Encapsulating Security Payload. Suojausprotokolla, joka vastaa IPSec liikenteen salauksesta ja varmennuksesta. |
| GRE | Generic Routing Encapsulation. Ciscon kehittämä tunnelointiprotokolla. Kapsuloi OSI-mallin verkkotason protokollia virtuaalisen point-to-point-linkin sisään. |
| IKE | Internet Key Exchange. IPSecin hyödyntämä protokolla, jolla valitaan salausasetukset. |
| ISAKMP | Internet Security Association and Key Management Protocol. Protokolla salausasetusten ja kryptografisten avainten luontiin. |
| L2F | Layer 2 Forwarding Protocol. Ciscon kehittämä tunnelointiprotokolla, jonka avulla luodaan VPN-yhteyksiä. |
| L2TP | Layer 2 Tunneling Protocol. Salaamaton VPN-tunnelointiprotokolla. |
| MD5 | Message-Digest algorithm 5. Vuonna 1991 julkaistu funktio, joka tuottaa 128-bittisiä tiivisteitä. |
| MS-CHAP | Microsoft Challenge Handshake Authentication Protocol. Autentikointiprotokolla käyttäjälle tai verkon laitteelle. |
| NAT | Network Address Translation. Osoitteenmuunnostekniikka. |
| PPP | Point-to-Point Protocol. Tuottaa yhteyksiä datalinkkikerroksiin. |

| | |
|---|---|
| PPTP | Point-to-Point Tunneling Protocol. TCP:tä käyttävä VPN-protokolla, joka hyödyntää GRE-tunnelointia ja PPP-pakettien kapsulointia. |
| SHA | Secure Hash Algorithm. Yksisuuntainen tiivistefunktio. |
| SSH | Secure Shell. Suojattu etähallintaprotokolla. |
| SSL | Secure Sockets Layer. Netscape Communicationsin kehittämä kryptografinen protokolla, joka suojaa dataa Internetin yli. |
| VPN | Virtual Private Network. Etäkäyttäjien ja toimipisteiden yhdistämiseen käytetty tekniikka. |

# 1 Johdanto

Idea insinöörityöhön syntyi työharjoittelun päätyttyä. Verkkosuunnittelijana minun vastuualueisiin kuuluivat pääasiassa palomuurilaitteiden konfigurointi- ja muutostyöt. Näitä olivat esimerkiksi VPN- ja IPSec-tunneleiden luonti. Töiden aikana huomasin, että Internetistä löytyy valtavasti informaatiota IPSec-tunneleiden asennuksesta, mutta ongelmatilanteista ei löytynyt juuri mitään. Jos etsii Internetistä tietoa IPSec-tunneleiden ongelmatilanteista, päätyy usein laitevalmistajien tukisivustoille. Näillä tukisivustoilla on usein yleisiä ratkaisumalleja, joita ei voi soveltaa käytäntöön.

Tämän työn tavoitteena on näyttää monipuolisten esimerkkien avulla yleisimpiä IPSec-tunnelin vikatilanteita ja antaa lukijalle valmiudet niiden ratkaisuun todellisessa ympäristössä.

# 2 Virtual Private Network

Virtual Private Network (VPN) on menetelmä, jonka avulla voidaan turvallisesti yhdistää kaksi yksityistä verkkoa julkisen verkon läpi. VPN käyttää vahvaa salausta, jolla varmistetaan yhteyksien turvallisuus. VPN-yhteyden ansiosta yrityksen lähiverkon palvelut ja tiedostot ovat normaalisti käytettävissä, ikään kuin etätyöntekijä olisi kytkeytyneenä lähiverkkoon paikan päällä.

## 2.1 Yksityisyyden suoja

VPN-yhteyksillä voidaan salata oma Internet-liikenne Internet-palvelutarjoajien valvonnalta ja verkkosivujen tarkkailulta. VPN-yhteyksillä voidaan poistaa myös verkkopalveluille asetetut maantieteelliset estot. Maantieteellisiä rajoituksia sisältävät mm. suoratoistopalvelut Netflix ja YouTube. VPN-yhteyksien avulla omaa sijaintia voi muuttaa virtuaalisesti - ja tällä tavalla saadaan pääsy laajempiin valikoimiin, kuten elokuviin ja musiikkivideoihin. VPN-palvelut ovatkin halpa ja tehokas keino oman Internet-liikenteen suojaukseen. Internet-palveluntarjoaja (engl. Internet Service Provider) kyllä havaitsee VPN-palvelimen käytön, mutta salauksen ansiosta ei näe siellä kulkevaa liikennettä. Verkkosivut

puolestaan havaitsevat vain sen, että yhteys on muodostettu VPN-palvelusta, mutta käyttäjän todellinen IP-osoite ei ole tiedossa. [1.]

### 2.2 Luottamus

Oman VPN-palvelun valinnassa tulee ottaa huomioon yrityksen luotettavuus. Vaikka VPN-palvelun hyödyntäminen suojaa liikenteen omalta Internet-palveluntarjoajalta, se ei estä VPN-palveluntuottajan tarkkailulta. VPN-yhteyden tarjoaja näkee osan liikenteestä ja sillä on mahdollisuus tallentaa sitä omiin lokitietoihinsa.

Jos sopimusehdot sallivat, se voi tarvittaessa luovuttaa tietoja ulkopuolisille. "Esimerkiksi englantilainen HideMyAss-niminen VPN-palveluntarjoaja nousi kyseenalaiseen julkisuuteen vuodettuaan FBI:lle LulzSec-hakkeriryhmään kuuluvan henkilön tiedot." Tämän takia ennen VPN-palvelun valintaa, tulee tutustua tietosuojaehtoihin tarkasti. Vaikka osa palveluista ilmoittaa, etteivät tallenna lokitietoja voi näin kuitenkin olla. Käyttäjä joutuu siis luottamaan palveluntarjoajaan ilmoittamiin tietoihin. Jos palveluntarjoajaa aletaan painostaa esimerkiksi oikeuskanteella, on tietosuojaehdot kuin veteen piirretty viiva. Useat ilmaiset VPN-palvelut myyvät käyttäjien verkkoliikennetietoja eteenpäin esimerkiksi kaupallisiin tarkoituksiin. Ilmaisten VPN-palveluiden rahastuskeinoina on usein myös rajoitettu yhteysnopeus. Internetistä löytää valtavasti tietoja eri VPN-palveluntarjoajista. Hyvä VPN-palvelu on sellainen joka ilmoittaa mm. seuraavat asiat: miten yhteys salataan, mitä VPN-protokollia on käytettävissä, palvelun tietosuojaehdot lokitietojen tallentamisen osalta, palvelinten fyysinen sijainti sekä minkä valtion lain alla palvelut sijaitsevat. [1.]

## 3 VPN-markkinat

VPN-palvelut ovat kovassa nousujohteessa. Grand View Research -konsultointiyrityksen suorittaman tutkimuksen mukaan, MPLS VPN:ään liittyvien markkinoiden arvellaan kasvavan noin 26,7 biljoonaan vuoteen 2020 mennessä. Verrattuna muihin toteutuksiin, Layer 2- ja 3 VPN-palvelut ovat halvempia toteuttaa ja tavoittavat eniten käyttäjiä maailmanlaajuisesti.

Videoneuvottelupalveluiden arvioidaan olevan tuottoisa ja nopeasti kasvava trendi yrityksissä. MPLS VPN -palvelut tarjoavat lyhytviiveisen ja turvallisen yhteyden, jotka ovat VoIP-tekniikan tärkeimpiä ominaisuuksia.

Suurimmat MPLS VPN -markkinat vuonna 2013 sijaitsivat Aasiassa ja Pohjois-Amerikassa. Näillä alueilla ovat suurimpia markkinatoimijoita, kuten Verizon Business, Sprint, Global Crossing ja Tata Communications. Myös Kiinan ja Intian VPN-markkinoilla on odotettavissa suurta kasvua lähivuosina. [2.]

# 4 VPN-tunnelointiprotokollat

## 4.1 Yleistä VPN-tunnelointiprotokollista

VPN-verkon päätepisteiden tulee käyttää samaa tunnelointiprotokollaa, jotta data olisi luettavissa. On olemassa monia turvatasoltaan erilaisia protokollia, kuten PPTP (Point-to-Point Tunneling Protocol), L2F (Layer Two Forwarding), L2TP (Layer Two Tunneling Protocol) ja IPSec. Näistä PPTP ja IPSec ovat turvallisuudessa tehokkaimpia. PPTP perustuu datapakettien kapselointiin IP-datagrammeiksi. Tämä kaksinkertainen suojaus tunnetaan point-to-point-tyyppisenä yhteytenä. Paikallisverkkoa koskevat tiedot kapseloidaan ensin PPP-sanomiin, ja nämä edelleen IP-sanomien sisään. IPSec sisältää kolme moduulia jotka ovat, (Authentication Header, Encapsulating Security Payload ja Security Association). Näillä varmistetaan luottamuksellisuus, yhtenäisyys ja käyttöoikeus. [3.]

### 4.1.1 Point to Point Tunneling Protocol

Tunnelointiprotokolla Point-to-Point on Microsoftin kehittämä, ja se on jatkoa PPP-protokollalle. PPTP:n toiminta perustuu TCP/IP-verkon läpi tapahtuvaan PPP-kehysten tunnelointiin. VPN-yhteyden muodostamiseen PPTP:llä, tarvitaan GRE- ja PPTP- pakettityyppejä. GRE voidaan ajatella kehyksenä, joka sisältää paketin tietoa järjestyksestä, tunnelointinumerosta ja määränpäästä. PPTP-kehys on TCP-paketti, joka puolestaan sisältää tietoja yhteyden kontrolli, yhteys -ja virheparametreista. PPTP- tai GRE-kehykset eivät sisällä todennusta, joten PPTP-protokollaa täytyy käyttää erillisten salausmenetelmien yhteydessä. Tähän tarkoitukseen voidaan käyttää esimerkiksi Challenge

Handshaking Authentication Protokollaa (CHAP) tai Password Authentication Protokollaa (PAP). Edellä olevat perustuvat PPP-kehyksien datan salakirjoitukseen. Salakirjoitus tapahtuu ennen kapselointia ja käyttäjän tunnistuksen yhteydessä luotujen salasanojen määrittelyillä.

PPTP on nykyään korvattu L2TP-protokollalla. Tähän on vaikuttanut eniten GRE-protokollan ongelmat ja vähäinen tuki. Tekniikan kehittyessä IPSec- ja SSL-protokollilla toteutetut VPN-tunnelit ovat syrjäyttäneet suuren osan edeltäjistään. [4.]

### 4.1.2 Layer Two Tunneling Protocol

Layer Two Tunneling Protocol (L2TP) pohjautuu PPTP - ja Cisco Layer Forwarding (L2F) -protokolliin. PPP-pakettien liikuttamiseen verkoissa käytetään L2TP-protokollaa. L2TP-liikenne koostuu pääasiassa UDP-kapseloiduista tarkkailu, käsky- ja tietopaketeista. L2TP käyttäytyy OSI-mallin siirtoyhteyskerroksessa, ja se nähdään huomattavasti monimutkaisempana kuin PPTP. L2TP ei tarjoa salausta, joten sitä suositellaan käytettävän IPSec:n kanssa. IPSec:n ja L2TP:n yhdistelmällä saavutetaan IPSec:n muodostama turvallinen yhteys, mihin kuuluu myös liikenteen syntyperän varmentaminen. Tällä yhdistelmällä varmistetaan datan yhtenäisyys ja suojautuminen toistohyökkäyksiltä. L2TP:n käytössä voi havaita lieviä nopeushaittoja, sillä liikenne on turvattu molempiin suuntiin. VPN-etäyhteyksien muodostamiseen L2TP on hyvä työkalu, ja tämä ominaisuus on mukana kaikissa Microsoftin Windows-palvelinkäyttöjärjestelmissä. [5.]

### 4.1.3 IP Security Architecture

IPSec on kokoelma protokollia ja niiden tärkein tehtävä on IP-paketin suojaus. IPSec tarjoaa kolme ensisijaista turvapalvelua: 1) tietojen alkuperän todennus; 2) tiedon eheyden varmentaminen; 3) tiedon luottamuksellisuus. Se tukee myös mekanismeja, jolla voidaan suojautua Denial of Service (DoS) eli palvelunestohyökkäyksiltä. IPSec määrittelee kaksi suojausprotokollaa: Authentication Header (AH) ja Encapsulating Security Payload (ESP). AH:n päätehtävä on tietojen alkuperän todentaminen ja tietojen eheyden varmistaminen. ESP:n rooli puolestaan on IP-paketin hyötykuorman salaus. [6.]

### 4.1.4 Secure Sockets Layer Virtual Private Network

Secure Socket Layer (SSL) on Netscapen kehittämä protokolla, joka sijoittuu OSI-mallin kuljetus- ja sovelluskerrosten väliin. Toisin kuin IPSec VPN, SSL VPN ei vaadi ohjelmiston asennusta käyttäjälle, joten ylläpitokustannukset ovat erittäin pieniä. SSL VPN:n tarkoitus on mahdollistaa VPN-käyttäjien pääsy esimerkiksi yrityksen sisäisiin sovelluksiin ja palvelimiin. SSL VPN ei ole standardi, joten kaikki olemassa olevat tuotteet eivät välttämättä toimi keskenään. Protokollan alkuperäinen tarkoitus oli suojata web-yhteyksiä, mutta helppokäyttöisyyden ansiosta se on yleistynyt myös VPN-yhteyksissä. [7.]

### 4.1.5 Security Association (SA)

Security Association eli turvallisuusliitto on menetelmä, jonka avulla VPN-yhteyttä halutaan suojata. Turvallisuusliitto määrittelee IPSec-tunnelissa käytettävät menetelmät, algoritmit ja kryptografiset ominaisuudet. Turvallisuusliiton neuvotteluun käytetään IKE-protokollaa. Siinä yhteyden initiaattori ehdottaa joukkoa oman turvallisuuspolitiikan mukaisesti, joista toinen osapuoli valitsee ensimmäisen omaan turvapolitiikkaansa.

Yhdelle VPN-yhteydelle voidaan määritellä useita turvallisuusliittoja. Usealla turvallisuusliitolla toimivia yhteyksiä voidaan niputtaa objekteiksi. Objektit helpottavat käsittelyä etenkin konfiguroinnin kannalta. Yhteyksien turvallisuusliittojen data tallennetaan Security Association Database (SAD) -tietokantaan. [8.]

## 4.2 Internet Key Exchange

Avaimenvaihtoprotokollan tarkoitus on yhdistää kaksi päätepistettä, jotka ylläpitävät itsenäisesti symmetristä salausavainta. Tämä avain salaa ja purkaa IP-paketteja säännöllisesti yhteyspisteiden välillä. Tuloksena IKE-neuvottelusta on turvallisuusliitto. IKE voi toimia kahdessa eri tilassa. Ensimmäinen tila on päätila ja sillä on kolme eri vaihetta. [9.]

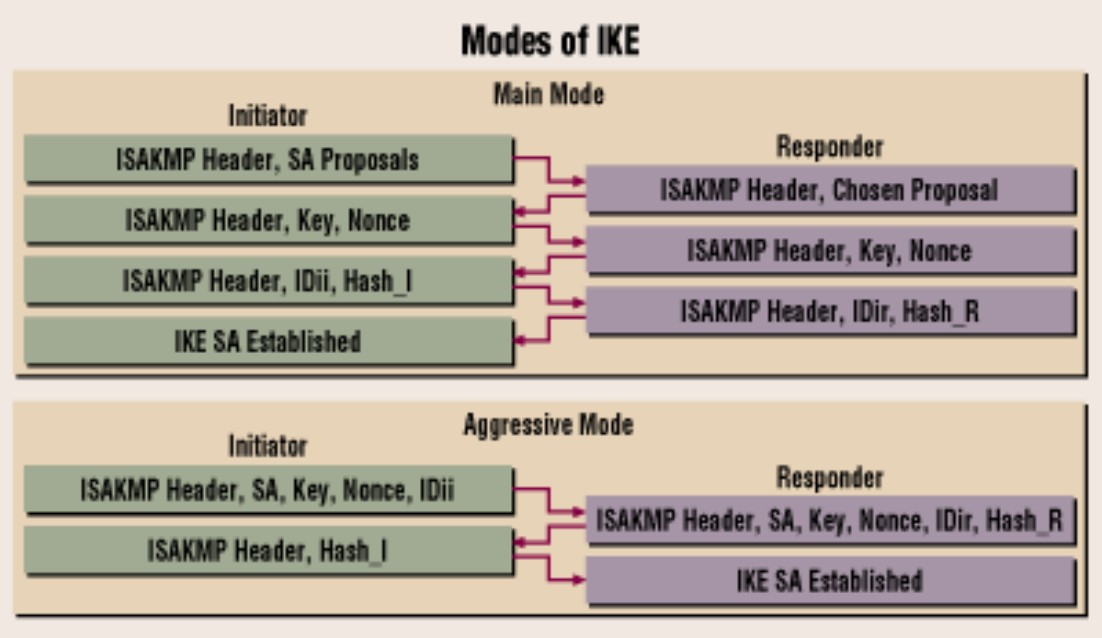
## 4.3 Päätila

Päätilan ensimmäisessä vaiheessa varmistetaan turvallisuusliittojen yhteydenmukaisuus. Toisessa vaiheessa luodaan Diffie-Hellmanin avulla salaiset avaimet ja lähetetään ne vastapareille. Tämän jälkeen lähetetään varmistuspyynnöt. Viimeisessä vaiheessa

varmistetaan toisen puolen identiteetti. Identiteetin arvo on vastapuolen IP-osoite salatussa muodossa. Jos identiteetti varmistuu oikeaksi, muodostuu vastapuolesta pari.

### 4.4 Aggressiivinen tila

Aggressiivinen tila tiivistää IKE-neuvottelut kolmeen pakettiin, jossa on kaikki tiedot turvallisuusliiton saavuttamiseksi. Vastaanottaja lähettää ehdotuksen, avaintunnuksen ja oman tunnuksensa samaan aikaan. Täten neuvottelu on nopeampaa, mutta lievästi alttiimpi hyökkäyksille. Aggressiivista tilaa käytetään tyypillisesti tilanteessa, missä palomuureille on määritelty dynaamiset ulkoiset IP osoitteet. [9.]




Kuvio 1. Päätilan ja aggressiivisen tilan eroavaisuudet [17.]

## 5 Testiympäristö

Testiympäristönä käytetään Metropolian tiloihin rakennettua laboratorioverkkoa. Käytössä on kaksi Cisco ASA 5505 -palomuuria, joiden ohjelmistoversio on 8.4. Näiden palomuurien välille luodaan usein VPN-yhteyksissä käytetty IPSec-tunneli. IPSec-tunnelin muodostamiseksi tarvitaan aina kaksi päätepistettä. Yleisesti molemmissa päädyissä on oma asiantuntija, joka suorittaa konfiguraatiot. Monesti voidaan kuitenkin joutua tilanteeseen, missä molemmat osapuolet vakuuttavat omien konfiguraatioiden olevan oikein,

vaikka näin ei oikeasti ole. Ristiriitatilanteissa vianhaun mekaniikat ovat tärkeässä osassa.

## 5.1 Missä vikatilanteita voi esiintyä

Vikatilanteita IPSec-tunneleissa aiheuttavat yleisimmin väärät ohjelmistoversiot: NAT, access-list, PSK, DH ja SHA. 99 % tapauksissa vikatilanteet johtuvat ihmisen tekemistä virheistä. Viimeinen prosentti sisältää harvinaisia tapauksia, missä eri laitevalmistajien palomuurit eivät voi muodostaa tunnelia esimerkiksi ohjelmointivirheiden takia. Työharjoittelun aikana asensin noin 50 IPSec-tunnelia eri laitteiden välille, ja vain yksi ei toiminut. Kyseessä oli Zyxelin ZyWALL, joka ei suostunut toimimaan Ciscon ASA-palomuurin kanssa. Myöhemmin ongelma korjaantui ZyWALL-palomuurin ohjelmistopäivityksen ansiosta.

### 5.1.1 Pääsylistat

Palomuurien yksi tärkeimmistä tehtävistä on pakettisuodatus. Suodatus tapahtuu pääsylistojen, ACL:n (engl. ”Access Control List”) perusteella. Oletuksena pääsylistoissa on sääntö, jonka mukaan kaikki, mitä ei ole erikseen sallittu, on kielletty. Pääsylistat koostuvat yhdestä tai useammasta kulunvalvontamerkinnöistä. Pääsylistojen avulla luodaan merkintä palomuurin käyttöoikeusluetteloon, joka määrittää liikenteen sallimisen tai estosäännön. [10.]

Pääsylistoja käytetään yrityksen laitepalomuurin edessä suodattamassa kaikki epätoivotut paketit pois, jolloin laitepalomuurille ei tule ylimääräistä kuormaa ei-toivottujen pakettien suodattamisessa. Kun paketti saapuu, palomuuri tarkastelee sen otsikkotietoja pääsylistassa oleviin sääntöihin. Pakettien otsikkotietoja ovat esimerkiksi IP, TCP, UDP ja ICMP. Yleisimmin suodatuksen kohteena ovat IP-osoitteet ja porttinumerot. [11.]

```
RAFUASA1(config)# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list host_sallinta; 1 elements; name hash: 0xa20992ae
access-list host_sallinta line 1 extended permit ip 10.2.2.0 255.255.255.0 any (hitcnt=0) 0xf5e98243
RAFUASA1(config)#
```

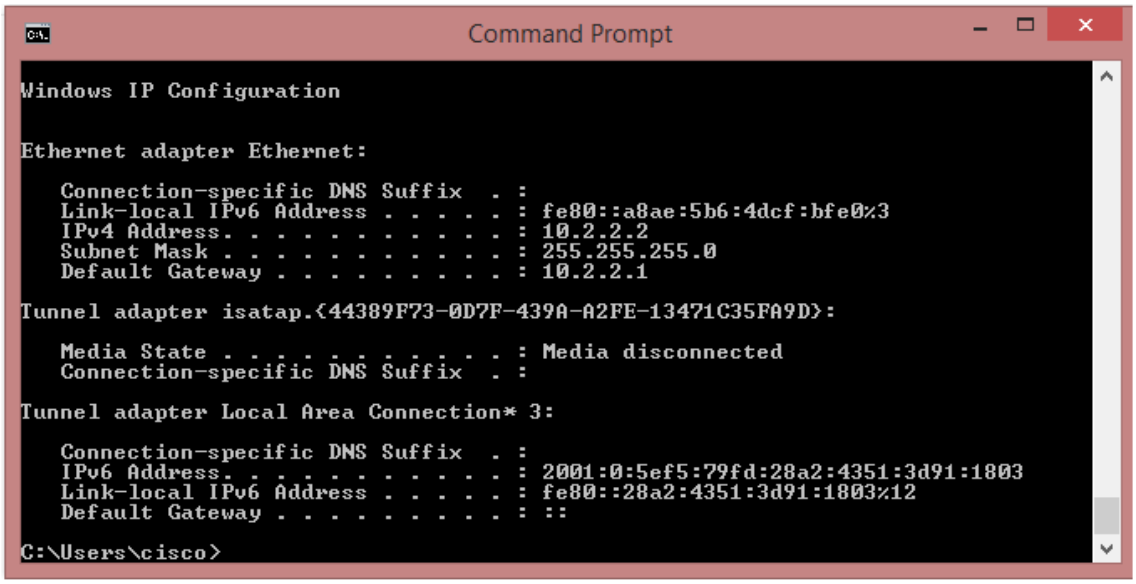
Kuvio 2. Esimerkki pääsylistasta, missä sallitaan kaikki sisäverkon 10.2.2.0 255.255.255.0 liikenne ulospäin

### 5.1.2 NAT

NAT (Network Address Translation) on osoitteenmuunnostekniikka, jonka avulla useat verkkolaitteet voivat käyttää yhteistä IP-osoitetta. Osoitteenmuunnostekniikan avulla myös tietoturva kasvaa. Tämä johtuu yksinkertaisesti siitä, että osoitteenmuunnosta käyttäviin laitteisiin ei ulkomaailmalta saa suoraa yhteyttä.

IPv4-protokolla tarjoaa $2^{32}$ (4,294,967,296) IP-osoitetta. Internetin jatkuvan tarpeen lisääntymisen takia nämä osoitteet eivät siis riitä kaikille mahdollisille verkkolaitteille. Tämä on suurin syy osoitteenmuunnostekniikan kehittämiselle. Vaikka maailmalta ei saa yhteyttä suoraan sisäverkkolaitteisiin, yhteys voidaan kuitenkin järjestää halutussa reitittimessä esimerkiksi porttiohjauksen (Port Forwarding) tai pääsylistojen avulla. [12.]

Esimerkki osoitteenmuunnoksesta.




Kuvio 3. Sisäverkon tietokoneen IPv4-osoite on **10.2.2.2**


Kuvio 4. Osoitemuunnoksen avulla sisäverkon tietokoneen IPv4-osoite näkyy maailmalle nyt osoitteena **194.110.231.252**

### 5.1.3 PSK

PSK eli Pre Shared Key on suosittu IPSec-tunneleissa käytetty varmennusmenetelmä. PSK on salainen avain, jonka osapuolet ovat jakaneet toisilleen ennen IPSec-tunnelin muodostamista. IPSec-tunnelin liikennöinnissä tiedot salataan ennen niiden lähettämistä. PSK on yksinkertaisesti yhteinen salasana, jolla varmistetaan, että vastaanottaja on se, kuka sanoo olevansa. Esimerkiksi Pekka ja Alissa sopivat yhteisen salasanan ASmdw12. Jos Pekka haluaa jakaa informaatiota Alisalle, hän avaa keskustelun sanomalla salasanan ASmdw12 ennen viestin lähettämistä. Täten Alissa tietää lähettäjän olevan varmasti Pekka. PSK-avain suositellaan vaihdettavan esim. tekstiviestillä tai salattuna tiedostona. [13.]

### 5.1.4 Diffie-Hellman

Diffie-Hellman on julkiseen avaimeen perustuva algoritmi, joka on julkistettu ensimmäistä kertaa vuonna 1976. Diffie-Hellmania käytetään usein VPN-tunnelin luontivaiheessa, kun sovitaan yhteisestä salauksesta. Ratkaisu perustuu potenssiin korottamisen laskusääntöihin ja logaritmin monimutkaisuuteen.

Diffie-Hellman toiminnan esimerkki:

Osapuolet Tommi ja Alissa haluavat luoda yhteisen avaimen.

1) Sovitaan yhteinen kantaluku esimerkiksi **g=5** ja primitiivinen alkio **p=21**, näitä lukuja ei tarvitse salata.

2) Tommi ja Alissa valitsevat satunnaisen luvun esimerkiksi Tommi **T=4** ja Alissa **A=7**. Tämä luku tulee salata.

3) Tommi lähettää Alissalle luvun T = (g^Tommi mod p) = **(5^4 mod 21) = 16**.

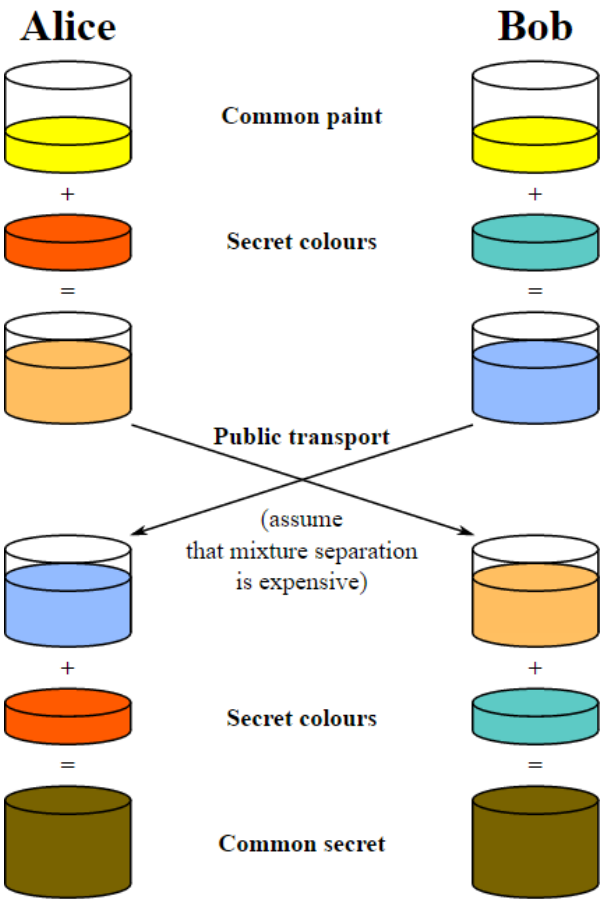
4) Alissa lähettää Tommille luvun A = (g^Alissa mod p) = **(5^7 mod 21) = 5**.

5) Tommi laskee salaisen avaimen käyttäen Alissan lukua kaavalla Tommi^T mod p = **5^4mod21= 16**.

6) Alissa laskee salaisen avaimen käyttäen Tommin lukua samalla kaavalla Alissa^A mod p = **16^7mod21 = 16**.

Yhteiseksi avaimeksi saadaan siis luku **16**.

Tulos on sama, koska kantaluku^Tommi*Alissa mod pritimiivinen alkio = kantaluku^Alissa*Tommi mod primitiivinen alkio. Yleisesti luvut valitaan suuriksi, jolloin nykyisillä algoritmeilla salausta ei voi purkaa. [14.]




Kuvio 5. Mallitynnyri esimerkki [18.]

### 5.1.5 Kryptografinen tiivistefunktio

Hash-funktion eli yksisuuntaisen tiivistefunktion käyttötarkoitus on muodostaa lyhyt tiivistelmä bittijonosta. Tiivistelmän tarkoitus on turvata ja nopeuttaa viestintää. Tiivisteen pituus on yleisesti 128 tai 160 bittiä riippumatta viestin alkuperäisestä pituudesta. Käytännössä syntyy monia identtisesti samanlaisia tiivistelmiä, mutta tärkeintä on, etteivät ne törmää keskenään. [15.]

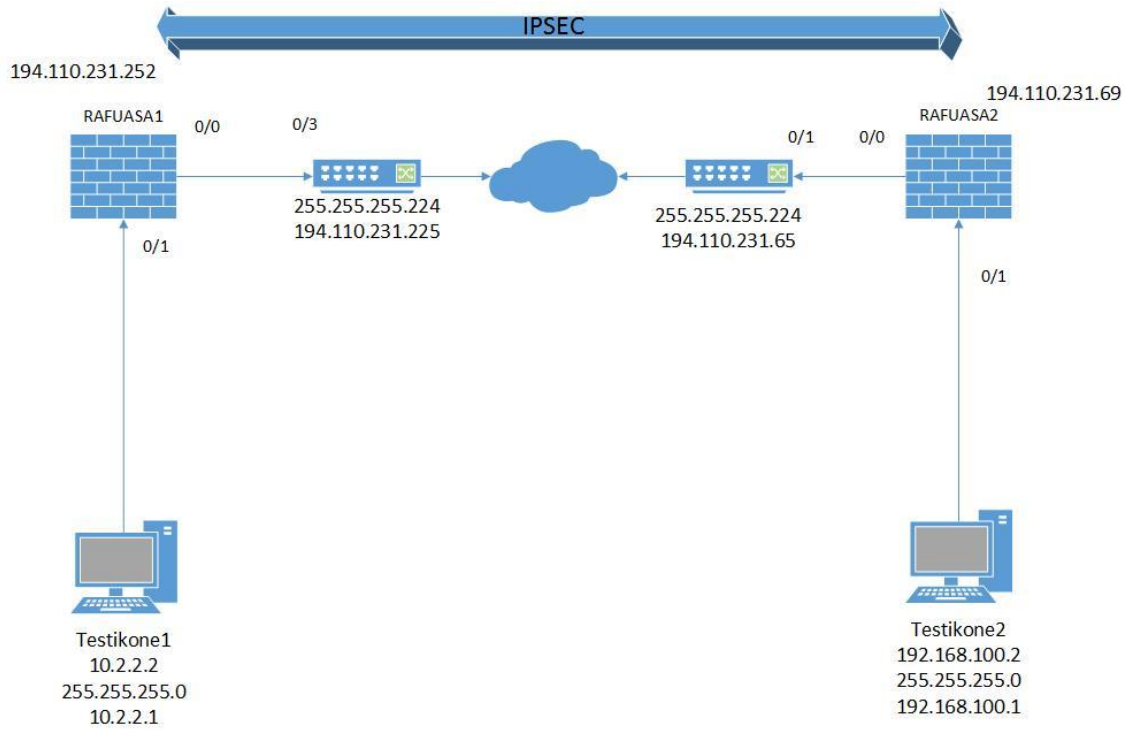
Tiiviste (hash) tunnetaan myös nimellä "digital fingerprint" tai "message digest" (MD). Vuonna 1991 kehitetyn MD5:n (Message Digest 5) tarkoitus oli tuottaa standardinomai-

sia 128-bittisiä tiivisteitä. Verkoissa MD5:ta käytetään tiedostojen alkuperän varmistamiseen vaikka useat asiantuntijat eivät sitä enää suosittele. Vuonna 2004 huomattiin, että helposti saatavilla olevilla laitteilla voitiin luoda törmäyksiä MD5:n luomiin tiivisteihin. Tämän jälkeen MD5:tä alettiin pitää turvattomana.

Vuonna 1993 julkaistu SHA-1 on puolestaan 160-bittinen tiivistefunktio, ja se nähdään MD5:n edeltäjänä. Teoriassa SHA:n tuottamien tiivistefunktioiden murtaminen on yhtä helppoa kuin MD5:n purkaminen. [16.]

## 5.2 Asennus ja konfigurointi

Tarkoituksena on luoda IKEv1 IPSec site-to site tunnel. Kaikki konfigurointi suoritetaan Command Line Interface:n (CLI:n) kautta, koska se tarjoaa enemmän mahdollisuuksia kuin GUI-käyttöliittymä. Konfiguraatiot ovat perusteiltaan samat molemmissa palomuureissa.




Kuvio 6. Testiympäristön verkkokuva

Corecess-kytkimet jakavat DHCP:lla palomuureille julkiset IPv4-osoitteet. Niillä ei ole vaikutusta muuhun toimintaan.

IPSec-tunnelin luonti alkaa ISAKMP-asetuksien määrittelyillä. Tässä pitää tietää, että Ciscon käyttöliittymässä ISAKMP ja IKE menevät usein sekaisin. Yleisesti ISAKMP sisältää avaimenvaihtomekaniikat ja toimii pohjana IKE-protokollalle. Konfiguroinnin syntaksi riippuu palomuurin versiosta. Vanhemmissa versioissa (8.4) alaspäin käytetään syntaksia **crypto isakmp policy** ja uudemmissa versioissa se on **crypto ikev1 policy**.

IPSec-tunnelin ehtojen määrittämiseksi luodaan ISAKMP-politiikka, joka sisältää viisi vaihetta.

1) Todentamismenetelmä. Todentamismenetelmää käytetään vastapuolen varmistamiseksi. Vaihtoehtoina crack, pre-share ja rsa-sig.

2) Salausmenetelmä. Salausmenetelmän tarkoitus on suojata liikenne päätepisteiden välillä. Vaihtoehtoina 3des, aes ja des.

3) Tiivistefunktio. Tiivistefunktiolla varmistetaan lähettäjän henkilöllisyys ja viestien koskemattomuus. Vaihtoehtoina md5 ja sha. Diffie-Hellman.

4) Diffie-Hellman määrittää tunnelin salausavaimen. Vaihtoehtoina group 1,2,5 ja 7.

5) Aikaraja. Aikarajalla määritellään avaimen ”parasta ennen” -hetki. Kun ehdot täyttyvät, avain uusitaan. Parasta ennen voidaan määritellä sekunteina tai kilobitteinä. Vaikka avaimenvaihdon aikaraja on vapaasti määriteltävissä, tulee huomioida, että lyhyet avaimenvaihtovälit kuormittavat palomuuria enemmän kuin pitkät välit.

(Kaikki tummennetut tekstit ovat palomuurissa suoritettavia komentoja)

**crypto ikev1 policy 1**

**authentication pre-share**

**encryption 3des**

**hash sha**

**group 2**

**lifetime 43200**

```
crypto ikev1 policy 1
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 43200
```

Kuvio 7. ISAKMP-määrittelyt

Seuraavaksi määritellään politiikka IPSec-tunnelin salausparametreille. Nimeksi valitaan FirstSet, salausmenetelmäksi esp-3des ja varmentamismenetelmäksi esp-md5-hmac.

**crypto ipsec ikev1 transform-set FirstSet esp-3des esp-md5-hmac**

```
crypto ipsec ikev1 transform-set FirstSet esp-3des esp-md5-hmac
```

Kuvio 8. Salausparametrit

Seuraavaksi muokataan pääsylistoja, joiden avulla hallitaan IPSec-tunnelissa kulkevaa liikennettä. Tässä tapauksessa sallitaan kaikki sisäverkon **10.2.2.0 255.255.255.0** TCP, UDP ja IP liikenne kohti **192.168.100.0 255.255.255.0** verkkoa. Pääsylistoilla voidaan halutessa rajata myös IPSec-tunnelin liikennettä.

**access-list l2l-list extended permit ip 10.2.2.0 255.255.255.0 192.168.100.0 255.255.255.0**

```
access-list l2l_list extended permit ip 10.2.2.0 255.255.255.0 192.168.100.0 255.255.255.0
```

Kuvio 9. Pääsylista

Pääsylistojen muokkauksien jälkeen luodaan tunneliryhmä. Tunneliryhmä on sarja tietueitä, jotka sisältävät IPSec-tunneleiden yhteysparametreja. Määritellään vastapuolen IP-osoite, IPsec-tunnelin tyyppi ja ikev1-avaimenvaihtometodi.

**tunnel-group 194.110.231.72 type ipsec-l2l**

**tunnel-group 194.110.231.72 ipsec-attributes**

**ikev1 pre-shared-key cisco123**

```
tunnel-group 194.110.231.72 type ipsec-l2l
tunnel-group 194.110.231.72 ipsec-attributes
 ikev1 pre-shared-key *****
```

Kuvio 10. Tunneliryhmän määrittelyt

Huomataan, että PSK ei ole enää esillä show running config-tilassa. Sen saa kuitenkin näkyviin komennolla **more system:running-config**.

Salauskartta kokoaa yhteen eri osat IPSec-tunnelin turvayhteydestä. Se pitää sisällään erilaisia parametreja, jotka määrittelevät IPSec-tunnelin liikennöinnin. Salauskarttoja voi olla monia, joten se tulee sidota edellä luotuihin salausparametreihin, pääsylistaan ja tunneliryhmään.

**crypto map abcmap 1 match address l2l-list**

**crypto map abcmap 1 set peer 194.110.231.72**

**crypto map abcmap map 1 set ikev1 transform-set FirstSet**

Lopuksi salauskartta pitää sitoa rajapintoihin (engl. interface), joissa IPSec-liikenne kulkee.

**crypto map abcmap interface outside**

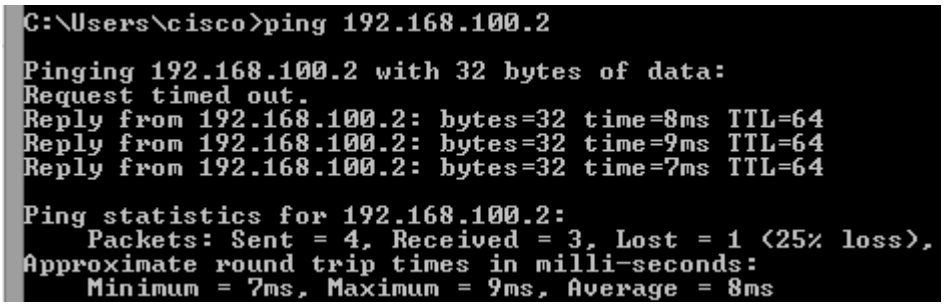
```
crypto map abcmap 1 match address l2l_list
crypto map abcmap 1 set peer 194.110.231.72
crypto map abcmap 1 set ikev1 transform-set FirstSet
crypto map abcmap interface outside
```

Kuvio 11. Salauskartan määrittelyt

Lopuksi kirjoitetaan tiedot muistiin komennolla **write memory**.

## 5.3 Toiminnan testaus

Konfigurointien jälkeen on hyvä testata tunnelin toimintaa. IPSec-tunneli voi olla kunnossa, mutta se ei ”nouse” ilman liikenteen simulointia. Tähän tarkoitukseen voidaan käyttää esimerkiksi yhteyskokeilua testikoneelta numero 1. Yhteyskokeilun voi suorittaa komentoikkunassa seuraavasti:




Kuvio 12. Yhteyskokeilu

Ensimmäinen yhteyskokeilu toimii herätteenä tunnelille. Se ei saa vastausta, koska avaimenvaihto on vielä kesken. Tästä eteenpäin tunneli on ylhäällä, joten tulevat yhteyskokeilut onnistuvat normaalisti.

Usein työelämässä vastaan tulee tilanne, jossa edellä olevaa yhteyskokeilua ei voi suorittaa. Syitä tälle voi olla esimerkiksi se, että verkkolaitteet ja sisäiset palvelut ovat eri henkilöiden tai yritysten hallinnassa. Myös laitteiden fyysinen sijainti, tila ja henkilöiden paikallaolo ovat kriittisiä tekijöitä. Tähän ongelmaan on olemassa kuitenkin ratkaisu.

Osassa palomuureista on olemassa keino simuloida liikennettä. Cisco ASA -palomuureissa liikenteen simuloimiseksi voidaan käyttää ”**packet-tracer**”-komentoa. Packet-tracer-komento sisältää yksityiskohtaisia tietoja pakettien prosessoinnista palomuurissa. Kyseisen komennon avulla saadaan helposti luettavissa olevaa tietoa paketin liikennöinnistä. Esimerkiksi jos lähtevä paketti hylätään virheellisen pääsylistan vuoksi, näyttöön tulee sanoma, jossa kerrotaan paketin tippuneen pääsylistojen kohdalla. Jokaisen uuden konfiguraation jälkeen on hyvä käyttää packet-tracer-komentoa. Tällä tarkistetaan vasta luodun säännöstön toimivuus ja havaitaan mahdolliset ristiriidat.

Esimerkkinä käytetään packet-tracer-komentoa, jonka avulla yritetään nostaa tunneli ylös.

**packet-tracer input inside icmp 10.2.2.2 1 1 192.168.100.2**

Komennolla simuloidaan inside rajapinnasta 10.2.2.2 osoitteesta lähtevää ICMP-pakettia kohti tunnelin toisessa päädyssä sijaitsevaa testikonetta 192.168.100.2.

Cisco ASA tulostaa kahdeksanvaiheisen tiivistelmän paketin liikennöinnistä. Jos tunnelissa olisi ollut ongelmia esimerkiksi salausten kanssa, niin kohdassa 7 olisi lukenut DROP. Yksityiskohtaisempaa tietoa paketin kulusta saa komennolla detailed, joka sijoitetaan packet-tracer-komennon loppuun seuraavasti:

**packet-tracer input inside icmp 10.2.2.2 1 1 192.168.100.2 detailed**

```
RAFUASA1(config)# packet-tracer input inside icmp 10.2.2.2 1 1 192.168.100.2

Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in   0.0.0.0         0.0.0.0         outside

Phase: 2
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 3
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
  inspect icmp
service-policy global_policy global
Additional Information:

Phase: 4
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source static sisaverkko sisaverkko destination static ulkoverkko ulkoverkko
Additional Information:
Static translate 10.2.2.2/0 to 10.2.2.2/0

Phase: 6
Type: HOST-LIMIT
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 11342, packet dispatched to next module
```

Kuvio 13. Packet-tracer-komennon tulostus

Liikenteen simuloinnin jälkeen tarkistetaan IPSec-tunnelin tila. Tähän tarkoitukseen voidaan käyttää muun muassa seuraavia komentoja:

**show crypto isakmp**

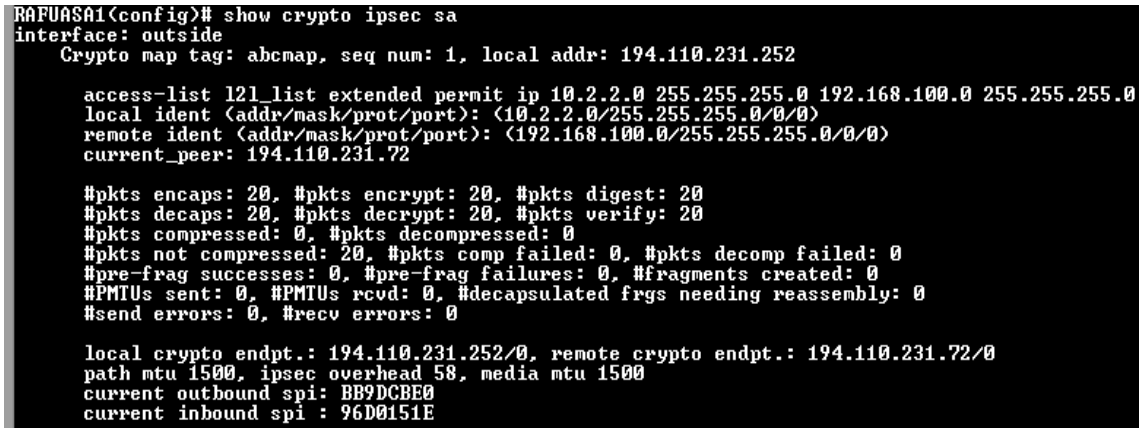

Kuvio 14. ISAKMP-komennon tulostus

Tämä komento tulostaa tiivistelmän aktiivisista tunneleista. Tulosteesta voidaan lukea tunnelin tyyppi, päätepiste, rooli ja tila.

Komennolla **show crypto ipsec sa** saadaan yksityiskohtaisempaa tietoa eri tunneleiden tilasta ja pakettien liikenteestä.


Kuvio 15. IPsec sa-komennon tulostus

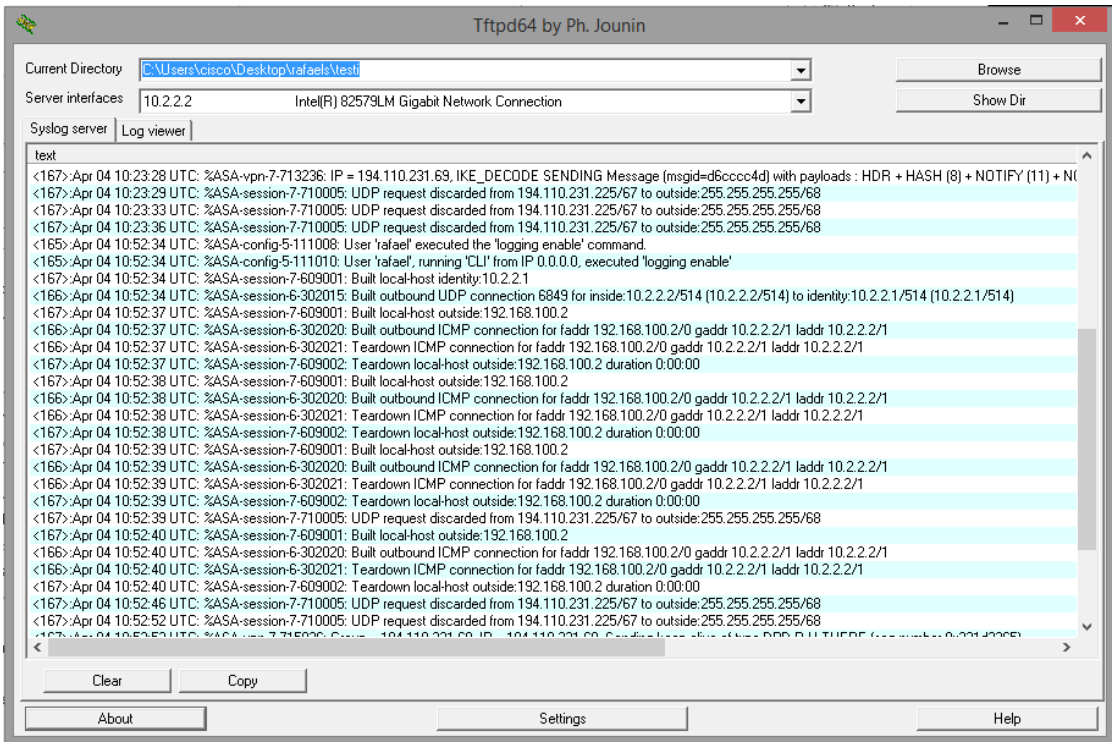
Tunneli on nostettu ylös liikenteen simuloinnilla, joten pakettikohtaiset tiedot näyttävät nollaa. Kun generoidaan oikeaa liikennettä ja tunneli toimii, näyttää tulostus seuraavalta:




Kuvio 16. Generoidun pakettiliikenteen tiedot

# 6 Vikatilanteiden simulointi

Tässä luvussa luodaan tarkoituksella vikatilanteita ja käydään läpi, miltä ne näyttävät palomuurissa. Vianhaussa käytetään apuna palomuurin lokipalvelua. Lokipalvelun tarkoitus on yksinkertaisesti kerätä ja tallentaa palomuurissa tapahtuvia viestejä. Näitä viestejä voivat olla esimerkiksi kirjautumiset laitteelle ja erilaiset virheilmoitukset. Palomuurissa kulkee viestejä nopeammin kuin ihminen pystyy niitä lukemaan. Tämän takia viestit on hyvä tallentaa, jotta niitä voidaan tarkastella halutessa. Tässä tapauksessa palomuurin lokiviestit tallennetaan TFTP-palvelimelle. TFTP-palvelimena käytetään ohjelmaa Tftpd64 by Ph.Jounin, ja sen ulkoasu näyttää seuraavalta.




Kuvio 17. Lokiviestien lukeminen ja tallentaminen

## 6.1 Vikatilanteen selvittäminen

IPSec-tunnelin toimimattomuuteen voi olla monia eri syitä. Aluksi tulee selvittää vian alkuperä ja sijainti konfiguraatiossa. Tähän tarkoitukseen apuna voi käyttää eri ISAKMP-vaiheita. Samaan aikaan kun tunneliin simuloidaan liikennettä, komennolla **show crypto isakmp** näkee, missä vaiheessa tunnelin muodostus on.

```
RAFUASA1(config)# show crypto isakmp

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1
Total IKE SA: 1

1   IKE Peer: 194.110.231.69
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_WAIT_MSG5
```

Kuvio 18. Esimerkki ISAKMP MM_WAIT_MSG5 -vaiheesta

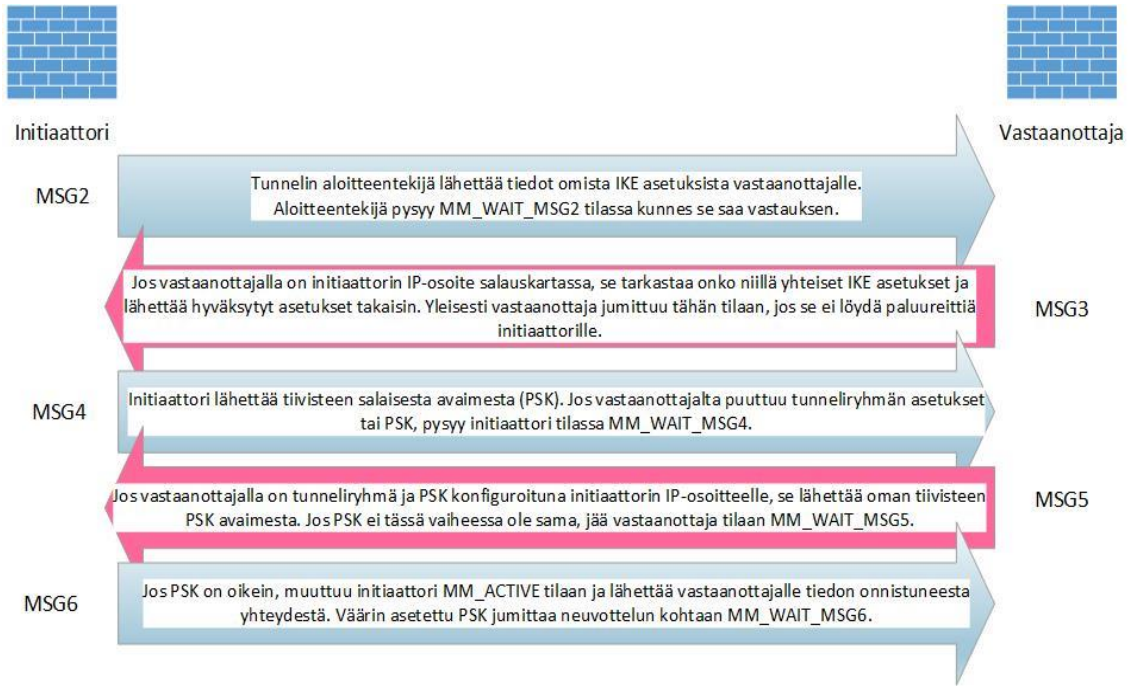
Ensimmäisessä esimerkissä ISAKMP on jumittunut vaiheeseen MM_WAIT_MSG5, koska vastaanottajan PSK oli asetettu väärin.

```
RAFUASA2(config-tunnel-ipsec)# show crypto isakmp

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 R
Total IKE SA: 1

1   IKE Peer: 194.110.231.252
    Type    : user             Role    : initiator
    Rekey   : no               State   : MM_WAIT_MSG2
```

Kuvio 19. Esimerkki ISAKMP MM_WAIT_MSG2 -vaiheesta

Toisessa esimerkissä ISAKMP on jumittunut vaiheeseen MM_WAIT_MSG2, koska IKE-asetuksissa oli erilaiset salausasetukset.

Seuraavassa kuvassa havainnollistetaan eri ISAKMP-vaiheita ja syitä, miksi tunnelin muodostus on jumittunut kyseiseen kohtaan.




Kuvio 20. ISAKMP-vaiheet

## 6.2 Pääsylistoista johtuvat vikatilanteet

Pääsylistoissa olevat merkkivirheet voivat olla syy IPSec-tunnelin toimintahäiriöille. Tunnelin asentamisen jälkeen kannattaa aina suorittaa packet-tracer-komento. Sillä nähdään, nouseeko tunneli pystyyn ja toimiiko sille määritetyt säännöstöt. Suoritetaan packet-tracer-komento RAFUASA1-palomuurissa seuraavasti:

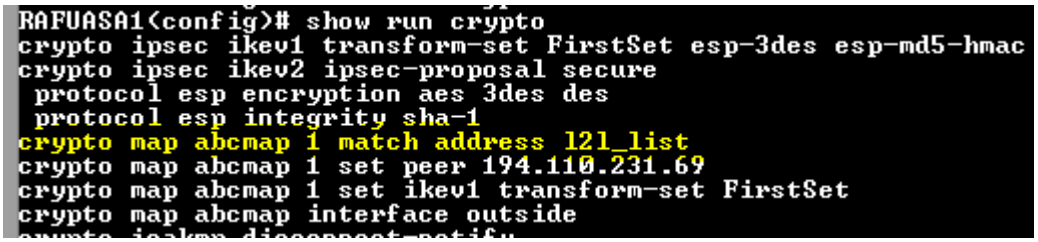
**RAFUASA1(config)# packet-tracer input inside icmp 10.2.2.2 1 1 192.168.100.2**

Ensimmäinen packet-tracer-yritys ei välttämättä onnistu, koska avaimenvaihto on vielä kesken. Toinen kokeilu onnistuu, jos tunnelin asetukset ovat kunnossa.

Pääsylistojen yleisimmät konfiguraatiovirheet sijaitsevat salauskartoissa ja virheellisissä osoitteissa. Pääsylistoihin liittyvissä vikatilanteissa packet-tracer-komennon mukaan yhteys menee läpi, mutta ei missään vaiheessa liikennöi tunneliin. Tämän voi havaita VPN-vaiheen puuttumisesta.


Kuvio 21. Phase 7

Tilanteen korjaamiseksi aloitetaan kirjoittamalla **show run crypto**. Aluksi tulee varmistaa, että salauskartta on sidottu samalla nimellä esiintyvään pääsylistaan.




Kuvio 22. Salauskartan asetukset

```
RAPUASA1(config)# show access-list
access-list cached ACL log flows: total 0, d
            alert-interval 300
access-list 121_list; 1 elements; name hash:
access-list 121_list line 1 extended permit
```

Kuvio 23. Pääsylistojen asetukset

Pääsylistoista tulee tarkistaa myös niiden osumat (engl. hitcount). Jokaisella kerralla liikenteen osuessa siihen tarkoitettuun pääsylistaan osumalaskuri kasvaa yhdellä. Jos pääsylista ei saa osumia, sillä ei ole mitään vaikutusta liikenteeseen.

```
(hitcnt=22)
```

Kuvio 24. Osumalaskuri

## 6.3 Osoitteenmuunnoksesta johtuvat vikatilanteet

Osoitteenmuunnoksista johtuvat vikatilanteet ovat VPN-tunneleissa yleisiä. Ennen tunnelin muodostamista tulee ottaa huomioon, ovatko vastapuolen osoitteet dynaamisia, staattisia ja miten reititys on hoidettu palomuurille. Osoitteenmuunnokset ovat aina tapauskohtaisia, joten niille ei voida määrittää yleistä ratkaisumallia. Seuraavissa esimerkeissä käydään läpi yleisimpiä ongelmia.

Ensimmäisessä esimerkissä IPSec-tunnelin asetukset ovat muuten oikein, mutta tunneliin liittyvät NAT-säännöstöt puuttuvat. Vianetsintä tulee aloittaa aina packet-tracer-komennolla ja ISAKMP-vaiheiden tarkkailulla. **packet-tracer input inside icmp 10.2.2.2 1 1 192.168.100.2**. Jos paketti tippuu kohdassa viisi, on vika todennäköisesti NAT-säännöstössä.

```
Phase: 5
Type: NAT
Subtype:
Result: DROP
Config:
nat (inside,outside) source dynamic any interface
Additional Information:
```

Jos paketti tippuu kohdassa viisi, tulee osoitteenmuunnossäännöstö tarkistaa komennolla **show nat detail**.

```
RAFUASA1(config)# show nat detail
Manual NAT Policies (Section 1)
1 (inside) to (outside) source dynamic any interface
    translate_hits = 9790, untranslate_hits = 245
    Source - Origin: 0.0.0.0/0, Translated: 194.110.231.252/27
RAFUASA1(config)#
```

Tulostuksesta voidaan lukea, että palomuurissa kaikki liikenne muunnetaan osoitteeksi 194.110.231.252. IPSec-tunnelissa tämä ei kuitenkaan toimi. Kun halutaan yhdistää päätepisteet **10.2.2.2** ja **192.168.100.2** pitää palomuurille kertoa, että näitä osoitteita ei haluta muuntaa. Korjauksena lisätään uusi NAT-säännöstö palomuuriin, jolla testikone1 voi liikennöidä kohti testikone2:ta ilman alkuperäisen osoitteen muutosta. Lisätään NAT-sääntö ja tarkastetaan tila uudestaan komennolla **show nat detail**. Kuvassa olevat sisäverkko ja ulkoverkko ovat erikseen määriteltyjä objekteja. Objektit sisältävät niille asetetut verkkotiedot, ja niiden käyttö helpottaa konfigurointia.

**nat (inside,outside) source static sisaverkko sisaverkko destination static ulkoverkko ulkoverkko**

```
RAFUASA1(config)# nat (inside,outside) source static sisaverkko sisaverkko des$
RAFUASA1(config)#
RAFUASA1(config)# show nat detail
Manual NAT Policies (Section 1)
1 (inside) to (outside) source dynamic any interface
    translate_hits = 9874, untranslate_hits = 246
    Source - Origin: 0.0.0.0/0, Translated: 194.110.231.252/27
2 (inside) to (outside) source static sisaverkko sisaverkko   destination static ulkoverkko ulkoverkko
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.2.2.0/24, Translated: 10.2.2.0/24
    Destination - Origin: 192.168.100.0/24, Translated: 192.168.100.0/24
```

Muutoksien jälkeen suoritetaan packet-tracer-komento ja tarkistetaan nouseeko tunneli.

**packet-tracer input inside icmp 10.2.2.2 1 1 192.168.100.2**

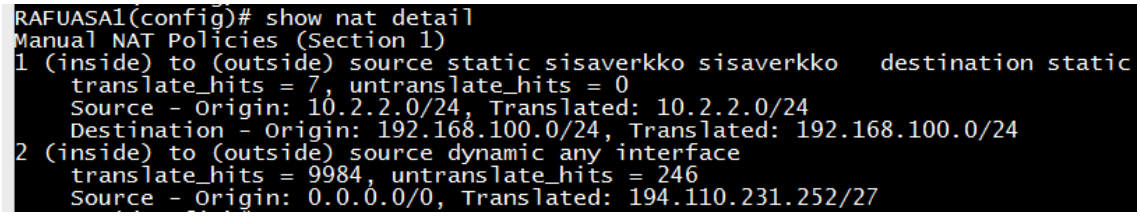
Tässä tapauksessa havaitaan, että paketit tippuvat edelleen kohdassa viisi. Huomattavaa on myös, että uusi NAT-säännöstö ei ole saanut yhtään osumaa. Tämä johtuu siitä, että Cisco ASA -palomuurissa sääntöjen järjestyksellä on väliä. Esimerkiksi tässä tapauksessa liikenne 10.2.2.0/24 -verkosta muuttuu osoitteeksi 194.110.231.252. Tästä syystä IPSec-tunneliin liittyvien sääntöjen pitää tulla ensin yleisiä sääntöjä. NAT-säännön järjestystä voi muuttaa asettamalla sille järjestysluvun. Järjestysluku kertoo, mihin kohtaan uusi sääntö sijoitetaan.

Poistetaan vanha sääntö komennolla:

**no nat (inside,outside) source static sisaverkko sisaverkko destination static ulkoverkko ulkoverkko**

Ja lisätään sama sääntö uudestaan ensin yleistä NAT-säännöstöä.

**nat (inside,outside) 1 source static sisaverkko sisaverkko destination static ulkoverkko ulkoverkko**

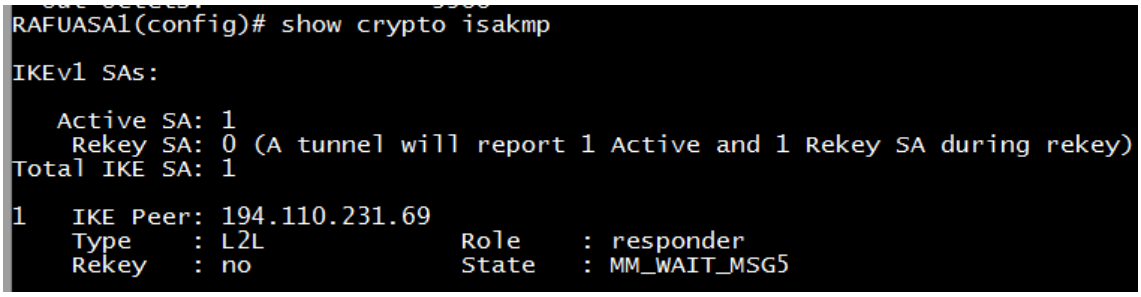



Muutoksien jälkeen tunneli toimii taas normaalisti. Myös uusi NAT-säännöstö on saanut osumia eli se toimii.

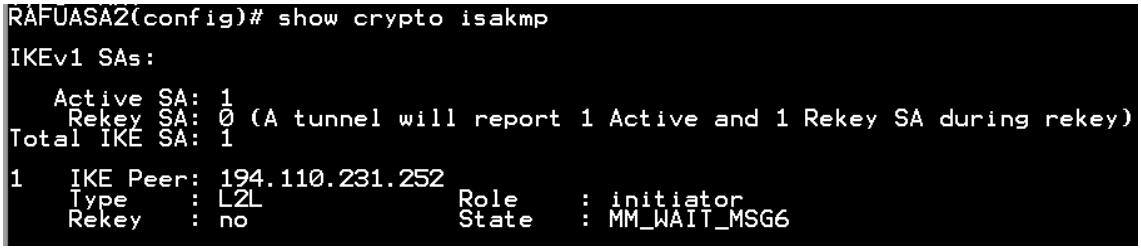
## 6.4 Esijaettujen avainten vikatilanteet

Esijaetut avaimet ovat suosituin varmennusmenetelmä IPSec Site-to-Site -tunneleissa. On kuitenkin hyvä pitää mielessä, että PSK ei tarjoa minkäänlaista suojausta. Hyvä esijaettu avain on pitkä, erikoismerkkejä sisältävä ja mitään tarkoittamaton salasana.

Esijaettu avain vaihdetaan osapuolten kesken ennen IPSec-tunnelin muodostamista. Jako voi tapahtua esimerkiksi tekstiviestillä tai salattuna PDF-tiedostona. Esijaetun avaimen väärinkirjoitus tai tunneliryhmän puuttuminen johtaa virheeseen. Edellä esitetyt ongelmat johtavat ISAKMP-neuvottelun jumittamiseen kohtaan MSG5 tai MSG6. Seuraavana on kaksi esimerkkiä.




Kuvio 25. Virheellisesti asennettu esijaettu avain RAFUASA1 palomuurissa




Kuvio 26. Virheellisesti asennettu esijaettu avain RAFUASA2 palomuurissa

Esijaettu avain ei näy normaalissa show running config-tilassa. Sen saa kuitenkin näkyviin komennolla **more system:running-config**. Tilanne korjaantuu, kun esijaetut avaimet ovat samat tunnelin päätepisteissä.

## 6.5 Diffie-Hellman ja tiivistefunktion vikatilanteet

Diffie-Hellman ja tiivistefunktioiden vikatilanteita syntyy, kun osapuolilla ovat erilaiset salauskartan asetukset. Kuviosta 20 (ISAKMP-vaiheet) voi havaita, että nämä vikatilanteet näkyvät ISAKMP-vaiheen jumittumisesta kohtaan MSG2 tai MSG3. Salauskartan vikatilanteet eivät valitettavasti ole aina näin selkeitä. Tämän takia niissä suositellaan käytettäväksi syvempää vianetsintää lokipalvelun avulla. Lokipalvelun voi aktivoida Ciscon palomuureissa komennolla **logging enabled**. Kun lokipalvelin on päällä ja suoritetaan packet-tracer-komentoja, saadaan yksityiskohtaista tietoa tunnelin neuvottelusta ja tilanteesta. Seuraavassa esimerkissä näytetään, mitä eriävät Diffie-Hellman-ryhmät aiheuttavat.

Suoritetaan komento packet-tracer input inside icmp 192.168.100.2 1 1 10.2.2.2 RAFUASA2-palomuurissa. Samaan aikaan luetaan lokipalvelinta RAFUASA1-palomuurista.

```
IP = 194.110.231.69, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + NOTIFY (11) + NONE (0) tot
IP = 194.110.231.69, All SA proposals found unacceptable
IP = 194.110.231.69, Error processing payload: Payload ID: 1
IP = 194.110.231.69, IKE MM Responder FSM error history (struct &0xcbe2bd08)  <state>, <event>:  MM_DONE,
V_START_MM-->MM_START, EV_START_MM-->MM_START, EV_START_MM-->MM_START, EV_START_MM-->MM_START, EV_START_MM
IP = 194.110.231.69, IKE SA MM:dd12f5e8 terminating:  flags 0x01000002, refcnt 0, tuncnt 0
IP = 194.110.231.69, sending delete/delete with reason message
IP = 194.110.231.69, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + VE

IP = 194.110.231.69, processing SA payload
Phase 1 failure:  Mismatched attribute types for class Group Description:  Rcv'd: Group 2  Cfg'd: Group 5
Phase 1 failure:  Mismatched attribute types for class Group Description:  Rcv'd: Group 2  Cfg'd: Group 5
IP = 194.110.231.69, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + NOTIFY (11) + NONE (0) tot
IP = 194.110.231.69, All SA proposals found unacceptable
IP = 194.110.231.69, Error processing payload: Payload ID: 1
IP = 194.110.231.69, IKE MM Responder FSM error history (struct &0xcbe2bd08)  <state>, <event>:  MM_DONE,
V_START_MM-->MM_START, EV_START_MM-->MM_START, EV_START_MM-->MM_START, EV_START_MM-->MM_START, EV_START_MM
IP = 194.110.231.69, IKE SA MM:e11b5d8a terminating:  flags 0x01000002, refcnt 0, tuncnt 0
IP = 194.110.231.69, sending delete/delete with reason message
IP = 194.110.231.69, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + VE
```

Kuvio 27. Kaappaus lokiviesteistä packet-tracer-simulaation aikana

```
IP = 194.110.231.69, processing SA payload
Phase 1 failure:  Mismatched attribute types for class Group Description:  Rcv'd: Group 2  Cfg'd: Group 5
Phase 1 failure:  Mismatched attribute types for class Group Description:  Rcv'd: Group 2  Cfg'd: Group 5
IP = 194.110.231.69, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + NOTIFY (11) + NONE (0) tot
IP = 194.110.231.69, All SA proposals found unacceptable
IP = 194.110.231.69, Error processing payload: Payload ID: 1
IP = 194.110.231.69, IKE MM Responder FSM error history (struct &0xcbe2bd08)  <state>, <event>:  MM_DONE,
_START_MM-->MM_START, EV_START_MM-->MM_START, EV_START_MM-->MM_START, EV_START_MM-->MM_START, EV_START_MM
IP = 194.110.231.69, IKE SA MM:b9790858 terminating:  flags 0x01000002, refcnt 0, tuncnt 0
```

Kuvio 28. Kaappaus lokiviesteistä osa 2

Packet-tracer-simulaation yhteydessä tulee etsiä toistuvia virheilmoituksia. Kriittisimmät virheilmoitukset palomuurissa sisältävät sanan failure. Edellisistä viesteistä löytyy useita ”failure”-viestejä, joita on syytä tarkastella syvemmin. Failure-viestissä kerrotaan saapuneesta Diffie-Hellman ryhmästä 2, kun taas toisessa palomuurissa on konfiguroitu Diffie-Hellman ryhmä 5.

```
Phase 1 failure:  Mismatched attribute types for class Group Description:  Rcv'd: Group 2  Cfg'd: Group 5
Phase 1 failure:  Mismatched attribute types for class Group Description:  Rcv'd: Group 2  Cfg'd: Group 5
```

Kuvio 29. IKE-neuvottelun virhe vaiheessa 1

Komennolla **show run crypto** voidaan tarkastella salauskarttojen asetuksia.

**RAFUASA1**

```
crypto ikev2 enable outside
crypto ikev1 enable outside
crypto ikev1 policy 1
 authentication pre-share
 encryption 3des
 hash sha
 group 5
 lifetime 43200
```

**RAFUASA2**

```
crypto ikev2 enable outside
crypto ikev1 enable outside
crypto ikev1 policy 1
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 43200
```

Lokiviestien ja salauskarttojen avulla pystyttiin selvittämään ongelman alkuperä. Tunnelin korjaus tapahtuu muuttamalla Diffie-Hellman-ryhmät samaksi **configure terminal** -tilassa.

**crypto ikev1 policy 1**

**no group 5**

**group 2**

# 7 Yhteenveto

Työn tavoitteena oli esitellä lukijalle yleisiä VPN-tekniikoita ja antaa apua IPSec-tunnelissa esiintyviin vikatilanteisiin. Tulevaisuudessa yritykset siirtyvät yhä enemmän IPv6-protkollan käyttöön, joka puolestaan kasvattaa monipuolisen IPSec:n suosiota entisestään. VPN-tekniikkaan liittyviä yksityiskohtia on selvitetty kirjallisuuden sekä verkkolähteiden pohjalta. Varsinainen tietoperusta muodostuu omakohtaisesta kokemuksesta, jota olen saanut nauttia työskennellessäni vanhemman asiantuntijan alaisuudessa.

Käytännön osuudessa luotiin IPSec-tunneli kahden Cisco ASA-5505 –palomuurin välille. Ciscon palomuurit olivat minulle entuudestaan tuttuja työelämästä ja koulussa suoritettujen kurssien perusteelta. Testiympäristön toteutukseen saatiin käyttöön kaksi julkista IP-osoitetta, joiden avulla mahdollistettiin realistinen ympäristö. Tunnelin asennus tapahtui oman tietotaidon perusteella eikä siinä ei esiintynyt ongelmia. Kun asetukset oli määritelty, siirryttiin vikatilanteiden simulointiin.

Tämän opinnäytetyön tekeminen oli mielenkiintoinen ja opettava kokemus. Oman testiympäristön synnyttämä vapaus lisää rohkeutta kokeilla uusia asioita, ilman pelkoa siitä, että aiheuttaisi rahallisia vahinkoja. Vikatilanteiden selvityksessä tuli vastaan myös paljon uusia asioita, mihin ei ollut ennen kiinnittänyt huomiota.

## Lähteet


1 Virtuaalinen erillisverkko. 2016. Verkkodokumentti. Vesa Viljanen. https://www.yksityisyydensuoja.fi/content/virtuaalinen-erillisverkko.

2 MPLS IP VPN Services Market Analysis. 2015. Verkkodokumentti. Grand View Research. http://www.grandviewresearch.com/industry-analysis/multi-protocol-labelled-switching-internet-protocol-virtual-private-network-market.

3 VPN-opas. 2016. Verkkodokumentti. Symantec. http://www.symantec.com/region/fi/resources/vpn.html.

4 E. Lewis, J. Davies. 2003. Deploying Virtual Private Networks with Microsoft Windows Server 2003, Microsoft Press, Redmond.

5 Virtual Private Networking. 2001. Perlmutter, Bruce – Zarkower, Jonathan L. Zarkower.

6 A Tool for Teaching Security Concepts. 2010. IPsecLite. ACM DL.

7 SSL VPN. 2006. Verkkodokumentti. Cisco. http://www.cisco.com/c/en/us/td/docs/ios/12_4t/12_4t11/htwebvpn.html#wp1053815.

8 IPSec Security Associations (SAs). 2002. Verkkodokumentti. Cisco. http://www.ciscopress.com/articles/article.asp?p=24833&seqNum=7.

9 Internet Key Exchange (IKE). 2002. Verkkodokumentti. Cisco. http://www.ciscopress.com/articles/article.asp?p=25474&seqNum=7.

10 Access Control List. 2003. Verkkodokumentti. Cisco. http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/acl_overview.html.

11 Tilaton pakettisuodatus. 2010. Verkkodokumentti. Wikipedia. https://fi.wikipedia.org/wiki/Tilaton_pakettisuodatus.

12 Configuring NAT. 2003. Verkkodokumentti. Cisco. http://www.cisco.com/c/en/us/td/docs/security/asa/asa80/configuration/guide/conf_gd/cfgnat.html.

13 Preshared key authentication. 2005. Verkkodokumentti. Microsoft. https://technet.microsoft.com/en-us/library/cc782582(v=ws.10).aspx.

14 Diffie-Hellman -avaimenvaihto (2-A). 2010. Verkkodokumentti. TUT. https://wiki.tut.fi/Tietoturva/Diffie-Hellman-avaintenvaihto(2-A).

15 Kryptografinen tiivistefunktio. 2012. Verkkodokumentti. TUT. https://sec.cs.tut.fi/maso/materiaali.php?id=198.

16 Mikä tiivistefunktio on vielä turvallinen? 2011. Verkkodokumentti. Nixu Oyj. https://www.nixu.com/fi/blogi/2011-03/mik%C3%A4-tiivistefunktio-viel%C3%A4-turvallinen.

17 IKE kuva. https://supportforums.cisco.com/sites/default/files/legacy/7/5/1/2157-ws22.gif.

18 Diffie-Hellman kuva. https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange#/media/File:Diffie-Hellman_Key_Exchange.svg.