jamk.fi

IP-salaimien evaluointi reititysverkossa

Riku Kuismanen

Opinnäytetyö
Joulukuu 2019
Tekniikan ala
Insinööri (AMK), Tietotekniikan koulutusohjelma

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Kuismanen, Riku	Opinnäytetyö, AMK	12/2019
	Sivumäärä 28	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi
IP-salaimien evaluointi reititysverkossa

Tutkinto-ohjelma
Tietotekniikan koulutusohjelma

Työn ohjaaja(t)
Karo Saharinen, Mika Rantonen

Toimeksiantaja(t)
Puolustusvoimien Logistiikkalaitos, Järjestelmäkeskus

Tiivistelmä

Tutkimuksen tilaajana toimiva Puolustusvoimien Logistiikkalaitoksen Järjestelmäkeskus suunnittelee ja toteuttaa erilaisia järjestelmä- ja verkkointegraatioita useille asiakkaille.

Toimeksiantona oli vertailla kahden eri IP-salaimen soveltuvuutta erään asiakkaan verkkoympäristöön ja päivittäisiin käyttötapauksiin. Tutkimuksen suunnitteluun osallistui tilaajan lisäksi tilaajan asiakas. Asiakkaan edustaja oli mukana myös toteutusvaiheessa.

Tutkimuksen toteutusvaiheessa suoritettiin useita testitapauksia, jotka kuvasivat asiakkaan päivittäistä toimintaa. Testaus suoritettiin laboratorioverkossa, joka kuvasi asiakkaan verkkoympäristöä hyvin tarkasti. Verkkoympäristö sisälsi usean eri suojaustason verkkoja. Testidatana käytettiin ICMP ECHO –viestejä ja videotiedostoja. Testauksessa käytettiin sekä unicast että multicast–tiedonsiirtoa. Testaus toteutettiin syksyllä 2017. Tutkimuksen pääpaino siirrettiin jo varhaisessa vaiheessa vain toisen salaimen testaukseen, koska huomattiin, että keskinäinen vertailu ei ollut järkevää.

Tutkimuksen tavoitteena oli testata asiakkaan päivittäisiä toimintoja IP-salatussa verkossa. Lisäksi tarkasteltiin muutamia erikoistapauksia. Näissä onnistuttiin hyvin ja suurempia teknisiä haasteita ei kohdattu. Kaikki testit saatiin suoritettua, ja avoimia kysymyksiä ei jäänyt. Testauksen tuloksena saatiin aikaan reunaehdot IP-salaimien käytölle asiakkaan nykyisen verkkoarkkitehtuurin ja asiakasjärjestelmien näkökulmasta.

Avainsanat (asiasanat)
IP-salain, suojaustaso, unicast, multicast

Muut tiedot (Salassa pidettävät liitteet)

jamk.fi

Description

Author(s)	Type of publication	Date
Kuismanen, Riku	Bachelor's thesis	12/2019
		Language of publication: Finnish
	Number of pages: 28	Permission for web publication: x

Title of publication

Evaluation of IP encryptors in routed network

Degree programme

Information Technology

Supervisor(s)

Saharinen Karo, Rantonen Mika

Assigned by

FDF Logistics Command, Joint Systems Centre

Abstract

The study was assigned by the Joint Systems Centre in FDF Logistics Command where the planning and implementation of systems and networks is carried out for many customers.

The assignment for the research was to compare the suitability of two different IP encryptors to a customer's network infrastructure and to daily use cases. The assigner and their customer participated in the planning of the research. The customer also participated to the execution part.

Many test cases describing the customer's daily operation were run in the execution phase of the research. Testing was executed in a laboratory network, which represented the customer's network infrastructure quite accurately. The network infrastructure contained several different security level networks. ICMP ECHO messages and video files were used as test data. Both unicast and multicast transmission was used in testing. The tests were run in autumn 2017. The main focus of the research was removed to testing one encryptor only in very early phase of the research it was noticed that a mutual comparison of ecryptors was not feasible.

The objective of the research was to test customer's daily operations in an IP encrypted network. Some additional special cases were also considered. The tests were run successfully without any major technical issues. All the test cases were completed and no open question remained after the testing. The preconditions for the use of IP encryptors in the current infrastructure of the customers network and systems were accomplished as the result of the research.

Keywords/tags

IP encryptor, security level, unicast, multicast

Miscellaneous (Confidential information)

Sisältö

Kuviot

Lyhenteet

AGW	Administration Gateway
AH	Authentication Header
BGP	Border Gateway Protocol
DHCP	Dynamic Host Configuration Protocol
ESP	Encapsulating Security Payload
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	Internet Protocol Security
JÄRJK	Järjestelmäkeskus
KS	Key Server
MPLS	Multiprotocol Label Switching
OSPF	Open Shortest Path First
PIM-SM	Protocol Independent Multicast-Sparse Mode

PIM-SSM	Protocol Independent Multicast-Source Specific Mode
PVLOGL	Puolustusvoimien Logistiikkalaitos
QoS	Quality of Service
SA	Security Associations
SSH	Secure Shell
ST	Suojaustaso
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

1 Lähtötilanne

1.1 Työn tilaaja

Työn tilaajana toimi Puolustusvoimien Logistiikkalaitoksen (PVLOGL) Järjestelmäkeskus (JÄRJK). PVLOGL on suoraan Pääesikunnan alla toimiva organisaatio. PVLOGL vastaa koko puolustusvoimien materiaalin hankkimisesta, elinkaaren hallinnasta, ja myös osallistuu materiaalin kunnossapitoon. PVLOGL suunnittelee tiedonsiirtoverkkoja asiakkailleen erilaisten asiakasjärjestelmien tiedonsiirtotarpeiden mukaisesti. Asiakkaita ja asiakasjärjestelmiä on useita. PVLOGL osallistuu tietoverkkojen koko elinkaaren hallintaan, rakentamisesta ylläpitoon.

Työn testausosiot suoritettiin JÄRJK:n Tiedonsiirtojärjestelmäsektorin laboratoriotiloissa Tikkakoskella syksyllä 2017.

1.2 Toimeksianto

PVLOGL:n eräällä asiakkaalla on tietojärjestelmiä, joiden tieto on salaista. Tästä johtuen tiedonsiirron ajaksi data on salattava. Opinnäytetyön tarkoitus oli evaluoida kahta IP-salainta tilaajan osoittamassa verkkoympäristössä. Toinen salaintuotteista oli valmiiksi käyttöönotettuna ja toinen asennettiin samaan ympäristöön rinnakkaiseksi salausratkaisuksi. Tutkittava asia oli, soveltuvatko molemmat IP-salaimet asiakkaan tarpeisiin.

Evaluoinnin perusteiksi valittiin soveltuvuus asiakasjärjestelmien tiedonsiirtotarpeisiin päivittäisessä toiminnassa. Asiakasjärjestelmien asettamien teknisten vaatimusten lisäksi tarkasteltiin salaimien konfiguroinnin, hallinnan ja ylläpidon helppoutta.

1.3 Tutkimusmenetelmät

Tutkimus koostui kolmesta vaiheesta. Ensimmäinen vaihe oli ympäristön rakentaminen ja konfigurointi. Toisessa vaiheessa suunniteltiin ja suoritettiin testaukset. Salaimia testattiin asiakasympäristön kaltaisessa laboratorioverkossa. Testattavia kohteita oli salaimien suoriutuminen normaalissa operoinnissa. Lisäksi tutkittiin salaimien selviytymistä erilaisista vikatilanteista. Salaimien ominaisuuksia tai suorituskykyä ei verrattu keskenään, koska salaimet eivät olleet tarkoitettu samanlaiseen käyttöön. Testeissä ei mitattu datamääriä, vaan testitulokset kertovat, toteuttaako salain asiakkaan vaatimuksen ja millä reunaehdoilla? Kolmannessa vaiheessa testitulokset analysoitiin ja tehtiin johtopäätökset.

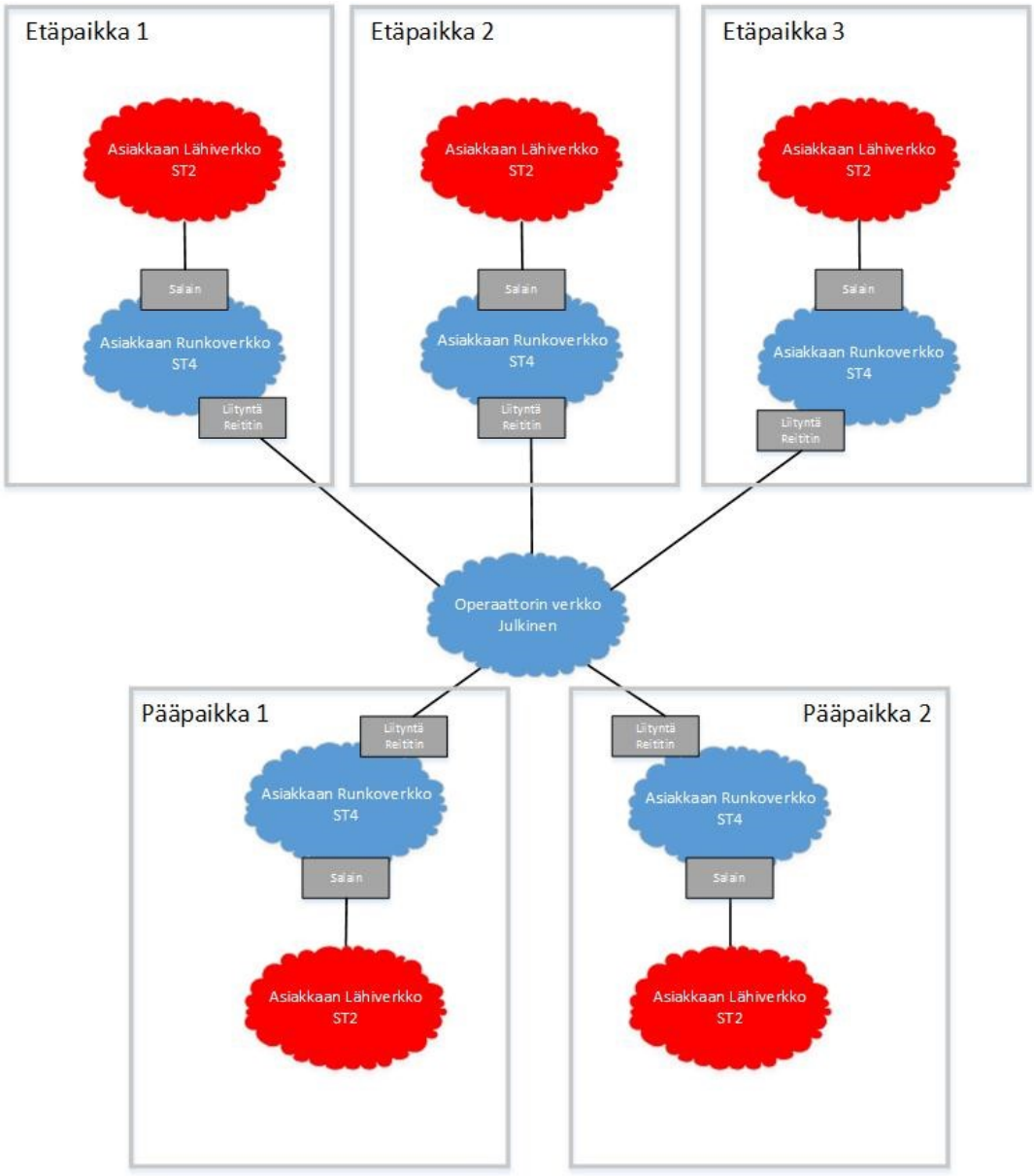
2 Evaluoinnin lähtökohdat

2.1 Tilaajan verkkoympäristö

Asiakasympäristö, jossa tutkimus suoritettiin, asetti salaimille tiettyjä suorituskykyvaatimuksia. Verkkoympäristö on reititetty IP-verkko, jossa asiakasjärjestelmät tarvitsevat sekä unicast- että multicast–tiedonsiirtoa. Järjestelmillä on lisäksi erilaisia tietoliikenneprofiileja sekä erilaisia tarpeita tietoliikenteen viiveelle ja viiveen vaihtelulle. Asiakasjärjestelmiin itseensä ei tässä työssä keskitytty, vaan niiden vaatimuksiin. Asiakasympäristö sisältää lisäksi kolmea eri tietoturvatasoa. Tietoturvatasot tuovat mukanaan vaatimuksen liikenteen salaamiselle. (Teknisen ICT-ympäristön tietoturvataso –ohje 2012.)

Verkkotopologia

Testausympäristön verkko voidaan jakaa loogisesti kolmeen eri tietoturvatasoon: suojaustaso II (ST2), suojaustaso IV (ST4) ja julkinen. Kuviosta 1 käyvät ilmi verkon eri suojaustasot.

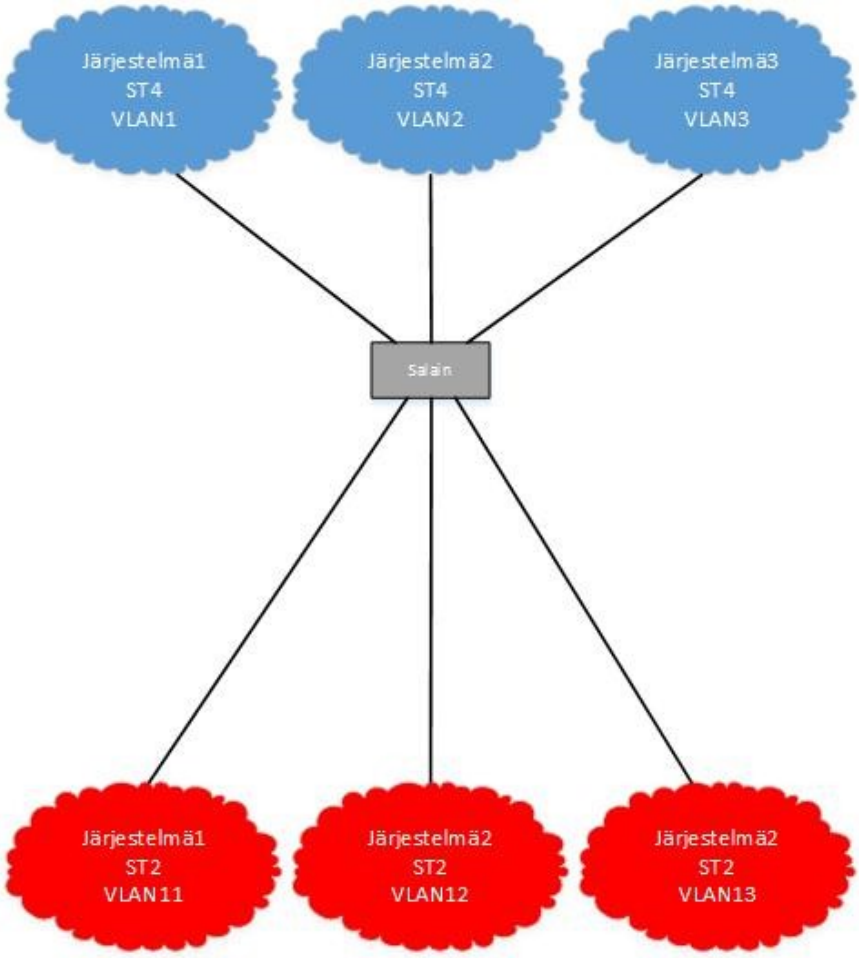


Kuvio 1. Verkon tietoturvatasot

Testiympäristössä lähetetään ja vastaanotetaan dataa pääpaikkojen välillä sekä pääpaikkojen ja etäpaikkojen välillä. Etäpaikoilta lähetetään lisäksi data multicast–protokollilla pääpaikoille. Etäpaikkojen välillä liikennöinti estetään. Data salataan siirron ajaksi, kun se siirretään ST4-verkon ja julkisen verkon yli.

2.2 Asiakasjärjestelmät

Testauksen perusteena ovat asiakkaan käyttämät järjestelmät. Järjestelmät ovat verkossa toisistaan loogisesti eroteltuina. Looginen erottelu tehdään käyttäen VLAN-tunnisteita ja virtuaalisia reititysinstansseja. Kuviossa 2 on esitetty järjestelmien looginen erottelu asiakkaan verkossa.



Kuvio 2. Järjestelmien looginen erottelu

3 Kryptografiset vaatimukset julkisella sektorilla

Salaustuotteille on asetettu kryptografiset vähimmäisvaatimukset, jotta niitä voidaan käyttää turvallisuusluokitellun tiedon salaamiseen, kun toimitaan korkean uhkatason

tietoverkoissa. Tällaisiksi verkoiksi luokitellaan julkiset, suojaamattomat tietoverkot. Myös alemman suojaustason verkot ja langattomat verkot luokitellaan korkean uhkatason ympäristöiksi. (Viestintäviraston NCSA-toiminnon hyväksymät salausratkaisut 2017.)

Kryptografinen vahvuus määritellään kyseisen menetelmän kyvyllä vastustaa kryptoanalyysiä. Vahvuuteen vaikuttaa tehokkaimpien laskentamenetelmien raskaus laskennallisesti. Tätä vahvuutta voidaan pitää vertailulukuna muihin menetelmiin verrattaessa. Vahvuuden kertoo sen rikkomiseen tarvittava resurssimäärä. (Viestintäviraston NCSA-toiminnon hyväksymät salausratkaisut 2017.)

Viestintävirasto on määrittänyt vähimmäisvaatimukset salaukselle erilaisissa käyttökohteissa. Vaatimukset koskevat käytettäviä algoritmeja ja avainpituuksia. Algoritmeille ja avainpituuksille on eri vaatimukset riippuen suojaustasosta. ST2 –tason salaukselle vaaditaan 512 –bittinen salausavain käytettäessä elliptisiä käyriä. ST4 –tasolle riittää 256 bittinen. Salaustuotteen kokonaisarvioinnissa täytyy ottaa huomioon myös käytettävä tietoliikenne- ja tietoturvaprotokollat, ja niiden versiot. (Viestintäviraston NCSA-toiminnon hyväksymät salausratkaisut 2017.)

4 IP-salauksen teoriaa

IP-liikenteen salaukseen ja tunnelointiin voidaan käyttää useita menetelmiä ja protokollia. Tässä työssä tutkitut salaimet käyttävät Internet Protocol Security (IPSec) -protokollaa salaukseen ja tunnelointiin.

IPSec

IPSEc on joukko protokollia, jotka mahdollistavat salatun VPN-tunnelin toteuttamisen julkisen verkon yli. IPSEc-salausta voidaan käyttää muidenkin tunnelointiprotokollien kanssa. IPSec mahdollistaa liikenteen salaamisen, salausavainten hallinnan ja datan lähettäjän todentamisen. (IPSec VPN Overview. 2019.)

Security Associations

Security Associations (SA) on joukko menetelmiä, joita käytetään VPN-tunnelin osapuolten välillä. Osapuolet sopivat nämä yhdessä ja ne sisältävät tiedon käytetystä salausalgoritmista ja avaimista, käytetyn moodin (tunneli vai kuljetus), avaimien hallintamenetelmän ja SA:n eliniän. Tunneli muodostetaan aina yhteen suuntaan yhden SA:n perusteella. Kaksisuuntaiseen liikennöintiin tarvitaan kaksi SA-paria. (IPSec VPN Overview. 2019.)

Salausavaimien hallinta

Salausavaimia voidaan hallita manuaalisesti tai automaattisesti. Automaattinen avaintenhallinta tapahtuu käyttäen Internet Key Exchange (IKE) –protokollaa (IETF). IKE:ssä voidaan käyttää tunnistautumiseen joko esijaettua avainta, tai sertifikaattia. Avaimet voidaan salata käyttäen useita eri algoritmeja. (IPSec VPN Overview. 2019.)

IPSec protokollat

IPSec jakautuu IP-verkossa kahteen protokollaan. Authentication Header (AH) –protokollalla varmennetaan paketin sisältö ja alkuperäisyys. Pakettiin lisätään tarkistussumma, joka lasketaan satunnaisfunktiolla luodusta merkkijonosta ja salaisesta avaimesta. Encapsulating Security Payload (ESP) –protokollalla salataan koko IP-paketti ja siihen lisätään uusi IP –otsikkokenttä. (IPSec VPN Overview. 2019.)

5 Salaintuotteet

Testauksessa käytettiin kahta eri IP-salainta. Salaimet testiin valitsi työn tilaajan asiakas. Advenican SecuriVPN ISA -tuotteella on hyväksyntä ST II -tasolle ja Instan Safelink salaimella ST III tasolle. Hyväksyntiä hallinnoi Traficomin Kybertuvallisuuskeskus. (Viestintäviraston NCSA-toiminnon hyväksymät salausratkaisut 2017.)

Salaimista oli markkinoilla useampaa eri vaihtoehtoa. Eroavaisuudet liittyivät salainten tarjoamaan kaistanleveyteen. Tutkimuksessa ei huomioitu kaistanleveyksiä, koska käytössä oli eri kaistanleveyttä tukevat salaimet. Safelinkistä oli käytössä 1GB versio ja ISA:sta 100 Mb versio.

5.1 Safelink

Insta Defsec Oy:n valmistama Safelink IP-salain oli testauksessa käytetyistä salaimista toinen. Salaimella on STIII-hyväksyntä. Safelink tukee multicast-liikennettä PIM-SM ja PIM-SSM (IETF) ja dynaamisia reititysprotokollia OSPF (Moy 1998) ja BGP (Rekhter, Li & Hares 2006). Salaimessa on palomuuritoiminnallisuuksia ja QoS-ominaisuuksia. Salain tukee myös VLAN-tunnisteita 802.1Q. (HomChaudhuri & Foschiano 2008) Liikenteen salaus on mahdollista sertifikaattiperusteisena tai esijaetulla avaimella. Käytetyt salausalgoritmit ovat riittävän vahvoja ST2-salaukseen. Safelinkissä on tarjolla myös muita palveluita, kuten DHCP-palvelin. Safelink tukee keskitettyä hallintaa. Avaimiston hallintaan on erillinen ympäristö.

Kuviossa 3. on Safelink IP-salain (Insta Defsec 2019)

Kuvio 3. Safelink IP-salain (Insta Defsec 2019)

5.2 SecuriVPN ISA

Toinen testattava IP-salain oli Advenican SecuriVPN ISA. Salain on ST2-hyväksytty ja tukee dynaamista reititystä. ISA on laajasti kansainvälisesti käytetty. Salain tukee dynaamista OSPF reititysprotokollaa. Hallinta on keskitetty, ja avaimistojen hallinta on

mahdollista eriyttää. Asiakasympäristössä käytetään VLAN-erottelua salaustunneleiden läpi. ISA:n tapauksessa erottelu on tehtävä muulla tavoin, esimerkiksi muualla verkkolaitteissa. Rajoituksena on myös IP-aliverkkojen tuettu maksimimäärä, joka on 16. Aliverkkojen kokoa ei ole rajoitettu. Tämä täytyy ottaa huomioon aliverkotusta ja reititystä suunniteltaessa.(Advenica 2018.) Kuviossa 4 on ISA IP-salain.

Kuvio 4. ISA IP-salain (Advenica 2018.)

6 Testit

6.1 Yleistä

Testit suoritettiin JÄRK:n laboratorioverkossa, joka kuvaa asiakkaan ympäristöä tarkasti. Testauksessa käytettiin myös ulkoista toimijaa apuna laitteiden konfiguroinnissa ja avaimiston tuottamisessa. Testien aloittamista todettiin nykyisen käytössä olevan salausratkaisun olevan vahvasti räätälöity kyseiseen asiakasverkkototeutukseen ja tätä ei haluta testejä varten lähteä muuttamaan. Näin ollen salaimien rinnakkaisen vertailun sijaan päätettiin testata, suoriutuuko kyseinen salain testiskenaarioista, jotka kuvaavat päivittäisessä toiminnassa eteen tulevia tilanteita.

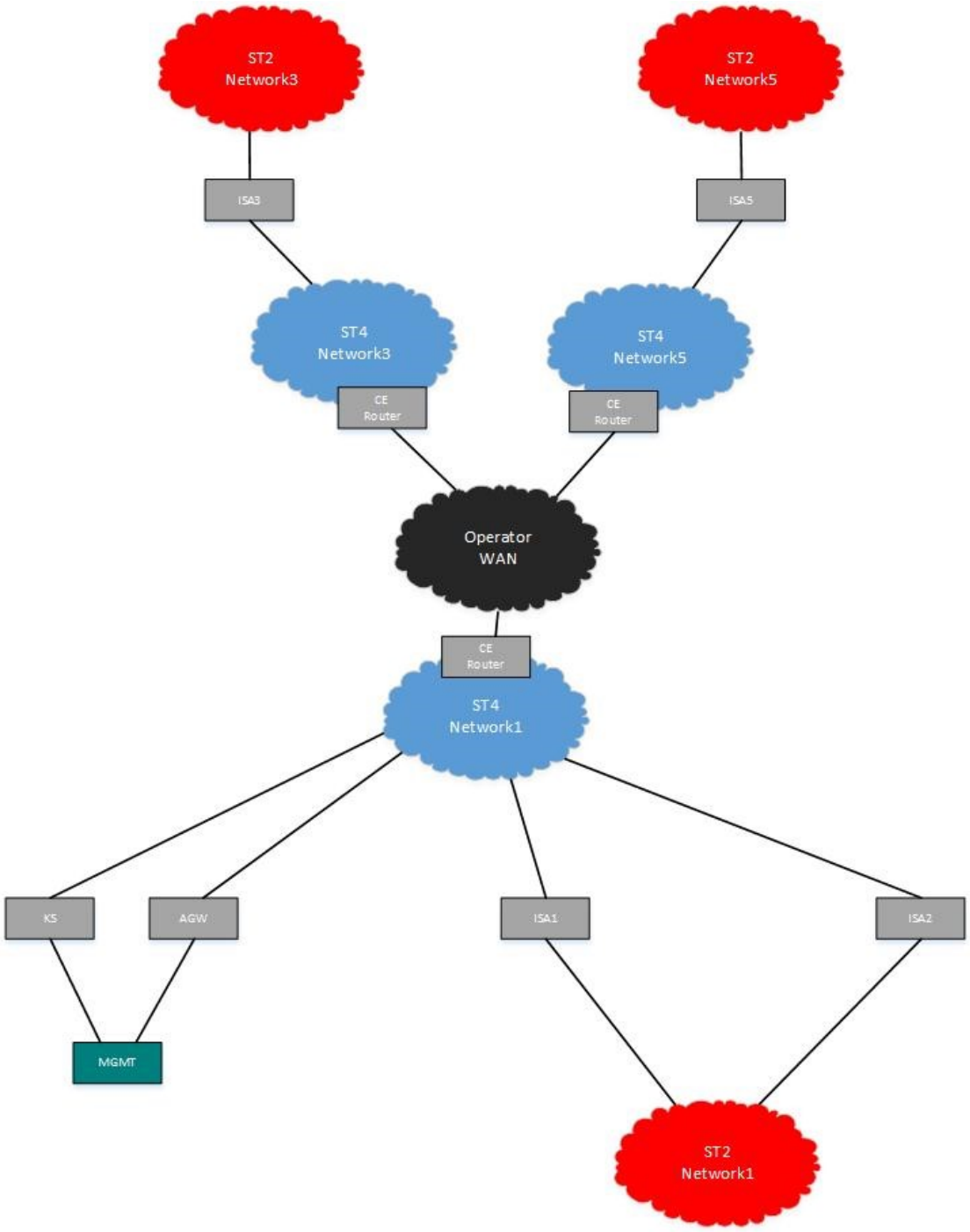
6.2 Testiskenaariot

6.2.1 Yleistä

Testausympäristö ISA-salaimien osalta oli kuvion 5 mukainen. Käytössä oli 4 IP-salainta, jotka ovat kuvassa ISA1- ISA5. ISA1 ja ISA2 –salaimet toimivat klusterina siten, että toinen on aktiivinen ja toinen valmiustilassa. ISA3 ja ISA5 –salaimet toimivat etäpaikkojen salaimina. Operaattorin verkkoa mallinsi laboratorion MPLS-runkoverkko. KS on avainpalvelin ja AGW salaimien hallintayhteyden salain. MGMT-palvelin on ISA-salaimien keskitetty hallintapalvelin.

Hallintapalvelin ja avainpalvelin olivat laitetoimittajan valmiiksi asentamia. Ympäristön rakentaminen voitiin aloittaa suoraan salaimien konfiguroinnilla. Verkkosuunnitelmat oli myös valmiiksi tehtyinä. Safelink-salaimet olivat valmiiksi asennettuina ja käytössä. Safelink-salaimien suorituskyky ja ominaisuudet olivat ennestään tuttuja ja tiedossa. Safelink-salaimia ei tässä tutkimuksessa testattu.

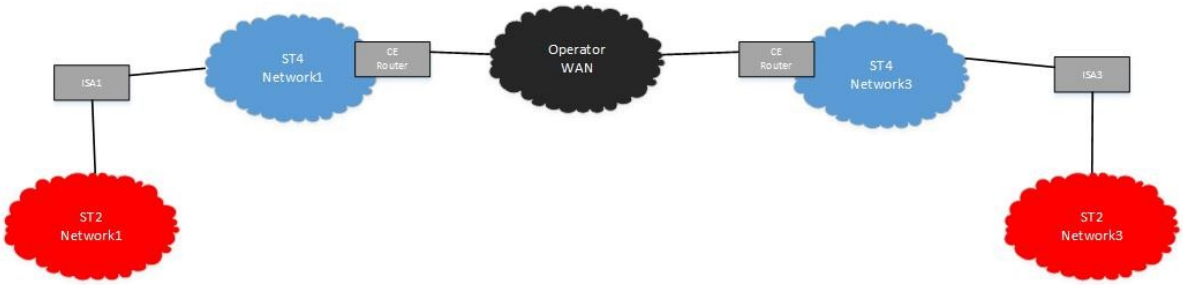
Ennen varsinaisia testien aloittamista todettiin nykyisen käytössä olevan salausratkaisun olevan vahvasti räätälöity kyseiseen asiakasverkkototeutukseen ja tätä ei haluta testejä varten lähteä muuttamaan. Tämän vuoksi testiskenaariot irrotettiin varsinaisesta verkkoympäristöstä, ympäristö rakennettiin erilliseksi. Verkko sisälsi silti loogisesti kaikki osat asiakkaan verkosta.



Kuvio 5. ISA-testausympäristö

6.2.2 Skenaario 1

Testiskenaarion tarkoitus oli todentaa, että salaustunnelit oli konfiguroitu oikein ja verkko mahdollistaa järjestelmien tietoliikenteen etäpaikan ja pääpaikan välillä. Testidatana käytettiin ICMP ECHO (PING) -viestejä (Postel 1981), joilla todennettiin IP-yhteydellisyys paikkojen välillä. Toisena sovelluksena käytettiin SSH-protokollaa, jolla otettiin etähallintayhteys etäpaikan ST2-verkossa olevaan palomuuriin pääpaikan ST2-verkossa olevalla työasemalla. Kolmantena sovelluksena lähetettiin videota etäpaikasta pääpaikkaan käyttäen UDP-protokollaa (Postel 1980) ja unicast-lähetystä. Lähettämiseen ja vastaanottamiseen käytettiin työasemia ja VLC-sovellusta. Kuviossa 6 on esitetty testiskenaarion looginen kuva.



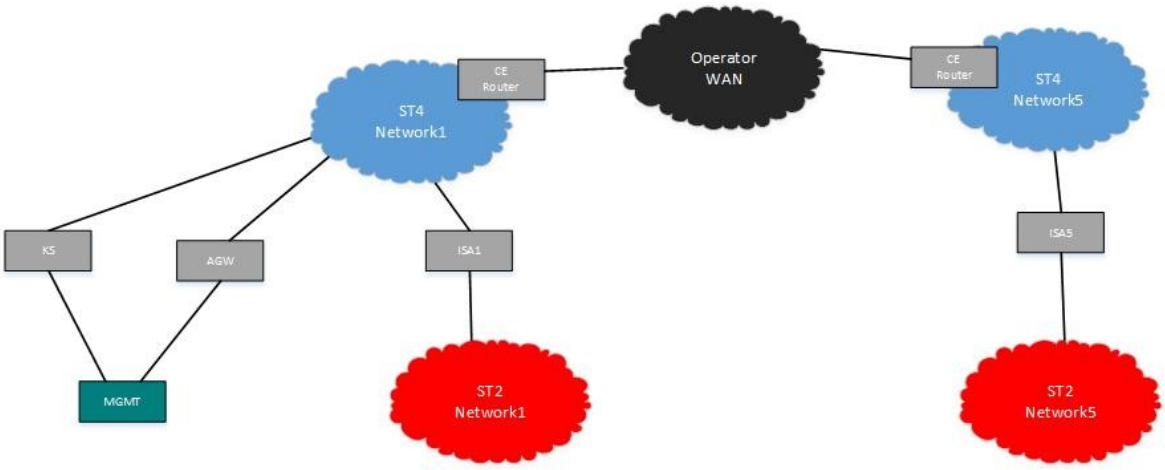
Kuvio 6. Testiskenaarion 1 looginen kuva

6.2.3 Skenaario 2

Testiskenaariossa testattiin etähallintaan ja kunnossapitoon liittyviä toimintoja. Ensimmäinen testauskohde oli etäpaikan salaimen liikennöinnin katkaisu keskitetystä hallinnasta. Samalla VPN -tunnelin läpi lähetettiin PING-viestejä, joilla todennettiin salaustunnelin katkeaminen. Keskitetyn hallinnan toimivuus todennettiin käynnistämällä etäpaikan salaimen tunnelit uudelleen.

Toisena testinä korvattiin salain toisella ennakkoon tyhjällä salaimella. Tilanne kuvasi rikkoutuneen laitteen korvaamista varalaitteella. Tämän suorittamiseen käytettiin laitevalmistajan ohjeistamaa prosessia, jota ei tässä työssä avata tarkemmin.

Kolmantena testauskohteena oli laitteen uudelleenkäynnistyksen aiheuttaman katkoksen pituus. Laitteet saattavat joskus jumiutua tai vaatia uudelleenkäynnistyksen muusta syystä. Sähkökatkot saattavat myös aiheuttaa uudelleenkäynnistyksen. Skenaarion 2 testitapaukset suoritettiin kuvion 7 mukaisessa loogisessa verkossa.

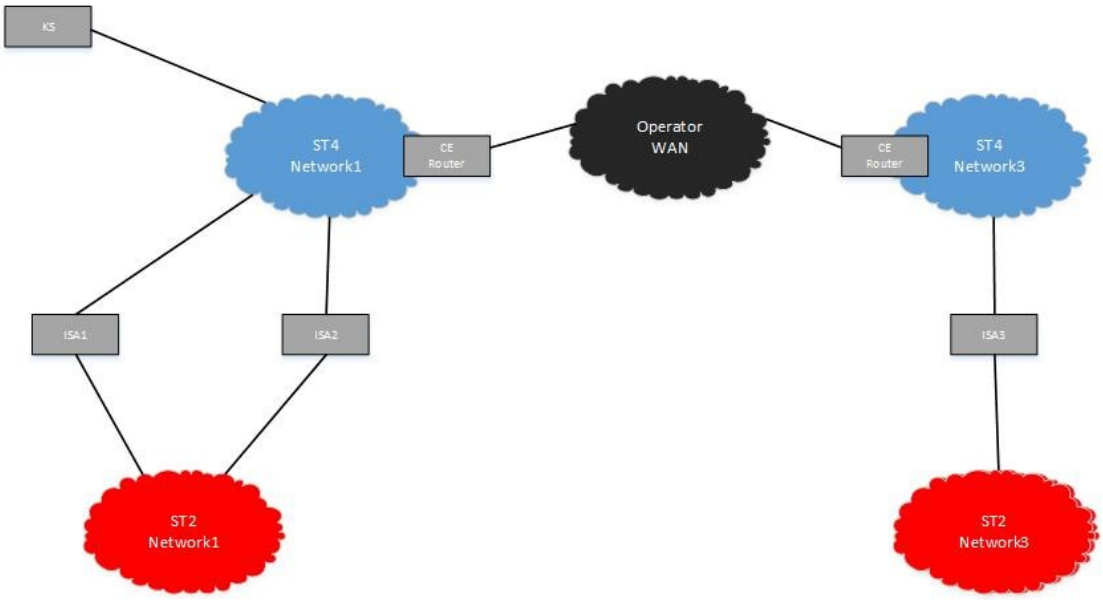


Kuvio 7. Testiskenaarion 2 looginen kuva

6.2.4 Skenaario 3

Testiskenaariossa testattiin kahdennuksen failover-toiminnallisuutta. Salaimet ISA1 ja ISA2 on konfiguroitu toimimaan kahdennettuna. Kahdennus on toteutettu Active Standby –tyylisesti. Tämä tarkoittaa sitä, että toinen salaimista on kerrallaan aktiivisena ja toinen on valmiustilassa. Salaimet tarkkailevat toistensa tilaa erikseen konfiguroidun ajan välein. Tässä tapauksessa tuo aika on kaksi sekuntia. Testissä kuvataan aktiivisen laitteen rikkoutumista uudelleenkäynnistämällä laite ja irrottamalla salaimen ST4-verkon liityntä. Testissä todennetaan toiminnallisuuden toimiminen ja mitataan palveluiden katkosaika salaustunneleiden uudelleenmuodostumisen vuoksi.

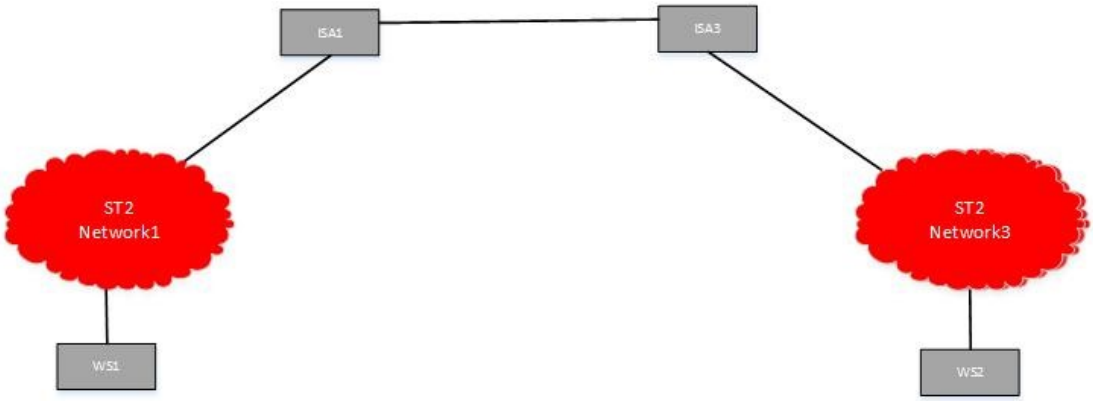
Toisena testitapauksena testattiin Fallback-moodin toimintaa. Salainlaitteille on luotu konfiguraatio toimimaan myös silloin, kun avaimiston hallintapalvelimelle ei saada yhteyttä. Tällöin otetaan käyttöön Fallback-moodi, jossa käytetään esijaettua avaimistoa. Testissä kytkettiin avaintenhallintapalvelin irti verkosta. Molemmat testitapaukset todennetaan kuvion 8 mukaisessa verkkoympäristössä.



Kuvio 8. Kahdennettu salain

6.2.5 Skenaario 4

Tässä skenaariossa testattiin vielä erillisinä testeinä multicastin läpimeno erillisjärjestelyin. Kaksi salainta kytkettiin suoraan toisiinsa mustan verkon (ST4) puolella. Salatuissa verkoissa oli multicast-liikenteen lähdekone. Tässä käytettiin normaalia työasemaa, jolla lähetettiin videota multicast ryhmäosoitteeseen. Toisen salaimen salatussa verkossa oli multicast-tilaajatyöasema, jolla tilattiin samaa multicast-ryhmää. Testi suoritettiin kuvion 9 mukaisessa ympäristössä.



Kuvio 9. Multicast testi

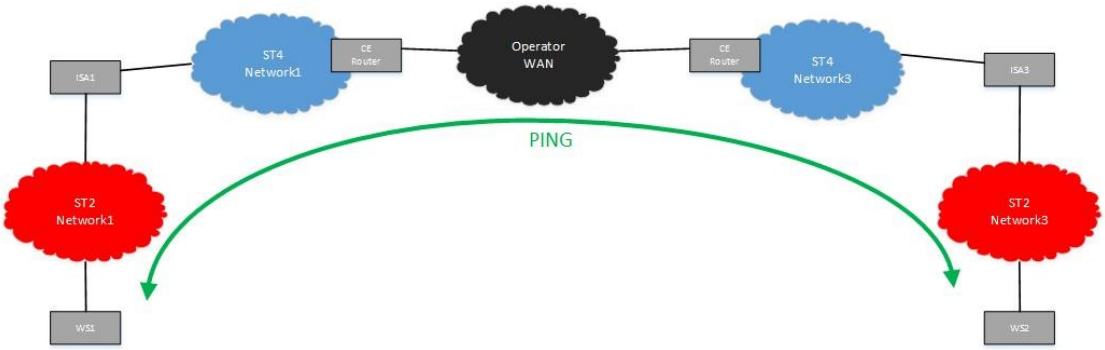
Toisena erillistestinä testattiin salaimen toiminta tilanteessa, jossa se on virheellisesti kytketty. Salaimen salaamaton ja salattu rajapinta kytkettiin samaan verkkoon ja tarkkailtiin laitteen toimintaa. Testissä käytettiin wireshark –sovellusta, jolla verkon liikennettä voidaan kaapata ja tarkastella.

7 Testitulokset

Testien suorittamiseen oli varattu aikaa yksi viikko. Viikon aikana kohdattiin muutamia teknisiä haasteita. Nämä eivät kuitenkaan vaikuttaneet testituloksiin.

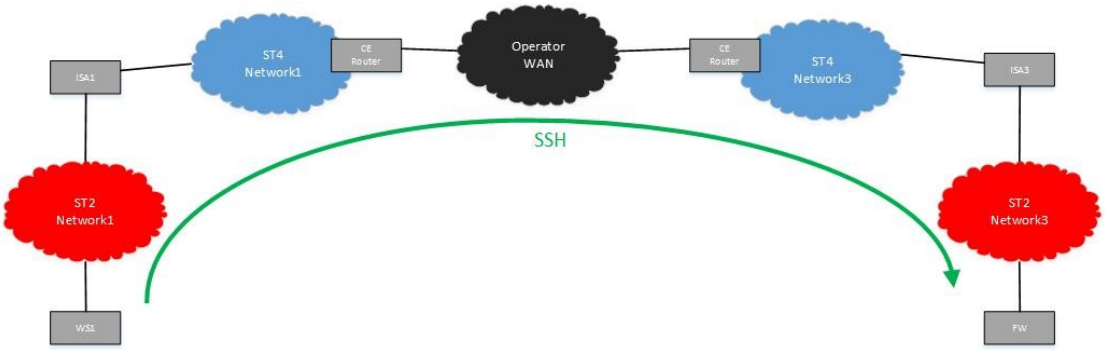
7.1 Testiskenaario 1

Skenaariossa oli tarkoitus selvittää, oliko IP-salaimet konfiguroitu oikein ja oliko saatu avaimisto toimiva. Ensimmäisen testin tarkoitus oli todentaa IP-yhteydellisyys päätepaikan ja etäpaikan välillä. Tämä todennettiin lähettämällä PING –viestejä ST2 –verkkojen välillä kuvion 10 mukaisesti. Yhteydellisyys todennettiin ilman ongelmia.



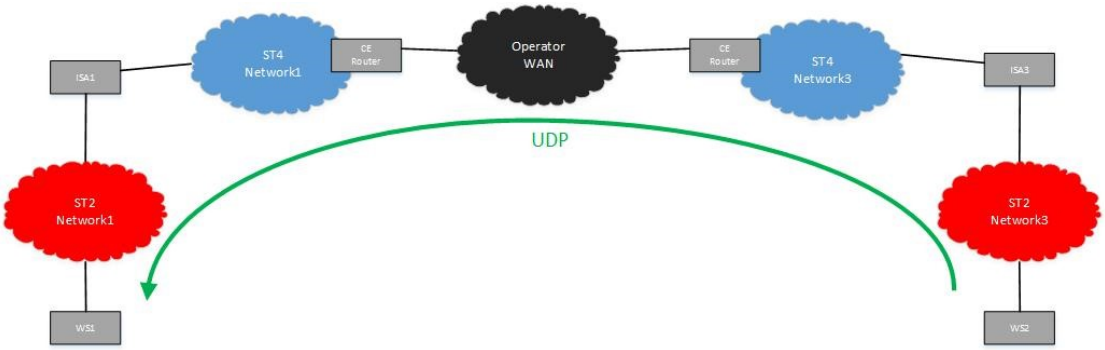
Kuvio 10. Yhteydellisyystesti

Toinen testi kuvasti esimerkiksi verkkolaitteen etähallintayhteyttä. Otettiin SSH-protokollalla hallintayhteys onnistuneesti etäpaikan ST2-verkon palomuuriin kuvion 11 mukaisesti. Testissä ei havaittu ongelmia.



Kuvio 11. Palomuurin etähallintatesti

Kolmannella testillä kuvattiin tavallista datavuon lähettämistä etäpaikasta pääpaikkaan. Tähän käytettiin videotiedostoa jota lähetettiin verkon yli etäpaikasta pääpaikkaan. Lähettäminen ja vastaanottaminen tehtiin VLC-sovelluksella. Lähettämiseen käytettiin UDP-protokollaa ja unicast-lähetystä kuvion 12 mukaisesti. Video saatiin vastaanotettua ja suoratoistettua pääpaikassa onnistuneesti. Videoon tuli jonkin verran häiriötä, mutta tämä ei johtunut IP-salauksesta. Häiriön todettiin johtuvan käytetystä videokodekista. Testi uusittiin oikeiden videokodekkien kanssa onnistuneesti.



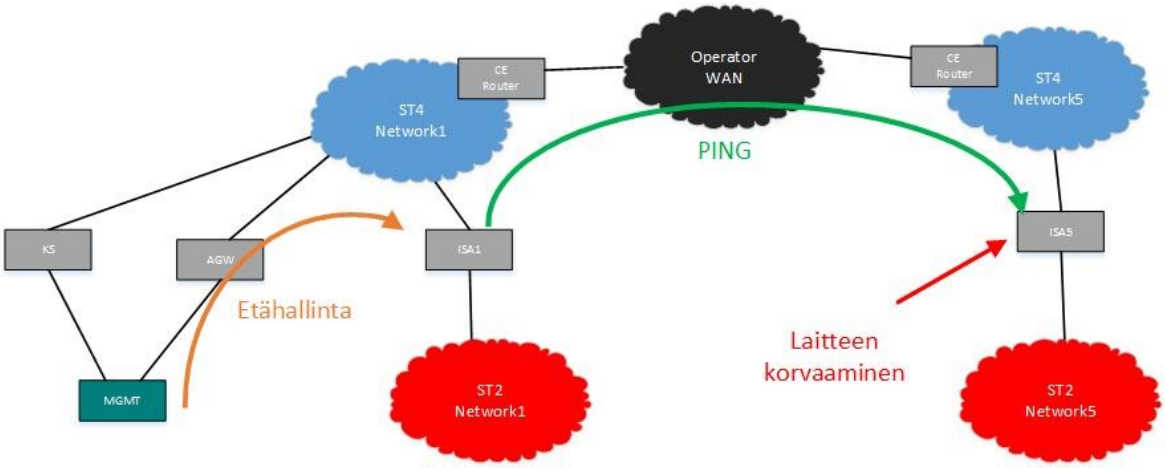
Kuvio 12. Unicast-videotesti

7.2 Testiskenaario 2

Tässä testiskenaariossa todettiin etähallinnan toimintaa. Tarkoitus oli selvittää, sopiiko ratkaisu asiakkaan käyttöön hallintaominaisuuksiltaan. Ensimmäisenä testinä katkaistiin salaustunneli käyttäen hallintapalvelimen yhteyttä. Liikenteen katkeaminen todennettiin IP-yhteydellisyyden katkeamisella. Ping-viestit eivät enää menneet perille. Hallintayhteys IP-salaimeen säilyi, kuten oli tarkoituskin. Salaimen liikennöinti käynnistettiin uudelleen, jolloin salaustunneli muodostui ja ping-viestit alkoivat jälleen kulkea perille. Etähallinta toimi moitteettomasti, vaikka hyötydatan kulkeminen oli keskeytynyt. Tämän mahdollisti hallintayhteyksien eriyttäminen muusta verkosta.

Toisessa testissä kuvattiin rikkoutuneen laitteen korvaamista ehjällä varalaitteella. Tähän saatiin laitevalmistajalta prosessi, jota seuraamalla laitevaihto onnistui ja salaustunnelit saatiin muodostettua uudelleen. Tätä prosessia ei tässä tutkimuksessa avata. Laitevaihto toimi halutulla tavalla.

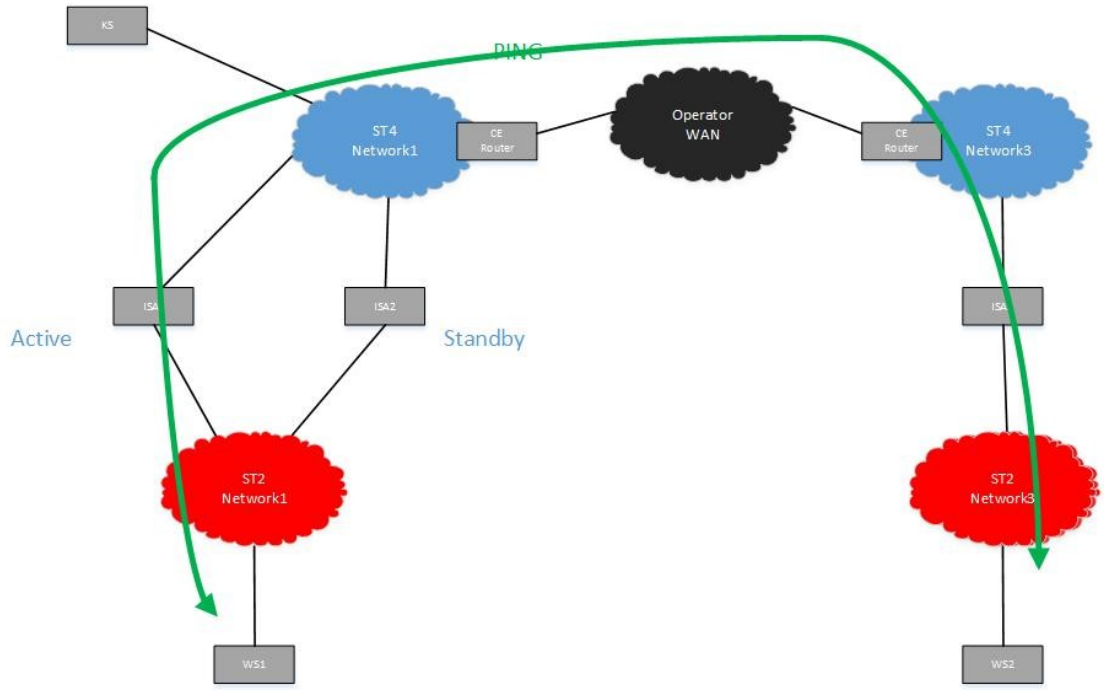
Kolmannessa testissä mitattiin katkosaikaa tilanteessa, jossa IP-salain käynnistyy uudelleen. Tällainen voi johtua useasta eri syystä ja on melko yleinen tilanne. Testaus suoritettiin käyttäen kahta työasemaa ja lähettämällä ping-viestejä työasemien välillä. Katkosaikojen keskiarvoksi saatiin noin kaksi minuuttia, mikä vastasi ennalta arvioitua arvoa. Katkoksen pituus oli riittävän lyhyt asiakkaan näkökulmasta katsottuna. Kuviossa 13 on esitetty skenaarion testitapaukset.



Kuvio 13. Etähallinta ja laitevaihto

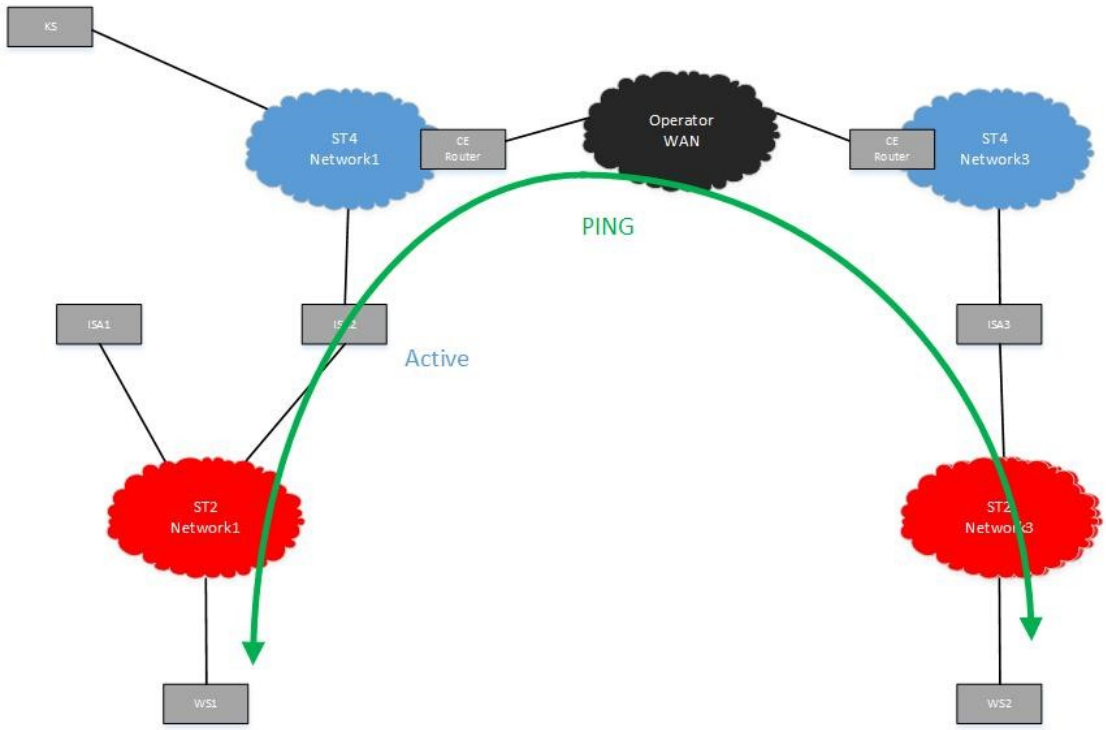
7.3 Testiskenaario 3

Testissä todennettiin kahdennetun salaimen toimintaa. Pääpaikassa tietoverkon ja salaustunnelien toimintaa pyritään varmentamaan kahdennuksella. Kahdennettu IP-salain toimii active/stanby –moodissa. Toinen IP-salaimista on aktiivisessa roolissa kerrallaan ja toinen valmiustilassa kuvion 14 mukaisesti.



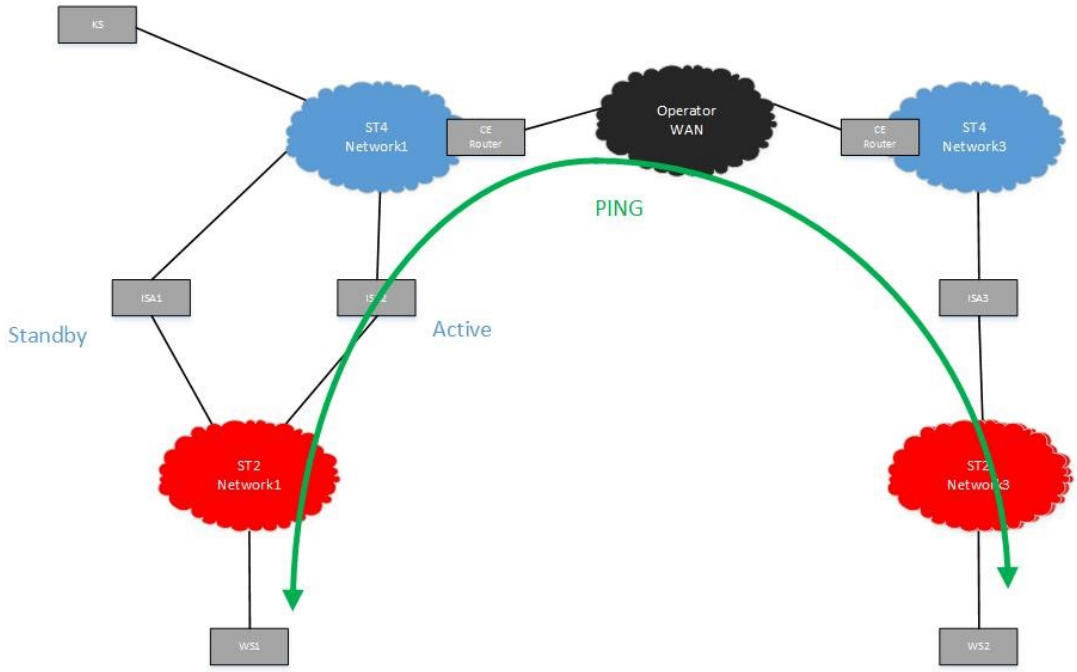
Kuvio 14. Kahdennustestin alkutilanne

Salaimet tarkkailevat toistensa tilaa jatkuvasti. Testissä aktiivisen salaimen ST4-verkon liityntä irrotettiin, jolloin salaustunnelit lakkasivat toimimasta. Salain myös käynnistettiin uudelleen. Testissä mitattiin aikaa tunneleiden uudelleenmuodostukselle. Testaukseen käytettiin työasemia ja ping-viestejä samalla tavalla kuin aiemmissa testeissä. Valmiustilassa oleva salain siirtyi aktiiviseksi, ja salaustunnelit muodostuivat uudelleen ilman ongelmia kuvion 15 mukaisesti. Katkosaika ping-viesteissä oli noin 15 sekuntia.



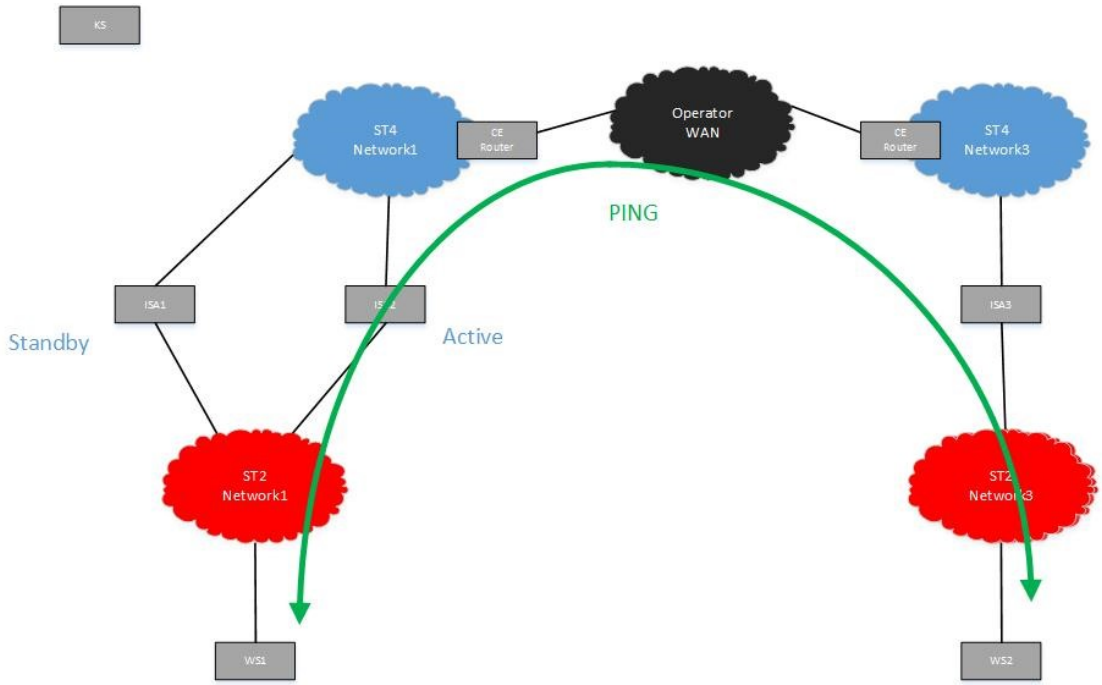
Kuvio 15. Salaustunnelin uudelleenmuosotuminen

Aktiivisesta roolista luopuva IP-salain jouduttiin käynnistämään uudelleen manuaalisesti, jotta se palautui osaksi kahdennusta. Lopputilanteessa kahdennus oli jälleen toiminnassa kuvion 16 mukaisesti. Katkosaika oli asiakkaan mielestä riittävän lyhyt.



Kuvio 16. Kahdennus on palautunut

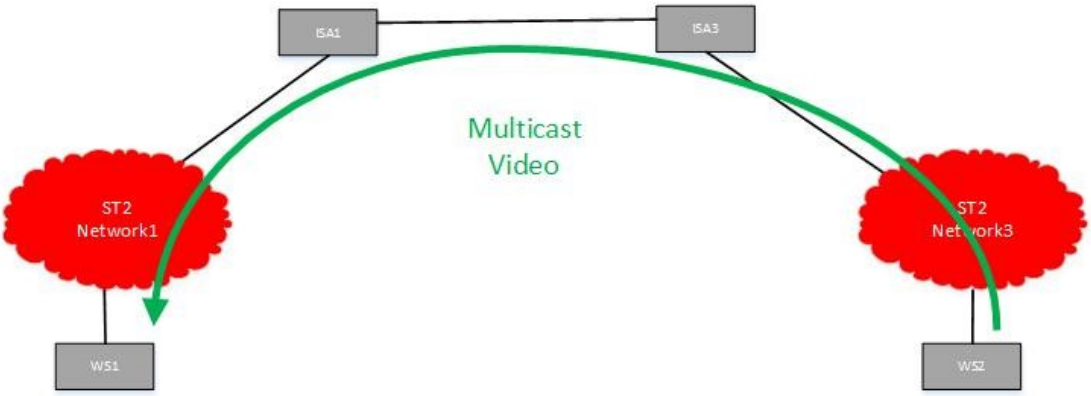
Toisessa testissä todennettiin Fallback-moodin toimintaa. Salaimet toimivat normaalitilanteessa sertifikaattipohjaisesti, mutta salaimille on tuotettu myös esijaetut avaimet avainpalvelimen yhteyden katkeamista varten. Testissä avaimien hallintapalvelin KS kytkettiin pois verkosta, jolloin salaustunnelien muodostaminen sen avulla ei onnistunut. Esijaettua avaimistoa käyttävä konfiguraatio otettiin käyttöön IP-salaimissa ISA1, ISA2 ja ISA3. Tunnelit muodostuivat onnistuneesti, ja testausdata saatiin kulkemaan kuvion 17 mukaisesti. Testaukseen käytettiin ping-viestejä. Esijaetun avaimiston käyttöönotto täytyi tehdä manuaalisesti jokaiselle IP-salaimelle.



Kuvio 17. Fallback-moodi käytössä ilman avainpalvelinta

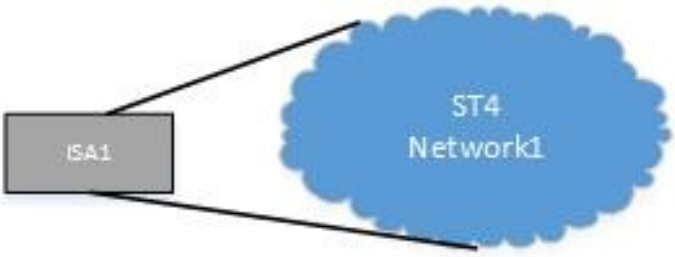
7.4 Testiskenaario 4

Testiskenaarion tarkoitus oli todentaa kaksi erillistä käyttötapausta ja toiminnallisuutta. Ensimmäisessä testissä todennettiin multicast liikenteen läpimeno salaustunnelin kautta. Tämä on oleellinen toiminnallisuus asiakkaan järjestelmien kannalta. Testiä varten IP-salaimet kytkettiin suoraan toisiinsa ST4-verkon puolelta. Multicast liikenteen lähettämiseen käytettiin VLC-sovellusta. Testidatana toimi videotiedosto. Lähettäjänä ja vastaanottajana toimivat työasemat kuvion 18 mukaisesti. Videon tilaaminen suoratoistona verkosta käyttäen multicast-ryhmäosoitetta onnistui ongelmitta.



Kuvio 18. Multicast-video toimii

Toisella testillä todennettiin laitteen toimintaa tilanteessa, jossa IP-salaimen ST4- ja ST2-verkot ovat yhdistyneet kuvion 19 mukaisesti. Kyseessä on virheellinen kytkentä, jossa eri salausluokkien tieto pääsee väärään verkkoon. IP-salain käyttää ARP-protokollaa tilanteen huomaamiseen ja menee error-tilaan. Salain täytyi käynnistää manuaalisesti uudelleen, jotta se voitiin palauttaa normaaliin tilaan, ja osaksi kahdennusta.



Kuvio 19. Virheellinen kytkentä

Kokonaisuutena testit osoittivat IP-salaimen suoriutuvan testiskenaarioista melko hyvin. Osa toiminnoista vaatii manuaalista operointia ja osa jopa itse fyysiselle laitteelle tehtäviä toimia. Tämä johtuu turvallisuusvaatimuksista liittyen laite- ja salausavainten hallintaan, joissa on merkittävä ero käytössä olevan ST III ja testatun ST II -salaimen kohdalla. Asia on huomioitava avaintenhallinta- ja ylläpitotoimenpiteitä suunniteltaessa.

8 Johtopäätökset

8.1 Tutkimuksen lopputulos

Tutkimuksen tarkoitus oli alun perin evaluoida kahta eri IP-salainta tilaajan asiakkaan verkkoympäristössä. Vaatimukset IP-salaimen suorituskyvylle ja toiminnallisuuksille tulivat asiakkaan järjestelmiltä. Järjestelmien tarpeet tietoverkolle olivat osittain toiminnallisia, kuten multicast protokollien käyttö ja varmennetut yhteydet. Järjestelmien datan arkaluonteisuus asetti verkolle myös vaatimuksia, joilla tietoturvaa voidaan parantaa, kuten eri turvaluokat ja looginen erottelu järjestelmien välillä. Ennen varsinaisia testejä ja niiden valmisteluja todettiin nykyisen käytössä olevan salausratkaisun olevan vahvasti räätälöity kyseiseen asiakasverkkototeutukseen ja tätä ei haluttu testejä varten lähteä muuttamaan. Tämän vuoksi testaus keskitettiin IP-salaimen testaamiseen keskinäisen vertailun sijaan. Laitteet olivat lainalaitteita ja testaukseen osallistui myös ulkopuolisia tahoja, joten ei ollut järkevää tuhlata kaikkien aikaa turhaan tekemiseen. Asiakkaan tahdosta päädyttiin testaamaan, suoriutuuko IP-salain annetuista skenaarioista ja millä reunaehdoilla.

Salainverkon avainpalvelin ja hallintapalvelin saatiin laitevalmistalta valmiiksi asennettuina. Laitteiden avaimistot oli myös valmiiksi tuotettu ulkopuolisen toimijan toimesta. Salainverkko konfiguroitiin yhteistyössä ulkoisen toimijan kanssa. Heillä oli jo ennestään kokemusta kyseisestä IP-salaimesta, joten konfigurointi sujui helposti.

Testiskenaariot oli mietitty etukäteen asiakkaan kanssa vastaamaan nykyisen kaltaista operointia. Skenaarioita jouduttiin hieman muuttamaan testauksen päämäärän vaihduttua. Testiskenaariot sujuivat hyvin. Pieniä teknisiä haasteita ilmeni, mutta ne saatiin ratkaistua ja testit suoritettua loppuun. Testauksen lopputulemana on, että IP-salain voisi sopia käytettäväksi nykyisen salaimen kanssa yhdessä. Nykyiseen verkkoarkkitehtuuriin ja asiakasjärjestelmien vaatimuksiin se ei pysty suoraan vastamaan, mutta salaimen käyttökohteet voisivat olla eri verkon osissa. IP-salaimen ST2-hyväksyntä myös muissa maissa tarjoaa mahdollisuuden esimerkiksi kansainvälisien yhteyksien salaamiseen.

8.2 Jatkokehitys

ISA-salaimen kehitystä kannattaa seurata jatkossakin. IP-salaimen tukemat protokollat ja toiminnallisuudet varmasti kehittyvät. Todennäköistä on myös, että järjestelmien vaatimukset kehittyvät jatkossa. Salaimen mahdollisuutta käytettäväksi ilman yhteyttä avaimistopalvelimeen voisi myös tutkia tarkemmin jatkossa. Nykyinen arkkitehtuuri toimii ilman yhteyttä aivaimistopalvelimeen.

IP-verkon salausta ei ole järkevää perustaa vain yhden tuotteen varaan. Useampi salaustuote tarjoaa joustavuutta erilaisiin verkon laajennustarpeisiin ja erilaisten järjestelmien vaatimuksiin. Useampi salaintuote antaa myös varmuutta toiminnalle tilanteessa, jossa esimerkiksi jonkin salauksen luotettavuus menetetään.

Testaus voisi olla järkevää uusia jopa samanlaisena uudestaan, koska testit suoritettiin 2017 syksyllä ja laitteet ovat varmasti kehittyneet tuon jälkeen.

8.3 Pohdinta

Opinnäytetyön tekeminen toimi hyvänä oppimiskokemuksena. Aiemmasta vastaavanlaisesta työstä on kulunut jo useampi vuosi, ja työelämässä tekeminen ja raportointi on luonteeltaan hyvin erilaista. Työssä haastavinta oli päättää, mille tasolle tekninen dokumentointi viedään. Haastavaa oli myös asettaa oletukset työn lukijan osaamisesta. Opinnäytetyön laatiminen toimi hyvänä muistutuksena tutkimuksen vaativuudesta ja työmäärästä. Työhön oli haastavaa löytää tarpeeksi aikaa, koska päivittäinen virkatyö vaatii oman veronsa. Välillä oli haastavaa löytää motivaatiota kirjoittamiseen, koska omat työtehtävät liittyvät samoihin asioihin.

Lähteet

HomChaudhuri S. & Foschiano M. 2008. Cisco Systems' Private VLANs: Scalable Security in a Multi-Client Environment

Fenner B. & Handley M. 2016. Protocol Independent Multicast - Sparse Mode (PIM-SM) https://tools.ietf.org/html/rfc7761 viitattu 21.11.2019.

Holbrook H. & Cain B. 2006. Source-Specific Multicast for IP
https://tools.ietf.org/html/rfc4607 viitattu 20.11.2019.

Insta DefSec. insta-safelink-esite. 2019. https://www.insta.fi/palvelut/kyberturvallisuus/insta-safelink-vpn viitattu 16.11.2019

IPSec VPN Overview. 2019. https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-ipsec-vpn-overview.html
Juniper Networks. viitattu 17.11.2019

Kaufmann C. & Hoffman P. 2010. Internet Key Exchange Protocol Version 2 (IKEv2)
https://tools.ietf.org/html/rfc5996 viitattu 20.11.2019.

Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen – kansalliset suojaustasot. 2018. Traficom Kybertuvallisuuskeskus.

Moy J. 1998. OSPF Version 2
https://www.rfc-editor.org/rfc/rfc2328.txt
viitattu 21.11.2019.

Postel J. 1981. Internet Control Message Protocol
https://tools.ietf.org/html/rfc777 viitattu 21.11.2019.

Postel J. 1980. User Datagram Protocol
https://tools.ietf.org/html/rfc768

Rekhter Y., Li T., Hares S. 2006. A Border Gateway Protocol 4 (BGP-4)
https://tools.ietf.org/html/rfc4271

Quantum-secure encryption. SecuriVPN. 2018. Advenica..

Viestintäviraston NCSA-toiminnon hyväksymät salausratkaisut. 2017. Traficom Kyberturvallisuuskeskus.

Teknisen ICT-ympäristön tietoturvataso –ohje . 2012. Helsinki: Suomen Yliopisto-paino Oy Valtiovarainministeriö.