jamk

Tietoturvallisen käyttäjänhallinnan kehittäminen testiympäristön avulla

Tietoturvastandardien ja -direktiivien ohjaamana

Valtteri Ojala

Opinnäytetyö, AMK
Marraskuu 2024
Tieto- ja viestintätekniikan tutkinto-ohjelma

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Ojala, Valtteri

Tietoturvallisen käyttäjänhallinnan kehittäminen testiympäristön avulla

Jyväskylä: Jyväskylän ammattikorkeakoulu. Marraskuu 2024, 38 sivua.

Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Tutkimuksellisessa kehittämistyössä käsiteltiin RADIUS-autentikointimallin soveltuvuutta organisaation tietoliikenneympäristöön, tavoitteena vastata ISO/IEC 27000 -tietoturvastandardin ja Euroopan Unionin laatiman kyberturvallisuusdirektiivin vaatimuksiin. Taustalla oli tarve parantaa käyttäjienhallintaa yrityksen ympäristössä, jossa käyttäjillä oli aiemmin jaettuja hallintatunnuksia. Tavoitteena oli luoda tekninen ja hallinnollinen malli, jota noudattamalla voi saavuttaa lähtökohdat hyvälle verkon turvallisuudelle, eheydelle ja käytettävyydelle.

Työssä rakennettiin testiympäristö, jossa luotiin RADIUS-protokolla autentikointipalvelimeksi osaksi pfSense palomuuria. Toteutuksessa käytettiin avoimen lähdekoodin FreeRADIUS-ohjelmistoa, ja autentikointia testattiin virtuaaliympäristössä, jossa hyödynnettiin eri käyttöjärjestelmällä olevia päätelaitteita. Testaus sisälsi tekniset näkökohdat, kuten salattujen yhteyksien varmistaminen, oletusarvoisesti estävän hallintapolitiikan ja lokitietojen seurannan. Testiympäristö rakennettiin virtualisointialustan päälle organisaation ympäristöä mukaillen.

Tulokset osoittivat, että RADIUS-protokolla voidaan implementoida organisaation ympäristöön vastaamaan ISO/IEC 27000 -tietoturvastandardin ja kyberturvallisuusdirektiivin vaatimuksia, mikäli protokolla implementoidaan niin teknisellä, kuin hallinnollisella puolella huolellisesti. Salasanojen ja muiden arkaluontoisten tietojen viestintä voitiin salata, istunnot katkaistiin määrätyn toimettomuusajan jälkeen ja pääsyoikeuksien rajaaminen todettiin toimiviksi.

Johtopäätöksenä todettiin, että RADIUS-protokolla tukisi merkittävästi organisaation tietoturva- ja käyttäjänhallintavaatimusten täyttämistä. Jatkokehitystä suositeltiin erityisesti monivaiheisen tunnistautumisen lisäämiseksi, sekä kovennuskäytäntöjen ja järjestelmälokien analysoinnin kehittämiseksi. Näillä toimenpiteillä voitaisiin edelleen parantaa autentikoinnin turvallisuutta ja hallittavuutta. Raportti esittelee lisäksi käytetyt menetelmät ja tulosten tarkastelun yksityiskohtaisesti.

Avainsanat (asiasanat)

RADIUS, ISO/IEC 27001, kyberturvallisuusdirektiivi, autentikointi, tietoturvavaatimukset

Muut tiedot (salassa pidettävät liitteet)

-

jamk

Description

Ojala, Valtteri

Developing Secure User Management Using a Test Environment

Jyväskylä: JAMK University of Applied Sciences, November 2024, 38 pages.

Degree Programme in Information- and Communication Technologies. Bachelor´s thesis.

Permission for open access publication: Yes

Language of publication: Finnish

Abstract

The study examined the applicability of the RADIUS authentication model in an organization's network environment, with the aim of meeting the requirements of the ISO/IEC 27000 information security standard and the European Union's cybersecurity directive. The background for the research stemmed from the need to improve user management in an environment where administrative credentials had previously been shared among users. The objective was to create a technical and administrative model that would establish a foundation for network security, integrity, and availability.

A test environment was built during the study, in which the RADIUS protocol was implemented as an authentication server integrated into a pfSense firewall. The implementation utilized the open-source FreeRADIUS software, and authentication was evaluated in a virtual environment that included endpoints running various operating systems. The testing focused on technical aspects such as ensuring encrypted communication, enforcing a default-deny access policy, and monitoring log data. The test environment was built on top of a virtualization platform to match the organization’s environment.

The results indicated that the RADIUS protocol can be implemented in an organization's environment to meet the requirements of the ISO/IEC 27000 information security standard and the cybersecurity directive, provided the implementation is carefully executed on both technical and administrative levels. Sensitive information, such as passwords, was successfully encrypted, sessions were terminated after a predefined period of inactivity, and access restrictions were found to be effective.

In conclusion, it was determined that the RADIUS protocol would significantly support meeting the organization's security and user management requirements. Further development was recommended, particularly in introducing multi-factor authentication (MFA), strengthening security practices, and enhancing the analysis of system logs. These measures would further improve the security and manageability of authentication. The report also provides detailed descriptions of the methods used and an analysis of the results.

Keywords/tags (subjects)

RADIUS, ISO/IEC 27001, network and information security directive, authentication, security requirements

Miscellaneous (Confidential information)

-

Sisältö

Kuviot

Lyhenteet

AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
ISMS	Information Security Management System
LAN	Local Area Network
NIS2	Network and Information Security Directive
PDCA	Plan-Do-Check-Act
RADIUS	Remote Authentication Dial In User Service
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UNIX	Uniplexed Information and Computing Service
VPN	Virtual Private Network
WAN	Wide Area Network

1 Tietoturvan haasteet ja sen kehittämisen merkitys

Tietoturva on noussut yhdeksi keskeisimmistä puheenaiheista globaaleissa haasteissa digitaalisten infrastruktuurien kehittyessä ja kyberhyökkäysten yleistyessä. Erityisesti kriittisen infrastruktuurin, kuten liikennejärjestelmien, muuttuessa entistä älykkäämmiksi tietoturvan tärkeys alalla korostuu enenevässä määrin. Uuden Euroopan Unionin verkko- ja tietoturvallisuusdirektiivin voimaantulon myötä on myös tieliikenneinfrastruktuuria operoivien organisaatioiden huolenaiheeksi noussut tietoturva ja sen nykytila. Direktiivi asettaa tarkkoja vaatimuksia organisaatioille, joihin lukeutuu riskienhallinta, toimintavarmuuden turvaaminen ja tietoturvauhkien ennaltaehkäisy. Tietoturvastandardi ISO/IEC 27001 tarjoaa organisaatioille viitekehyksen, jonka avulla tietoturvaa voidaan kehittää järjestelmällisetsi ja tehokkaasti ISO/IEC 27002 standardin tarjoamien ratkaisujen avulla.

Euroopan Unionin uusi verkko- ja tietoturvadirektiivi NIS2 asettaa yrityksille entistä tarkempia velvoitteita tietoturvan hallintaan. Direktiivi korostaa erityisesti organisaation vastuuta tietoturvan ja kriittisen infrastruktuurin suojaamisessa (NIS2 – Euroopan unionin kyberturvallisuusdirektiivi n.d.). ISO/IEC 27000 -standardisarjan viitekehyksen järjestelmällinen toteuttaminen mahdollistaa yrityksien vastaamisen myös NIS2 tuomiin vaatimuksiin. Työn tavoitteena oli selvittää, kuinka RADIUS-autentikointiprotokolla kykenisi täyttämään ISO/IEC 27001-tietoturvastandardisarjan ja NIS2 verkko- ja tietoturvadirektiivin vaatimukset organisaation tietoliikenneympäristössä. Tutkimuksen ajankohtana uusi kyberturvallisuuslaki oli käsittelyssä Suomen valiokunnassa, ja uuden lain ennustetaan astuvan voimaan vielä vuoden 2024 loppuun mennessä.

Toimeksiantaja tutkimukselle oli kansainvälinen älyliikenneteknologiaa tuottava yritys SWARCO Finland Oy. Kehitystyö toteutettiin rakentamalla virtuaalinen testiympäristö, joka simuloitiin vastaamaan organisaation omaa Traffic Gateway -palvelun rakennetta ja vaatimuksia. Tämän avulla arvioitiin RADIUS-protokollan soveltuvuutta organisaation tietoturvan ja käyttäjänhallinnan kehittämiseen. Työssä tarkastellaan testiympäristöä hyödyntäen, kuinka RADIUS-protokollaa käyttämällä voidaan vastata osakseen näihin vaatimuksiin painottaen erityisesti autentikointiin liittyvien riskien hallintaa ja tietojen suojaamista.

Tutkimuksen tulokset tarjoavat tietoa, miten protokollan eri ominaisuuksia voidaan hyödyntää lopullisessa organisaation tuotantoympäristössä ja miten protokollaa voi kehittää jatkoa ajatellen. Testiympäristössä hyödynnettiin avoimen lähdekoodin FreeRADIUS-ohjelmistoa, ja autentikointia

testattiin kolmella eri käyttöjärjestelmällä varustetulla päätelaitteella. Lisäksi analysointiin kuului keskeisiä tietoturvanäkökulmia, kuten salattujen yhteyksien toteutus, oletusarvoisesti estävän hallintapolitiikan soveltaminen ja lokitietojen seuranta. Näiden avulla pyrittiin vastaamaan organisaation tietoturvavaatimuksiin sekä mahdollistamaan käyttäjänhallinnan keskittäminen.

Tutkimuksessa selvitettiin, kuinka testiympäristössä saadut tulokset voidaan skaalata vastaamaan organisaation tietoliikenneympäristöä, samalla sivuten hallinnollista osa-aluetta. Tämä lähestymistapa tarjosi turvallisen tavan arvioida protokollan toimintaa ilman riskiä varsinaisen tuotantoympäristön häiriöille ja palvelukatkoksille. Tulokset antoivat käsityksen siitä, miten RADIUS-protokollaa voidaan toteuttaa osana Traffic Gateway -palvelua täyttäen tekniset ja hallinnolliset vaatimukset.

2 Tutkimusasetelma

2.1 Tutkimuskysymykset ja tavoitteet

Ideologiana on hyödyntää testiympäristöä RADIUS-autentikointiprotokollan soveltuvuuden arvioimiseksi organisaation Traffic Gateway -palvelun tietoturvatarpeisiin. Testiympäristön avulla voidaan simuloida autentikointiprosessia, joka vastaisi osaa organisaation todellista ympäristöä, ilman suoraa vaikutusta tuotantoympäristöön. Tällainen lähestymistapa tarjoaa hallitun ja riskittömän tavan tarkastella soveltuvuutta. Teoreettisia viitekehyksiä tutkimuksessa ovat ISO/IEC 27001 -standardin tietoturvavaatimukset, ISO/IEC 27002 -standardin mukaiset tietoturvakontrollit sekä NIS2 -direktiivin ohjeistus.

Ensimmäisenä tutkimuskysymyksenä tarkastellaan teknisiä ratkaisuja, joilla varmistetaan, että RADIUS-protokolla täyttää tietoturvan standardisarjan vaatimukset sisältäen suojausvaatimukset, kuten käyttäjien autentikoinnin turvallisuuden ja tapahtumien hallinnan. Toisena tutkimuskysymyksenä selvitetään, kuinka RADIUS-protokollan implementointi vastaa Euroopan Unionin uuden kyberturvallisuusdirektiivin asettamiin vaatimuksiin, jotka painottavat järjestelmien toimintavarmuutta, eheyttä ja tietoturvaa. Tässä yhteydessä tarkastellaan esimerkiksi tietoliikennedatan eheyttä, haitallisten toimien havaitsemismekanismeja sekä protokollan kykyä tukea käyttäjien ja pääsyn hallintaa.

Kolmantena tutkimuskysymyksenä tutkitaan hallinnollisten toimenpiteiden roolia tehokkaan käyttäjänhallinnan toteutuksessa. Tämä sisältää käyttäjien koulutuksen, käyttöoikeuksien hallinnan ja säännöllisten auditointien merkityksen tietoturvan ylläpidossa. Hallinnolliset toimenpiteet tukevat autentikointiprotokollan tuomien hyötyjen maksimoimista ja varmistavat sen pitkäaikaisen käytettävyyden sekä luotettavuuden organisaation ympäristössä. Tutkimuksen tavoitteena on suunnitella ja toteuttaa RADIUS-protokollaan pohjautuva autentikointimenetelmä testiympäristön avulla, joka voisi täyttää sekä ISO/IEC 27001 että kyberturvallisuusdirektiivin vaatimukset.

2.2 Tutkimusmenetelmät

Tutkimusmenetelmänä valikoitui tutkimuksellinen kehittämistyö, joka keskittyy arvioimaan ratkaisua, joka täyttää standardien mukaiset tietoturvavaatimukset ja vastaisi yrityksen tarpeisiin. Työssä käytetään viitekehyksinä ISO/IEC 27001 -standardia ja EU:n asettamaa kyberturvallisuusdirektiiviä, jotka muodostavat säännöstön ympäristön arvioinnille tutkimuksen lopussa. Näiden viitekehysten mukaisesti suunniteltu järjestelmä täyttää korkean tason tietoturvavaatimukset ja varmistaa autentikointiprotokollan teknisen luotettavuuden sekä tietoturvallisuuden. Näihin standardeihin vastaamalla toimeksiantaja voi kehittää Traffic Gateway -palvelua entistä luotettavammaksi ja turvallisemmaksi. Työssä selvitetään, miten RADIUS-protokolla kykenee tukemaan ISO/IEC-tietoturvastandardisarjaa sekä kyberturvallisuusdirektiivin asettamia vaatimuksia. Viitekehysten mukaiset hallinnolliset ja tekniset toteutukset tarjoavat selkeän pohjan, jonka avulla vaatimuksiin voidaan vastata. Erityisesti tarkastellaan, miten protokollan ominaisuudet täyttävät standardien ja direktiivin määrittämät ehdot.

ISO/IEC 27001- ja ISO/IEC 27002 -standardien mukaisia tietoturvakontrolleja sovelletaan autentikointiprosessin suunnittelussa ja toteutuksessa. Näiden kontrollien avulla varmistetaan, että käyttöön otettavat tietoturvatoimenpiteet ovat riittäviä ja vastaavat palvelun tarpeita. Samalla varmistetaan, että ne täyttävät standardien asettamat vaatimukset tietoturvan hallinnalle ja riskienhallinnalle. Tutkimuksessa huomioidaan myös NIS2-direktiivin vaikutukset, jotka korostavat kriittisten infrastruktuurien ja digitaalisten palveluiden tietoturvaa. Uuden autentikointiprotokollan suunnittelu toteutetaan siten, että se täyttää direktiivin asettamat raportointi- ja riskienhallintavaatimukset. Tämä takaa, että autentikointimallilla voidaan tukea organisaation kykyä vastata direktiivin mukaisiin tietoturvavelvoitteisiin ja parantaa sen valmiutta reagoida tietoturvapoikkeamiin.

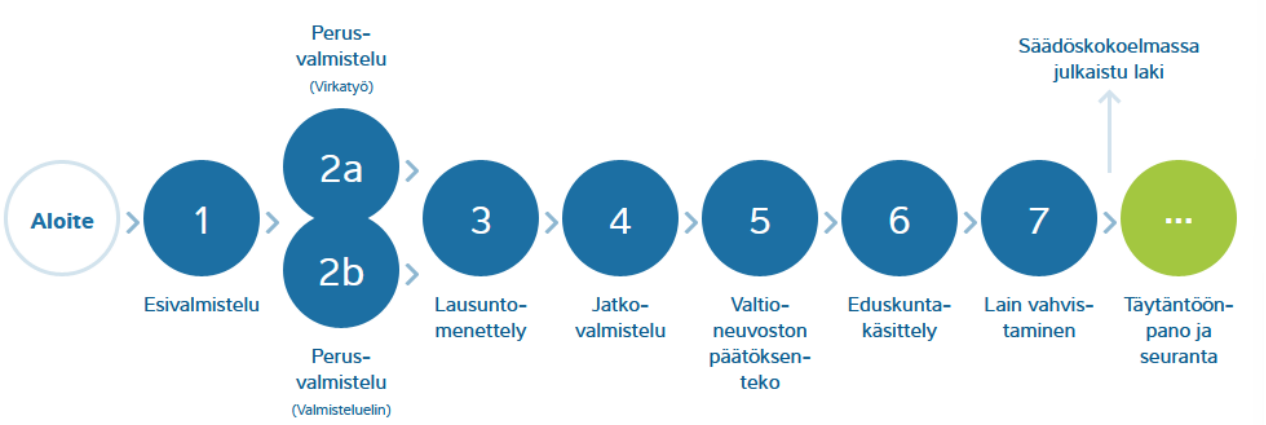
3 Tausta ja viitekehykset

3.1 Lainsäädäntö

3.1.1 Yleistä

Suomessa lainsäädäntö kattaa kaikki voimassa olevat lait ja säädökset sekä lakien säätämisen, jota käyttää perustuslain mukaisesti eduskunta (Lainsäädäntö n.d.). Lakiehdotukset valmistellaan asiaankuuluvassa ministeriössä, ja suurempien, periaatteellisesti merkittävien hankkeiden valmistelu tapahtuu usein komiteoissa tai toimikunnissa, joissa on edustajia eri hallinnonaloilta, puolueista ja muista intressiryhmistä. Eri tahojen näkemyksiä kuullaan lausuntokierroksilla ja erityisissä kuulemistilaisuuksissa, jotta päätöksenteossa otetaan huomioon laajasti eri näkökulmat. (Lainvalmistelun prosessiopas n.d.)

Tutkimuksen yhtenä osa-alueena on tarkastella tietoturvan tasoa uuden NIS2 -direktiivin näkökulmasta. Kyseessä on kuitenkin uusi valmisteltava laki, jolloin se käy tavanomaisen lainvalmistelun prosessin (LVM044:00/2022 2024). Lakihankkeet valmistellaan komiteoissa, joissa kuullaan eri tahojen lausunnot. Valtioneuvoston yleisistunnossa käsitellään ministeriössä valmistellut lakiesitykset, ja eduskunta päättää näiden lakien hyväksymisestä valiokuntien valmistelun jälkeen. (Lainvalmistelun prosessiopas, Lakien säätäminen n.d.) Kuviossa 1 on lainvalmistelun yleinen prosessikaavio, jota tämäkin lakivalmistelu noudattaa.



Kuvio 1. Lainvalmistelun prosessikaavio (Lainvalmistelun prosessiopas n.d.)

3.1.2 Euroopan Unionin uusi verkko- ja tietoturvadirektiivi

Aikaisemman Euroopan Unionin verkko- ja tietoturvadirektiivin velvoitteiden ansiosta kansallinen tietoturvan taso on parantunut, mutta ensimmäinen NIS (eng. Network and Information Security Directive) on nykyisin vanhentunut. Euroopan unioni on laatinut uuden verkko- ja tietoturvadirektiivin NIS2, joka astui voimaan joulukuussa 2022, ja se on saatettava osaksi kansallista lainsäädäntöä 17. lokakuuta 2024 mennessä. (LVM044:00/2022 2024)

Uuden kyberturvallisuusdirektiivin NIS2 tavoitteena on parantaa Euroopan Unionin ja sen jäsenvaltioiden kyberturvallisuutta erityisesti kriittisillä sektoreilla, joihin kohdistuvat entistä tiukemmat riskienhallinta- ja raportointivelvoitteet. Direktiivi määrittää kriittisille sektoreille vähimmäistoimenpiteet, joiden avulla voidaan hallita niihin kohdistuvia kyberturvallisuusriskejä (NIS2 – Euroopan unionin kyberturvallisuusdirektiivi n.d.).

Näitä vaatimuksia noudattamalla pyritään estämään merkittävät poikkeamat ja varmistamaan, että kriittiset toimijat ylläpitävät yhteiskunnan turvallisuuden kannalta tarvittavaa kyberturvallisuuden tasoa. Direktiivin täytäntöönpano lisää velvoitteiden piiriin kuuluvien yritysten ja julkisyhteisöjen määrää ja laajentaa soveltamisalaa, mikä asettaa uusia vaatimuksia organisaatioille sekä aiheuttaa kustannuksia velvoitteiden toteuttamisesta. Lisäksi se tuo julkishallinnolle lisätehtäviä, jotka edellyttävät viranomaisilta uudenlaista osaamista ja resursseja direktiivin tehokkaaksi toimeenpanemiseksi. Tämä laajentaa kyberturvallisuuden valvontaa, vahvistaa riskienhallinnan käytäntöjä ja auttaa parantamaan koko EU-alueen yhteiskunnan turvallisuutta (Valtioneuvosto 2024).

Direktiivi korostaa avoimuuden ja vastuullisuuden merkitystä sekä rakentaa kestävyyttä kyberturvauhkia vastaan, ja sen toimeenpano vaatii organisaatioilta merkittävää sitoutumista. Hyötyjen kuitenkin arvioidaan ylittävän selvästi kustannukset, sillä tietoturvallisuuden hallintajärjestelmä, joka perustuu esimerkiksi ISO/IEC 27001 -standardiin, tukee organisaation pitkäjänteistä tietoturvakehitystä (Pulkkanen 2024). Pulkkanen (2024) painottaa, että tietoturvan hallintajärjestelmän käyttöönotto ja vaiheittainen strategia, joka huomioi organisaation erityispiirteet ja nykyiset kyvykkyydet, mahdollistaa kestävät tulokset ja tukee toiminnan jatkuvuutta pitkällä aikavälillä.

Erityisesti vaatimukset, kuten riskienhallinta, hyökkäysten raportointi, vahva pääsynhallinta ja toiminnan jatkuvuus ovat relevantteja tälle tutkimukselle. NIS2 edellyttää organisaatioita toteuttamaan kattavia riskienhallintakäytänteitä, jotka liittyvät verkkoinfrastruktuurin ja palvelujen suojaamiseen. Tämä työ keskittyy autentikointiprotokollan käyttöönoton vaikutuksiin osana vahvempaa riskienhallintakehystä. RADIUS parantaa pääsynhallintaa ja estää luvattoman pääsyn verkkoihin ja järjestelmiin. Kyberhyökkäysten sattuessa NIS2 edellyttää organisaatioita ilmoittamaan nopeasti viranomaisilla ja osapuolille, jotka voisivat kärsiä hyökkäyksestä. Autentikointiprosessin parantaminen RADIUS-protokollalla mahdollistaa organisaation jatkokehityksen hyökkäyksen havaitsemiseen ja raportointiin. NIS2 vaatii organisaatioilta myös pääsynhallinnan ja käyttäjäntunnistamisen vahvoja käytänteitä erityisesti silloin, kun organisaatiossa käsitellään kriittisiä järjestelmiä. RADIUS on keskeinen osa tässä vaatimuksessa, sillä se tarjoaa vahvan autentikointiratkaisun monivaiheisella tunnistautumisella ja käyttäjänhallinnalla.

3.1.3 Suomen kyberturvallisuuslaki

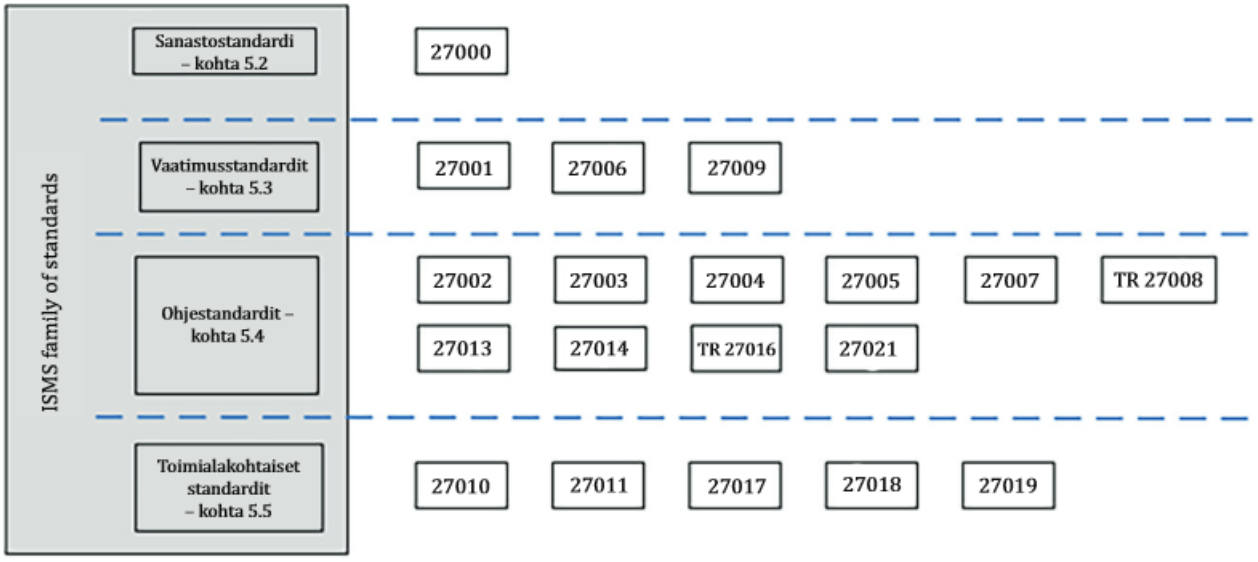
Uuden kyberturvallisuuslain tavoitteena on toimeenpanna NIS2-direktiivin mukaiset tietoturvavaatimukset ja vahvistaa sekä Suomen että EU jäsenvaltioiden välistä tietoturvan tasoa. Laki keskittyy erityisesti riskienhallintaan, poikkeamien käsittelyyn ja raportointiin sekä säännölliseen valvontaan ja auditointiin, mikä auttaa varmistamaan kriittisten toimintojen turvallisuuden. Kyberturvallisuuden valvontaan Suomeen perustetaan uusi kansallinen viranomainen, jonka vastuulla on seurata lain täytäntöönpanoa ja varmistaa, että direktiivin asettamat vaatimukset toteutuvat asianmukaisesti. Toimeksiantajan valvontaviranomaisena toimii Traficom, joka valvoo, että toimijat noudattavat riskienhallinnan ja poikkeamien raportoinnin vaatimuksia direktiivin soveltamisalan mukaisesti. Lisäksi laki sisältää säännöksiä velvoitteiden noudattamisen valvonnasta ja direktiivin täytäntöönpanoa edellyttävistä viranomaistehtävistä ja yhteistyöstä (HE 57/2024 2024).

Tutkimuksen kirjoittamisen ajankohtana kyberturvallisuuslaki on käsittelyssä suomen valiokunnassa. Täytäntöönpano on kuitenkin hyvällä mallilla ja tämänhetkistä versiota pystyy jo hyödyntämään (Isaksson 2024.). Isaksson kirjoittaa myös, että uuden lain ennustetaan astuvan voimaan vielä vuoden 2024 loppuun mennessä.

3.2 Standardit

Standardit ovat julkaisuja, joihin on kirjattu yhteisesti sovittuja vaatimuksia, suosituksia tai ominaisuuksia tuotteille, niiden valmistukselle tai testaukselle sekä järjestelmille tai palveluille. Ilman näitä yhteisiä sopimuksia arki ei olisi yhtä sujuvaa ja turvallista (Mitä standardi tarkoittaa? n.d.). Sanakirjan mukaan standardit määritellään eri toimijoiden yhdessä laatimiksi normatiivisiksi asiakirjoiksi, jotka sisältävät vaatimuksia tai suosituksia esimerkiksi tuotteiden ominaisuuksista, valmistusmenetelmistä tai muista vastaavista. Standardia voidaan käsitteenä laajentaa kattamaan myös periaatteita, sääntöjä, kriteerejä tai vaatimuksia. (Kielitoimiston sanakirja, standardi 2024.)

Tietoturvallisuuden johtamisjärjestelmällä organisaatiot voivat suojata tieto-omaisuuttaan ja hallita riskejä järjestelmällisesti. Tietoturvallisuuden johtamisjärjestelmän rakentamisessa apuna toimii standardisarja ISO/IEC 27000, joka sisältää suosituksia tietoturvallisuuden hallintaan, riskeihin ja kontrollointiin. Tämä standardisarja tarjoaa selkeät raamit organisaatioille tietoturvallisuuden kehittämiseksi ja ylläpitämiseksi, kuten kuvattu kuviossa 2. (SFS-EN ISO/IEC 27000:2020 n.d.)



Kuvio 2. Tietoturvallisuuden hallintajärjestelmästandardisarjan keskinäiset suhteet (SFS-EN ISO/IEC 27000:2020.)

Tietoturvallisuuden hallintajärjestelmästandardisarja koostuu toisiinsa liittyvistä standardeista, jotka kattavat tietoturvallisuuden hallintajärjestelmiä koskevat vaatimukset (ISO/IEC 27001), sertifiointielimiä koskevat vaatimukset (ISO/IEC 27006) sekä toimialakohtaiset toteutukset (ISO/IEC

27009). Lisäksi sarja tarjoaa ohjeita hallintajärjestelmien toteuttamiseen, käsittelee yleisiä prosesseja ja antaa toimialakohtaisia suosituksia tietoturvan hallinnan kehittämiseksi (SFS-EN ISO/IEC 27000:2020.)

Tämän tutkimuksen pääpaino on ISO/IEC 27001:2022 standardissa, missä esitetään tarkemmin tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, ylläpitämistä ja jatkuvaa parantamista koskevat vaatimukset. Standardi sisältää myös organisaation tarpeisiin mukautettua tietoturvariskien arviointia ja käsittelyä koskevat vaatimukset. Vaatimukset ovat yleisluonteisia ja täten soveltuvat kaikentyyppisille ja -kokoisille organisaatioille (Mts. n.d.). ISO/IEC 27001:2022 standardin vaatimuksien täyttäminen tapahtuu hyödyntäen ISO/IEC 27002:2022 standardia, mikä tarjoaa parhaat menetelmät tietoturvakontrollien toteuttamiseen eri organisaatioiden ympäristöissä. ISO/IEC 27002 toimii täydentävänä ohjeistuksena ISO/IEC 27001 standardille, jotta organisaatiot saisivat käsityksen myös käytännön toteutuksesta, miten vaatimuksiin kuuluu vastata.

Standardi on tarkoitettu käytettäväksi standardiin ISO/IEC/IEC 27001 perustuvan tietoturvallisuuden hallintajärjestelmän toteuttamisprosessissa. Se sopii myös ohjeistukseksi yleisesti hyväksyttyjen tietoturvallisuuden hallintakeinojen toteuttamiseen. Standardia voidaan hyödyntää toimiala- tai organisaatiokohtaisten tietoturvallisuuden hallintaohjeiden kehittämisessä, sillä siinä otetaan huomioon toimialaa tai organisaatiota koskevat tietoturvallisuuden riskiympäristöt (SFS-EN ISO/IEC 27000:2020.)

3.3 Verkkoteknologiat

3.3.1 Yleistä

Verkkoteknologiat viittaavat protokolliin ja menetelmiin, joiden avulla tietoverkkoja rakennetaan ja ylläpidetään. Verkkoteknologioihin kuuluvat esimerkiksi tietoliikenneprotokollat TCP/IP, HTTP ja HTTPS. Nämä protokollat määrittelevät, miten tietoa siirretään laitteiden kesken tietoverkossa. Tässä työssä ei käydä läpi eri verkkoteknologioita tai niiden käyttötarkoituksia. On tärkeää ymmärtää, miten eri verkkoteknologiat kattavat laajan osa-alueen erilaisia ratkaisuja, joiden avulla voidaan rakentaa toimivia ja etenkin turvallisia tietoverkkoja, joissa tietojen eheys, saatavuus ja luottamuksellisuus ovat taattuja.

Tutkimuksen näkökulmasta keskeistä on, miten käyttäjänhallinta, pääsynvalvonta ja toimintojen seuranta voidaan toteuttaa tietoturvallisesti. Tämän saavuttamiseksi hyödynnetään AAA-protokollaa, mikä toimii perustana RADIUS-protokollalle. Näiden protokollien avulla voidaan varmistaa, että käyttäjien autentikointi tapahtuu varmennetusti, käyttöoikeudet kohdistuvat oikein määritellyille henkilöille, sekä järjestelmän käyttö ja tapahtumat ovat jäljitettävissä. Protokollat tarjoavat hyvin joustavuutta vastata erilaisten verkkojen ja päätelaitteiden asettamiin vaatimuksiin ja rajoituksiin.

3.3.2 Pääsynhallinta

Keskeinen osa pääsynhallintaa on AAA-protokolla. Se tulee sanoista ”tunnistautuminen, valtuutus ja valvonta” (eng. Authentication, Authorization and Accounting), ja sen avulla voidaan hallita organisaation käyttäjien käyttöoikeuksiin liittyvää tietoturvastandardia (Pääsynhallinta ja tunnistaminen n.d.). AAA-protokolla toimii perustana, kun tavoitteena on tietoturvallinen käyttäjänhallinta ja käyttäjien valvonta.

> Tunnistautumisprosessissa käyttäjät todistavat henkilöllisyytensä saadakseen pääsyn sovellukseen. Tunnistuksessa käytetään lisäksi usein monimenetelmäistä todentamista, joka lisää prosessiin käyttäjäkohtaisen tietoturvatason vaikeuttaen näin valtuuttamattomien käyttäjien pääsyä sovellukseen. (Pääsynhallinta ja tunnistaminen n.d.)

> Valtuutus on prosessin seuraava vaihe, jossa käyttäjä kirjataan sisään sovellukseen ja hänet täytyy valtuuttaa suorittamaan tiettyjä tehtäviä tai käsittelemään dataa. Valtuutusratkaisujen käyttöönotolla varmistetaan, ettei käyttäjillä ole laajoja käyttöoikeuksia ja etteivät he kirjaudu järjestelmiin järjestelmänvalvojan oikeuksilla. (Pääsynhallinta ja tunnistaminen n.d.)

> Valvonta tarkoittaa käyttäjien sekä yrityksen datan käyttöajankohtien seurantaprosessia. Tämän AAA-protokollan osa-alueen avulla varmistetaan, että jokaisella käyttäjällä on oma käyttöoikeustili ja että kukin käyttäjätili voidaan yhdistää tiettyyn henkilöön tai laitteeseen. (Pääsynhallinta ja tunnistaminen n.d.)

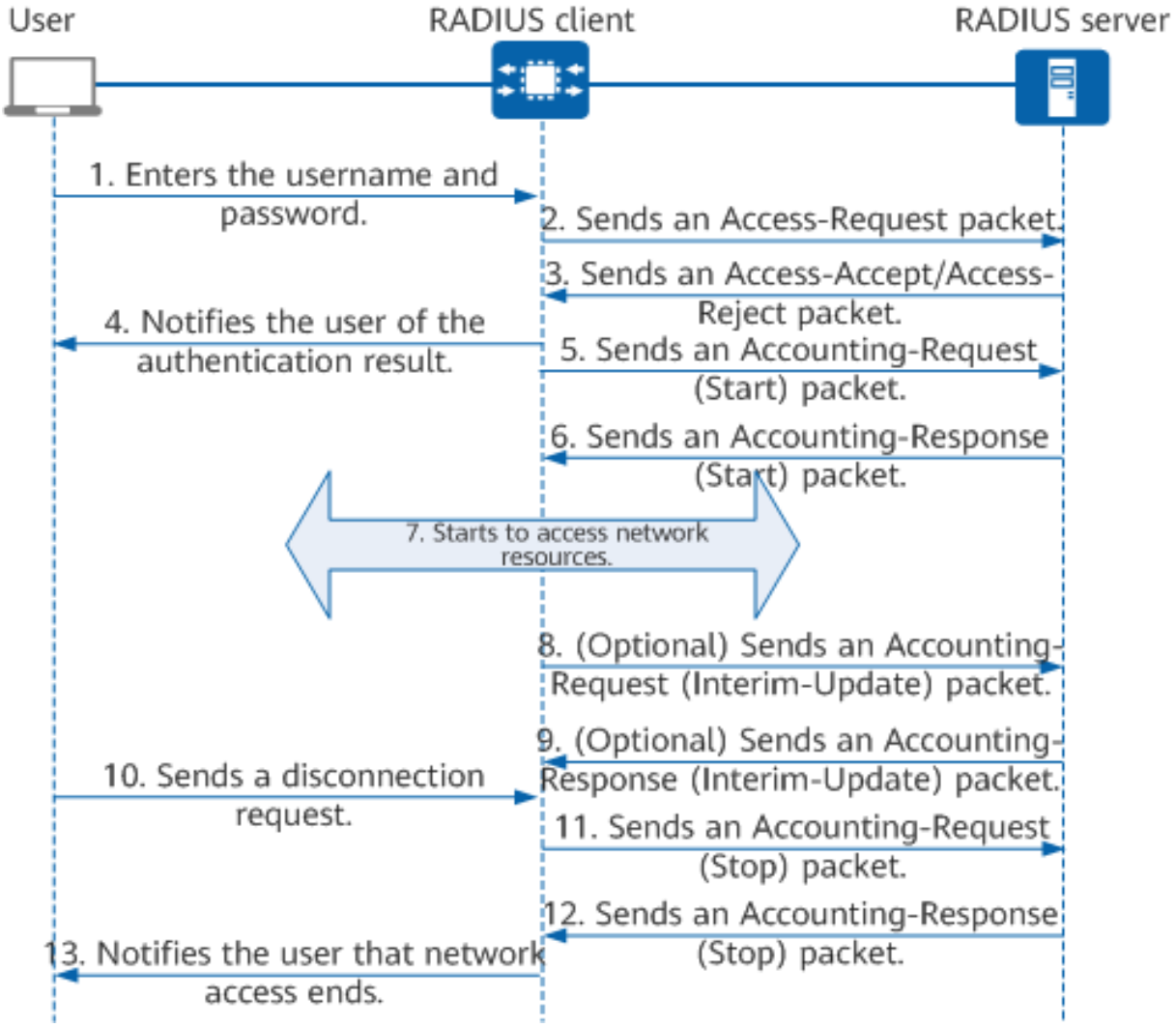
AAA-protokollia on olemassa useita eri vaihtoehtoja, kuten RADIUS, Ciscon kehittämä TACACS+ sekä uusin autentikointiprotokolla Diameter. Diameter on enemmän mobiiliyhteyksissä käytetty

protokolla, täten se on monimutkaisempi arkkitehtuuriltaan kuin esimerkiksi RADIUS. Suurimpia eroja näiden kahden protokollan välillä on, että Diameter sallii myös autentikointipyyntöjen lähettämisen palvelimelta päätelaitteelle päin. Lisäksi Diameter on yhteysorientoitunut protokolla, kun RADIUS ei vaadi jatkuvaa yhteyttä vaan käsittelee autentikointipyynnöt UDP protokollan avulla. (What's the Difference Between RADIUS and Diameter protocol? 2022).

3.3.3 RADIUS-protokolla

RADIUS lyhenne tulee sanoista "Remote Authentication Dial-In User Service". Sen on kehittänyt Livingston Enterprises, Inc vuonna 1991. Protokolla oli alun perin käytetty yhdistämään Michiganin yliopistot toisiinsa. RADIUS käyttää UDP protokollaa liikennöintiin, ja on yleensä Windows tai UNIX laitteen taustalla pyörivä palvelinprosessi. Palvelin odottaa, kunnes saa pyynnön asiakaslaitteelta tai esimerkiksi NAS-palvelimelta, joita voivat olla laitteita tai järjestelmiä kuten langattomia yhteyspisteitä tai VPN-järjestelmiä. (What is RADIUS? n.d.)

Päätelaite lähettää RADIUS asiakaslaitteelle kirjautumispyynnön, jonka jälkeen asiakaslaite välittää RADIUS protokollalla pyynnön palvelimelle verifioidakseen kirjautumispyynnön (Beschokov, M. n.d.). Mikäli kirjautumistiedot ovat oikeat ja käyttäjällä on pyydetyt resurssit sallittu, RADIUS palvelin lähettää hyväksytyn kirjautumisen vastauksena RADIUS asiakaslaitteelle. Reaaliaikaisen kirjanpidon ollessa käytössä ympäristössä, liikennöintiin kuuluu myös aikavälein lähetettävät päivityspaketit. Mikäli istunnosta ei lähetetä päivityspaketteja tiettyyn aikaikkunaan mennessä, palvelin lähettää yhteyden katkaisupyynnön, jolloin myös seuranta katkeaa ja saadaan varmennetumpaa dataa siitä, miten yhteys on ollut aktiivisena. (Xiaoguang & Yuting 2024.) Koko autentikointiprosessi lisäominaisuuksilla on kuvattuna kuviossa 3.



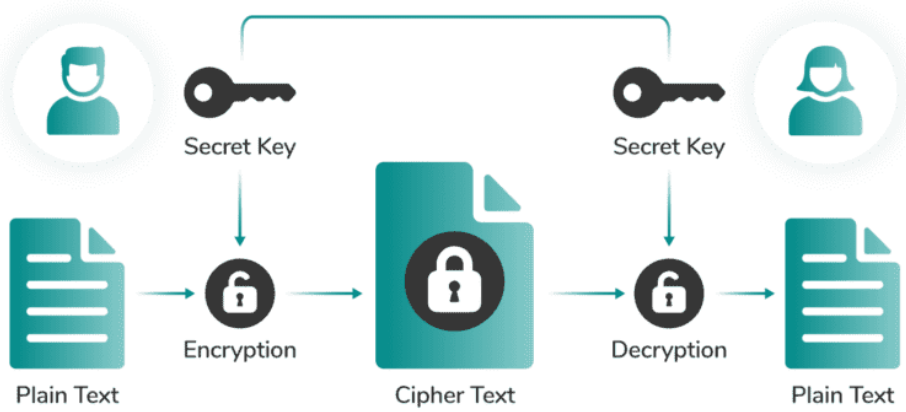
Kuvio 3. RADIUS autentikointi, auktorisointi ja monitorointi sekvenssikaaviona (Xiaoguang & Yuting 2024)

Toimeksiantaja päätyi RADIUS protokollaan siksi, koska se on arkkitehtuuriltaan yksinkertaisempi kuin Diameter protokolla. RADIUS on kevyempi suoritettava ja täyttää standardien tuomat vaatimukset autentikoinnista. Työssä otetaan myös huomioon se, että organisaation Traffic Gateway-palvelussa liikkuu paljon dataa, jonka vuoksi halutaan käyttää UDP protokollaa liikennöintiin sen keveyden ansiosta. Huomioitavaa on, että UDP protokolla toimii sokeasti, jolloin se ei välitä tietoa siitä, jos yhteys on jostain syystä epäonnistunut.

3.4 Salausmenetelmät

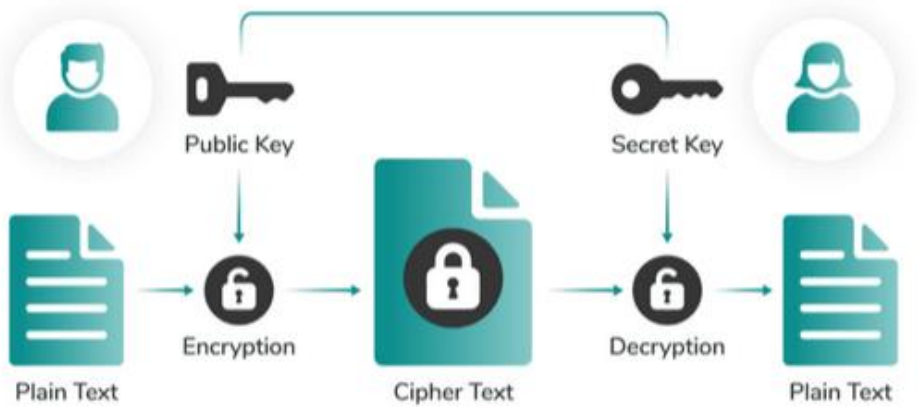
Salaus on olennainen osa modernia tietoturvaa, sillä sen avulla tieto muunnetaan luettavasta muodosta salatuksi muodoksi, mikä suojaa sitä luvattomalta käytöltä. Prosessi perustuu siihen, että luettava data (selkoteksti) muutetaan salatuksi muodoksi (salateksti) käyttämällä tiettyä algoritmia ja salausavainta. Ainoastaan henkilöt, joilla on oikea avain, voivat purkaa salatun tekstin takaisin selkokieliseksi ja lukea sen. (Laurente-Ticong 2023.) Symmetrisellä sekä epäsymmetrisellä salauksella on omat vahvuutensa ja sovelluskohteensa. Suurten tietomäärien salaamiseen symmetrinen salaus on tehokkaampi sen nopeuden ansiosta, kun taas epäsymmetristä salausta suositaan avainten jakelussa ja pienten tietomäärien suojaamisessa sen paremman tietoturvan vuoksi. Monissa järjestelmissä hyödynnetään molempia salaustekniikoita, jotta voidaan hyödyntää kummankin menetelmän etuja. (Difference Between Symmetric and Asymmetric Key Encryption 2024.)

RADIUS-protokollassa salauksella on tärkeä rooli, sillä se suojaa käyttäjätunnuksia, salasanoja ja muuta tietoliikennettä niiden siirron aikana. Protokolla käyttää symmetristä salausmenetelmää, joka perustuu yhteiseen jaettuun salaisuuteen autentikointipalvelimen ja asiakaslaitteen välillä. Symmetrisessä salauksessa käytetään yhtä avainta, jota hyödynnetään sekä tiedon salaamiseen että purkamiseen. Menetelmä on yksinkertainen ja erityisen tehokas suurten tietomäärien käsittelyssä, minkä vuoksi sitä käytetään esimerkiksi AES-algoritmissa, jota Yhdysvaltain hallinto käyttää luokitellun tiedon salaamiseen. Symmetrisen salauksen vahvuutena on sen nopeus ja soveltuvuus tilanteisiin, joissa salausavain on jo jaettu turvallisesti. (Laurente-Ticong 2023; Nico 2021) Symmetrisen salauksen rakenne on kuvattu kuviossa 4.



Kuvio 4. Symmetrinen salaus (Laurente-Ticong 2023)

Asymmetrinen salaus, joka tunnetaan myös julkisen avaimen salauksena, hyödyntää avainparia tiedon salaamisessa ja purkamisessa. Julkista avainta käytetään tiedon salaamiseen, ja vain yksityisellä avaimella voidaan purkaa salattu tieto. Tämä menetelmä lisää tietoturvaa, sillä vaikka julkinen avain olisi saatavilla, tieto ei ole luettavissa ilman yksityistä avainta. Epäsymmetrisen salauksen turvallisuus perustuu siihen, että avainpari mahdollistaa tietoturvallisen tiedonsiirron ja parantaa tiedon suojausta molempien avainten avulla, kuten kuvattu kuviossa 5. Tämä tekee menetelmästä erityisen sopivan avainten hallintaan ja pienempien tietomäärien suojaamiseen. (Symmetric Encryption vs Asymmetric Encryption n.d.)



Kuvio 5. Asymmetrinen salaus (Laurente-Ticong, L. 2023.)

4 Toteutus

4.1 Lähtötilanne

4.1.1 Analyysi

Lähtötilanteen analyysissa tarkastellaan käytössä olevia käytäntöjä, verkon rakennetta ja ympäristön teknisiä tarpeita. Arvioinnin avulla tunnistetaan ne vaatimukset, joihin autentikointimallin on vastattava. Lisäksi analyysi tarjoaa selkeän kuvan tarvittavista muutoksista järjestelmän rakenteisiin ja konfiguraatioihin. Organisaation ympäristö koostuu useista eri käyttöjärjestelmistä, jotka sisältävät sekä Windows- että UNIX-pohjaisia järjestelmiä. Näillä järjestelmillä on eri käyttötarkoituksia, mutta niitä hallitaan keskitetysti Traffic Gateway -palvelusta, joka toimii liikenteen reitittä-

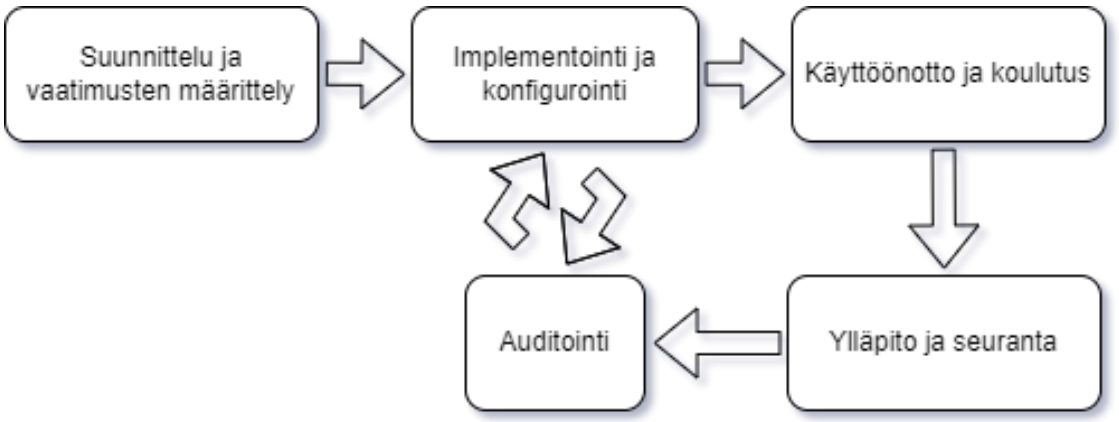
jänä ja on osana ympäristön tietoturvallisuuden keskipistettä. Nykytilanteessa on kuitenkin havaittu puutteita käyttäjien tunnistamisessa ja käyttöoikeuksien hallinnassa. Ilman yksilöllisiä käyttöoikeuksia ja henkilökohtaisia tunnisteita on haastavaa varmistaa, että vain valtuutetut käyttäjät pääsevät käsiksi resursseihin, mikä heikentää järjestelmän tietoturvaa ja tapahtumien jäljitettävyyttä.

Työn toteutus ei keskity suoraan organisaation tuotantoympäristöön, vaan RADIUS-protokollaa testataan erillisessä testiympäristössä. Testiympäristö mallintaa yleisimpiä käyttöjärjestelmiä ja simuloituja reititystoimintoja Traffic Gateway -palvelussa. Tämän avulla voidaan arvioida, miten keskitetty autentikointimalli toimisi todellisessa käyttöympäristössä, ilman että organisaation tuotantoverkon toiminnallisuutta vaarannetaan.

Tietoturvan standardisarja painottaa käyttöoikeuksien hallinnan merkitystä ja selkeiden käyttöoikeuspolitiikkojen määrittämistä. Näiden periaatteiden mukaisesti järjestelmien tulisi tarjota yksilölliset käyttöoikeudet, jotka rajoittuvat vain käyttäjän työtehtäviin tarvittaviin resursseihin. Samalla tietoturvadirektiivi korostaa riskiperusteisen tietoturvatoiminnan merkitystä, jotta järjestelmä kykenee varautumaan mahdollisiin tapaturmiin ja tukemaan tapahtumien jäljittämistä. Näiden viitekehysten pohjalta on selkeää, että tietoturvan kehittäminen edellyttää keskitettyä ja hallittua autentikointimallia, jonka avulla voidaan parantaa sekä ympäristön turvallisuutta että hallittavuutta.

4.1.2 Implementoinnin prosessimalli

Kuviossa 6 on esiteltynä implementointiin luotu prosessimalli, jota voisi hyödyntää siirryttäessä testiympäristössä validoidusta RADIUS-protokollan toteutuksesta organisaation tuotantoympäristöön. Mallin perustana on projektinhallinnan hyviksi todettuja käytäntöjä, ja sen rakenteessa on hyödynnetty osittain hyvin tunnettua PDCA-prosessimallia. Tämä prosessimalli sopisi implementointiin hyvin, koska se on suunniteltu jatkuvan kehityksen sykliseen malliin. PDCA-prosessimallia käytetään erityisesti silloin kun organisaatio haluaa suunnitella, toteuttaa, tarkastaa ja parantaa prosessejaan järjestelmällisesti.



Kuvio 6. Vaihekaavio prosessimallista

Ensimmäisessä vaiheessa keskitytään suunnitteluun ja vaatimusten määrittelyyn. Tässä vaiheessa autentikointimallin keskeiset tavoitteet ja organisaation tietoturvavaatimukset määritellään tarkasti. Tavoitteita verrataan tietoturvastandardeihin ja kyberturvallisuusdirektiiveihin, jotta prosessille saadaan selkeät suuntaviivat. Määrittelyvaiheessa otetaan huomioon myös erityistarpeet ja käyttöympäristö, mikä varmistaa mallin käytettävyyden organisaation tuotantoympäristössä.

Toisessa vaiheessa toteutetaan RADIUS-palvelimen implementointi ja konfigurointi. Tässä yhteydessä palvelin asennetaan ympäristöön ja konfiguroidaan organisaation Traffic Gateway -palvelun yhteyteen. Konfiguroinnissa määritellään autentikointiasetukset ja käyttöoikeuspolitiikat, jotka hallitsevat käyttäjien pääsyä järjestelmiin. Lisäksi luodaan yksityiskohtainen dokumentaatio, joka kattaa asetukset, konfiguraatiot ja mahdolliset ylläpidon vaatimukset. Kolmannessa vaiheessa toteutetaan käyttöönotto ja siihen liittyvä koulutus. Autentikointimallin käyttöönotossa käyttäjille järjestetään koulutusta uuden järjestelmän toiminnasta ja turvallisista käytänteistä.

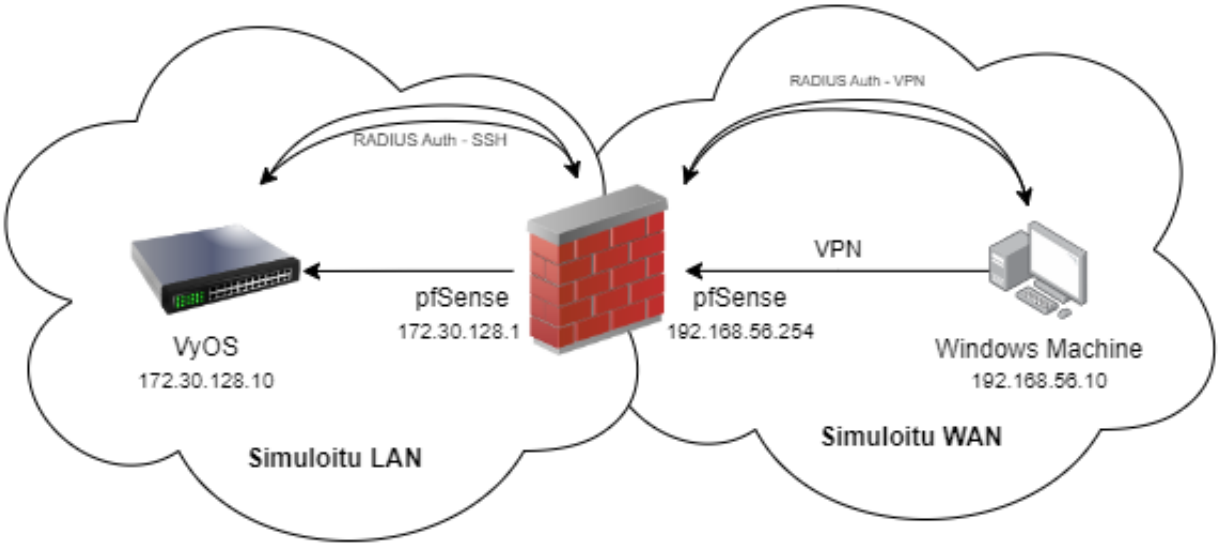
Käyttöönoton jälkeen siirrytään ylläpitoon ja seurantaan, mikä muodostaa jatkuvan vaiheen organisaation ISMS-prosessissa. Ylläpitoon kuuluu järjestelmän säännöllinen auditointi, käyttöoikeuksien hallinta ja ympäristön päivitykset vastaamaan muuttuvia tietoturvavaatimuksia. Seuranta mahdollistaa poikkeamien havaitsemisen ja korjaavat toimenpiteet, jotka ylläpitävät järjestelmän turvallisuutta pitkällä aikavälillä. Prosessimalliin on lisätty auditointi osaksi säännöllistä kehitystyötä. Järjestelmän toimivuutta ja vaatimustenmukaisuutta tarkastellaan säännöllisissä auditoinneissa, joiden avulla voidaan tunnistaa kehityskohteita ja varmistaa, että autentikointimalli vastaa organisaation muuttuvia tarpeita.

4.2 Tekninen toteutus

4.2.1 Ympäristö

Tekninen toteutus keskittyy RADIUS-palvelimen asennukseen, konfigurointiin ja sen hyödyntämiseen päätelaitteiden autentikointiprosesseissa. Kuviossa 7 on havainnollistettu toteutukseen suunniteltu testiympäristö, joka simuloi organisaation todellista käyttöympäristöä. Testiympäristössä Windows-päätelaite toimii ulkoverkosta tulevan liikenteen simulointiin. Käyttäjä muodostaa salatun VPN-tunnelin palomuurin sisäverkkoon, ja tunnelin autentikointi toteutetaan RADIUS-protokollalla. Tämä menetelmä varmistaa, että vain valtuutetut käyttäjät pääsevät sisäverkon resursseihin.

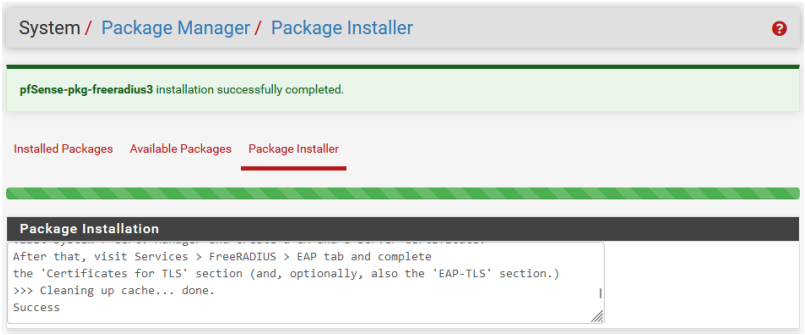
Sisäverkossa sijaitseva VyOS toimii simuloituna reitittimenä, joka hallinnoi liikennettä sisäverkossa. VPN-tunnelin yli toteutettavan SSH-yhteyden autentikointi tapahtuu myös RADIUS-protokollan avulla, mikä parantaa autentikointiprosessin tietoturvaa ja hallittavuutta. Toteutusprosessin aikana huomioidaan tietoturvastandardien, kuten ISO/IEC 27000 -sarjan, ja kyberturvallisuusdirektiivin asettamat vaatimukset.



Kuvio 7. Testiympäristön verkkotopologia

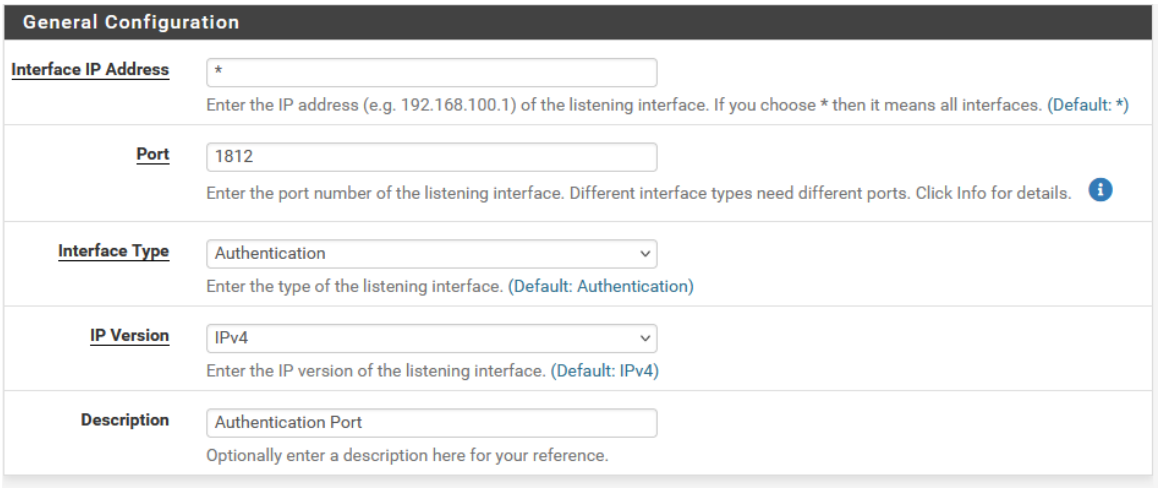
4.2.2 RADIUS-palvelimen asennus ja konfigurointi

RADIUS-palvelimena toimii tässä toteutuksessa FreeRADIUS, mikä löytyy valmiina palvelimella jo toimivasta pfSensen palomuurista. pfSense on yksi maailman luotetuimpia avoimeen lähdekoodiin pohjautuva palomuuriratkaisu. Palvelu toimii omalla käyttöjärjestelmässään FreeBSD kustomoidulla kernelillä ja sisältää myös monia kolmannen osapuolen asennettavia lisäominaisuuksia, kuten RADIUS. (Getting Started n.d.) Asennus tapahtuu pfSensen käyttöliittymän kautta löytyvästä pakettikirjastosta. Pakettikirjastosta löytyy valmiina FreeRADIUS-paketti, ja asennus käynnistyy klikkaamalla plusikonia. Palomuuri lataa automaattisesti tarvittavat tiedostot ja asentaa FreeRADIUS-paketin yhdessä kaikkien sen vaatimien riippuvuuksien kanssa, kuten kuviossa 8 on esitelty.



Kuvio 8. FreeRADIUS asennus

Palvelin määritellään kuuntelemaan autentikointipyyntöjä kaikista osoitteista ja portissa 1812 (ks. kuvio 9). Portti määritellään ”Authentication”-tyypiksi, jolloin se kuuntelee ja käsittelee autentikointipyynnöt. Lopuksi konfiguraatioon on mahdollinen kirjoittaa lyhyt kuvaus, mikä helpottaa järjestelmänvalvojien työskentelyä tunnistamalla portti kuvauksen perusteella.



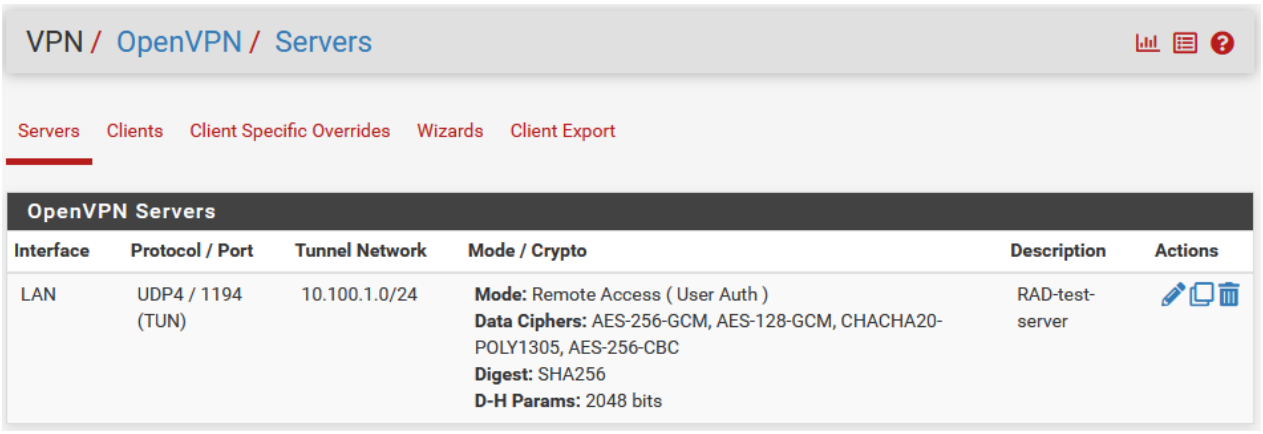
Kuvio 9. Konfigurointi verkkoliitäntään

Testiympäristön ollessa eriytetyssä virtuaaliverkossa, tämä on hyväksyttävä tapa. Tuotantoympäristössä olisi hyvä eriyttää autentikointiliitännät ja rajata käyttö sekä palvelut paremmin hallittuihin osoitteisiin ja portteihin. Esimerkiksi voisi hyödyntää porttikonfiguraatioita siten, että ulkoverkosta tulevat autentikoinnit kuunnellaan portissa 1812 ja lähiverkosta tulevat autentikoinnit kuunnellaan portissa 1813. Porteille olisi myös hyvä määritellä rajatut IP-osoitteet, jolloin vain tietyistä lähteistä tulevat autentikointipyynnöt otetaan käsittelyyn. Konfiguroidut verkkoliitännät näkyvät kuviossa 10.

Kuvio 10. Verkkoliitännät

Seuraava vaihe on OpenVPN-palvelimen perustaminen pfSenseen. VPN-palvelin määritellään käyttämään omaa väliverkkoa, ja toimintatila valitaan etäkäyttöön käyttäjätunnuksilla, tämä toimintatila mahdollistaa käyttäjien autentikoinnin RADIUS-tunnuksilla ja soveltuu hyvin tähän testitilanteeseen. Virtuaaliympäristön vuoksi OpenVPN-palvelin on liitetty LAN-porttiin, mikä tässä tapauksessa simuloi WAN-porttia, kuten esitelty kolumnin ensimmäisessä kohdassa kuviossa 11.

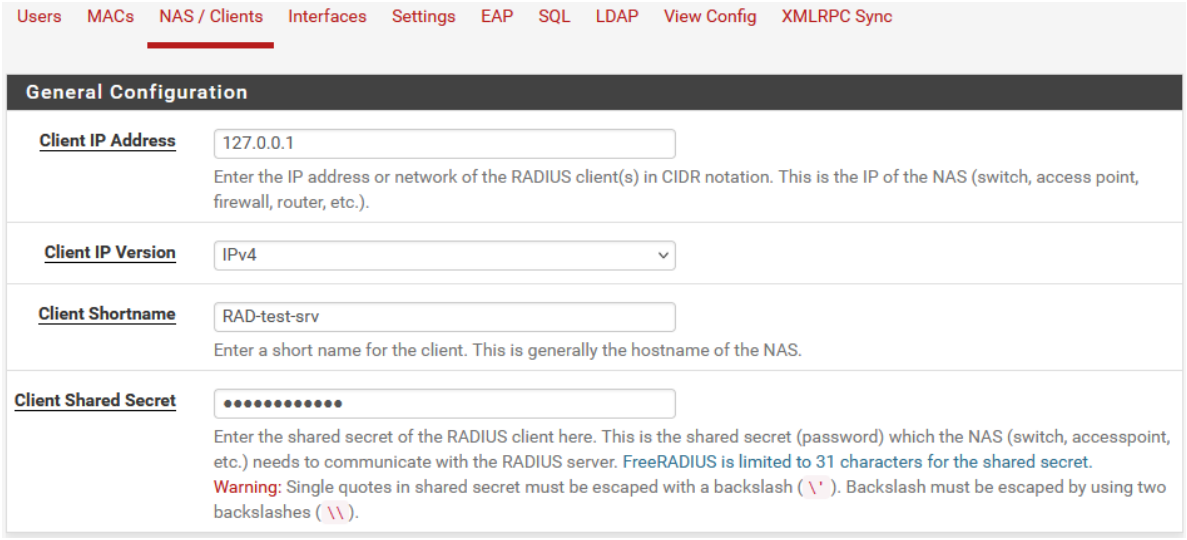
Tämä mahdollistaa liikenteen reitittämisen virtuaalisesti, ikään kuin liikenne tulisi ulkoisesta verkosta. OpenVPN:n gateway-osoite määritellään pfSensen sisäverkkoon, mikä mahdollistaa tunnelin toimimisen läpikulkuliitäntänä (eng. passthrough interface). Windows-päätelaitteen liikenne reititetään OpenVPN-tunnelin kautta VyOS-reitittimelle, joka sijaitsee sisäverkossa. Tämän avulla käyttäjä pystyy ottamaan SSH-yhteyden sisäverkon resursseihin.



Kuvio 11. OpenVPN-palvelin

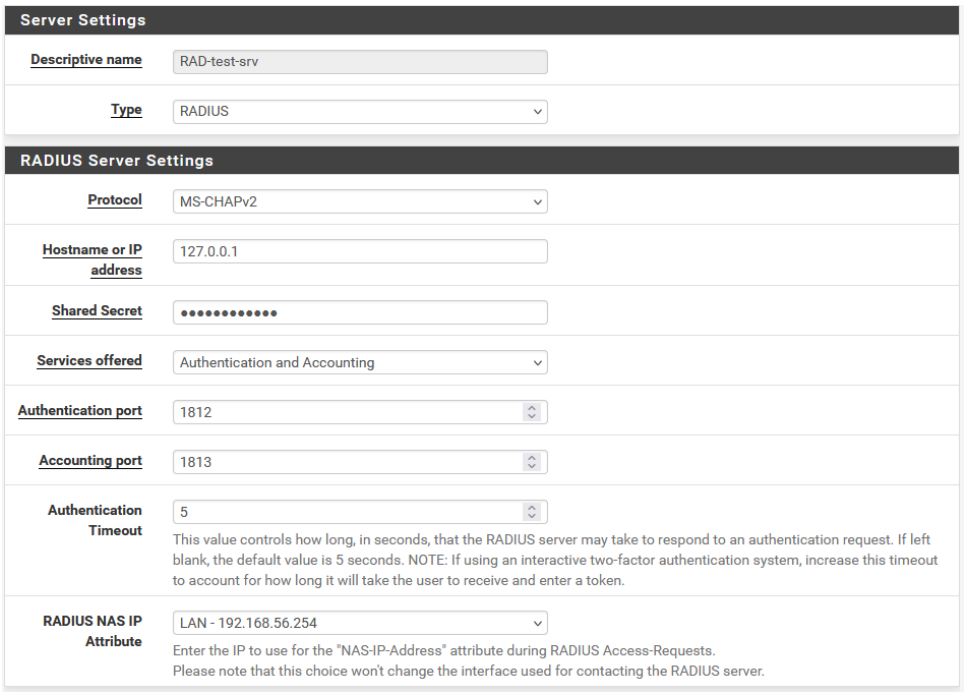
4.2.3 Päätelaitteiden konfigurointi

RADIUS-testiympäristön käyttöönotto edellyttää myös päätelaitteiden konfigurointia, työssä on otettu esimerkiksi kolme eri käyttöjärjestelmällä olevaa päätelaitetta. Tämä osio sisältää tarvittavat toimenpiteet, jotta laitteet saadaan liitettyä uuteen autentikointijärjestelmään. Luku käy läpi ensiksi Windows-pohjaisen päätelaitteen konfiguroinnin ja sen jälkeen UNIX-pohjaisen VyOS-päätelaitteen konfiguroinnin. Päätelaitteita lisätään palomuurin RADIUS-palvelimen asetuksista löytyvästä ”NAS/Clients” välilehdeltä. Konfiguraatiot on esitelty kuviossa 12, mihin on asetettu palvelimen IP-osoite, mikä tässä tapauksessa on pfSensen loopback-osoite, nimi ja jaettu salaisuus, millä RADIUS-autentikointiprotokolla varmentaa yhteyden autentikointiin.



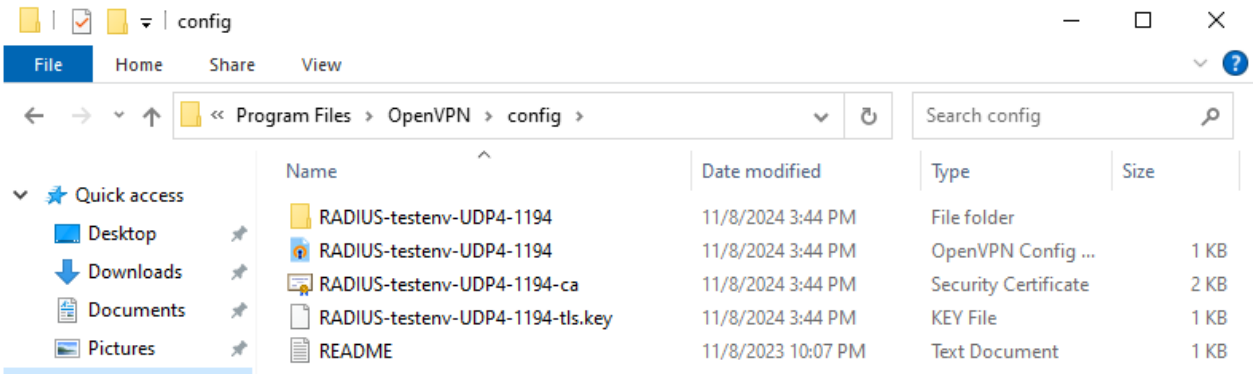
Kuvio 12. Päätelaitteen konfigurointi palvelimelle

RADIUS-palvelin täytyy aktivoida, jotta sen voi ottaa käyttöön. Palomuurin käyttäjäasetuksien takaa löytyvästä autentikointipalvelimet-valikosta saadaan luotua uusi palvelin. Palvelimelle määritellään tyypiksi ”RADIUS”, IP-osoite, jaettu salaisuus ja tarjottavaksi palveluiksi ”Authentication and Accounting”. IP-osoitteeksi määritellään pfSensen oma loopback-osoite, kuten kuviossa 13.



Kuvio 13. Autentikointipalvelimen konfigurointi

Windows-päätelaite konfiguroidaan asentamalla OpenVPN-asennuspaketti, joka on ladattu palomuurin käyttöliittymästä hyödyntäen pfSensestä löytyvää ”Client Export Utility”-työkalua. Asennuspaketti sisältää kaikki tarvittavat konfiguraatiot yhteyden muodostamiseen (ks. kuvio 14). Konfiguraatiotiedostot sisältävät OpenVPN yhteyteen tarvittavat konfiguraatiot, kuten palvelimen IP-osoitteen, portit ja salausmenetelmät. Lisäksi tiedostot sisältävät varmennustietoja ja yksityisen avaimen, mitkä ovat osa varmennusprosessia yhteyden muodostamisessa.



Kuvio 14. OpenVPN konfiguraatiotiedostot

VyOS-reittitimen konfigurointi tapahtuu määrittämällä sille staattinen IP-osoite lähiverkon aliverkosta. Reitittimen IP-osoite pysyy täten lähiverkossa samana ja tämä mahdollistaa sen, että resurssi on aina löydettävissä ja hallittavissa määritellystä osoitteesta. Tutkimus ei käy konfigurointiprosessia yksityiskohtaisesti läpi, mutta tarkastelemalla porttikohtaisia konfiguraatioita kuviossa 15 ja staattisia reitityksiä kuviossa 16 voidaan todeta, että konfiguraatiot vastaavat testaussuunnitelmaa.

```
vyos@vyos:~$ show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
eth0             172.30.128.10/28                  u/u
lo               127.0.0.1/8                       u/u
                 ::1/128
```

Kuvio 15. VyOS porttikonfiguraatiot

```
S>* 0.0.0.0/0 [1/0] via 172.30.128.1, eth0, weight 1, 00:30:12
C>* 172.30.128.0/28 is directly connected, eth0, 00:30:18
```

Kuvio 16. VyOS reititystaulu

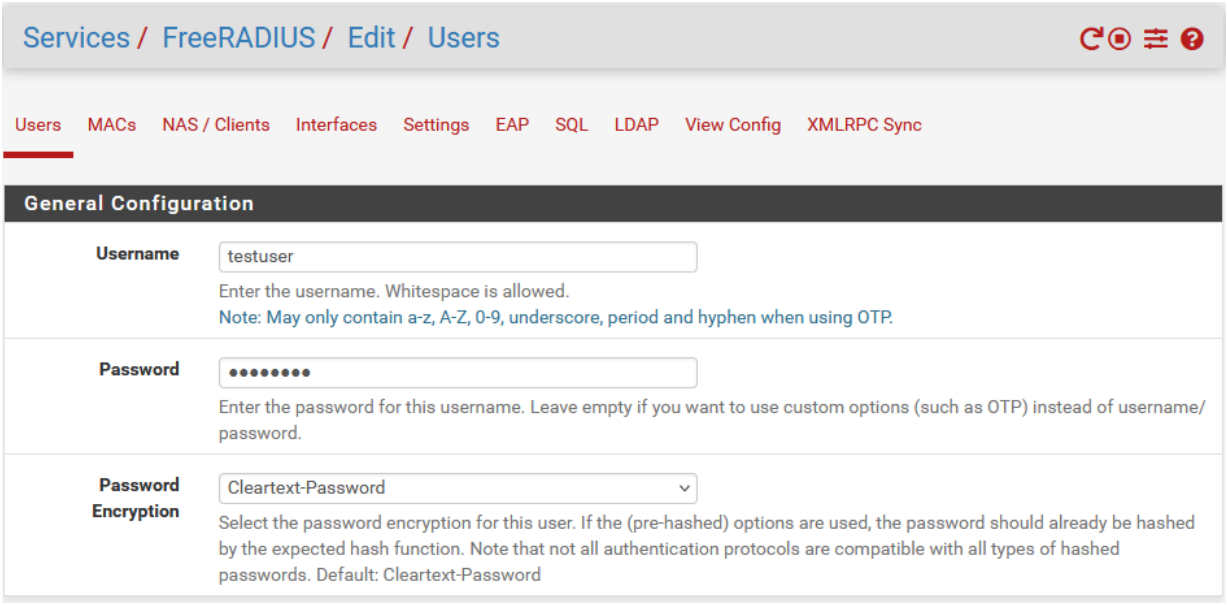
Verkkoasetusten määrittämisen jälkeen on konfiguroitava RADIUS-protokolla reitittimellä käyttöön. Parametriksi määritellään RADIUS-palvelimen IP-osoite, jaettu salaisuus, sekä palvelimella kuunteleva portti, kuten kuviossa 17 on konfiguroitu. Lopuksi määritellään palomuuriasetukset reitittimellä sallimaan kaikki liikenne, jotta varmistetaan rajoittamaton liikenne testiympäristössä.

```
host-name vyos
login {
    radius {
        server 172.30.128.1 {
            key **********
            port 1812
        }
    }
    user vyos {
        authentication {
            encrypted-password **********
        }
    }
}
```

Kuvio 17. Autentikointimenetelmät

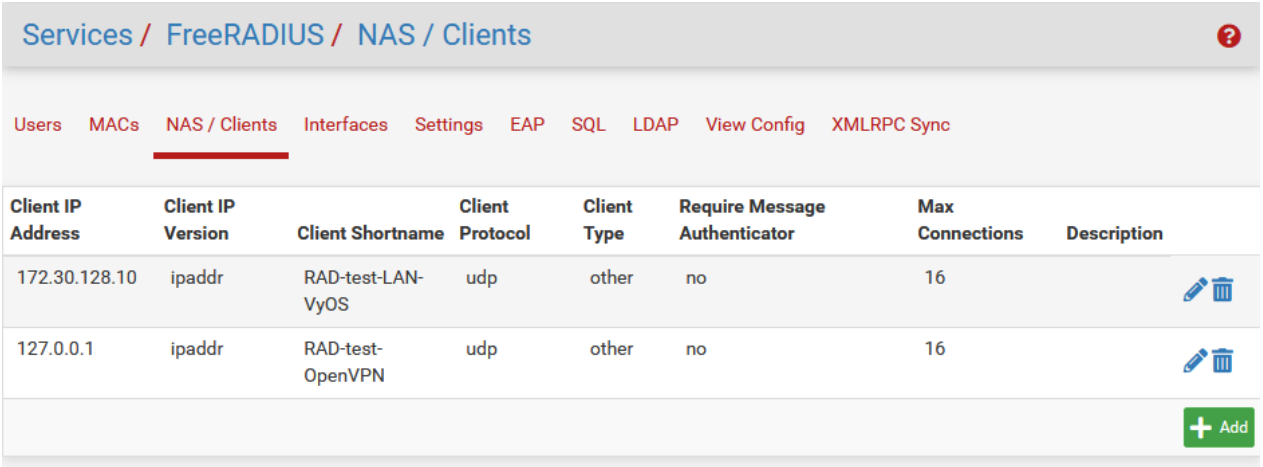
4.2.4 Käyttäjätilien lisäys ja hallinta

Käyttäjien lisääminen ja käyttöoikeuksien hallinta ovat keskeisimpiä vaiheita autentikointiprotokollan konfiguroinnissa. Käyttäjien luonti tapahtuu RADIUS-palvelimen käyttöliittymästä. Luontiprosessi on yksinkertainen, sillä siihen ei tarvita kuin kaksi pakollista parametria, käyttäjätunnus ja salasana (ks. kuvio 18). Lisäasetukset ovat vapaaehtoisia, mutta tutkimuksen laajuuden rajoissa niitä ei käsitellä. Tuotantoverkossa lisäasetusten optimointi on erittäin suositeltavaa.



Kuvio 18. Käyttäjätilin luonti

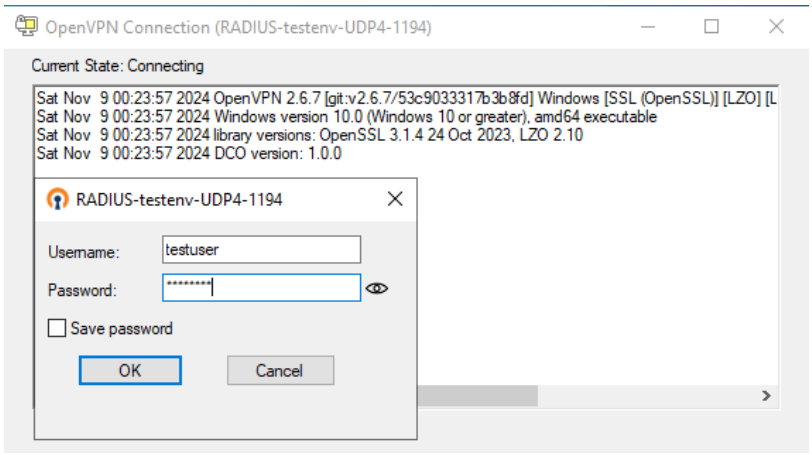
RADIUS-palvelimen konfiguraatioihin määritellään VyOS-reitittin sille asetetulla staattisella IP-osoitteella, ja lyhyt selite asiakaslaitteen tunnistamista varten. Kuviossa 19 on listattu sekä palvelin- että päätelaitteet konfiguroinnin jälkeen. Konfiguraatiot sisältävät myös jaetun salaisuuden. Lisäasetuksina voidaan määritellä asiakaskohtainen liikennöintiprotokolla, tyyppi ja määrä, montako yhteyttä voi asiakaskoneelta olla samanaikaisesti.



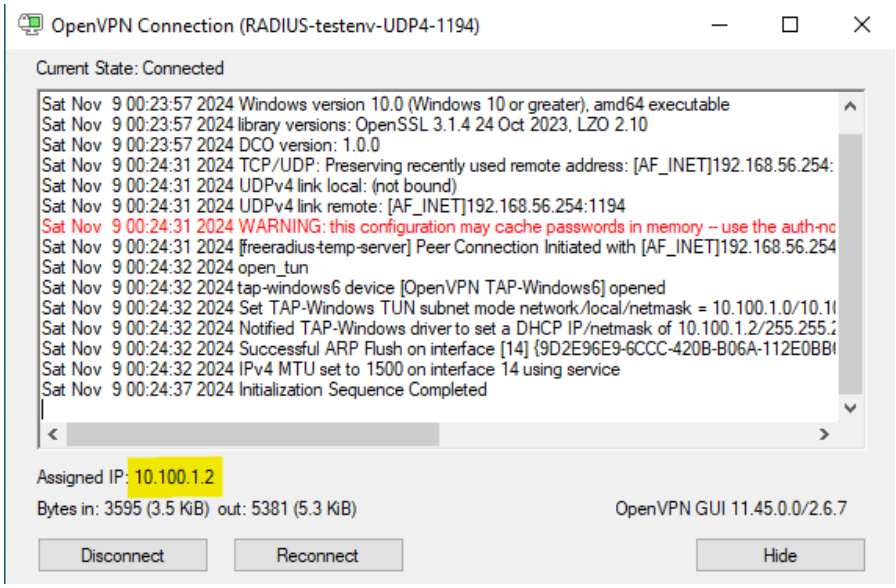
Kuvio 19. Asiakaslaitteet listattuna

4.2.5 Testaus ja validointi

Testauksella varmistetaan ratkaisun toimivuus ja yhteensopivuus eri laitteiden kanssa. Validointivaiheessa testataan autentikointijärjestelmän käytettävyys ja varmistetaan, että RADIUS toimii suunnitellusti koko ympäristössä. Testausvaihe alkaa Windows -päätelaitteen VPN-yhteyden avaamisella RADIUS-käyttäjätunnuksella. OpenVPN-yhteyteen tunnistautuminen tapahtuu yhdistämisen yhteydessä. Syöttämällä RADIUS-testikäyttäjän tunnukset sovelluksen kirjautumisikkunaan kuviossa 20 esitellyllä tavalla, yhteys muodostuu ja kuviossa 21 näkyy yhdistämisen jälkeen VPN-väliverkosta sille määrätty IP-osoite.



Kuvio 20. OpenVPN autentikointi



Kuvio 21. VPN yhteys muodostettu.

Tarkastamalla palomuurin autentikointilokista, kirjautuminen näkyy onnistuneesti myös palvelimen päässä (ks. kuvio 22). Kun VPN-tunneli on muodostettu, Windows-päätelaitteen reititystauluun on ilmestynyt uusi reitti, hahmoteltuna punaisella alaviivalla kuviossa 23. Tämä reitti osoittaa lähiverkkoon, missä VyOS-reititin sijaitsee. Reititystaulusta vahvistamalla voi varmistaa, että Windows-päätelaite voi nyt liikennöidä turvallisesti sisäverkon resursseihin.

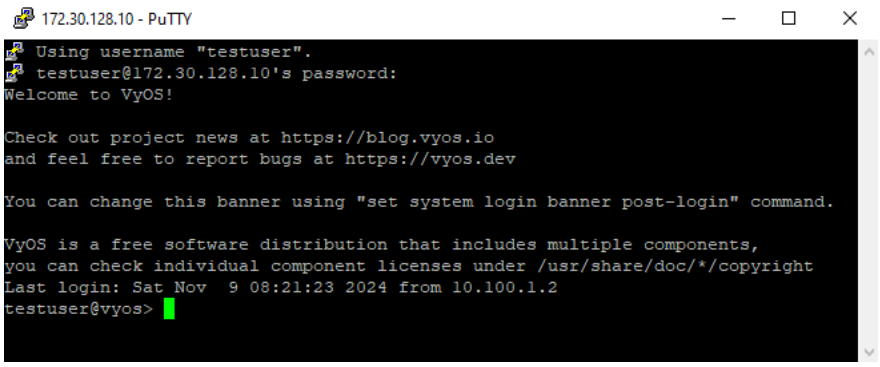
```
Nov  9 10:24:31 RADIUS-testenv openvpn[398]: user 'testuser' authenticated
```

Kuvio 22. Lokitettu onnistunut autentikointi.

```
===========================================================================
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0   192.168.56.254    192.168.56.10     281
       10.100.1.0    255.255.255.0         On-link       10.100.1.2     281
       10.100.1.2  255.255.255.255         On-link       10.100.1.2     281
     10.100.1.255  255.255.255.255         On-link       10.100.1.2     281
        127.0.0.0        255.0.0.0         On-link        127.0.0.1     331
        127.0.0.1  255.255.255.255         On-link        127.0.0.1     331
  127.255.255.255  255.255.255.255         On-link        127.0.0.1     331
     172.30.128.0  255.255.255.240      10.100.1.1       10.100.1.2     281
     192.168.56.0    255.255.255.0         On-link    192.168.56.10     281
    192.168.56.10  255.255.255.255         On-link    192.168.56.10     281
```

Kuvio 23. Windows reititystaulu VPN-tunneliyhteydellä.

Windows-päätelaitteelta voi nyt ottaa SSH-yhteyden VyOS-reitittimeen VPN-tunnelin ylitse. Yhteyden muodostamisen aikana konsoli pyytää käyttäjää syöttämään käyttäjätunnuksen ja salasanan. Syöttämällä RADIUS-testikäyttäjän tunnukset, voidaan yhteys testata päätelaitteelta päätelaitteelle ja onnistuneen autentikoinnin jälkeen pääsy on sallittu (ks. kuvio 24).



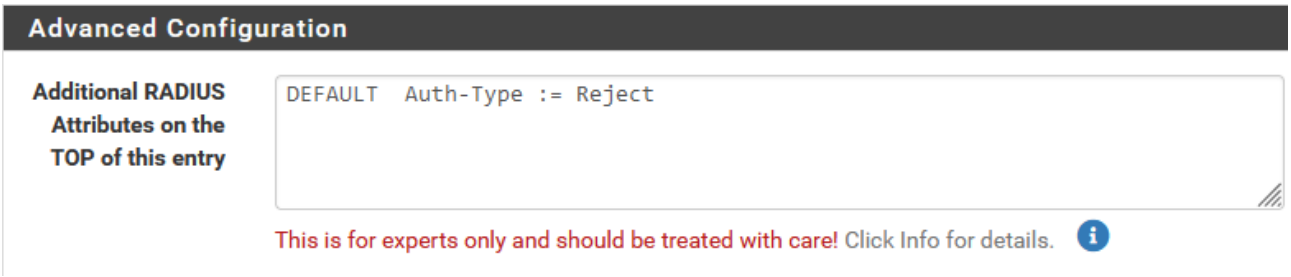
Kuvio 24. Onnistunut autentikointi

4.3 Vaatimustenmukaisuuden varmistaminen

Osuus käsittelee niitä prosesseja ja toimenpiteitä, joiden avulla varmistetaan, että juuri implementoitu autentikointimalli täyttää organisaation- sekä tietoturvastandardien vaatimukset. Vaatimustenmukaisuuden varmistaminen on välttämätön vaihe toteutuksessa, sillä sen avulla voidaan osoittaa, että organisaation autentikointi on tietoturvallisella tasolla. Tavoitteena on varmistaa ISO/IEC 27002 hallintakeinojen avulla, onko uusi autentikointimalli vaatimusten mukainen. Raportin laajuuden vuoksi tutkimus ei käy läpi koko ISO/IEC 27001 taulukkoa liittyen todentamiseen, vaan poimii sieltä tutkimukseen oleellisimmat osuudet ja vertaa niiden vaatimustenmukaisuutta juuri tehtyyn testaukseen. Tutkimukseen valikoitui neljä ISO/IEC 27002 standardin mukaista vaatimusta, jotka ovat listattuna alla.

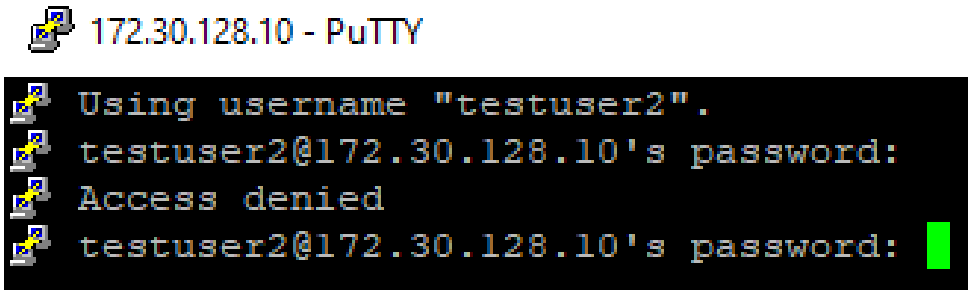
Hallitaan sitä, mihin tietoihin kullakin käyttäjällä on pääsy. (SFS-EN ISO/IEC 27002:2002. 8.3 Tietoihin pääsyn rajoittaminen. 94–95. 2022.)

Työssä on määritelty kaksi testikäyttäjää, toisen autentikointityypiksi on asetettu oletuksena ”Reject”. Kuviossa 25 esitelty lisäparametri on konfiguroitu siten, että käyttäjä ei voi autentikoitua mihinkään resurssiin, ellei pääsyä ole erikseen sallittu.



Kuvio 25. Oletusarvoisesti estetty yhteys

Windows-päätelaitteelta kirjautuminen VyOS-reitittimeen kielletyllä testikäyttäjällä ei onnistu, koska sitä ei ole sallittu järjestelmässä (ks. kuvio 26). Asetusta on mahdollista hyödyntää siten, että oletuksena kaikkien laitteiden pääsy evätään ja tällä tavoin saadaan hallitusti sallittua ainoastaan käyttäjien ne resurssit mihin heillä on tarpeellinen päästä autentikoimaan.



Kuvio 26. Hylätty kirjautuminen

Järjestelmän olisi annettava hälytys, jos se havaitsee kirjautumisen hallintakeinojen mahdollisen tai onnistuneen murtoyrityksen (SFS ISO/IEC 27002:2022. A1.8.5. 2022).

Tämän vaatimuksen täyttäminen on mahdollista konfiguroida RADIUS siten, että se luo hälytykset epäonnistuneista kirjautumisyrityksistä. Konfiguraatioon on mahdollista asettaa parametrit siten, että se luo hälytyksiä epäonnistuneista yrityksistä. Lisäksi SIEM (eng. Security Information and Event Management) järjestelmä edesauttaisi lokien todenmukaisuutta. SIEM-järjestelmällä on mahdollista luoda myös hälytyksiä, kun järjestelmässä havaitaan poikkeavaa tai epäilyttävää toimintaa, kuten epäonnistuneita kirjautumisyrityksiä.

Järjestelmä ei saisi lähettää salasanoja selväkielitekstinä verkon kautta (SFS ISO/IEC 27002:2022. A1.8.5. 2024).

Työssä on käytetty VPN-tunnelia, mikä mahdollistaa salatun yhteyden järjestelmien välillä. VPN-tunneli varmistaa, että kaikki liikenne, kuten kirjautumistiedot kulkevat verkossa salatussa muodossa. Päätelaitteet ovat vaihtaneet salausavaimet keskenään avatessaan SSH-yhteyden, kuten kuviossa 27 on nähtävissä. Tämän jälkeen paketteja seuraamalla liikenne oli täysin salattua, eikä sitä ole mahdollista saada selkokieliseksi ilman salausavainta. Lisäksi VPN-yhteys lisää tietoturvaa myös salaamalla kaiken muunkin liikenteen, kirjautumistietojen lisäksi.

No.	Time	Source	Destination	Protocol	Lengtl	Info
29	9.143696	10.100.1.2	172.30.128.10	SSHv2	270	Client: Key Exchange Init
30	9.146525	172.30.128.10	10.100.1.2	SSHv2	1134	Server: Key Exchange Init
31	9.158240	10.100.1.2	172.30.128.10	SSHv2	1262	Client: Diffie-Hellman Key Exchange Init
32	9.173163	172.30.128.10	10.100.1.2	TCP	60	22 → 49183 [ACK] Seq=1104 Ack=2853 Win=64128 Len=0
33	9.175756	172.30.128.10	10.100.1.2	SSHv2	1454	Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len…
34	9.186053	10.100.1.2	172.30.128.10	SSHv2	134	Client: New Keys, Encrypted packet (len=64)
35	9.186198	172.30.128.10	10.100.1.2	SSHv2	238	Server: Encrypted packet (len=184)
36	9.226455	10.100.1.2	172.30.128.10	TCP	54	49183 → 22 [ACK] Seq=2933 Ack=2688 Win=262912 Len=0
37	9.231529	172.30.128.10	10.100.1.2	TCP	60	22 → 49183 [ACK] Seq=2688 Ack=2933 Win=64128 Len=0

Kuvio 27. Pakettikaappaus salatusta yhteydestä

Järjestelmän olisi katkaistava käyttämättömät istunnot määritellyn toimettomuusajan jälkeen (SFS ISO/IEC27002:2022. A1.8.5. 2022).

Standardin mukaan järjestelmän tulee katkaista käyttämättömät yhteydet määritellyn ajan jälkeen. Tämä vaatimus parantaa järjestelmän turvallisuutta vähentämällä riskiä siitä, että hyökkääjät pääsisivät hyödyntämään toimettomana olevia yhteyksiä siihen, että voisivat toimia verkossa huomaamattomasti. Tämän vaatimuksen täyttämiseksi RADIUS-palvelimella on konfiguroitu ”idle_timeout”-parametri päätelaitteen konfiguraatioissa, kuviossa 28 näkyvällä tavalla. Tämä asetus määrittelee ajan, jonka jälkeen käyttämättömät istunnot katkaistaan automaattisesti. Alla olevassa esimerkkikonfiguraatiossa on testaukseen konfiguroitu aikakatkaisun arvoksi 30 sekuntia.

```
/usr/local/etc/raddb/clients.conf

client "RAD-test-LAN-VyOS" {
        ipaddr = 172.30.128.10
        proto = udp
        secret = [redacted]
        require_message_authenticator = no
        nas_type = other
        ### login = !root ###
        ### password = someadminpass ###
        limit {
                max_connections = 16
                lifetime = 0
                idle_timeout = 30
        }
}
```

Kuvio 28. Yhteyskohtainen aikakatkaisu

Lisäksi on mahdollista konfiguroida käyttäjäkohtaiset aikakatkaisurajat toimettomuudelle. Testikäyttäjälle on konfiguroitu 60 sekunnin aikakatkaisu toimettomuuden jälkeen, kuten kuviossa 29. Tästä generoituu myös tarvittaessa lokitietoja, joista voidaan varmistaa, että aikakatkaisu toimii tarkoitetusti.

```
/usr/local/etc/raddb/users

"testuser" Cleartext-Password := [redacted], Idle-Timeout := 60
```

Kuvio 29. Käyttäjäkohtainen aikakatkaisu

Kyberturvallisuusdirektiivi ja uusi kyberturvallisuuslaki korostaa tarkkaa käyttäjien tunnistusta ja valtuutettujen käyttäjien hallinnan tärkeyttä. Näihin vaatimuksiin pystytään vastaamaan hyödyntämällä RADIUS-protokollan optimointimahdollisuuksia. Lisäksi tietoturvadirektiivi vaatii nopeaa reagointia vakavista tietoturvatapahtumista ja mahdollisista tietoturvarikoksista. Tähän vaatimukseen ei tässä testiympäristössä pystytä täysin vastaamaan, mutta esimerkiksi implementoimalla SIEM-järjestelmä ja kehittämällä lokitusjärjestelmiä, RADIUS-protokollan avulla kyetään vastaamaan tähän vaatimukseen.

5 Tulokset

Luvussa arvioidaan, kuinka testiympäristössä käytetty RADIUS-toteutus vastaa organisaation tuotantoympäristön vaatimuksia. Tuloksien ohessa tarkastellaan myös, miten autentikointiprotokollaa olisi mahdollista jatkokehittää entisestään, jotta tietoturvaa saataisiin edelleen parannettua. Vaikutukset tietoturvan näkökulmasta ovat merkittäviä, sillä käyttäjäkohtainen pääsynhallinta, erityisesti hallinnollisiin laitteisiin ja verkon eri segmentteihin, on protokollan ansiosta paljon paremmin hallittavissa. Tämä vähentäisi organisaation aiemmin havaittua riskiä siitä, että käyttäjillä olisi laajempia oikeuksia kuin heidän työtehtävänsä edellyttäisivät. Lisäksi RADIUS-toteutuksen myötä voidaan tarkastella kirjautumisista syntyvää lokidataa, mikä mahdollistaa luvattomien kirjautumisyritysten havaitsemisen ja tehokkaamman estämisen verrattuna nykyiseen toteutukseen.

Testiympäristössä todettu salausmenetelmä ja päätelaitteiden välinen viestintä ilman selkokielistä dataa parantavat merkittävästi tietoturvaa jokapäiväisessä käytössä. Tämä vastaa myös ISO/IEC 27001 -standardin vaatimuksia salausmenetelmistä. Lisäksi käyttäjien kirjautuneiden istuntojen aikakatkaisu estää hyökkääjiä hyödyntämästä auki jääneitä yhteyksiä ja maskeeraamasta omaa liikennettään työntekijän liikenteen sekaan. Näin RADIUS-protokolla tarjoaa konkreettisia parannuksia organisaation tietoturvatasoon ja tukee standardien mukaista toimintaympäristöä.

5.1 Tutkimuskysymysten tarkastelu

Tutkimuksessa vastattiin tutkimuksen alussa esitettyihin tutkimuskysymyksiin perustuen testiympäristössä saatujen tulosten ja niiden analysoinnin pohjalta. Kysymykset käsittelivät protokollan teknistä toteutusta, tietoturvavaatimusten täyttämistä, sekä hallinnollisten toimenpiteiden merkitystä protokollan hyödyntämisessä.

Ensimmäisenä tutkimuskysymyksenä oli selvittää, kuinka RADIUS-protokolla voidaan toteuttaa siten, että se täyttää ISO/IEC 27001 -standardin vaatimukset. Testiympäristössä toteutettu RADIUS-protokolla vastaa näihin vaatimuksiin erityisesti autentikoinnin, tietojen luottamuksellisuuden ja järjestelmän käytettävyyden osalta. Teknisesti järjestelmässä saavutettiin vaatimustenmukainen salattu liikenne, toimivat lokitus- ja hälytystoiminnot sekä istuntojen aikakatkaisu. Nämä ominaisuudet noudattavat ISO/IEC 27002 -standardissa kuvattuja parhaita käytäntöjä.

Toisena tutkimuskysymyksenä oli selvittää, kuinka RADIUS-protokollan implementointi voi tukea kyberturvallisuusdirektiivin vaatimuksia järjestelmien käytettävyydestä, eheydestä ja tietoturvasta. Testiympäristön tulokset osoittavat, että RADIUS tukee näitä vaatimuksia tarjoamalla luotettavan autentikointimekanismin, joka on jatkokehityksen myötä laajennettavissa segmentoidun verkkoarkkitehtuurin ja modernien salausmenetelmien avulla. Viestinnän eheys varmistetaan salauksen avulla, mikä estää liikenteen muokkaamisen tai sieppaamisen päätelaitteiden välillä. Lisäksi vähimmän etuoikeuden periaatteen mukaisesti käyttöoikeuksia voidaan rajoittaa vain niille käyttäjille, jotka niitä todella tarvitsevat, mikä lisää järjestelmän turvallisuutta ja hallittavuutta.

Kolmantena tutkimuskysymyksenä tutkimus selvitti, mitä hallinnollisia toimenpiteitä tarvitaan, jotta käyttäjähallintaa voidaan toteuttaa protokollaa hyödyntäen tehokkaasti ja turvallisesti.

Vaikka tutkimus keskittyi tekniseen toteutukseen, projektin aikana tunnistettiin useita hallinnollisia toimenpiteitä, jotka tukevat protokollan käyttöä. Ensisijaisesti käyttöoikeuksien hallinnan ja käyttöoikeuspolitiikkojen päivittäminen ajantasaisiksi ennen implementointia on keskeistä, jotta vain valtuutetut käyttäjät pääsevät käsiksi määriteltyihin resursseihin. Käyttäjien säännöllinen tarkastelu ja käyttäjätilien elinkaaren hallinta auttavat varmistamaan, että tarpeettomat tilit poistetaan ja käyttöoikeudet päivitetään työnkuvan muuttuessa. Näiden toimenpiteiden lisäksi jatkuva koulutus turvallisista kirjautumiskäytännöistä, kuten monivaiheisesta tunnistautumisesta ja kertakäyttöisistä salasanoista, on tärkeää turvallisen autentikoinnin ylläpitämiseksi.

Yhteenvetona tutkimus onnistui selvittämään, miten RADIUS-protokollan tekninen toteutus, tietoturvastandardien ja -direktiivin noudattaminen, sekä hallinnolliset käytännöt tulee yhdistää organisaation autentikointijärjestelmän kehittämiseksi. Tulokset osoittavat, että järjestelmän jatkokehitys on yksi keskeisimpiä etappeja kohti vaatimustenmukaista toteutusta. Tutkimustuloksia on mahdollista hyödyntää organisaation varsinaisessa toteutuksessa.

6 Pohdinta

6.1 Projektin arviointi

Projektin päätavoitteena oli suunnitella ja toteuttaa RADIUS-autentikointimalli, joka kykenee täyttämään ISO/IEC 27001-standardin ja uuden kyberturvallisuusdirektiivin vaatimukset. Tarkastelemalla erityisesti projektin vahvuuksia ja haasteita, voidaan tutkimusta hyödyntää organisaation oikeaan implementointiin. Projektissa saavutettiin keskeiset tavoitteet, mutta samalla havaittiin kehitysalueita, jotka ohjaavat varsinaista implementointia.

Testiympäristössä saavutettu tulos on lupaava, mutta järjestelmän käyttökelpoisuutta olisi myös hyvä arvioida suuremmassa ja monimutkaisemmassa ympäristössä. Tällä varmistetaan, miten järjestelmä toimii luotettavasti eri verkoissa, käyttöjärjestelmissä ja kuormitustilanteissa. Projektissa toteutettiin autentikointi vain yhdellä todennusmenetelmällä, jatkossa voisi harkita lisätodennusmenetelmien kuten MFA tai OTP sisällyttämistä. Kehitettävää olisi myös monipuolisemman verkon ja ympäristön toteutuksessa siten, että ympäristöä testattaisiin useammalla käyttäjällä ja käyttäjien tasolla. Esimerkiksi lisäämällä tarkempia käyttöoikeusmäärityksiä, voidaan antaa tietyille käyt-

täjille oikeuksia tiettyihin resursseihin. Yksi merkittävä kehityskohde on tarkempien käyttöoikeusmääritysten toteuttaminen. Oletusarvoisesti kieltävän pääsyn periaatteen tarkempi soveltaminen ja käyttäjäryhmien roolien määrittely lisäävät ympäristön turvallisuutta ja hallittavuutta. Näillä toimilla voidaan varmistaa, että vain valtuutetut käyttäjät pääsevät käsiksi tiettyihin resursseihin, mikä vähentää merkittävästi luvattoman käytön riskiä.

Projektin tuloksena luotu RADIUS-pohjainen autentikointimalli tarjoaa jo osittaisen vaatimusten mukaisen pääsynhallinnan, mutta testiympäristö korosti myös konfiguraation jatkokehityksen merkitystä. Ympäristön koventaminen nousee esiin yhtenä tärkeimmistä vaiheista tuotantoon siirtymisen yhteydessä. Kovennus, kuten protokollan asetusten optimointi ja lokitietojen hallinta, on kriittistä turvallisuuden ylläpitämiseksi. Projektin aikana opittiin, että lokien kerääminen ja niiden analysointi ovat keskeisiä osia tietoturvallisuuden valvontaa ja kehittämistä. Lokit mahdollistavat paitsi mahdollisten tietoturvapoikkeamien havaitsemisen myös järjestelmän käytön jäljitettävyyden, mikä tukee organisaation laajempia tietoturvatavoitteita.

Yhteenvetona voidaan todeta, että tutkimus onnistui luomaan hyvät lähtökohdat turvallisen autentikointimallin implementoinnille. Tulokset tarjoavat arvokasta tietoa siitä, miten RADIUS-protokollaa voidaan soveltaa organisaation autentikointijärjestelmän parantamiseen. Testiympäristössä saadut havainnot ja suositukset tukevat organisaation pyrkimystä siirtyä tietoturvastandardien mukaisiin käytäntöihin. Lisäksi tutkimuksen tulokset muodostavat perustan tuleville parannuksille ja jatkokehitykselle, jotka edistävät entistä turvallisempaa ja tehokkaampaa pääsynhallintaa.

6.2 Jatkokehitys

Tutkimuksen aikana havaittiin kehitysehdotuksia, joiden avulla RADIUS-protokollaa voitaisiin hyödyntää entistä tehokkaammin ja saavuttaa korkeampia tietoturvan tasoja organisaation tuotantoympäristössä. Teknisenä näkökulmana jatkokehityksessä nousee yhdeksi tärkeimmäksi ympäristön kovennukset. Kovennuksilla tarkoitetaan järjestelmän konfiguraatioiden ja käyttäjäoikeuksien tarkempaa optimointia, jotka voivat vähentää merkittävästi järjestelmän haavoittuvuutta. IP-osoitteiden ja porttien rajauksilla voidaan RADIUS-palvelin konfiguroida siten, että se kuuntelee vain tiettyjä osoitteita ja portteja, mikä pienentää hyökkäyspinta-alaa. Tämä mahdollistaa autentikointiliikenteen ohjaamisen tarkasti määriteltyjä reittejä pitkin, mikä vähentää mahdollisuuksia

palvelimen väärinkäytölle. Samalla vahvempien salausmenetelmien käyttöönotto parantaa autentikointiprosessin suojaa moderneja hyökkäysmenetelmiä vastaan ja tukee tiedon eheyttä sekä luottamuksellisuutta.

Lokituksen parantaminen on myös keskeinen jatkokehityskohde. Tarkemman lokidatan kerääminen ja säilyttäminen erillisellä lokipalvelimella parantaisi lokitietojen turvallisuutta ja jäljitettävyyttä. Tämä mahdollistaisi paitsi onnistuneiden ja epäonnistuneiden kirjautumisten seurannan myös haitallisten toimijoiden hyökkäysyritysten tunnistamisen ja reagoinnin mahdollisiin tietoturvapoikkeamiin. Myös MFA ja OTP ovat merkittäviä lisäturvatoimenpiteitä, jotka tarjoavat suojaa erityisesti korkeamman riskin tilanteissa. MFA:n avulla käyttäjiltä edellytetään vahvempaa todentamista lisäämällä toinen vaihe kirjautumisprosessiin, mikä vaikeuttaa merkittävästi luvattomia pääsy-yrityksiä. OTP lisää erityisesti etätyössä olevien käyttäjien tietoturvaa, sillä kertakäyttöiset salasanat vähentävät riskiä, että varastettu salasana mahdollistaisi pääsyn kriittisiin järjestelmiin. Monivaiheinen tunnistautuminen on myös keskeinen osa NIS2-direktiivissä määriteltyjä tietoturvakäytäntöjä, mikä korostaa sen tärkeyttä jatkokehityksessä.

Lähteet

Beschokov, M. 2024. How does RADIUS work? Artikkeli. Viitattu 20.10.2024. https://www.wallarm.com/what/radius-remote-authentication-dial-in-user-service-protocol

Difference Between Symmetric and Asymmetric Key Encryption. 2024. Artikkeli GeeksForGeeks sivustolla. Viitattu 16.11.2024. https://www.geeksforgeeks.org/difference-between-symmetric-and-asymmetric-key-encryption/

Getting Started. N.d. Overview. Artikkeli. Viitattu 2.11.2024. https://www.pfsense.org/getting-started/

HE57&2024 vp. 2024. Lakiesitys. 5.1.4 Valvonnan järjestäminen. Viitattu 3.11.2024. https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_57+2024.aspx

Isaksson, R. 2024. Kyberturvallisuuslaki & NIS2: kansalliset lainsäädännöt ja soveltaminen. Blogiteksti. Yleiskatsaus Suomen kyberturvallisuuslakiin. Viitattu 14.11.2024. https://www.digiturvamalli.fi/blogi/kyberturvallisuuslaki-nis2-kansalliset-lainsaadannot-ja-soveltaminen

Standardi. N.d. Kielitoimiston sanakirja. Viitattu 18.10.2024. https://www.kielitoimistonsanakirja.fi/#/standardi

Lainsäädäntö. N.d. Verkkojulkaisu. Eduskunta. Viitattu 17.10.2024. https://www.eduskunta.fi/FI/naineduskuntatoimii/kirjasto/aineistot/kotimainen_oikeus/kotimaiset-oikeuslahteet/Sivut/Lainsaadanto.aspx

Lainvalmistelun prosessiopas. N.d. Artikkeli Finlex verkkosivuilla. Viitattu 17.10.2024. https://lainvalmistelu.finlex.fi/

Laurente-Ticong, L. 2023. Encryption Types, Methods, and Use Cases Explained. Artikkeli. Viitattu 16.11.2024. https://www.enterprisenetworkingplanet.com/security/encryption-types/

LVM044:00/2022. Kyberturvallisuusdirektiivin (NIS2-direktiivi) kansallista toimeenpanoa tukeva työryhmä. Annettu 12.12.2022. Viim. muutos 8.2.2024. Viitattu 18.10.2024. https://valtioneuvosto.fi/hanke?tunnus=LVM044:00/2022

Mitä standardi tarkoittaa? N.d. SFS Verkkosivut. Viitattu 18.10.2024. https://sfs.fi/standardeista/mika-on-standardi/

Nico, P. 2021. Encryption choices: rsa vs. aes explained. Blogikirjoitus. Viitattu 16.11.2024. https://preyproject.com/blog/types-of-encryption-symmetric-or-asymmetric-rsa-or-aes

NIS2 – Euroopan unionin kyberturvallisuusdirektiivi. 2024. Viitattu 18.10.2024. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis2-euroopan-unionin-kyberturvallisuusdirektiivi

Pulkkanen, A. 2024. NIS2-yleiskatsaus: Historia, keskeinen sisältö ja merkitys yritysjohdolle. Blogiteksti. Viitattu 3.11.2024. https://www.digiturvamalli.fi/blogi/nis2-yleiskatsaus-historia-keskeinen-sisalto-ja-sen-merkitys-yritysjohdolle

Pääsynhallinta ja tunnistaminen. N.d. Blogiteksti. Viitattu 20.10.2024. https://www.enfo.fi/palvelumme/tietoturva/digitaalinen-identiteetti/paasynhallinta-ja-tunnistaminen

SFS-EN ISO/IEC 27000:2020. Tietoturvallisuuden standardisarja. N.d. Viitattu 20.10.2024. https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/ISO/IEC-iec-27000-tietoturvallisuuden-standardisarja/#

Symmetric Encryption vs Asymmetric Encryption: How it Works and Why it's Used. N.d. Artikkeli Device Authority sivustolla. Viitattu 16.11.2024. https://deviceauthority.com/symmetric-encryption-vs-asymmetric-encryption/

What is RADIUS? N.d. Artikkeli. Viitattu 20.10.2024. https://www.fortinet.com/lat/resources/cyberglossary/radius-protocol

What's the Difference Between RADIUS and Diameter protocol? 2022. Blogiteksti. Viitattu 20.10.2024. https://rublon.com/blog/radius-vs-diameter/

Xiaoguang, Z. & Yuting, Z. 2024. What IS RADIUS? How Does RADIUS Work? Artikkeli. Viitattu 20.10.2024. https://info.support.huawei.com/info-finder/encyclopedia/en/RADIUS.html