Tuomas Paavola

Sophos-palomuuri palveluna

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

27.10.2016

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Tuomas Paavola Sophos-palomuuri palveluna 50 sivua + 1 liitettä 27.10.2016
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot ja tietoliikenne
Ohjaaja(t)	Tekninen konsultti Arto Väisänen Yliopettaja Janne Salonen

Tässä opinnäytetyössä tutustuttiin tietoturvaan yleisesti ja keskityttiin tietoturvan toteuttamiseen palomuurin avulla. Työssä perehdytään Sophos UTM -palomuurien ominaisuuksiin ja toimintaan. Toiminnallisuuden esittelyn jälkeen työssä käydään läpi Dustin Finland Oy:n palomuuripalvelu.

Työn perusta on tietoturva, koska se koskettaa kaikkia ja siihen on syytä suhtautua vakavasti. Tietoturva koostuu luottamuksellisuudesta, käytettävyydestä ja eheydestä. Tietoturvan voi jakaa kahdeksaan eri osa-alueeseen.

Sophoksen Unified Threat Management on keskitetty ratkaisu tietoturvauhkien torjuntaan. Se tarjoaa myös työkalut VPN-etäyhteyksien luomiselle. UTM-palomuuri voidaan toteuttaa fyysisesti, virtuaalisesti, ohjelmistolla tai pilvipalveluna. Palomuurin kahdentaminen lisää käytettävyyttä ja vikasietoisuutta. UTM tarjoaa kaikki tarpeelliset verkon suojaamiseen ja toimivuuteen vaikuttavat perusominaisuudet, joiden keskeisimpiä ominaisuuksia on palomuurin pakettisuodatus, nimenmuunnos, DHCP-palvelut ja osoitteenmuunnos.

Asiakkaan ottaessa Dustin Finland Oy:n palomuuripalvelun määritellään palvelusopimus, jonka jälkeen palomuuripalvelun asiakkaalle luodaan tietoturvasuunnitelma, jonka pohjalta tehdään laitevalinnat. Palvelusopimuksen solmittua noudatetaan prosessikaaviota, joka tehtiin tätä insinöörityötä varten. Prosessikaavio on esitetty työn loppuosassa ja sen eri vaiheet on myös selitetty.

Avainsanat	Sophos, UTM, Palomuuripalvelu

Author(s) Title Number of Pages Date	Tuomas Paavola Sophos Firewall as service 50 pages + 1 appendices 27 October 2016
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructor(s)	Arto Väisänen, Techology Consultant Janne Salonen, Principal Lecturer

This thesis focuses on information security in general and implementing it using firewalls. The thesis examines Sophos UTM firewall and its features and functionality. Dustin Finland Oy offers Firewall as service. Firewall as service is explained after the theory and the functionality.

The base of this thesis is information security because it concerns everyone and it should be taken seriously. Information security consists of confidentiality, availability and integrity. Information security can be divided into eight different sections.

Sophos Unified Threat Management is a centralized defense tool for security threats. It also offers other services like VPN-remote connections. UTM firewall can be deployed with hardware appliances, software installations, virtualization or cloud-based solution. The High Availability feature makes the system redundant. UTM offers all the necessary tools for protecting the network like packet based firewall, DNS, DHCP and NAT.

A service contract is signed when a customer buys the Firewall service from Dustin Finland Oy. After signing the contract, a process diagram is followed, the customer receives a security plan and needed devices are selected based on the requirements of the security plan. The process diagram was created while working with this thesis. The different parts of the process diagram is explained on the thesis.

Keywords	Sophos, UTM, Firewall as service

Sisällys

Lyhenteet

ATP	Advanced Threat Protection. Edistyneiden uhkien torjunta.
BIND	Berkeley Internet Name Domain. Avoimen lähdekoodin ohjelma, joka kehitettiin Berkeleyn yliopistossa internetin nimenselvitys tarpeisiin 1980-luvun alkupuolella.
DNS	Domain Name System. Internetin nimipalvelujärjestelmä.
DHCP	Dynamic Host Configuration Protocol. Protkolla, jonka avulla jaetaan IP-osoitteita.
FTP	File Transfer Protocol. TCP-protokollan avulla toimiva tiedostonsiirtomenetelmä.
HA	High Availability. Järjestelmän suunnittelussa käytäntö, jolla pyritään varmistamaan tietty toimivuus jatkuvasti.
ICMP	Internet Control Message Protocol. Internetprotokolla, joka kuuluu OSI-mallin kuljetuskerrokseen. Protokollan avulla lähetetään laitteiden välillä viestejä, jotka kertovat laitteen tilasta.
IETF	Internet Engineering Task Force. Organisaatio, jonka tarkoituksena on parantaa internetin toimivuutta.
IGMP	Internet Group Management Protocol. Internetprotokolla, joka kuuluu OSI-mallin kuljetuskerrokseen. Protokollaa avulla eri asiakkaat voivat liittyä multicast-ryhmään, joiden kautta voidaan lähettää dataa yhdeltä monelle.
IP	Internet Protocol. Internetprotokolla, joka huolehtii IP-pohjaisten tietoliikennepakettien toimittamisesta. IP-osoitteet mahdollistavat pakettien toimittamisen.
IPS	Intrusion Prevention System. Verkkohyökkäyksien estämiseen tarkoitettu teknologia, joka perustuu pakettien signatuurien tutkimiseen.

LAN	Local Area Network. Lähiverkko.
NAT	Network Address Translation. Osoitteenmuutostekniikka, jolla säästetään julkisia IP-osoitteita.
OSI	Open Systems Interconnection. OSI-malli kuvaa tiedostonsiirtoprotokollien yhdistelmää seitsemässä kerroksessa.
RDP	Remote Desktop. Etätyöpöytäyhteys.
SSL	Secure Socket Layer. Salausprotokolla.
SMTP	Simple Mail Transfer Protocol. TCP-protokollaa käyttävä sähköpostipalvelimien viestinvälitysprotokolla.
SUM	Sophos UTM Manager. Keskitetty Sophos UTM -palomuurien hallinta yhden portaalin kautta.
TCP	Transport Control Protocol. Internetprotokolla, joka kuuluu OSI-mallin kuljetuskerrokseen. Internetin kautta kommunikoivat laitteet muodostavat toisiinsa yhteyden, jonka avulla varmistetaan tavujonojen siirto luotettavasti.
UDP	User Datagram Protocol. Internetprotokolla, joka kuuluu OSI-mallin kuljetuskerrokseen. Mahdollistaa tiedostojen siirron ilman laitteiden välistä yhteyttä.
UTM	Unified threat management. Tietoturvan ja verkon palveluiden hallinnon yhdistäminen yhden laitteen alle.
VPN	Virtual Private Network. Virtuaalinen yksityisverkko.
WLAN	Wireless Local Area Network. Langaton lähiverkko.
XSS	Cross Site Scripting. Haitallisen koodin syöttäminen verkkosivulle.

1 Johdanto

Verkon ylitse liikkuu päivä päivältä entistä enemmän dataa. Datamäärien kasvaessa suojattavan datan määrä kasvaa. Lähestulkoon jokaisessa suomalaistaloudessa on käytössä tietokone ja internetyhteys. Suurinta osaa näistä tietokoneista ei kuitenkaan ole suojattu tarpeellisesti. Tietoturva koskettaa yritysten ja valtion laitoksien ohella myös yksityisihmisiä, vaikka suurin osa yksityisihmisistä ei mielläkään tietoturvan tarpeellisuutta.

Yksityisihmisten tietokoneet eivät välttämättä sisällä yhtä arkaluontoista tai kaupallisesti arvokasta tietoa kuin yritysten ja valtion käytössä olevat tietokoneet, mutta ne voivat silti olla oivallinen hyökkäyksen kohde heikon suojauksen takia. Saastuneita koneita voidaan käyttää suurella volyymilla yrityksiin kohdistuvissa hyökkäyksissä, niin kuin OP-pankki kärsi alkuvuodesta 2015 palvelunestohyökkäyksen, joka lamaannutti verkon pankkipalvelut täysin.

Tässä opinnäytetyössä tutustutaan tietoturvaan ja sen toteuttamiseen. Työssä tutkitaan tietokoneiden, palvelimien ja tietoliikenneverkkojen tietoturvaamista palomuureilla. Opinnäytetyössä keskitytään tietoturvan toteuttamiseen palveluna Sophos UTM -palomuureilla. Työssä käsitellään SG-sarjan muurien toimintaa, konfiguroimista ja ylläpitämistä. Työssä käydään läpi Dustin Finland Oy:n palomuuripalvelun nykytila ja pyritään kehittämään palvelusta parempi. Työ tehdään toimeksiantona Dustin Finland Oy:lle, joka on osa Dustin Groupia.

2 Tietoturva

Tietoturvan kasvavaa merkitystä korostaa digitalisaatio, jonka myötä nopeasti lähes kaikki data muuttuu sähköiseksi. Tietoturva koskettaa niin yksityisihmistä kuin yrityksiä. Yksityisihminen on erityisesti vastuussa omasta tietoturvastaan. Tietovarkauksia ja tietokoneiden saastuttamisia tapahtuu päivittäin. Viestintäviraston kyberturvallisuuskeskus tiedottaa ajankohtaisesti uusista löydetyistä haavoittuvuuksista ja tietojen kalastelusta. Kyberturvallisuuskeskus ohjeistaa internetkäyttäytymisessä siinä, kuinka käyttäjä suojaa itsensä laitteineen verkon uhilta.

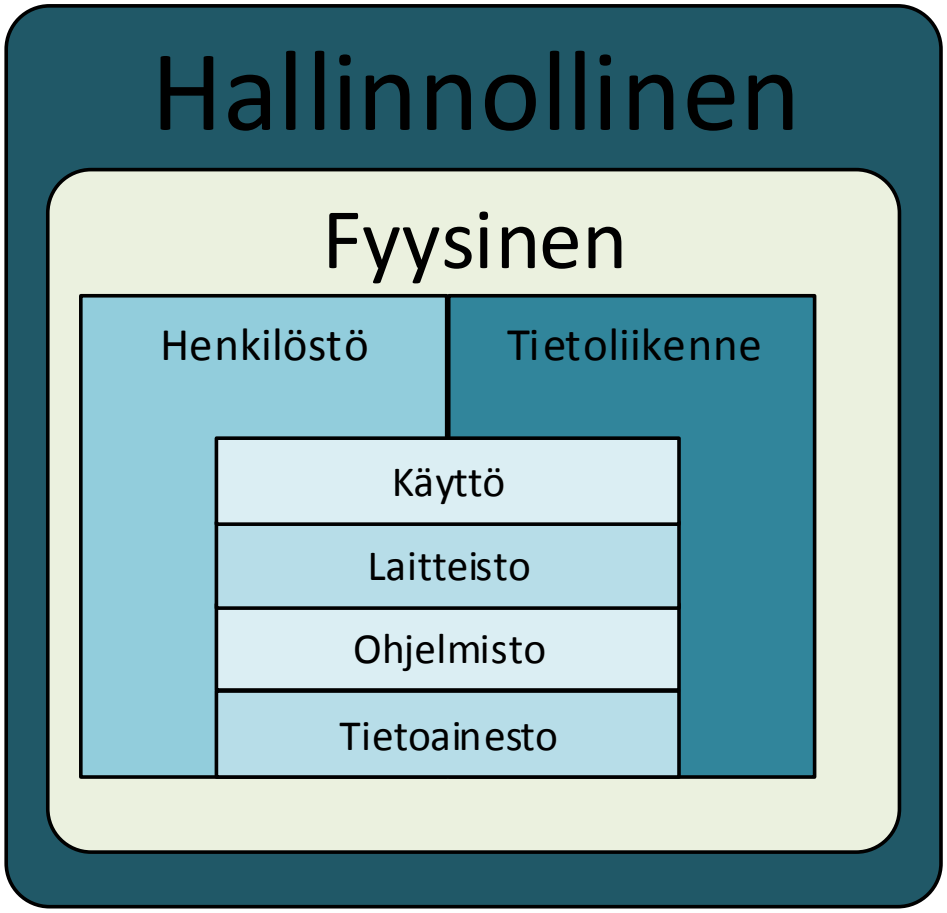
Yksityisihminen pystyy suojautumaan verkon uhilta päivittämällä internetissä käyttämänsä laitteet uusimmilla ohjelmistoversioilla tai hankkimalla ilmaisen tai maksullisen virustorjuntaohjelmiston ja palomuurin. Internetin palveluntarjoajat tarjoavat lähestulkoon jokainen kuukausimaksullista virustorjunta/palomuuriohjelmaa. Nämä ohjelmat ovat usein täysin riittäviä suojaamaan yksityisten ihmisten laitteita.

Yrityksien on syytä suhtautua tietoturvaan vakavasti. Yrityksien tulee huolehtia tietoturvastaan, koska jatkuvuuden ja tuottavuuden kannalta on erittäin tärkeää, että ulkopuoliset tahot eivät pääse käsiksi yrityksien tietoihin. Yrityksillä on tietoja omista työntekijöistään, laskutuksestaan, budjeteistaan, projekteistaan, asiakkaistaan ja niin edelleen. Vaikka osa tiedoista on rahassa mitattuna arvokkaampia kuin toiset, tulisi yrityksien suojata kaikkia mahdollisia tietojaan ja välttää niiden luovuttamista ulkopuoliselle taholle ellei niin ole erikseen sovittu. [1, s. 7.]

Klassisen tiedon arvoon perustuvan määritelmän mukaan tietoturva koostuu luottamuksellisuudesta, käytettävyydestä ja eheydestä. Luottamuksellisuus tarkoittaa sitä, että tietojärjestelmän tietoja voivat käyttää vain siihen oikeutetut henkilöt. Käytettävyys tarkoittaa kertoo, että tiedot ovat saatavilla tietojärjestelmästä oikeassa muodossa ja tarpeeksi nopeasti. Eheydellä tarkoitetaan tietojärjestelmän tietojen paikkansa pitävyyttä ja sitä, että ne eivät sisällä virheitä. Klassinen määritelmä on nykymaailmassa riittämätön, sillä tiedon tuottajan tai omistajan identiteetti jätetään huomioimatta. Myöskään laitteistojen tai tieto- ja tietoliikennejärjestelmien arvoa ei huomioida. Laajennettu tietoturvan määritelmä kattaa klassisen tietoturvan määritelmän lisäksi kiistämättömyyden, pääsynvalvonnan ja autenttisuuden. Kiistämättömyydellä tarkoitetaan tietojärjestelmän luotettavaa tapaa henkilötietojen tunnistamiseen ja tallentamiseen. Kiistämättömyys pyritään toteuttamaan käyttämällä salausmenetelmin suojattuja tunnistusmekanismeja

tai biometrisiä tunnisteita. Tämä voidaan tehdä esimerkiksi älykortti- ja sormenjälkitunnistuslaitteiden avulla. Pääsynvalvonta tarkoittaa menetelmiä rajoittaa tietojärjestelmän resursseiden käyttöä rajaamalla käyttäjien käyttöoikeuksia. Autenttisuus tarkoittaa tietojärjestelmän käyttäjien ja osallisten laitteiden luotettavaa tunnistusta. [3, s. 4-6.]

Tietoturvan voi jakaa osa-alueisiin. Valtiovarainministeriö jakaa tietoturvan kahdeksaan osa-alueeseen kuvan 1 mukaisesti.



Kuva 1. Tietoturvan osa-alueet

Hallinnollinen turvallisuus liittyy vahvasti kaikkiin muihin tietoturvallisuuden osa-alueisiin, koska sillä pyritään varmistamaan tietototurvan kehittäminen, johtaminen sekä turvallisuudesta vastaavien elimien yhteydenpito organisaation sisällä ja ulkopuolella. Organisaatioiden tietohallinnot ovat yleensä vastuussa hallinnollisesta turvallisuudesta. [3, s. 10.]

Fyysinen turvallisuus kattaa rakennuksen tilojen ja tiloissa olevien laitteiden suojaamisen erilaisilta fyysisiltä uhilta. Fyysisiä uhkia ovat ihmiset ja ympäristö. Ihmisen aiheuttamia vahinkoja kuten ilkivaltaa ja murtoja pyritään estämään vartioinnilla ja valvonnalla. Ympäristön aiheuttamia uhkia voivat olla vesi- ja palovahingot, sekä eri sähkö- ja lämmityslaitteiden toimintahäiriöt. Fyysisestä turvallisuudesta vastaa yleensä kiinteistöhuolto, mutta tietohallinnon tulee olla siitä tietoinen ja osallistua sen suunnitteluun. Tietojärjestelmien suojaamiseen tulee kiinnittää erityistä huomiota. [3, s. 11.]

Henkilöstöturvallisuus on henkilöstöhallinnon vastuulla, mutta tietohallinto osallistuu sen toteuttamiseen. Henkilöstöturvallisuus koskee nimensä mukaisesti henkilöstöön liittyviä asioita. Joita ovat tietojärjestelmän käyttäjien toimintakyvyn varmistaminen, käyttäjien pääsyn rajoitus organisaation tietoihin ja tietojärjestelmiin, tietojärjestelmiin liittyvät koulutukset, tietojärjestelmiä koskevat oikeudet ja vastuut sekä henkilöiden taustatietojen selvitykset kuuluvat henkilöstöturvallisuuteen. [3, s. 11.]

Tietoliikenneturvallisuus on organisaation tietohallinnon vastuulla. Sen tarkoituksena on huolehtia organisaation lähi- (LAN) ja laajaverkkojen (WAN) sekä muiden tiedonsiirtoon liittyvien viestimisjärjestelmien turvallisuudesta. [3, s. 12.]

Laitteistoturvallisuus on pääsääntöisesti tietohallinnon vastuulla. Laitteistoturvallisuuteen kuuluu organisaation tietojärjestelmään kytkeytyvien laitteiden toiminnan varmistaminen mitoittamalla laitteet oikein, testaamalla toiminnan ja järjestämällä laitteille huollon. Laitteiden kuluminen ja vanhentuminen, kuten myös laitteiden käytöstä aiheutuvien vaaratekijöiden ja loukkaantumisriskin arviointi ja minimointi tulee ottaa huomioon laitteistoturvallisuutta miettiessä. [3, s. 12.]

Ohjelmistoturvallisuus sisältää organisaation käyttämien ohjelmiin liittyvät asiat kuten ohjelmistoversioiden ja lisenssien. Ohjelmistoturvallisuudella pyritään varmistamaan, että käytettävät ohjelmistot ovat sopivia suunniteltuun käyttötarkoitukseen, ohjelmistot ovat keskenään yhteensopivia ja niiden toiminta on luotettavaa ja virheetöntä. Tietohallinto on vastuussa myös ohjelmistoturvallisuudesta. [3, s.11–12.]

Tietoaineistoturvallisuus käsittää tietojen säilyttämisen, varmistamisen ja palauttamisen sekä tuhoamisen toimet. Manuaalisen tietojenkäsittelyn asiakirjat ja automaattisen tietojenkäsittelyn tulosteet kuuluvat tietoaineistoturvallisuuteen. Organisaation arkistoin-

nista vastaava yksikkö on tietohallinnon ohella vastuussa tietoaineistoturvallisuudesta. [3, s. 11.]

Käyttöturvallisuus koskettaa jokaista turvallisuuden osa-aluetta.

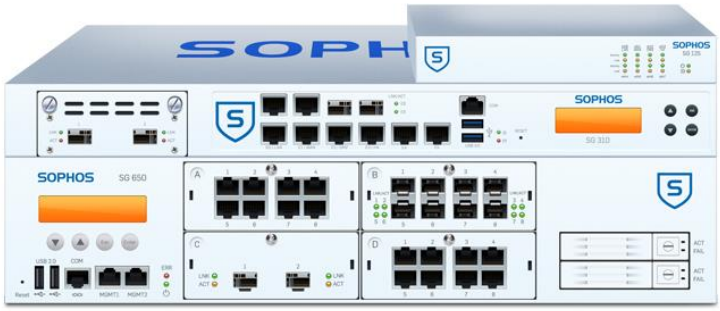
Tässä insinöörityössä keskitytään pääasiallisesti tietoliikenneturvallisuuteen samalla sivuten laitteistoturvallisuutta, henkilöstöturvallisuutta ja käyttöturvallisuuteen. Palomuurilla varmistetaan tietoliikenneturvallisuuden toteutuminen, mikä koskettaa näitä muitakin turvallisuuden osa-alueita.

3 Sophos UTM

Verkon toiminallisuuden parantamiseksi ja uhkien vähentämiseksi on kehitetty uuden ajan palomuuri, jonka tarkoituksena on yhdistää useamman eri laitteen ominaisuudet yhden laitteen alle. Sophos on käyttää tästä termiä Unified Threat Management, joka suomeksi käännettynä tarkoittaa yhdistettyä uhkien hallintaa. Vastaavia laitteita samankaltaisilla ominaisuuksilla löytyy muiltakin valmistajilta, usein puhutaan Next Generation Fire Wall-laitteista.

Sophos tarjoaa neljä eri vaihtoehtoa UTM:n toteutukseen. Perinteinen vaihtoehto on Solphoksen valmistama fyysinen laite. UTM voidaan asentaa ohjelmistona Intel-pohjaiselle tietokoneelle, jossa on tarpeeksi tehoa. Virtuaalilaitetoteutus on mahdollista eri virtualisointialustoilla, mukaan lukien VMware, Citrix, Microsoft Hyper-V ja Linux KVM. Sophos tarjoaa myös mahdollisuutta käyttää UTM:ää pilvipalveluna Amazon Web Servicessä.

Sophos UTM -laitteita on tarjolla kolmessa eri kokoluokassa, joita ovat Small, Medium ja Large. Jokaisesta kokoluokasta löytyy useampi malli.



Kuva 2. Sophos UTM -laitteita eri kokoluokissa Small, Medium ja Large

Small-kokoluokan laitteet ovat työpöytämallisia eli pienikokoisia ja ne soveltuvat pöydälle tai pieneen laitekaappiin. Medium-kokoluokan laitteet ovat yhden räkkiyksikön kokoisia. Large-kokoluokan laitteet ovat kahden räkkiyksikön kokoisia.

Tärkeimmät palomuurin tietoturva- ja toiminnalliset ominaisuudet käydään läpi omissa luvuissaan.

3.1 High Availability

High availability tarkoittaa suoraan käännettynä korkeata saatavuutta tai korkeata käytettävyyttä. Tarkoitus on siis tehdä tietojärjestelmästä toimintakelpoinen ongelmatilanteissa.

Ongelmatilanteita, jotka johtuvat laiteviasta, rikkoutumisesta tai jumiutumisesta, varten on syytä varmentaa palomuurin toiminta HA-ratkaisulla. Oletusarvoisesti HA-laitteilla pyritään siihen, että peruskäyttäjä ei edes huomaa ongelmaa vaan pystyy jatkamaan toimintaansa normaaliin tapaan. Kun HA-laite vikaantuu, tai ei toimi kuten pitäisi, niin normaalisti toimiva HA-laite ottaa haltuun verkkoliikenteen hallinnoinnin. Tästä käytetään termiä failover.

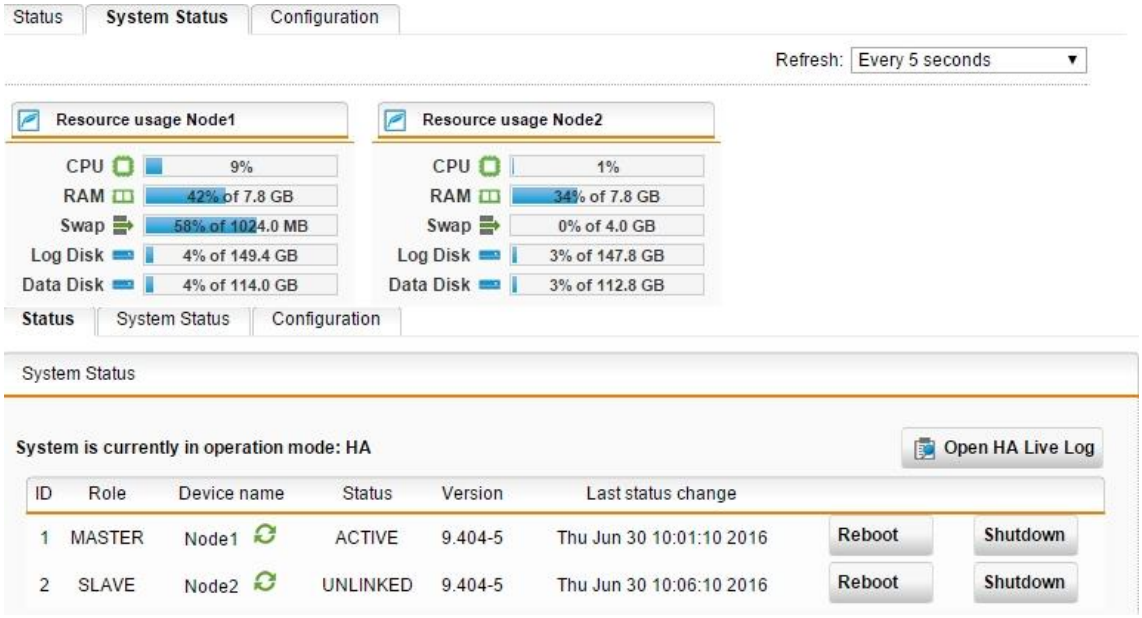
Sophos UTM -palomuureilla on mahdollista toteuttaa kahta erityyppistä HA-failoveria, Clusteria ja Hot Standbytä. HA-klusterin pystyttäminen vaatii kaksi identtistä laitetta tai virtuaalilaitetta, joilla molemmilla on sama ohjelmiston versionumero. Korkean saatavuuden toteuttamiseen vaaditaan voimassa oleva lisenssi, joka sisältää tämän ominaisuuden. Jokainen klusteriin liitettävä laite saa oman noodin ID-numeron väliltä 1-10. HA-klusteriin voidaan liittää maksimissaan 10 laitetta. Hot Standby -järjestelmässä noodien ID-numerot ovat yksi ja kaksi.

Cluster (Active-Active) -ratkaisussa palomuurit, jotka osallistuvat klusteriin, toimivat aktiivisina laitteina. Tämä tarkoittaa sitä, että yksittäisten laitteiden kuormitusta saadaan pienennettyä jakamalla tehtäviä eri laitteille. Master-noodi kontrolloi kuorman tasausta, joten erillistä kuormantasaajalaitetta ei tarvita. Master-noodi tutkii jokaisen data-paketin ennen kuin ne ohjataan muille noodeille, jotta verkon suoritusteho saadaan pidettyä korkeana. Master-noodin kuormitus pysyy alhaisempana, kun se ohjaa raskaammat tehtävät, kuten virustarkistuksen, IPsec-liikenteen ja tunkeutumisen eston muille noodeille. Klusterin toiminta jatkuu normaalisti, laitteen hajotessa, mutta kasvattaa muiden klusterin laitteiden kuormitusta.

Hot Standby (Active-Passive) -ratkaisussa palomuurit toimivat Master- ja Slave-rooleissa. Master-noodiksi määriteltävä palomuuri hoitaa kaiken toiminallisuuden. Slave-noodiksi määriteltävä palomuuri on Standby-tilassa eli valmiina siirtymään Master-noodiksi. Slave noodi ottaa hetkellisesti Master-roolin, kun laitteita päivitetään, jotta saadaan minimoitua verkon katkosta päivitystilanteesta johtuen. UTM -ohjelmistoversio

9 myötä latenssi, jonka aikana toinen laite ottaa toiminnan haltuun, on pudonnut alle kahteen sekuntiin. Tämä mahdollistaa palomuurin yhteyksien synkronoimisen sekä IPsec-tunnelien synkronoimisen, jonka ansioista VPN -yhdyskäytävää käyttävien ei tarvitse muodostaa IPsec-tunneleita uudestaan.

HA-klusteriin osallistuvat palomuurinoodit tarkkailevat toistensa tilaa ja toimintaa lähettämällä ryhmälähetys UDP-paketin, jota kutsutaan sydämen lyönniksi englanniksi heart-beat signal. Palomuurinoodit, jotka eivät jonkin teknisen vian takia lähetä tätä pakettia, todetaan kuolleiksi.



Kuva 3. Hot Standby HA -ratkaisun tilannenäkymä

High Availability -asetuksista pystytään tarkastelemaan järjestelmän prosessorin, muistin ja levyn käyttöä. Asetuksista nähdään myös palomuuriklusteriin osallistuvien muurin tila ja ne voidaan käynnistää uudelleen tai sammuttaa.

3.2 Network Services

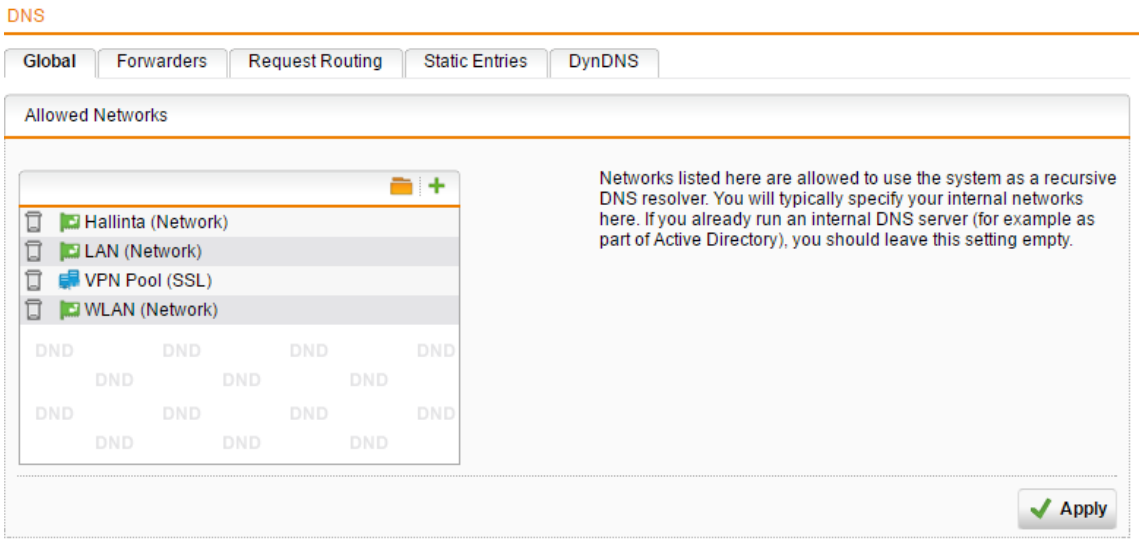
Verkkopalveluiden DNS, DHCP ja NTP asetukset löytyvät Sophos UTM -palomuurin Network Services -valikosta. DNS ja DHCP käsitellään omissa luvuissaan, mutta NTP jätetään käsittelemättä. NTP eli Network Time Protocol on sovelluskerroksen protokolla, jonka avulla välitetään täsmällinen aikatieto eri laitteiden välillä.

3.2.1 DNS

DNS on internetprotokolla, joka kuuluu OSI-mallin seitsemännelle kerrokselle eli sovelluskerrokselle. Lyhenne tulee sanoista Domain Name System. Sen päätarkoitus on kääntää verkkotunnukset ja tietokoneiden isäntänimet IP-osoitteiksi. DNS yksinkertaisuudessaan mahdollistaa laitteiden ja palvelimien keskinäisen kommunikoinnin ilman, että tiedetään IP-osoitetta.

Sophos UTM käyttää avoimen lähdekoodin BIND-ohjelmistoa DNS välityspalvelimessaan. Se varastoi nimikyselyitä välimuistiin mahdollistaen turvallisen ja tehokkaan nimenselvityksen sisäisen verkon palvelimille ja päätelaitteille.

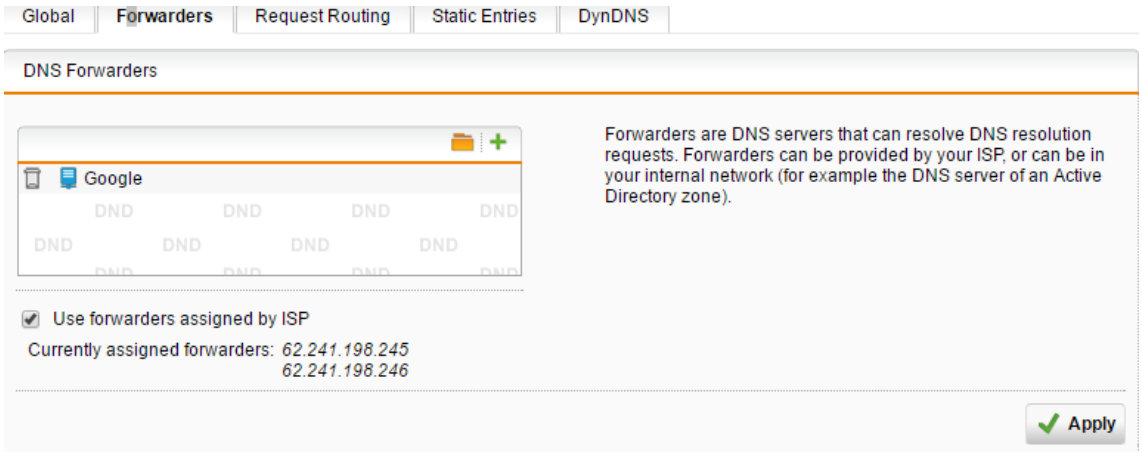
Silloin kun käytössä ei ole sisäisiä DNS-palvelimia, voidaan palomuurin DNS-välityspalvelin määritellä käsittelemään nimenselvitystä. Kaikki sisäiset verkot, joista tehdään nimenselvitystä, määritellään sallituiksi DNS-välityspalvelimen Global-välilehden asetuksissa. Any verkko-objektia ei saa missään tapauksessa määritellä sallituksi verkoksi, jotta järjestelmä ei altistu ulkoverkosta tuleville hyväksikäyttöyrityksille.



Kuva 4. Rekursiivinen DNS -selvitys

Kuvassa nähdään, että palomuuri on määritelty kolmelle eri verkko-objektille ja vpn-käyttäjille toimimaan DNS-välityspalvelimena.

Nimenselvitys internetin suuntaan vaatii erillisen DNS-palvelimen, joka on verkon reunalla lähellä internetiä. Nämä DNS -palvelimet mahdollistavat esimerkiksi verkkosivujen tavoittamisen niiden nimillä ja sähköpostin lähettämisen ilman, että tiedetään palvelimien IP-osoitteita. Palvelimet suorittavat IP-osoitteiden käännön hakemalla välimuististaan tietoja tehdyistä hauista ja vertailemalla niitä muihin tietueisiin. Tiedon löytyessä välimuistista palautetaan se tietoa kyselyn tehneelle käyttäjälle, jos tietoa ei löydy, niin selvitys lähtee eteenpäin, kunnes tieto löytyy.

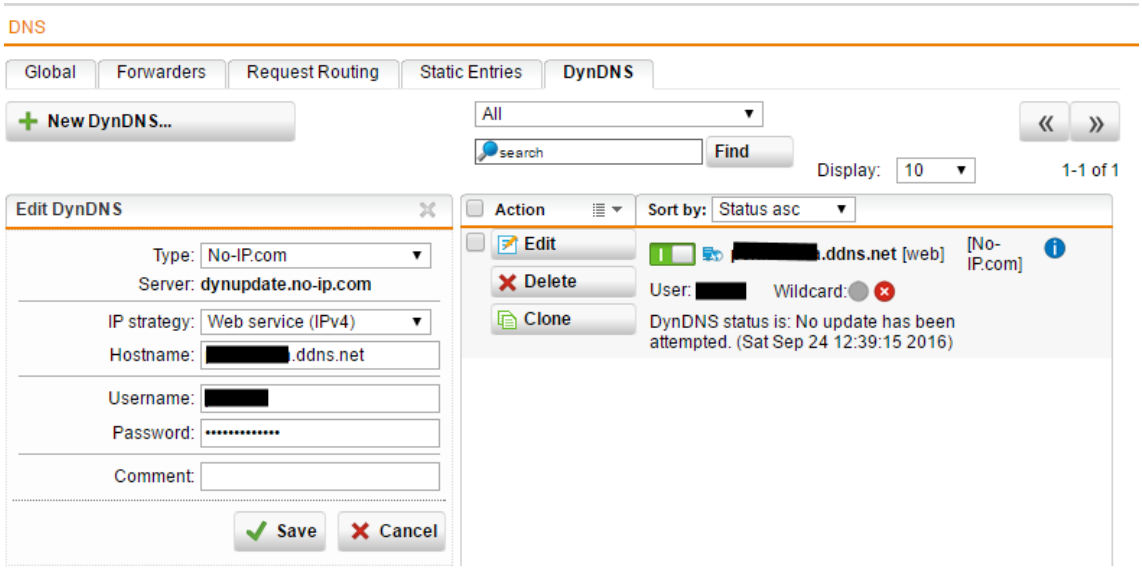


Kuva 5. DNS Forwarders

Forwarders-välilehden asetuksista voidaan määritellä DNS-palvelimet, jotka tekevät ulkoverkkoon suuntautuvat nimenselvityskyselyt. Näitä kutsutaan myös nimityksellä resolveri (Resolver). Palvelimia voidaan määritellä useampia. Internet-yhteyden palveluntarjoajan DNS-palvelimia, Googlen DNS-palvelimia voidaan käyttää, jos käytössä ei ole erillistä DNS-palvelinta.

Sisäverkon toimialueiden (Domain) turvallisuus parantuu, kun nimenselvityskyselyitä eteenpäin jatkavat DNS-palvelimet eivät tiedä kyseistä toimialuetta, vaan tieto välitetään erillisen sisäisen DNS-palvelimen kautta. Tämä onnistuu määrittelemällä reitti toimialueesta (Domain) sisäiselle DNS-palvelimelle, jonka jälkeen määritellyt resolverit pystyvät tekemään nimenselvitystä tietämättä kuitenkaan toimialuetta.

Vaihtuvien IP-osoitteiden takia on helpompaa käyttää kiinteätä isäntänimeä (Hostname), jonka dynaaminen DNS (DynDNS) mahdollistaa. Dynaaminen DNS palveluntarjoaja tarjoaa käyttäjälle tietyn staattisen domain-nimen, joka on löydettävissä, vaikka IP-osoite vaihtuisi. Sophos UTM tukee useita ulkopuolisia palveluntarjoajia.



Kuva 6. Dynaaminen DNS

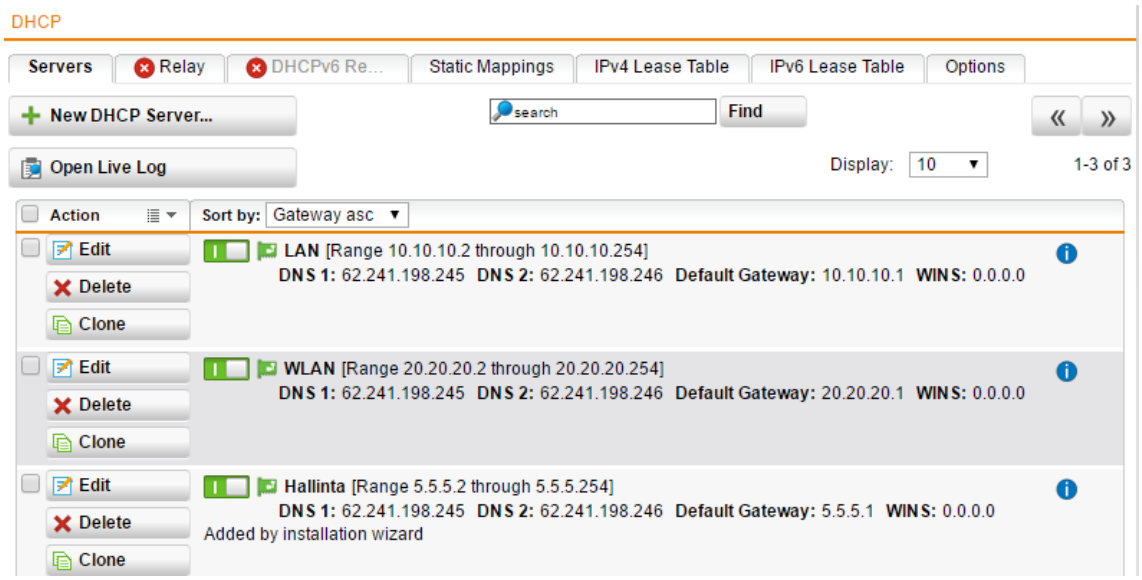
Kuvassa näkyy, että palomuurille on määritelty kiinteä isäntänimi. Käyttäjä kirjautuu palveluntarjoajalta saamilla tunnuksillaan ja määrittää asetukset.

3.2.2 DHCP

DHCP on lyhenne, joka tulee sanoista Dynamic Host Configuration Protocol. Se on verkkoprotokolla, jonka ensisijaisena tarkoituksena on jakaa IP-osoitteita lähiverkkoon kytkeytyville laitteille automaattisesti. DHCP-palvelin jakaa IP-osoitteet ennalta määritellystä alueesta. DHCP-palvelin jakaa DHCP-asiakasohjelmille IP-osoitteen lisäksi tiedot käytettävästä oletusyhdyskäytävästä sekä nimenselvityksestä (DNS). DHCP-palvelimen antamat IP-osoitteet ovat voimassa määritellyn ajan, jonka jälkeen DCHP-asiakasohjelma, esimerkiksi tietokone, joutuu uusimaan tietonsa.

Sophos UTM voi toimia DHCP-palvelimena (DHCP Server) tai DHCP-välittäjänä (DHCP Relay).

DHCP-palvelimeksi määriteltynä palomuuri hoitaa DHCP-palvelut kytketyille sekä muille määritellyille verkoille. DHCP-palvelin luodaan DHCP-valikon Servers-välilehdeltä.



Kuva 7. DHCP-palvelin

Kuvasta nähdään, että palomuurilta jaetaan IP-osoitteet LAN-, WLAN- ja Hallinta-verkoille.

DHCP-välittäjäksi määriteltynä palomuuri välittää ulkoisen DHCP-palvelimen palvelut määritellyille verkoilla. Tällä hetkellä Sophos UTM tukee ainoastaan yhden DHCP-välittäjän määrittelemistä.

3.3 Network Protection

Verkon suojaamiseen keskittyvät asetukset käydään läpi tämän luvun alaotsikoissa. Network Protection -asetuksista löytyvät Firewall, NAT ja Intrusion Prevention, jotka kaikki käsitellään omissa alaotsikoissa. Näiden lisäksi asetuksista löytyvät Server Load Balancing- ja VoIP-asetukset, jotka jätetään käsittelemättä.

Server Load Balancingin avulla pystytään jakamaan palomuurille saapuvaa verkkoliikennettä eri palvelimille.

VoIP eli Voice over IP tarkoittaa puheluita internetin ylitse. Sophos UTM tarjoaa tuen SIP- ja H.323-protokollille.

3.3.1 Firewall

Palomuuri on yksi keskeisimpiä UTM:n ominaisuuksia. Palomuuriosio sisältää pakettisuodatuksen, maakohtaiset estot ja poikkeukset sekä ICMP-asetukset.

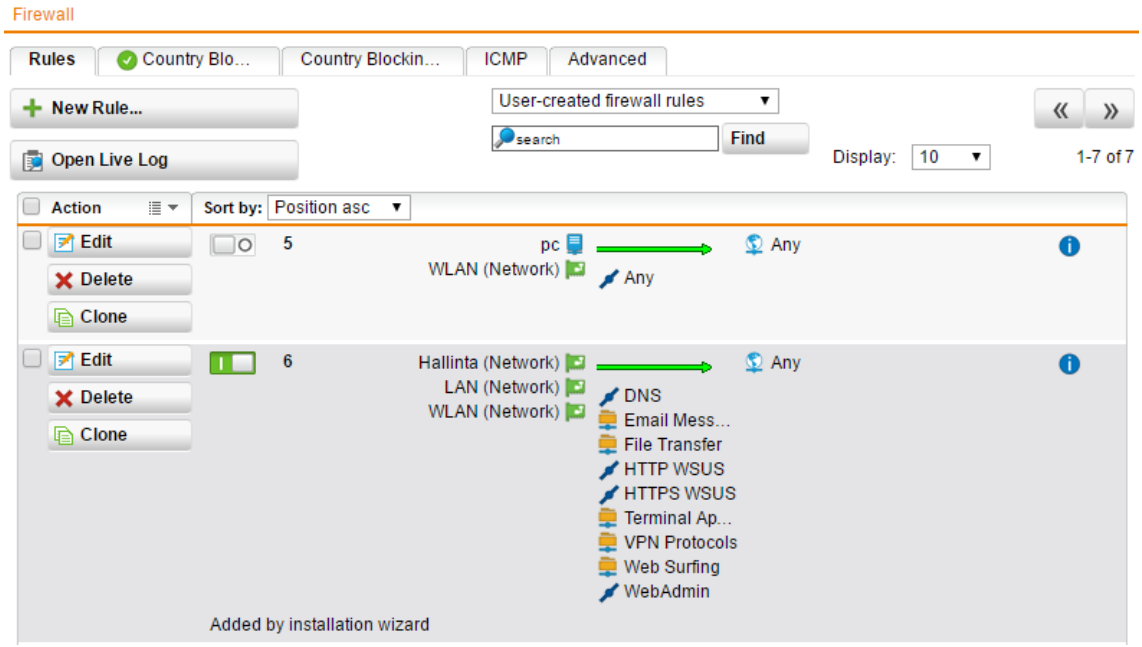
Pakettisuodatus on nykyaikaisen palomuurin vanhimpia perusominaisuuksia. Sen toiminta perustuu siihen, että ennalta määritellystä lähteestä ennalta määritellyn internetprotokollan mukainen liikenne ennalta määriteltyyn kohteeseen sallitaan tai pudotetaan.

Pakettisuodatuksessa tehdään useampia eri sääntöjä. Täten muodostuu lista säännöistä. Sääntölistaa luetaan ylhäältä alaspäin. Liikenteen saapuessa palomuurille aletaan sääntölistaa käydä läpi sääntö kerrallaan. Kun palomuurisäännön ehdot täyttyvät, lopetetaan listan läpikäynti ja liikenne sallitaan tai kielletään riippuen siitä, mitä säännössä on määritelty. Sen takia tärkeimmät ja kaikista tarkimmin määritellyt säännöt sijoitetaan listan yläosaan. Listan alaosassa oletusarvoisesti kielletään kaikki muu liikenne, jota ei ole erikseen sallittu, erityistä kieltosääntöä ei välttämättä ole määritelty palomuurisäännöissä, vaan se on oletusarvo.

Palomuurisääntöjen laatijan on syytä tuntea mahdollisimman tarkasti verkon toiminta, koska palomuurisääntöjä luodessa tulisi käyttää periaatetta, että vain tarpeelliset yhteydet ja palvelut sallitaan tietyille käyttäjille tai tietyille aliverkoille. Palomuurisäännöt on syytä määritellä aina mahdollisimman suppeasti, jotta saadaan vähennettyä mahdollisia väärinkäytöksiä.

Nykyaikaisilla palomuureilla on mahdollista kerätä lokia palomuurin sallimista ja pudottamista paketeista. Lokin keräämien on syytä ottaa käyttöön tarkemmin rajattujen sääntöjen kohdalla ja kieltosääntöjen. Lokia keräämällä mahdollisten ongelmatilanteiden selvitys helpottuu.

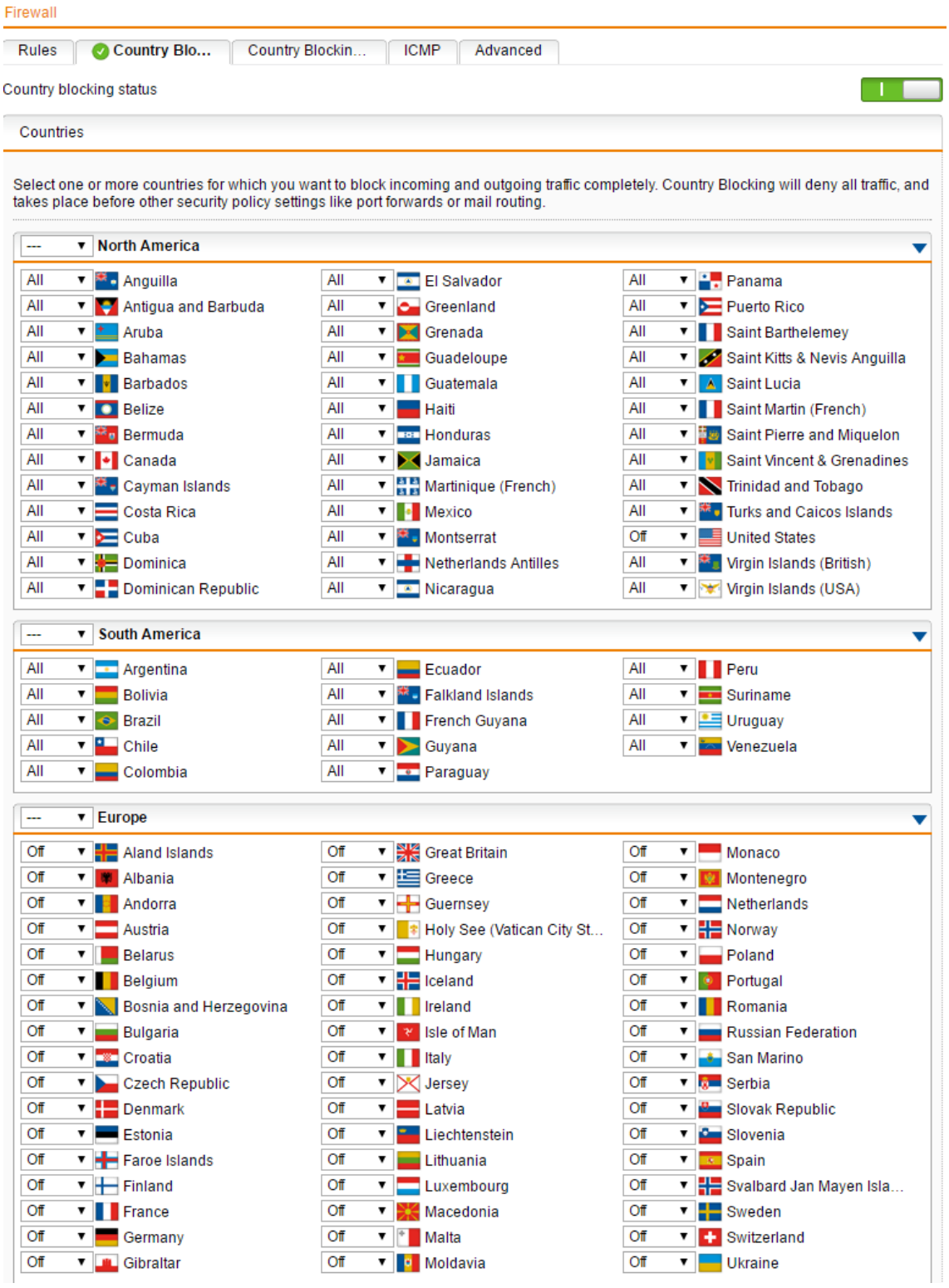
Sääntöä luotaessa voidaan määritellä säännölle ryhmä, jotta helpotetaan sääntöjen hallintaa. Tämä on järkevä käytäntö varsinkin suuremmissa ympäristöissä, kun sääntöjä joudutaan muokkaamaan, poistamaan ja kloonaamaan.



Kuva 8. Palomuurisäännöt

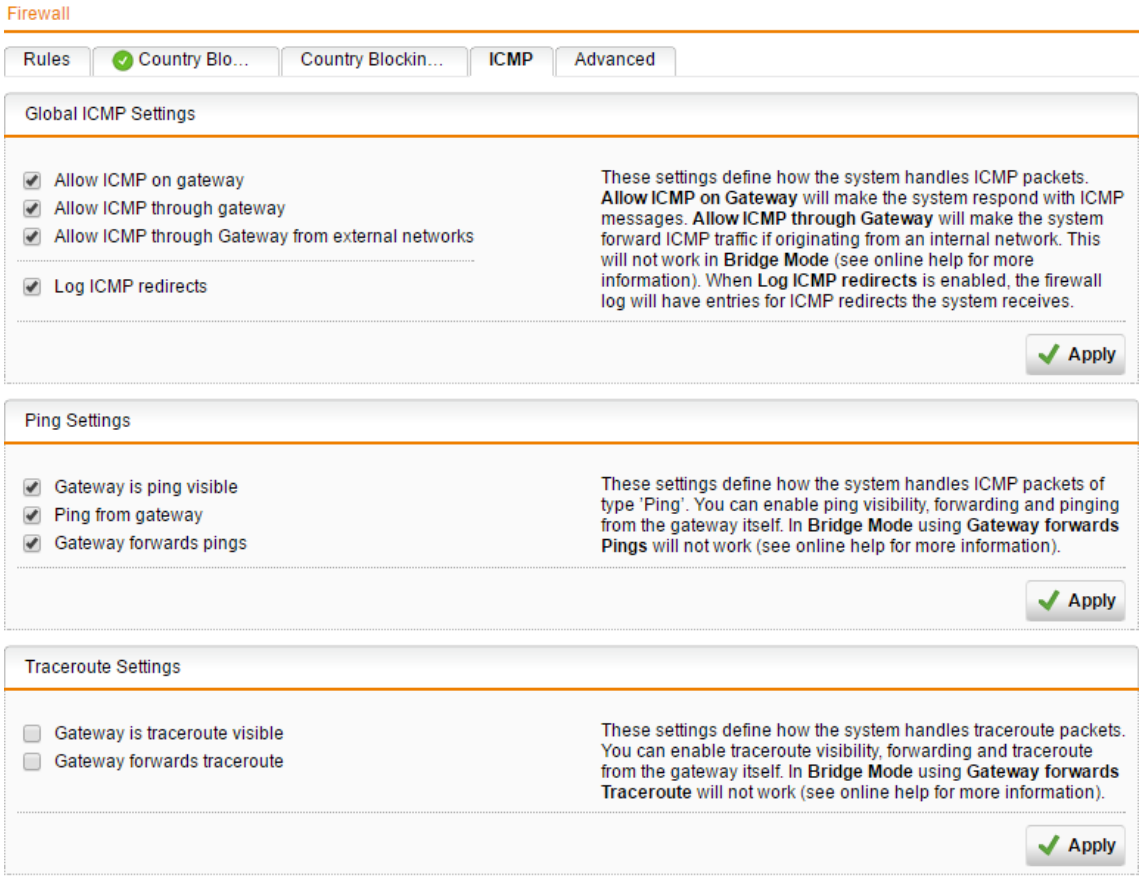
Kuvassa näkyy kaksi palomuurisääntöä, joista ylempi sallii kaiken liikenteen PC-objektista ja WLAN-verkosta internetin suuntaan, mutta sääntö on pois päältä. Alempi sääntö sallii kolmesta eri verkosta määritellyt protokollat internetin suuntaan. Säännöt saadaan päälle ja pois, napsauttamalla virtakytkimen näköistä painiketta.

Palomuurilla pystytään myös rajoittamaan liikennettä maan tai sijainnin perusteella. Tämä perustuu GeoIP-prosessiin, jolla voidaan määritellä IP-osoitteen fyysinen sijainti. Asetuksissa voidaan estää kohdemaahan lähtevä verkkoliikenne ja kohdemaasta saapuva liikenne tai molemmat. Asetuksen voi myös jättää pois päältä. Maakohtaisiin estoihin voidaan tehdä poikkeuksia tietyille rajapinnoille määrittelemällä sallitut erikseen.



Kuva 9. Firewall Country Blocking

Kuvassa nähdään, että palomuurilla on estetty verkkoliikenne kokonaan koskien tiettyjä maita.



Kuva 10. ICMP

Palomuurilla on sallittu ICMP-viestit ja niistä kerätään lokia. Palomuuri myös vastaa pingiin, siltä voidaan pingata muita laitteita ja se päästää pingi-kyselyt muille laitteille läpi. Traceroute on työkalu, jonka avulla selvitetään mitä reittiä tietoliikennepaketit kulkevat määränpäähänsä. Ominaisuus ei ole sallittu.

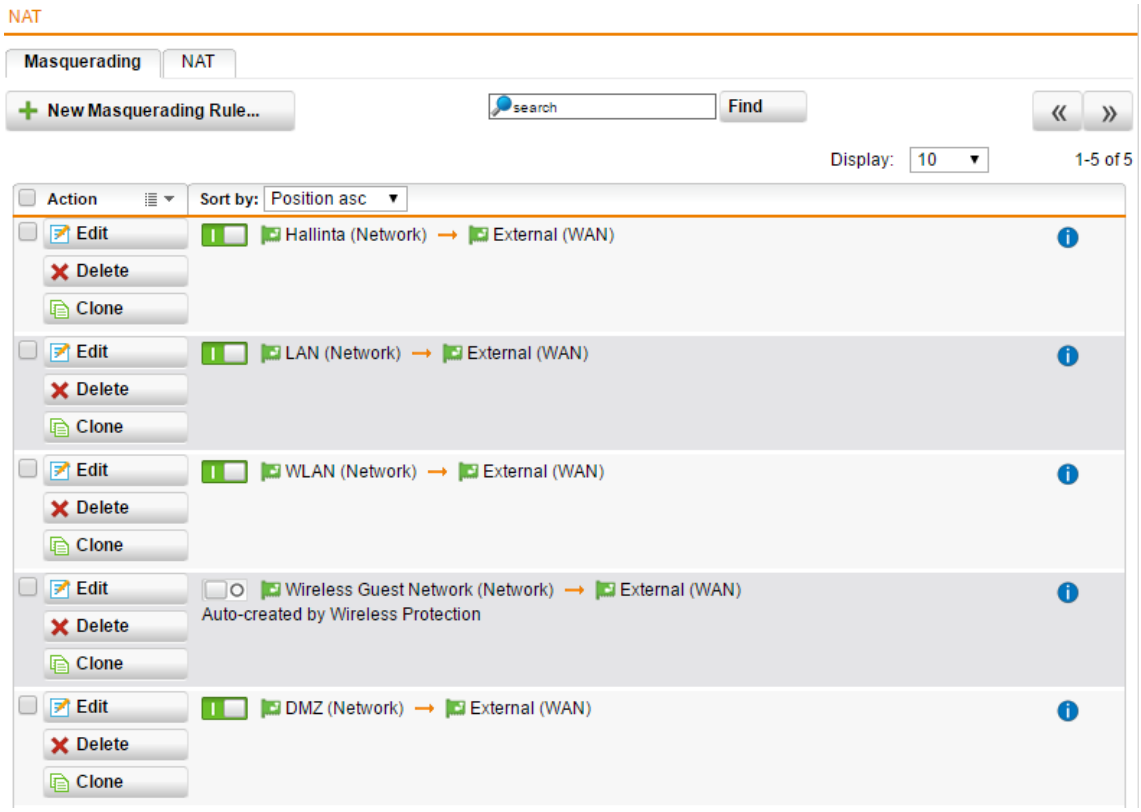
3.3.2 Network Address Translation

Julkisia IP-osoitteita on rajallinen määrä. Sen takia kehitettiin internettekniikka Network address translation (NAT), joka suomennettuna tarkoittaa osoitteenmuunnosta. Osoitteenmuunnos poistaa osittain ongelman julkisten IPv4-osoitteiden loppumisesta.

Internetin alkuvaiheessa julkisia IP-osoitteita oli helpompi ostaa itselleen, joten on mahdollista, että isoilla yrityksillä, valtion elimillä, sairaaloilla tai kouluilla saattaa olla useita julkisia IP-osoitteita käytössään. Mahdollisesti näillä toimijoilla voi olla kokonaisia B- tai C-luokkia käytössä. B-luokassa yhdessä verkossa julkisia IP-osoitteita on 65536 ja C-luokassa taas 256.

NAT toimii yksinkertaisemmillaan siten, että se muuttaa sisäverkon IP-osoitteen palveluntarjoajan tarjoamaksi julkiseksi IP-osoitteeksi. Ominaisuutta tarvitaan etenkin, kun on käytössä vain yksi julkinen IP-osoite, mutta useat laitteet kommunikoivat internetiin yhtäaikaisesti.

Sophos UTM:n toimiessa yhdyskäytävänä internettiin tehdään sisäverkon yksityisten osoitteiden osoitteenmuutos julkisiksi osoitteiksi Masquerading -asetuksissa. Sisäverkoille määritellään säännöt, joista halutaan liikennöidä internetin suuntaan. Säännössä määritellään sisäverkko-objekti ja ulkoverkko-objekti, jonka takaa löytyy käytettävä julkinen IP-osoite. Julkisia IP-osoitteita voi olla useampia, joten on mahdollista valita eri säännöille eri IP-osoitteet. Masqurading -sääntölistaa käydään läpi samalla tavalla kuin palomuurin sääntölistaa, joten listan yläosaan määritellään tarkemmat sääntömääritykset.



Kuva 11. NAT Masquerading

Kuvassa nähdään, että jokaisesta verkosta liikennöidään ulos samalla julkisella IP-osoitteella, joka löytyy External-objektista (WAN).

NAT-välilehdeltä pystytään myös luomaan erikoisempia ja tarkempia osoitteenmuutos-sääntöjä. Sääntöjä luetaan kuten palomuurisääntöjä, joten tarkemmat säännöt tulee sijoittaa sääntölistan yläosaan.

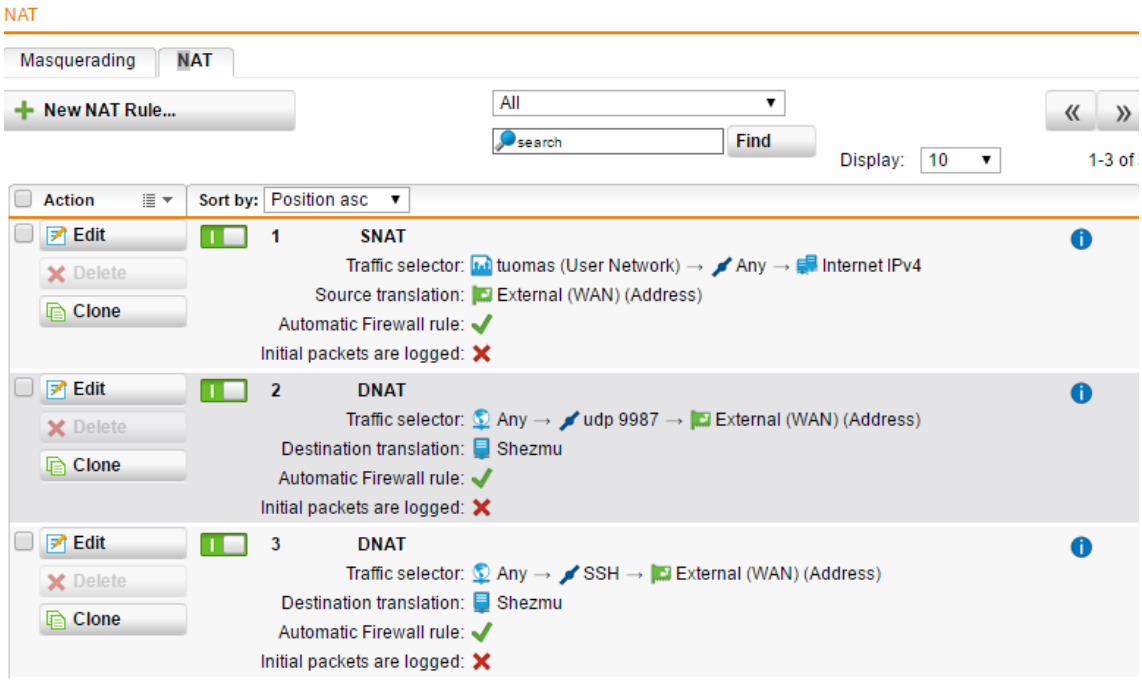
SNAT-sääntö on samankaltainen kuin masquerading-sääntö, mutta tässä säännössä määritellään lähdeosoite, voidaan vaihtaa palvelun porttinumeroa sekä määritellään kohdeosoite tarkasti, eikä sitä ole sidottu ensisijaiseen ulkoverkon-objektiin. Sisäverkon objekti saa siis uuden osoitteen.

DNAT-säännön avulla sisäverkon palveluita voidaan avata julkisesta verkosta käytettäväksi. Sääntöön määritellään kohdeosoite (esimerkiksi Internet), josta voidaan kutsua tiettyä määriteltyä palvelua julkisella IP-osoitteella. Sisäverkosta löytyvän palvelun IP-osoite määritellään ja porttinumero voidaan vaihtaa osoitteenmuutoksen yhteydessä. DNAT-sääntöjen määritykset tapahtuvat ennen palomuurisääntöjä, joten on muistettava luoda tarvittavat palomuurisäännöt tai ne voidaan luoda automaattisesti DNAT-sääntöä luodessa.

1:1 NAT -sääntöjen avulla voidaan muuttaa jokin verkko toiseksi verkoksi. Toiminta voidaan kohdistaa niin kohde- kuin lähdeverkkoonkin. Esimerkiksi sisäinen verkko voidaan muuttaa julkiseksi verkoksi.

Full NAT -säännöllä voidaan muuttaa lähde ja kohde osoitteet sekä niiden palvelut.

No NAT -säännöillä voidaan varmistaa, että tiettyjen objektien kohdalla ei tehdä ikinä osoitteenmuutosta.



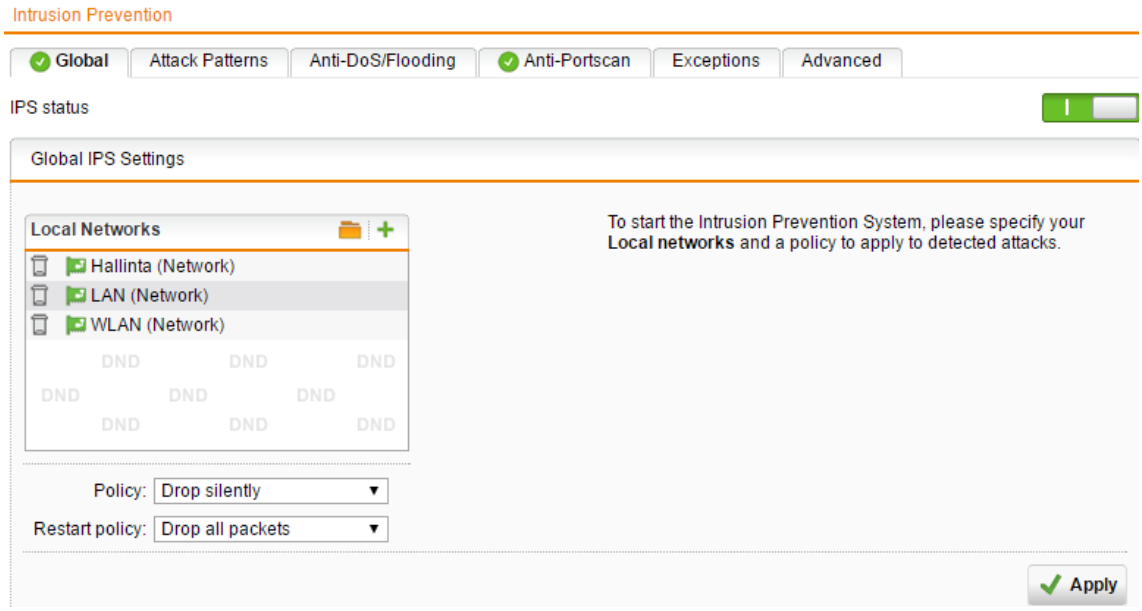
Kuva 12. NAT-säännöt

Kuvassa on kolme erilaista NAT-sääntöä, joista jokainen on käytössä. SNAT-sääntö on määritelty VPN-käyttäjälle tuomas, jotta käytettäessä VPN-yhteyttä mistä tahansa saadaan tietty IP-osoite. DNAT-säännöt on määritelty, jotta palvelimen takaa löytyvät palvelut ovat käytettävissä internetistä julkisella IP-osoitteella.

3.3.3 Intrusion Prevention

Intrusion Prevention System tarkoittaa suomeksi tunkeutumisenestojärjestelmää. IPS-ominaisuuksilla varustettu laite tarkastelee verkkoa ja järjestelmää. Palomuuri pysäyttää IPS-hyökkäykset, eikä päästä niitä etenemään verkkoon asti. Toiminta perustuu signatuureihin, jotka päivittyvät automaattisesti jatkuvasti.

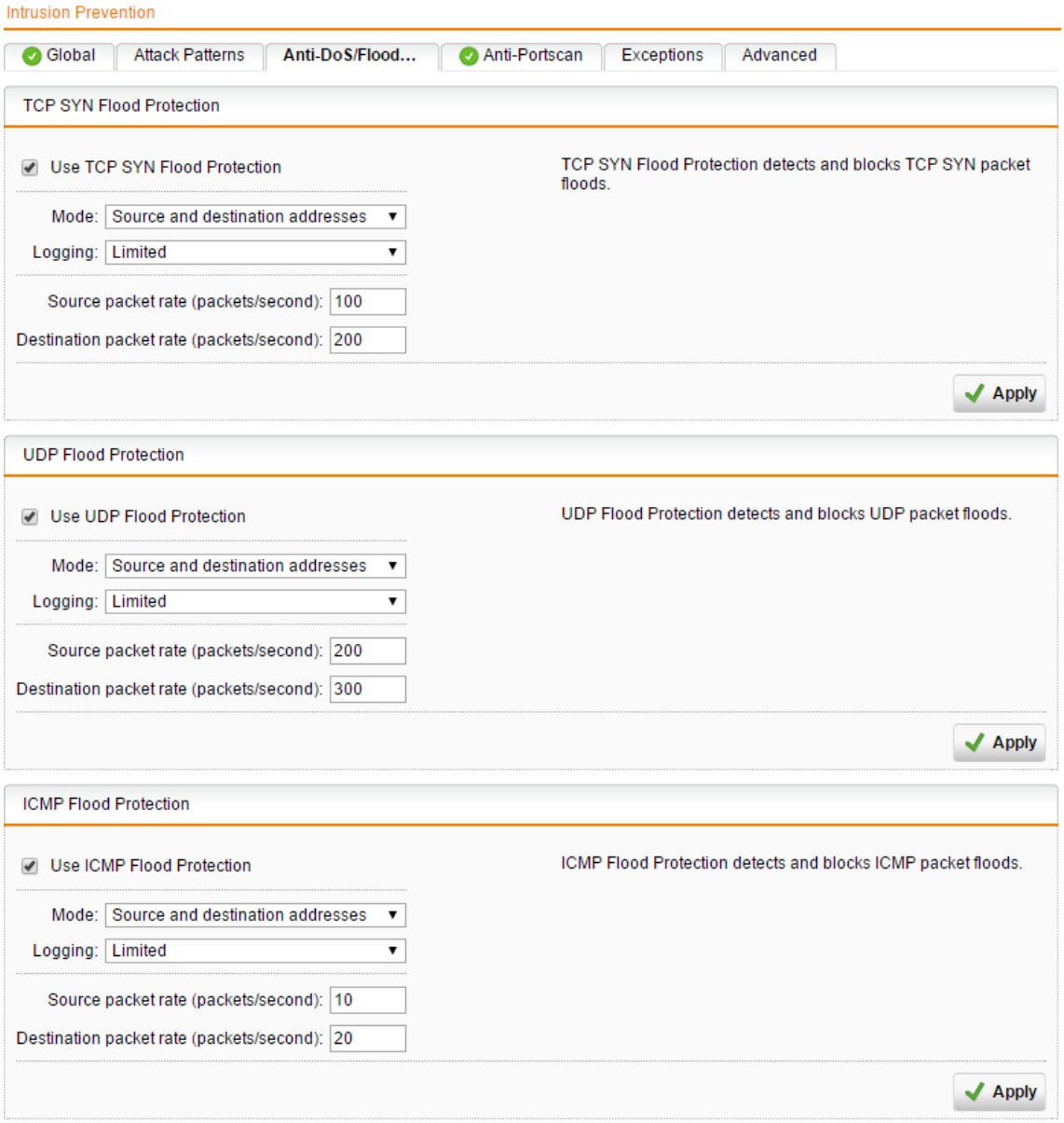
IPS-ominaisuuksien käyttöönottaminen vaatii suojattavien verkkojen määrittelemisen. IPS kuormittaa palomuurin prosessointitehoa ja vaikuttaa siirtonopeuksiin, koska jokainen paketti tutkitaan määritellyn hyökkäyskaaviosääntökannan mukaan. Sääntökanta tulee optimoida käytössä olevien palveluiden mukaisesti.



Kuva 13. IPS:n käyttöönotto

Kuvasta nähdään, että IPS on määritelty käyttöön kolmessa eri verkossa, ja liikenne pudotetaan huomaamattomasti.

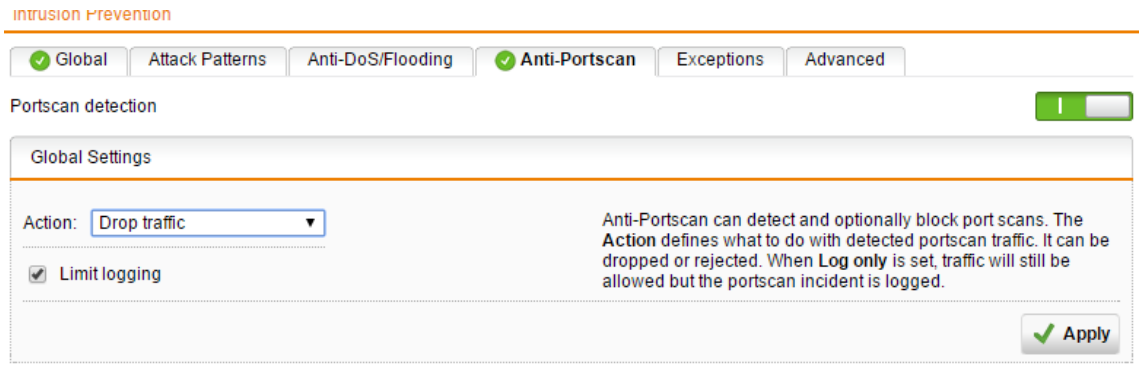
IPS-ominaisuuksiin kuuluu suojautuminen verkon tulvauksesta TCP-, UDP- ja ICMP-pakettien avulla. Asetuksissa voidaan määritellä frekvenssi, jolloin pakettipurskeeseen puututaan. Voidaan määrittää, että puututaan lähde- tai kohdeosoitteisiin tai molempiin. Lokin kerääminen pakettitulvista on mahdollista.



Kuva 14. Tulvaamisen esto

Kuvassa nähdään, että palomuurilla on otettu käyttöön tulvaamiselta suojaaminen kaikilla protokollilla.

Hakkerit saattavat etsiä haavoittuvuuksia, joiden avulla kaapataan tai tehdään palvelunestohyökkäyksiä skannaamalla apuohjelmien avulla avonaisia palveluita ja päätelaitteita, jotka näkyvät ulkoverkkoon. Anti-Portscan ominaisuuden avulla voidaan estää kyseinen toiminta. Palomuurin havaitessa tiuhaan tahtiin kyselyitä eri palveluille tietystä kohdeosoitteesta on käynnissä skannaus, joka voidaan havainnon jälkeen blokata automaattisesti.



Kuva 15. Anti-Portscan

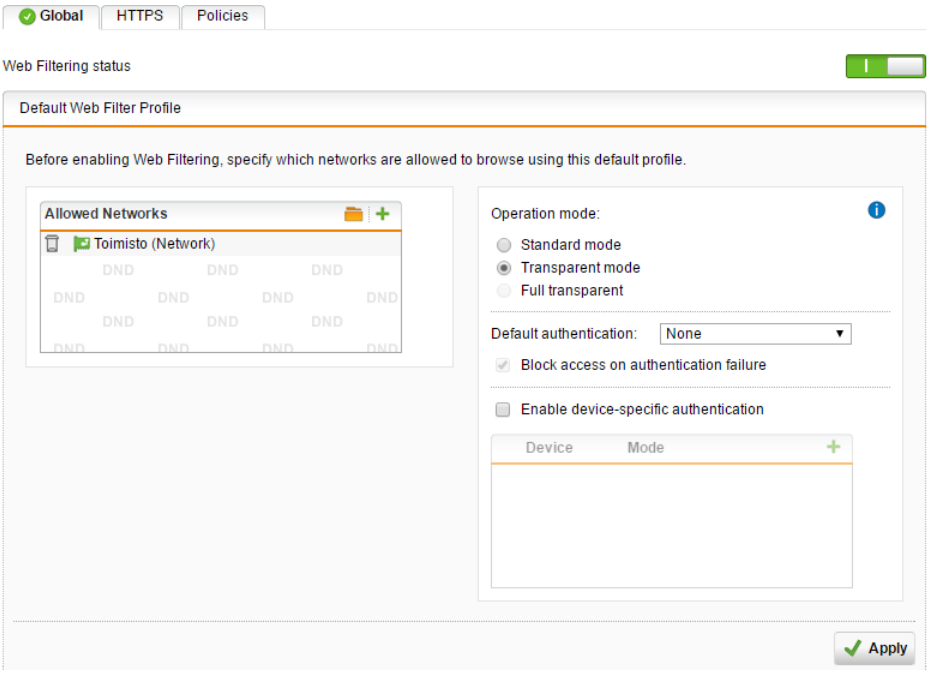
Kuvassa on otettu käyttöön Anti-Portscan ja määritelty, että liikenne pudotetaan, jos havaitaan epämääräistä toimintaa.

3.4 Web Protection

Web Protectionin asetukset keskittyvät verkon haittojen estoon ja verkon toiminnan muokkaamiseen sovellustasolla. Sovelluskohtaisesti voidaan tehdä eri sääntöjä, jotka voidaan kohdistaa ryhmä- ja käyttäjäkohtaisesti. Asetuksista käydään läpi Web Filtering ja Application Control omissa alaotsikoissaan.

3.4.1 Web Filtering

Web Filtering on palomuurin ominaisuus, jolla pystytään puuttumaan verkkoselaukseen. Ominaisuuden käyttöönottaessa palomuuri toimii myös http- ja https-välityspalvelimena tallettaen välimuistiinsa sivustoista tietoja. Verkkoselaamisesta tulee turvallisempaa, koska sivut voidaan tutkia virusten ja muiden haittaohjelmien varalta. Verkkosivustoille pääsyä voidaan rajoittaa kategorioittain. Säännöt voivat olla ryhmä- ja käyttäjäkohtaisia.



Kuva 16. Web Filtering -status

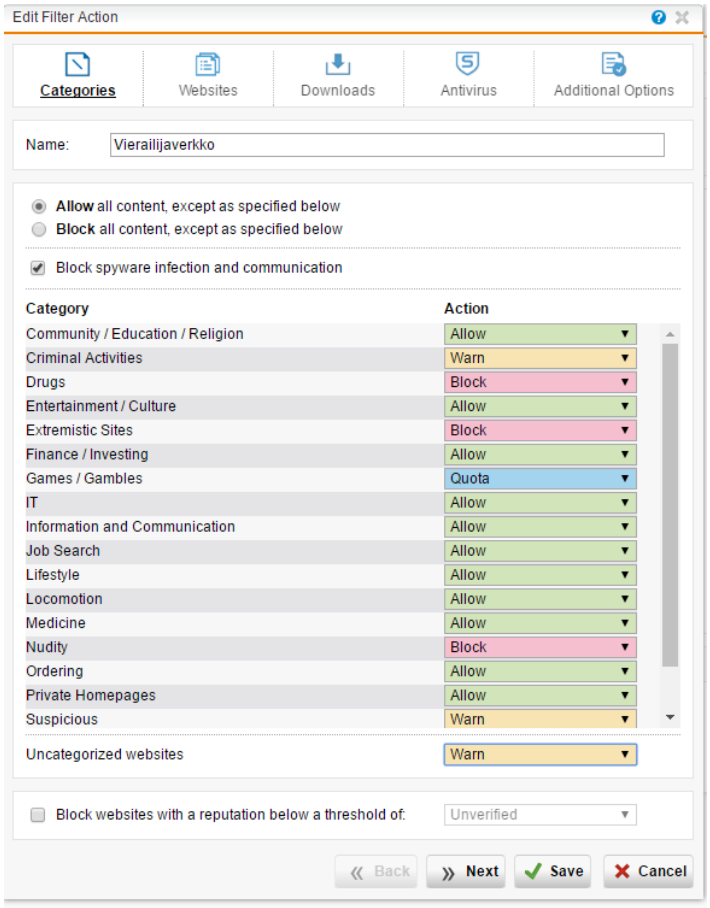
Web Filtering ominaisuus otetaan käyttöön laittamalla ominaisuus päälle ja valitsemalla sisäverkot, joiden verkkoliikenteeseen puututaan sekä määrittelemällä toimintatila, jossa Web Filtering toimii. Toimintatiloja on kolme erilaista. Kuvassa 4 näkyy, että toimistoverkko on määritelty käyttämään Web Filtering -ominaisuuksia Transparent-tilassa.

Standard-tilassa Web Filter kuuntelee pyyntöjä TCP-protokollalle 8080, jotka tulevat asiakasohjelmilta sallituiksi määritellyistä sisäverkoista. Web Filter pitää olla määriteltynä käyttäjien internetselaimien asetuksissa http-välityspalvelimeksi. Jos halutaan kerätä dataa käyttäjäkohtaisesta verkkoselaamisesta, niin käyttäjät voidaan todentaa. Todentaminen on mahdollista usealla eri tavalla. Niitä ovat muun muassa Active Directory, OpenDirectory, eDirectory, selaimessa tehtävä todennus, Web Filter välityspalvelimelle tehtävä todennus sekä Sophoksen oma todennusagentti, joka on ladattavissa palomuurin käyttäjäportaalista.

Transparent-tilassa käyttäjien ei tarvitse erikseen määritellä internetselaimen asetuksia. Web Filtering puuttuu kaikkiin asiakasohjelman selaimella tekemiin http-yhteyksiin. Asiakasohjelma ei ole tietoinen Web Filter -palvelimesta. Selaimen omat välityspalvelinasetukset eivät toimi, kun Web Filteri -ominaisuutta käytetään transparent-tilassa. Video- ja musiikkisuoratoistopalvelut eivät välttämättä käytä http-yhteyksille tyypillistä protokollaa 80, jolloin protokolla pitää erikseen sallia palomuurisäännöllä. Myös FTP-

palvelut vaativat toimiakseen protokollan 21 sallimisen palomuurilta. Käyttäjien todentaminen on mahdollista kolmella eri tavalla, jotka ovat Active Directory, Sophoksen todennusagentti ja selaimessa tehtävä todennus.

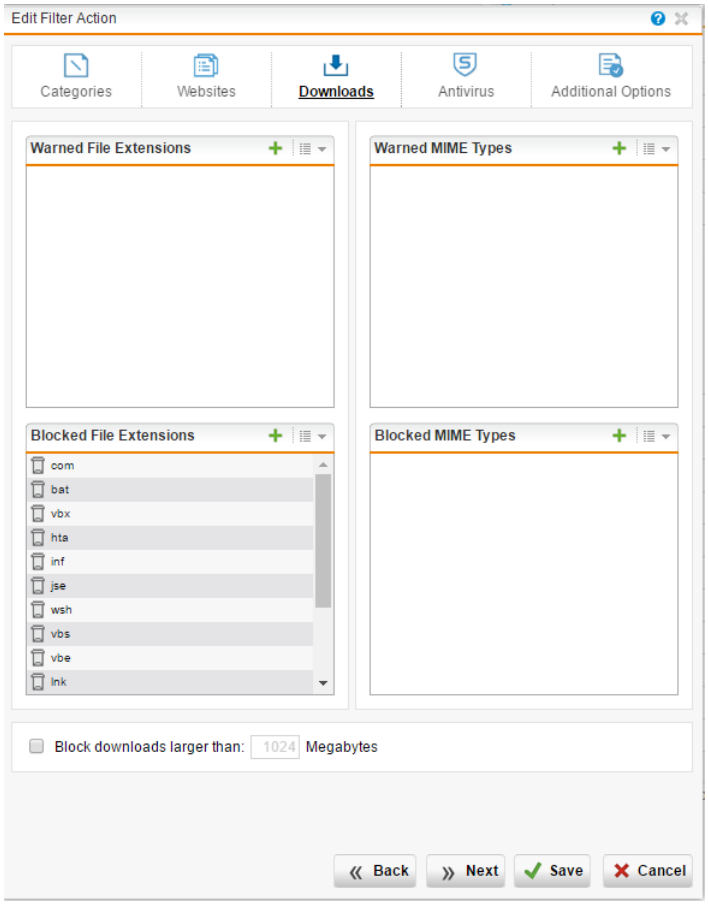
Full transparent -tila on mahdollista ottaa käyttöön, jos palomuuria käytetään siltaavassa tilassa. Siltaavassa tilassa palomuuri välittää liikenteen eteenpäin, jotta tuntematon kohde löytyisi. Tässä tilassa asiakasohjelman IP-osoitetta ei korvata oletusyhdyskäytävän IP-osoitteella vaan sen oma IP-osoite säilytetään. Käyttäjien todentamiseen on mahdollista käyttää samoja vaihtoehtoja kuin Transparent-tilassa.



Kuva 17. Web Filtering Filter Action Categories

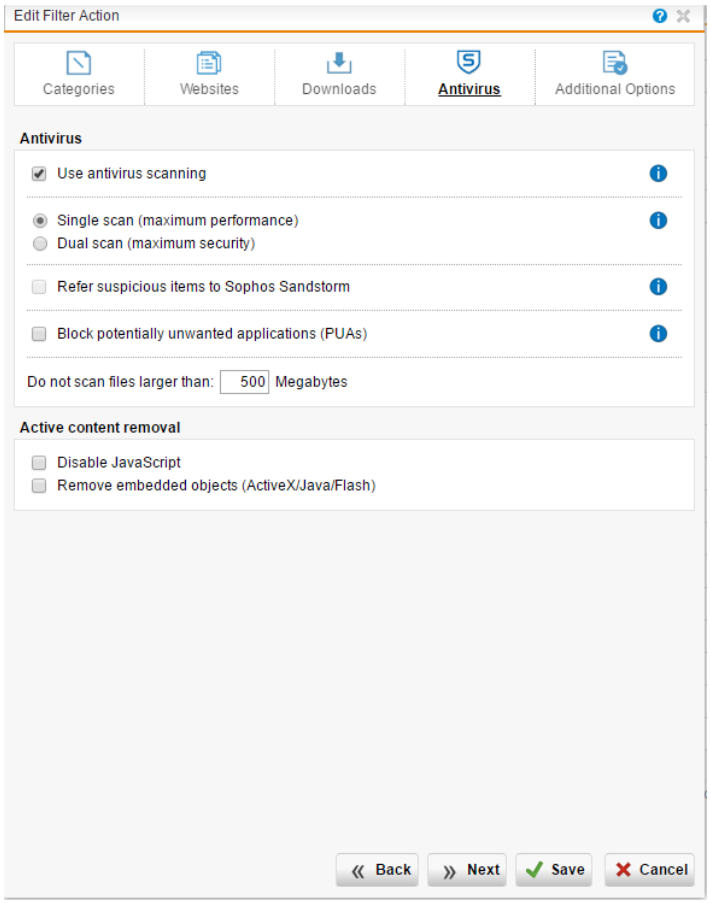
Verkkosivut luokitellaan sisältönsä perusteella kategorioihin. Web Filtering mahdollistaa suodattamien luomisen, joiden avulla voidaan sallia, estää, varoittaa tai rajoittaa sivustoilla vierailu. Kuvassa 5 on tehty vierailijaverkolle suodatin. Suodatin on asetettu estämään Spywaren ja sallimaan kaikki sivustot paitsi ne kategoriat, joiden toiminta on listassa erikseen määritelty. Keltaisella värillä näkyvä varoitustoiminto on määritelty

rikolliseen toimintaan, epämääräiseen ja määrittelemättömiin kategorioihin kuuluville sivustoille. Näille sivustoille mennessä käyttäjä saa palomuurilta varoituksen selaimeensa, josta ilmenee, että käyttäjä on menossa mahdollisesti haitalliselle sivustolle. Punaisella värillä näkyvä estotoiminto on määritelty sivustoille, jotka kuuluvat huumeet-, ekstremistinen toiminta- tai alastomuus-kategoriaan. Näille sivustoille käyttäjä ei pääse. Sinisellä värillä näkyvä rajoitustoiminto on määritelty pelit ja uhkapelit-kategoriaan. Näillä sivustoilla vieraillessa käyttäjällä on erikseen määritelty datamäärä käytettävissä.



Kuva 18. Web Filtering Filter Action Downloads

Suodattamien asetuksista voidaan varoittaa tiedostoa tai MIME-viestiä ladattaessa. Tiedostojen ja MIME-viestien lataus voidaan myös estää kokonaan. Kuvassa 6 nähtävässä suodattimessa on estetty tiedostojen lataaminen, jotka ovat listan mukaista tiedostoformaattia.



Kuva 19. Web Filtering Filter Action Antivirus

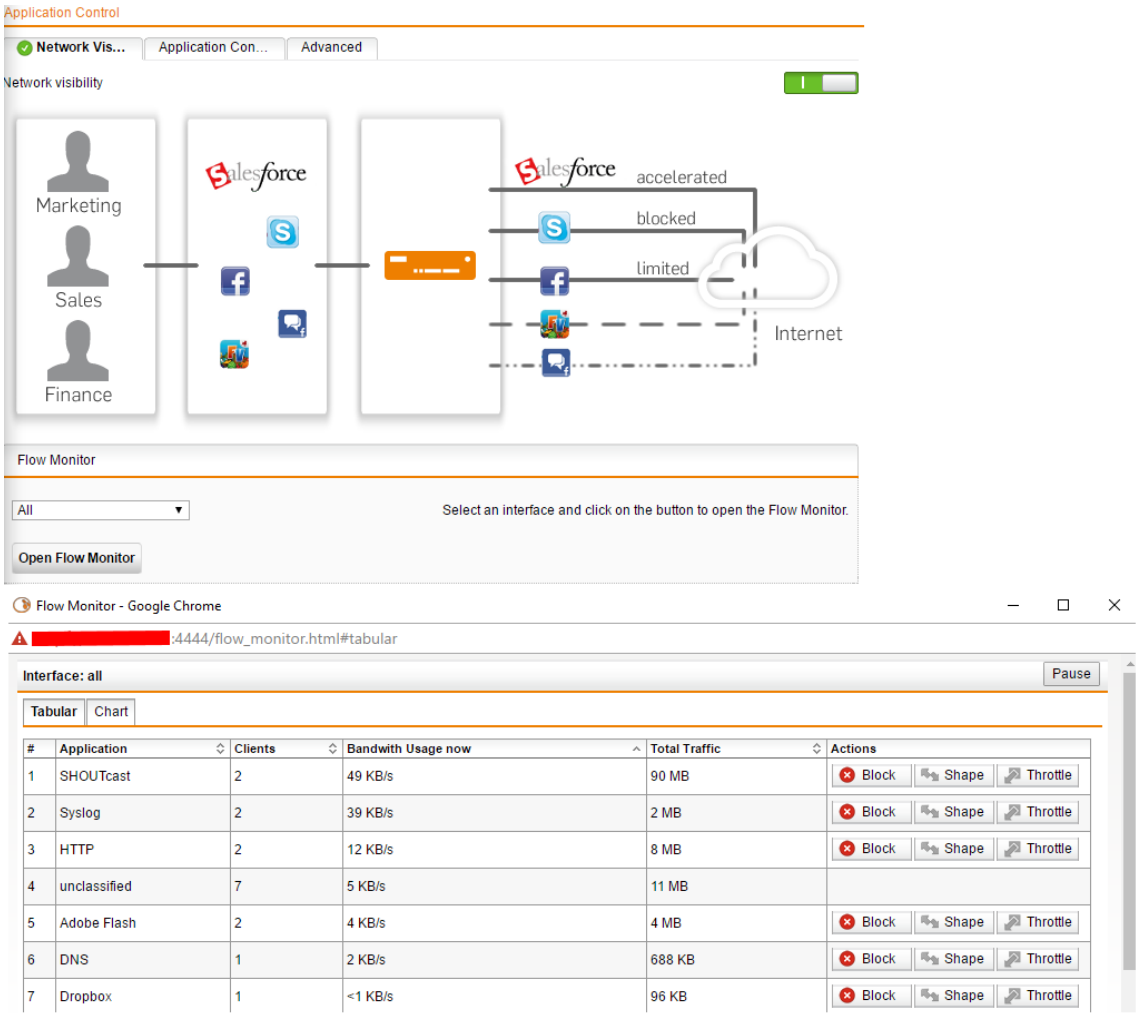
Suodattimien asetuksista voidaan myös määritellä Web Filtering tekemään virustarkistusta. Kuvassa 7 nähtävässä suodattimessa virustarkistus on otettu käyttöön. Virustarkistus tehdään yhdellä virustarkistimella, joka on kevyempi ja aikaa säästävämpi vaihtoehto, kuin järeämpi ja tarkempi kahdella eri virustarkistimella tehtävä tarkistus.

3.4.2 Application Control

Application Control eli ohjelmakohtainen hallinta on palomuurin ominaisuus, jolla pystytään halutulla tavalla muokkaamaan verkkoliikennettä sen tyypin mukaan. Palomuuri osaa tunnistaa ja luokitella verkkoliikenteen OSI-viitemallin seitsemännellä kerroksella toimivan luokittelumoottorinsa avulla.

Ohjelmakohtainen hallinta otetaan käyttöön asettamalla Network Visibility -välilehden asetukista Network Visibility päälle, jonka jälkeen palomuuri pystyy havaitsemaan eri ohjelmat verkkoliikenteestä. Käyttöönoton jälkeen määritellään ohjelmat, jotka ovat

sallittuja tai kiellettyjä tietystä kohdeverkosta. Ohjelmalistasta löytyy useita verkossa pyöriviä ohjelmia ja sitä päivitetään jatkuvasti.



Kuva 20. Application Control ja Flow Monitor

Network Visibility -välilehdeltä löytyvän Flow Monitor -työkalun avulla nähdään ohjelmakohtaisesti, kuinka paljon ohjelman hetkellinen kaistanleveyden käyttö on sekä kuinka paljon liikennettä kyseinen ohjelma on käyttänyt. Ohjelman toiminta voidaan estää työkalun avulla. Ohjelmille voidaan tehdä kaistanleveyden varauksia ja rajoituksia. Skypelle voidaan varata tarpeeksi kaistanleveyttä, jotta varmistetaan videoneuvotteluiden ja puheluiden sulava toiminta. Facebook-selausta voidaan rajoittaa, jotta kaistanleveydestä suurin osa on hyötykäytössä.

3.5 Email Protection

UTM tarjoaa mahdollisuuden sähköpostin suojaamiseen SMTP- ja POP3-välityspalvelimien avulla. Sähköpostit voidaan tarkistaa virusten ja malwaren varalta. Roskapostit voidaan estää useamman eri perusteen mukaan. Salattujen sähköpostiviestien lähetys onnistuu helposti ja nopeasti käyttämällä SPX -salausta.

SMTP eli Simple Mail Transfer Protocol on sähköpostin luotettavaan ja tehokkaaseen välittämiseen kehitetty protokolla. SMTP käyttää yleensä TCP-protokollaa 25. Sähköposti voidaan toimittaa protokollan avulla saman verkon sisällä tai muihin verkkoihin, jotka ovat tavoitettavissa välityspalvelimien tai yhdyskäytävän kautta. Sähköpostia lähettäessä sähköpostiohjelma toimii SMTP-asiakkaana, joka luo kahden suuntaisen siirtokanavan SMTP-palvelimena toimivan sähköpostipalvelimen välille. SMTP-asiakkaan velvollisuus on siirtää sähköpostiviestit yhdelle tai useammalle SMTP-palvelimelle tai ilmoittaa siirtämisen epäonnistumisesta.

Palomuurin SMTP-välityspalvelin ominaisuus toimii sovellustasolla. Sitä voidaan käyttää sisäisen sähköpostin suojaamiseen etähyökkäyksiltä. Se mahdollistaa tehokkaan sähköpostien suodattamisen ja tarkistuksen roskapostien sekä virusten varalta. SMTP-välityspalvelin tarvitsee toimivan DNS-palvelimen, jotta nimenselvitys onnistuu.

Email Protection SMTP -asetuksista kytketään ominaisuus päälle ja valitaan asetusvaihtoehto tavallisen tilan ja profiilitilan väliltä. Tavallisessa tilassa kaikki toimialueet jakavat samat asetukset, mutta poikkeuksia voi tehdä toimialuenimiin, sähköpostiosoitteisiin ja isäntänimiin. Toiminallisia rajoitteita ei ole profiilitilaan verrattuna. Profiilitilassa yksittäisille toimialueille tai toimialueryhmille voidaan tehdä profiileja, joissa asetukset eroavat yleisistä asetuksista, kuten poikkeuksia malwaren- ja roskapostin suodattamiseen.

SMTP-välityspalvelimen reititys asetuksista määritellään kaikki käytettävät toimialueet, jotka saavat lähettää sähköpostia. Toimialueiden määrittelyssä voidaan käyttää jokerimerkkinä (*) tähteä nimen alkuosassa. Sähköpostit määritettyihin toimialueisiin tulee reitittää sisäiselle sähköpostipalvelimelle. Reititys voidaan tehdä staattisen listan mukaan, johon on määritelty kaikki eri sähköpostipalvelimet IP-osoitteella. Lista käydään läpi ylhäältä alas-periaatteella. Reititys on mahdollista toteuttaa myös DNS-isäntänimellä, jolloin määritellään täydellinen toimialuenimi esimerkiksi exchan-

ge.mail.com. Viimeinen vaihtoehto toteuttamiseen on MX-arvoihin perustuva reititys, jolloin palomuurin sähköpostin siirtovälittäjä tekee nimikyselyn vastaanottajan toimialueen MX-tietueesta. Palomuurin oletusyhdyskäytävä ei saa olla määriteltynä toimialueiden MX-tietueeksi, koska palomuuri ei toimita itselleen postia.

Vastaanottajien varmistus on mahdollista tehdä lähettämällä varmistus palvelimelle, joka varmistaa vastaanottajan. Vastaanottajat voidaan varmistaa myös Active Directoryn kautta. Vastaanottajien varmistusta ei ole pakko ottaa käyttöön, mutta se on suositeltavaa, jotta vältytään korkealta roskapostilta ja sanakirjahyökkäyksiltä, joilla pyritään arvaamaan käyttäjien salasanoja.

Malwaren estäminen onnistuu SMTP-yhteyden aikana, kun ominaisuus otetaan käyttöön. Tarkistusmoottori hylkää viestit, jotka sisältävät malwarea. Skannaaminen on mahdollista tehdä kahdella eri virustutkalla, jolloin maksimoidaan tunnistettujen uhkien määrä, mutta se on hitaampaa kuin yhdellä virustutkalla skannaaminen, mikä maksimoi tehokkuuden. Sophos Sandstorm käsitellään Advanced Protection –luvussa. Se on mahdollista ottaa käyttöön tämän ominaisuuden tueksi.

Sähköpostiviesteistä voidaan laittaa karanteeniin tiettyä MIME-tyyppiä sisältävät viestit. Karanteeniin on mahdollista laittaa audiosisältöä, videosisältöä tai suoritettavia komentoja sisältäviä MIME-tyyppejä. Lisäksi on mahdollista laittaa itsemääriteltyjä MIME-tyyppejä karanteeniin sekä sallia erikseen tiettyjä MIME-tyyppejä.

Liitetiedostoja sisältävät sähköpostit voidaan suodattaa ja laittaa karanteeniin. Liitetiedostot, jotka aiheuttavat karanteenin, voidaan itse määrittää listaan.

Roskapostia voidaan estää heti SMTP-yhteyden aikana. Se on mahdollista kahdella eri tavalla: hylätä postit, jotka ovat varmistetusti roskapostia, hylätä postit, jotka luultavasti ovat roskapostia. Toinen vaihtoehto hylkää todennäköisesti myös normaaleja posteja, kuten uutiskirjeitä. Roskaposteja vastaan käytetään mustan aukon listoja, jotka sisältävät tunnettujen roskapostin lähettäjien IP-osoitteita. Automaattisten listojen lisäksi on mahdollista määritellä omia mustan aukon listoja. Roskapostin käsittelyyn on eri mahdollisuuksia. Roskapostista voidaan antaa varoitus, jolloin sähköpostin otsakkeeseen lisätään roskapostilippu ja aiheeseen roskapostimerkki. Roskaposti voidaan estää ja laittaa karanteeniin. Saapuvat roskapostit voidaan sallia ja poistaa välittömästä, jolloin käytetään mustan aukontoimintoa.

Sähköpostiviestien liitteet voidaan skannata arkaluontoisen datan varalta. Mikäli liitetiedostosta löytyy sääntölistaan määriteltyä dataa, niin sähköposti voidaan lähettää SPX-suojattuna tai se voidaan pudottaa mustaan aukkoon.

Sähköpostin salaaminen onnistuu palomuurin sähköpostisuojauksen SPX-ominaisuuden avulla. SPX on käyttöliittymätön ja täten helppo ottaa käyttöön ja muunneltavissa. SPX-lyhenne tulee sanoista Secure PDF Exchange. Kun SPX-ominaisuus on käytössä, niin palomuurille lähetetyt salaamattomat sähköpostiviestit ja niiden liitteet muunnetaan salasanalla suojatuksi PDF-tiedostoiksi. SPX-asetuksista voidaan määritellä, että sähköpostin lähettäjä tai vastaanottaja voi määritellä käytettävän salasanan, palomuuri generoi salasanan vastaanottajille ja tallettaa sen vastaanottajakohtaisesti tai että palomuuri generoi kertakäyttöiset salasanat vastaanottajille.

SPX-salatut sähköpostiviestit voidaan toteuttaa kahdella tavalla. On mahdollista käyttää Micrsoft Outlook -lisäosaa, jolloin käyttäjä painaa Encrypt-painiketta ja kirjoittaa viestinsä, joka sitten salataan. Toinen vaihtoehto on käyttää sähköpostisuojauksen datan suojausominaisuutta, joka automaattisesti salaa sähköpostiviestit, jos viestissä on jotain arkaluontoista tietoa. Datan suojausominaisuuden asetuksista voidaan määritellä, mitkä sanat tai tiedot aiheuttavat toimenpiteitä.

Palomuuri toimittaa salatut sähköpostit vastaanottajan sähköpostipalvelimelle, jonka jälkeen vastaanottaja voi lukea sähköpostiviestin Adobe Reader -ohjelmalla käyttäen valittua salasanaa. Kaikki laitteet, jotka tukevat PDF-tiedostoja voivat lukea SPX-suojattuja sähköpostiviestejä.

Vastaanottaja pystyy myös vastaamaan sähköpostiviestiin turvallisesti käyttämällä SPX-ominaisuuden vastausportaalia. SPX-vastaukselle ja salasanoille on mahdollista määrittää vanhentumisajat.

SPX-salausta voidaan käyttää kummankin SMTP-asetusvaihtoehdon kanssa. Simple-asetusvaihtoehtoa käyttäessä voidaan valita yleismallinen SPX-sapluuna, joka määrittelee PDF-tiedoston ulkoasun, salasana-asetukset, ohjeet vastaanottajalle ja SPX-vastausportaalin asetukset. Profile-asetusvaihtoehtoa käyttäessä on mahdollista määrittää eri SPX-sapluunoita eri SMTP-profiileille. SPX-sapluunat on muokattavissa asiakaskohtaisesti ja niihin voidaan määritellä eri logoja ja tekstejä.

SPX-salauksen käyttöönottaminen tapahtuu kytkemällä ominaisuus päälle SPX Encryption asetuksista, jonka jälkeen valitaan käytettävät SPX-profiilit ja määritellään SPX-vastausportaalin asetukset ja SPX-vanhentumisajat.

3.6 Advanced Protection

Palomuurin Advanced Protectionin ominaisuudet keskittyvät edistyneiden uhkien torjuntaan. Edistyneiden uhkien torjumiseen ja havainnointiin on käytössä Advanced Threat Protection ja Sophos Sandstorm.

Advanced Threat Protectionin ominaisuus mahdollistaa saastuneiden ja vaarantuneiden päätelaitteiden löytämisen, jonka jälkeen päätelaitteiden verkkoliikenne voidaan pudottaa pois tai siitä voidaan antaa hälytys. ATP analysoi kaikkea saapuvaa ja lähtevää verkkoliikennettä uhkien varalta käyden läpi DNS- ja http-pyynnöt sekä muut IP-paketit yleisesti. Palomuuri tunnistaa uhat uhkamalliensa mukaan, jotka päivittyvät Sophos Labin alati päivittyvästä tietokannasta. ATP:n toimintaa voidaan tehostaa, kun käytössä on myös IPS- ja Web Protection -ominaisuudet.

Käyttöönottaminen tapahtuu kytkemällä ominaisuus päälle ATP-asetuksista, jonka jälkeen ATP käsittelee kaiken verkkoliikenteen, joka kulkee palomuurin lävitse. Asetuksissa voidaan tehdä tiettyjen verkkojen tai isäntien kohdalla poikkeuksia, jos halutaan olla käyttämättä ATP-ominaisuutta. ATP saattaa tunnistaa jotkin sivustot virheellisesti uhkiksi, jonka takia on mahdollista tehdä poikkeuksia IP-osoitteella tai toimialueen nimen perusteella, jotta vältytään hälytyksiltä ja nämä sivustot toimivat normaalisti ATP:tä käyttäessä. ATP:n havaitsemat uhat näkyvät palomuurin Dashboard-välilehdellä, joka on myös palomuurille kirjautumisen jälkeen ensimmäinen sivu.

Sophos Sandstorm on edistyneitä jatkuvia uhkia vastaan kehitetty tietoturvaominaisuus, joka toimii hiekkalaatikkoperiaatteella. Hiekkalaatikko on eristetty ja turvallinen ympäristö, jonka tarkoitus on mallintaa tietokone järjestelmää. Hiekkalaatikko mahdollistaa, yrityksen verkkoa vaarantamatta, epämääräisten ohjelmien testaamisen ja tarkkailun, jonka avulla saadaan selville niiden tarkoitus ja toimintaperiaate.

Sandstorm toiminta koostuu neljästä vaiheesta. Ensiksi tiedostoille tehdään kaikki tavanomaiset tarkistukset malwaren, huonojen URLien ja muiden haittojen varalta. Mikäli

tiedosto on suoritettava-tiedosto tai se sisältää jotain suorituskomentoja, eikä se ole ladattu turvalliseksi määritellyltä verkkosivustolta, niin tiedostoa kohdellaan epäilyttävänä. Epäilyttävän tiedoston hajautusarvo lähetetään Sophos Sandstormille analysoitavaksi. Seuraavaksi Sophos Sandstorm tarkistaa, onko tiedoston hajautusarvo tuttu. Jos on, niin tiedosto palautetaan palomuurille, josta se välitetään käyttäjälle tai estetään riippuen analyysin tuloksesta. Tiedostot, joiden hajautusarvot ovat tuntemattomia lähetetään, Sophos Sandstormin analysoitavaksi. Analyysin valmistuttua tieto lähetetään palomuurille ja sen perusteella tiedosto estetään tai toimitetaan käyttäjälle. Palomuuri saa Sophos Sandstormin tietokannasta tarkat tiedot, joista koostetaan raportti jokaista uhkaa kohden.

Sophos Sandstorm on erikseen lisensoitava ominaisuus palomuureille ja muille Sophos-tietoturvatuotteille.

3.7 Webserver Protection

Webserver Protectionin asetukset keskittyvät verkossa olevien palvelimien turvaamiseen. Palvelimien turvaamisen hoitaa Web Application Firewall eli WAF. Se on käänteinen välityspalvelin. WAF muodostuu, kun internetin ja web-palvelimen välille luodaan virtuaalinen web-palvelin.

Web-palvelimille suuntautuva liikenne kulkee ensiksi virtuaalisen web-palvelimen läpi, joka suodattaa liikenteen ja täten suojaa oikeita web-palvelimia erilaisilta hyökkäyksiltä. Web-palvelimia voidaan suojata virusten varalta, XSS-aukkojen hyväksikäytöltä, SQL-injektioilta ja muilta mahdollisilta haavoittuvuuksilta. Sääntöprofiilien avulla on mahdollista luoda eri suojaustason web-palvelimia. WAF mahdollistaa myös käyttäjien todentamisen, vaikka alkuperäinen web-palvelin ei tukisi todentamista.

WAF otetaan käyttöön määrittelemällä web-palvelin palomuurille. Palvelimien sertifikaatti ladataan palomuurille, jotta se osaa tunnistaa palvelimen. Seuraavaksi luodaan virtuaalinen web-palvelin, jonka asetuksiin määritellään, mitkä toimialueet ja oikeat web-palvelimet ovat käytössä. Asetuksissa määritellään, mihin palomuurin osoitteeseen virtuaalinen web-palvelin sidotaan sekä käytettävä protokolla http vai https. Jos käytössä on https, niin pitää valita oikean palvelimen sertifikaatti. Virtuaalisen web-

palvelimen palomuurisääntö profiilia valittaessa voidaan määritellä, mitä turvaominaisuuksia otetaan käyttöön.

3.8 Site-to-site VPN

Yrityksillä saattaa olla useita toimipisteitä tai liikekumppaneita, joiden kanssa tehdään yhteistyötä ja verkon resursseja pitää pystyä käyttämään myös toisesta paikasta. Toimistojen välille ei tarvitse rakentaa runkolinjoja, vaan tämä on mahdollista julkisen internetin ylitse käyttämällä VPN-tunneleita.

VPN eli virtual private network tarkoittaa virtuaalista yksityisverkkoa. Yksinkertaisuudessaan molemmissa pisteissä on laitteet, joille on annettu määritykset tunnelin muodostamiseen. Tunnelin lävitse lähtevä liikenne salataan valitulla algoritmilla ja kapseloidaan IP-pakettiin. Tunnelin lävitse saapuvan liikenteen salaus puretaan ja ohjataan se oikeaan kohteeseen. [3, s.284–285.]

Sophos UTM -palomuurilla on mahdollista toteuttaa IPSec VPN -tunnelien lisäksi SSL VPN -tunneleita. Amazonin tarjoama virtuaalinen pilvipalvelu on myös mahdollista yhdistää palomuurin sisäiseksi verkoksi ja sen hallitseminen on mahdollista IPSec-tunnelin avulla. Amazonin pilvipalvelun palvelimet ovat ulkomailla, joten emme luota siihen, eikä siitä käydä tarkemmin läpi. IPSec-protokollan toiminta käydään läpi omassa alaotsikossa ja kuinka IPSec-tunneli pystytetään. SSL käsitellään tarkemmin omassa alaotsikossaan ja käydään läpi, kuinka se pystytetään.

Sophos UTM WebAdmin Site-to-site VPN -välilehden avatessa nähdään VPN-tunnelien tilanne. Tunnelin tilan ilmaisevat värikoodatut ikonit. Vihreä väri tarkoittaa, että yhteys on täysin toiminnassa. Keltainen väri tarkoittaa, että yhteys toimii osittain. Punainen väri tarkoittaa, että yhteys ei toimi.

3.8.1 IPsec

IPsec on IETF:n RFC standardoima joukko tietoliikenneprotokollia. IPsec toimii verkkokerroksella OSI-viitemallissa suojaten ja todentaen IP-paketit tunnelin välillä. [1, s.243.]

IPsec-standardi toimii kahdella eri salausmuodolla ja kahdella eri protokollalla. Salausmuodot ovat siirtomuoto ja tunnelimuoto. Protokollat ovat AH (Authentication Header) ja ESP (Encapsulated Security Payload). Lisäksi ISAKMP (Internet Security Association Key Management Protocol) protokollaa käytetään tunnelin muodostamiseen ja salausavainten vaihdon suorittamiseen.

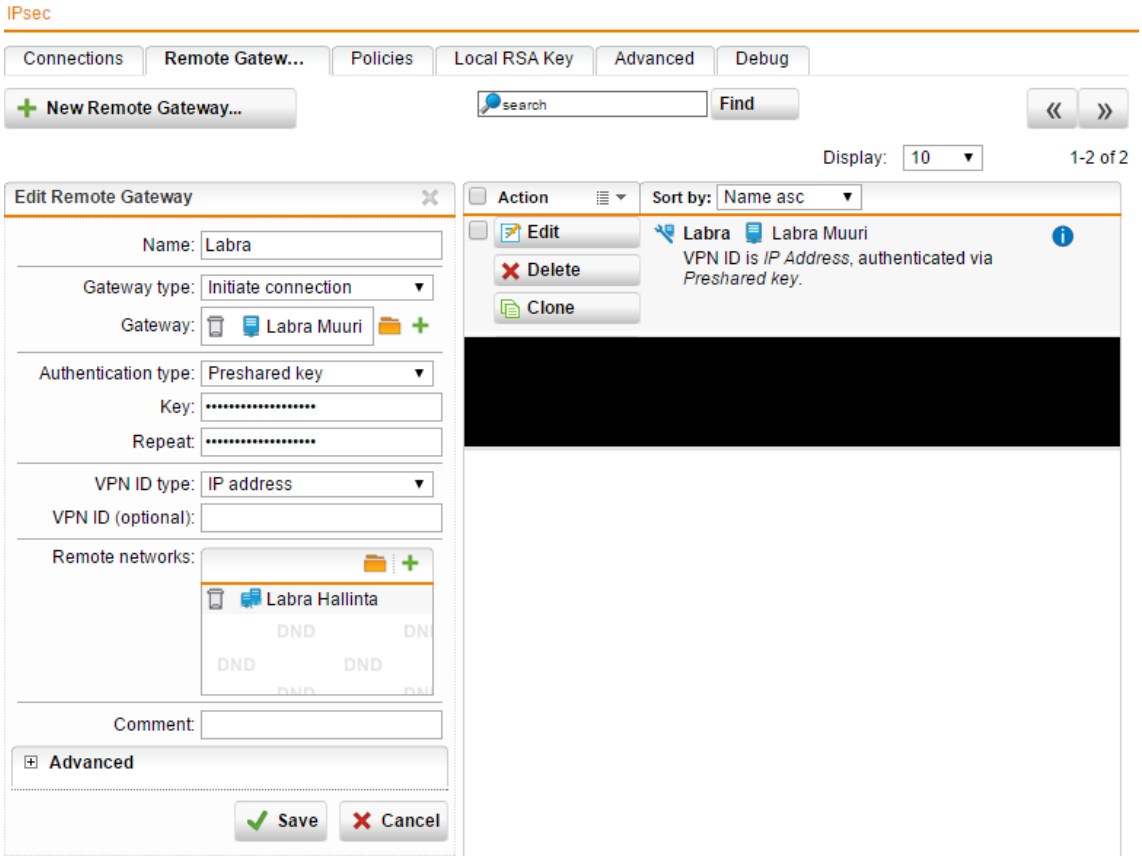
Authentication Header on protokolla, jonka avulla todennetaan IP-pakettien lähettäjä ja varmennetaan IP-paketin yhtenäisyys. Se mahdollistaa uudelleensoittojen eston. AH-protokollaa voidaan käyttää itsenäisesti tai yhdistelmänä ESP-protokollan kanssa. AH käyttää TCP-protokollaa 51.

Encapsulating Security Payload on protokolla, jonka avulla suojataan koko IP-paketti ja todennetaan sen sisältö. Se mahdollistaa uudelleensoittojen havaitsemisen. ESP käyttää TCP-protokollaa 50.

Siirtomuodossa alkuperäistä IP-pakettia ei kapseloida uudeksi paketiksi vaan alkuperäinen IP-otsikko säilytetään ja loppupaketti lähetetään selkotekstinä AH-protokollalla todennettuna tai salattuna ESP-protokollalla. Koko paketti voidaan todentaa AH-protokollalla tai hyötykuorma voidaan salata ja todentaa käyttäen ESP-protokollaa. Kuitenkin alkuperäinen otsikko lähetetään selkotekstinä internetin ylitse.

Tunnelimuodossa koko IP-paketti eli otsikko ja hyötykuorma kapseloidaan uuteen IP-pakettiin. IP-paketille lisätään IP-otsikko, josta käy ilmi tunnelin toisen pään laitteen osoite. IP-osoitteet kapseloidun paketin sisällä pysyvät ennallaan ja alkuperäinen paketti todennetaan AH-protokollalla tai suojataan ja todennetaan käyttäen ESP-protokollaa.

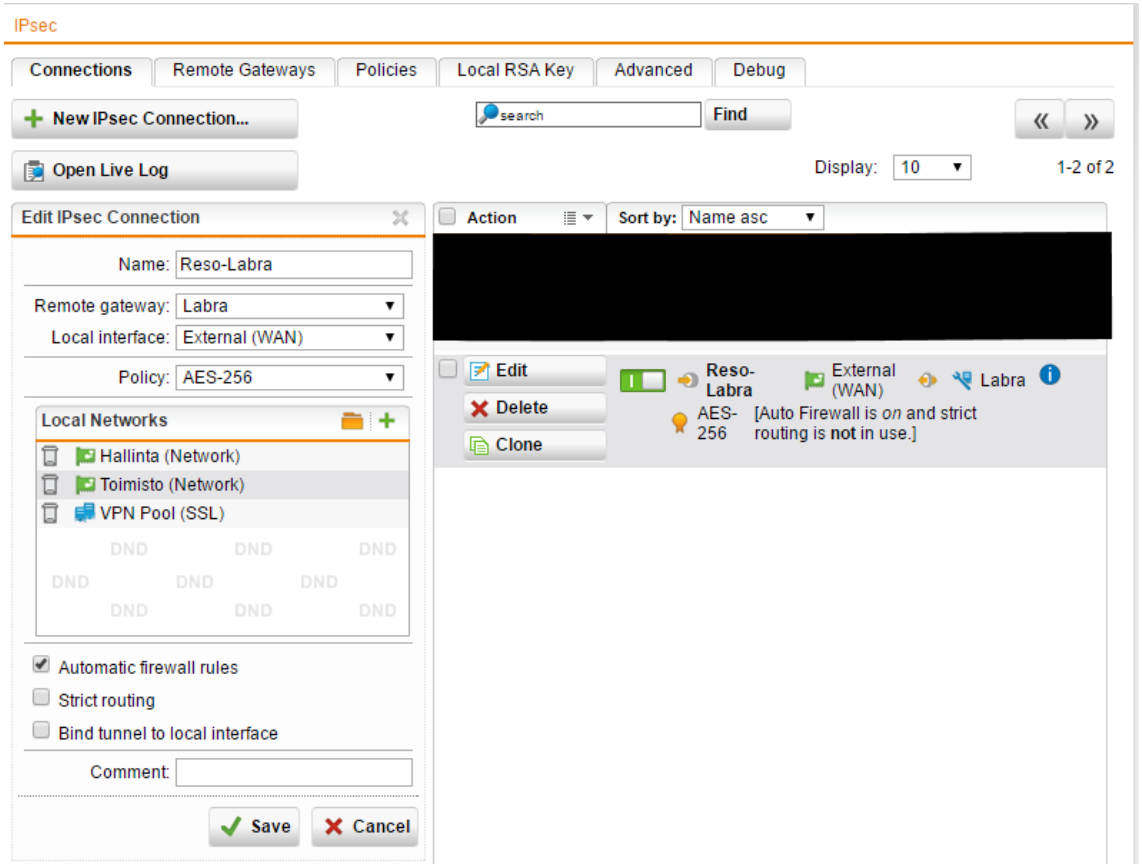
Sophos UTM -palomuurilla voidaan toteuttaa IPsec VPN -tunneleita ainoastaan tunnelimuodossa. Tunnelimuotoa tulee käyttää aina kun käytetään turvallisuusominaisuuksilla varustettua laitetta, kuten palomuuria, VPN-tunnelin muodostamiseen. IPsec-yhteyden muodostamisen voi aloittaa kumpi tahansa tunnelin päätelaitteista.



Kuva 21. IPsec-yhteyden muodostuksen oletusyhdyskäytävä

IPsec-yhteyden muodostamiseen vaaditaan oletusyhdyskäytävän määritteleminen. Oletusyhdyskäytävälle annetaan nimi ja se määritellään ottamaan yhteyden tunnelin toisen puolen oletusyhdyskäytävälle. Yhteyden todennustyyppi valitaan ja määritellään salainen avain, jonka täytyy olla tunnelin molemmissa päissä identtinen. Lopuksi kerrotaan mitkä verkot tunnelin toisesta päästä löytyvät. Kuvassa 21 nähdään, että Labra-niminen yhteys ottaa yhteyden Labra Muuriin, jonka takaa löytyy verkko Labra Hallinta.

Kun oletusyhdyskäytävä on luotu, niin voidaan määritellä IPsec-yhteys. Yhteydelle annetaan nimi, määritellään käytettävä oletusyhdyskäytävä ja minkä paikallisen rajapinnan takaa yhteys muodostetaan. Samalla määritellään paikalliset verkot, jotka mainostetaan IPsec-yhteydessä, sekä salausmenetelmä ja luodaan automaattiset palomuuri säännöt tarvittaessa.



Kuva 22. IPsec-yhteyden konfiguraatiot

Kuvassa 22 on määritelty Reso-Labra niminen IPsec-yhteys, joka on sidottu kuvassa 21 määriteltyyn Labra-oletusyhdyskäytävään. Salausmenetelmäksi on valittu AES-256 ja tehty automaattiset palomuurisäännöt. Paikalliset verkot ovat Hallinta, Toimisto ja VPN-käyttäjät.

3.8.2 SSL

SSL eli Secure Sockets Layer on IETF:n RFC standardoima salausprotokolla, joka toimii OSI-viitemallin esitystapakerroksella. SSL:n tarkoitus on varmistaa yhteyden luotettavuus, eheys ja osapuolten todentaminen. Todennusta voidaan käyttää sekä palvelimien aitouden varmentamiseen, sekä käyttäjien todentamiseen. [3, s.390.]

SSL toimii kahden eri protokollan avulla, jotka ovat Handshake ja Record Layer.

Handshake eli kättelyprosessissa käyttäjä lähettää palvelimelle viestin kertoen, mitä salausmenetelmiä se pystyy käyttämään, jonka jälkeen palvelin valikoi käytettävän

salausmenetelmän ja lähettää käyttäjälle vahvistustiedon. Sertifikaattien avulla voidaan tunnistaa kättelyn osapuolet. Loppuvaiheessa kättelyä sopivat osapuolet istuntoavaimen valinnasta samalla tavalla kuin yhteyden alkuvaiheessa. Kättelyn päättyessä yhteys on salattu, eikä salausmenetelmiä, sertifikaatteja tai istuntoavaimia pysty enää vaihtamaan. [3, s.391.]

Record Layer on TCP-protokollan päällä toimiva protokolla, jonka tarkoitus on varmistaa viestien osioiminen, pakkaaminen, salakirjoitus ja eheyden varmistus. Salakirjoittaessa viestejä käytetään salaista avainta ja eheyden varmistamisessa tiivistefunktiota. [3, s.391.]

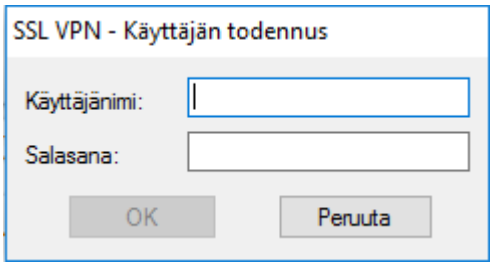
SSL-protokollaa voidaan hyödyntää useiden muiden internetprotokollien kanssa, kuten HTTPS. Tällöin normaalisti salaamattomasta http-liikenteestä tulee salattua. Sähköpostin SMTP-liikenne ja tiedostonsiirrossa käytettävä FTP-liikenne voidaan myös salata SSL:n avulla. [3, s.390.]

Toimipiste kohtaisia SSL VPN -yhteyksiä muodostaessa pitää ottaa huomioon, että tunnelin päätelaitteet toimivat eri rooleissa. Yhteyden muodostamisen aloittaa asiakasohjelman roolissa oleva päätelaite ja palvelimen roolissa oleva päätelaite vastaa asiakasohjelman kyselyyn, jonka jälkeen yhteys voidaan muodostaa.

3.9 Remote access

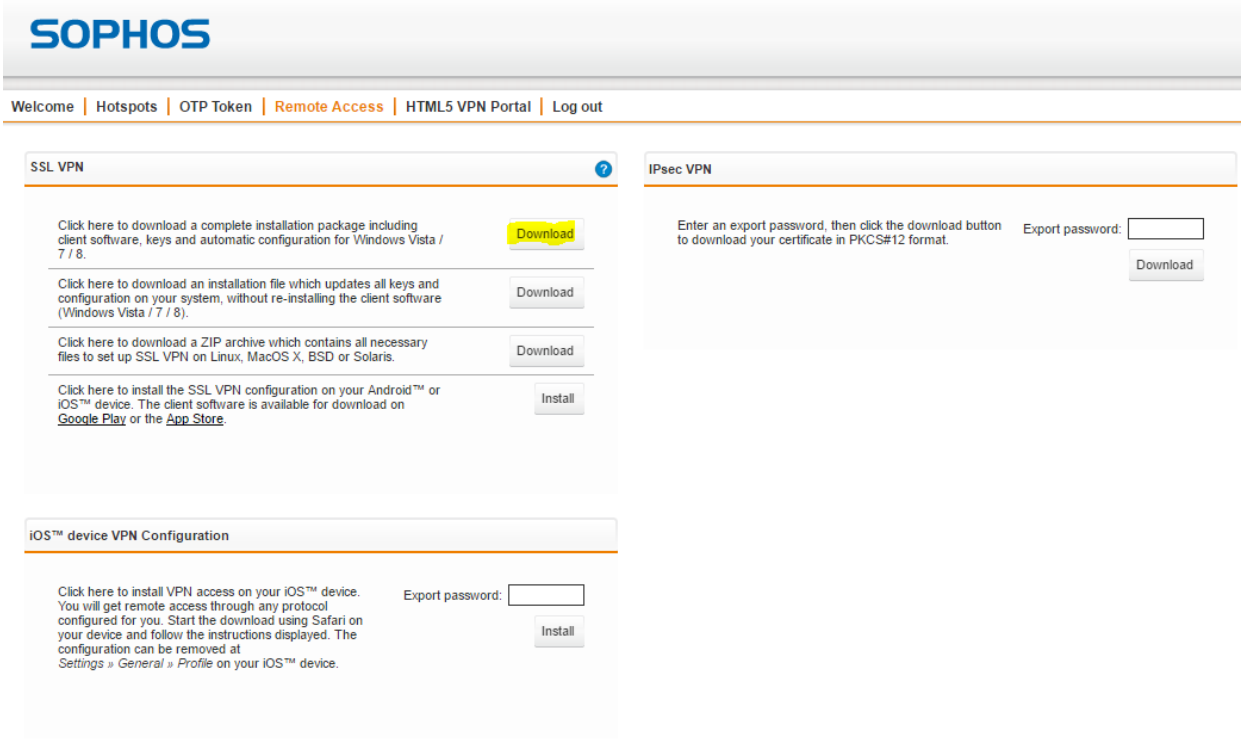
Sophos UTM-palomuuri mahdollistaa helposti turvallisten etäyhteyksien muodostamisen. Turvallinen yhteys on mahdollista virtuaalisen erillisverkon ansiosta, eli VPN:n (Virtual Private Network). Etäkäyttäjä muodostaa internetin yli suojatun yhteyden palomuurille, jonka jälkeen käyttäjä pystyy käyttämään resursseja ja palveluita. VPN-yhteyttä käyttämällä käyttäjä voi käyttää turvallisesti verkkoa, vaikka käytössä olisi jokin julkinen tai salaamaton langaton verkko.

VPN-yhteydet voidaan toteuttaa useammalla eri tunnelointiprotokollalla.



Kuva 23. SSL VPN -ohjelman kirjautumisruutu

SSL protokollan avulla muodostaminen onnistuu Sophoksen tarjoamalla SSL VPN -ohjelmalla tai mahdollisesti OpenVPN-lähdekoodin ohjelmien avulla. Kuvassa 23 näkyvän, että SSL VPN -ohjelman pystyy lataamaan palomuurin käyttäjäportaalista. Ensiksi määritellään SSL-profiili, jossa luodaan käyttäjät, jotka voivat käyttää yhteyttä, määritellään verkot, joita käyttäjän on mahdollista käyttää VPN-yhteyden avulla. Tunnelin muodostamisessa käytettävät salausasetukset määritellään asetuksissa. Käyttäjät voidaan luoda paikallisesti tai tuoda Active Directorysta, eDirectorysta, LDAPsta, Tacacs+sta tai Radiuksesta.



Kuva 24. Sophos User Portal

Kuva 24 on Sophoksen käyttäjäportaalista, jonne käyttäjät pääsevät kirjautumaan tunnuksillaan, voidaan ladata VPN-ohjelma. Ohjelma sisältää konfiguraatiotiedoston, ja

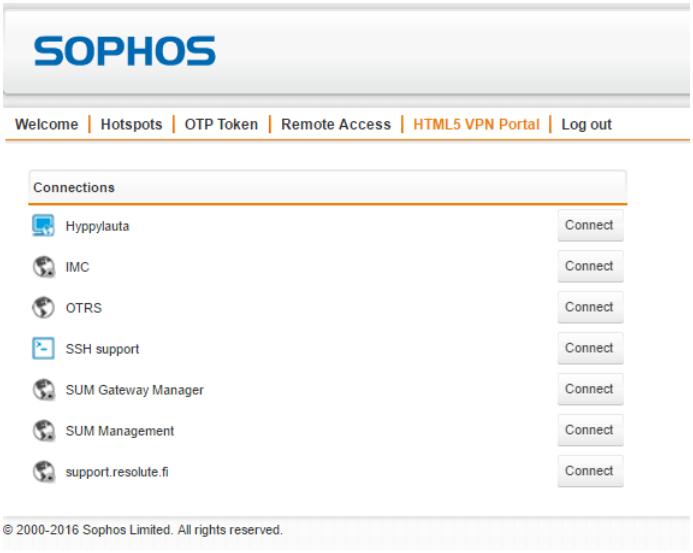
jonne on määritelty, mihin resursseihin käyttäjä pääsee. Jos VPN-asetuksiin tehdään muutoksia, niin käyttäjäportaalista voidaan ladata pelkkä konfiguraatiotiedosto, jonka ajamalla saa VPN-yhteyden taas toimimaan.

PPTP eli point to point tunneling protocol, tarkoittaa yksinkertaisuudessaan kahden pisteen välistä salattua tunnelia. PPTP-etäyhteys tukee ainoastaan todennusta paikallisesti tai käyttämällä Radiusta. PPTP-etäyhteyden käyttäminen ei vaadi erillistä asiakasohjelmaa, vaan yhteys voidaan muodostaa suoraan Windows-koneelta tai iOS-laitteelta palomuurille.

L2TP over IPsec on kahden protokollan yhdistelmä. L2TP on lyhenne toisen kerroksen tunnelointiprotokollasta. OSI-viitemallin toisella kerroksella liitetään kaksi pistettä toisiinsa, mutta ei voida taata luotettavuutta. Silloin tarvitaan IPsec-protokollan tuomaa todentamista, luotettavuutta ja yhtenäisyyttä. Yhteys toimii samaa tapaan kuin PPTP, mutta kulkee IPsec salatun tunnelin lävitse. Yhteys luodaan määrittelemällä rajapinta, johon otetaan yhteyttä etäyhteyttä muodostaessa, käytettävä todennusmenetelmä ja sertifikaatti. Käyttäjien todentaminen on mahdollista paikallisesti ja Radiuksesta.

IPsec-menetelmällä voidaan toteuttaa myös käyttäjien etäyhteyksiä. Määritellään IPsec-etäyhteyden nimi ja käytettävä oletusyhdyskäytävä. Asetuksissa määritellään, mitkä verkot ovat käytettävissä etäyhteydellä. Etäyhteyden salausmenetelmä ja salausavaimen tyyppi valitaan.

HTML5 VPN Portal on käyttäjäportaalista löytyvä ominaisuus, jonka avulla voidaan ottaa yhteys palomuurilla määriteltyihin palveluihin. Käyttäjäportaaliin voidaan määritellä RDP-yhteyksiä Windows-koneille ja VNC-yhteyksiä Linux-koneille sekä yhteyksiä selainpohjaisiin webohjelmiin, jotka käyttävät http- tai https-protokollaa. Mahdollista on myös määritellä Telnet- ja SSH-yhteyksiä määriteltyihin kohteisiin käyttäjäportaalin kautta.



Kuva 25. HTML 5 VPN Portal

Kuvan 25 mukaan palomuurilla on määritelty Remote Desktop -palvelu Hyppylauta-kohteeseen, SSH-yhteys SSH Support -kohteeseen, ja loput palvelut ovat selaimessa käytettäviä palveluita.

Ciscon VPN-ohjelman käyttäminen on myös mahdollista. Yhteydelle määritellään käytettävät sertifikaatit sekä etäyhteyden käytettävät verkot ja käyttäjät.

4 Sophos yrityksenä

Jan Hruska ja Peter Lammer tapasivat Oxfordissa noin 1980-luvun puolivälissä ja perustivat yrityksen nimeltä Sophos. He valmistivat oman kannettavan tietokoneen, mutta se ei päätynyt ikinä myyntiin, koska tietokoneet ja niiden käyttö olivat tuolloin harvinaisempia sekä valmistuskustannukset olivat liian suuret. Sen sijaan he päättivät kehittää salausmenetelmiä yhteisesti käytössä olevien tietokoneiden tietoturvan parantamiseksi. Yrityksen ensimmäinen virustorjuntaohjelmisto julkaistiin vuonna 1989. [4; 5; 6.]

Salausohjelmia ja virustorjuntaohjelmistoja tehnyt yritys on kasvanut ajan myötä yhdeksi nykypäivän noteeratuimmista tietoturvayrityksistä. Vuonna 2015 yrityksen palkkalistoilla on noin 2500 ihmistä, ja yrityksen liikevaihto on 450 miljoonaa dollaria. Yritys on menestynyt erinomaisesti useammalla eri Gartner-neljänneksillä. Syyskuun 2015 Gartner UTM -neljänneksessä Sophos on johtajasarakkeessa. Edellä ovat ainoastaan Checkpoint ja Fortinet. Sophos on Gartner-analyysin mukaan oivallinen vaihtoehto pie-

nimmille ja keskisuurille yrityksille. Järkevän hintatason, helpon käyttöliittymän ja päätelaitteiden integraation lisäksi Sophoksen tukipalvelu on asiantuntevaa ja palvelua saa useammalla eri kielellä.

Kuva 26. Gartner UTM:n neljännes

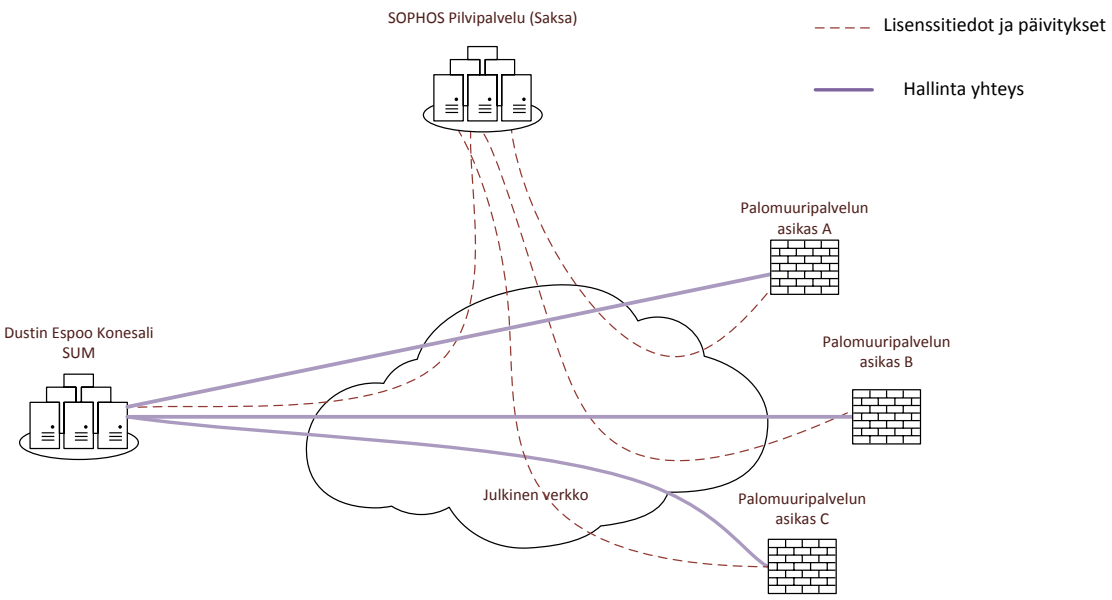
Päivitetystä Gartnerista vuodelta 2016 nähdään, että Sophos on edelleen merkittävä UTM-valmistaja.

5 Palomuuri palveluna

Dustin Finland Oy tarjoaa yrityksien tietoturvaratkaisuksi palomuuripalvelua. Tietoturvan takaa palomuurin oikeanlainen konfigurointi sekä säännöllinen ja ammattimainen ylläpito.

Palvelun hinnoittelu on asiakaskohtaista, ja hinta muodostuu eri tekijöistä. Hintaan vaikuttavat valittu laitemalli, lisensoidut ominaisuudet, vaste-aika ja asiakkaan tarpeet, esimerkiksi kuinka paljon muutoksia joudutaan tekemään kuukaudessa.

Palvelun palomuurit liitetään SUM-hallintajärjestelmään, joka sijaitsee Dustin Finland Oy:n konesalissa Espoossa. SUM-hallintajärjestelmän kautta palomuureista saadaan tietoa laitekohtaisesti, sekä niiden hallintaan päästään käsiksi. Hallintajärjestelmästä voidaan ladata ja asentaa ohjelmistopäivitykset sekä sammuttaa ja käynnistää uudelleen palomuurit.



Kuva 27. SUM-hallinta ja palvelun palomuurit

Sääntömuutokset tehdään asiakkaan tekemien tikettien perusteella, jonka ansiosta voidaan seurata, kuinka paljon sääntömuutoksia on tehty ja mitä muutoksia on tehty. Tiketteihin reagoidaan sovitun vasteajan puitteissa.

Asiakkaan kanssa pidetään kaksi kertaa vuodessa palaveri, jossa käydään läpi asiakkaan palomuurin toimintaan liittyviä asioita. Raportoidaan mahdolliset ongelmat ja käydään läpi parannusehdotukset sekä mahdolliset asiakkaan verkon toiminallisuuteen liittyvät muutokset.

Palvelusta on tarjolla kolme erilaista pakettia, jotka Mini, Medi ja Maxi. Palvelupaketit on suunniteltu käyttäjämäärien mukaan, mutta räätälöitävissä asiakkaan tarpeiden mukaan.

Mini-palomuuripalvelu sopii yrityksille, joilla käyttäjämäärä on alle 50 henkilöä, eikä verkon toiminta ole yrityksen toiminnan kannalta kriittistä. Mini-palomuuripalvelu toteutetaan Sophos SG135 -laitteella. Laite on pienikokoinen ja voidaan asentaa sekä pöydälle että laitekaappiin.

Kuva 28. Sophos SG135 edestä ja takaa

Medi-palomuuripalvelu on tarkoitettu yrityksille, joiden käyttäjämäärä on 50–150 käyttäjän välillä ja verkon toiminta on yrityksen toiminnan kannalta tärkeää. Medi-palomuuripalvelu toteutetaan Sophos SG230 -laitteella. Laite kahdennetaan, jotta verkon toiminta taataan ongelmatilanteissakin.

Kuva 29. Sophos SG230 edestä ja takaa

Max-palomuuripalvelu on suunnattu yrityksille, joilla käyttäjämäärä ylittää 150 käyttäjää ja verkon toiminta on yrityksen kannalta kriittistä. Tämä palvelu soveltuu esimerkiksi yrityksille, jotka tuottavat palveluita verkkoon muiden käytettäväksi. Maxi-palomuuripalvelu toteutetaan Sophos SG330 -laitteella. Laite kahdennetaan, jotta verkon toiminta taataan ongelmatilanteissakin.

Kuva 30. Sophos SG330 edestä ja takaa

Palvelupaketin valinnan jälkeen suunnitellaan asiakkaan verkon tarpeiden ja vaatimusten mukaan palomuurin säännöt ja muut ominaisuudet. Palvelun palomuurin toiminnallisuus voidaan rakentaa täysin tyhjältä pöydältä, jos asiakkaalla ei ole ennestään palomuuria, jonka säännöt ja ominaisuudet luotaisiin uudelle palomuurille. Seuraavassa luvussa käydään läpi palomuuripalvelun nykytilanne, palomuuripalvelunprosessit ja tulevaisuuden näkymät.

5.1 Palvelun nykytilanne

Palomuuripalveluun kuuluu perusominaisuuksia ja lisäominaisuuksia. Kun asiakas ottaa palomuuripalvelun laaditaan tietoturvasuunnitelma ja valitaan palomuurilaite suunnitelman pohjalta. Sen jälkeen tehdään laitteiden asennukset asiakkaan tiloihin. Asennuksen yhteydessä tehdään palomuurin peruskonfigurointi ja alkuperäisasetusten varmuuskopiointi. Palomuuripalvelun laitteet ovat etävalvonnassa vuorokauden ympäri.

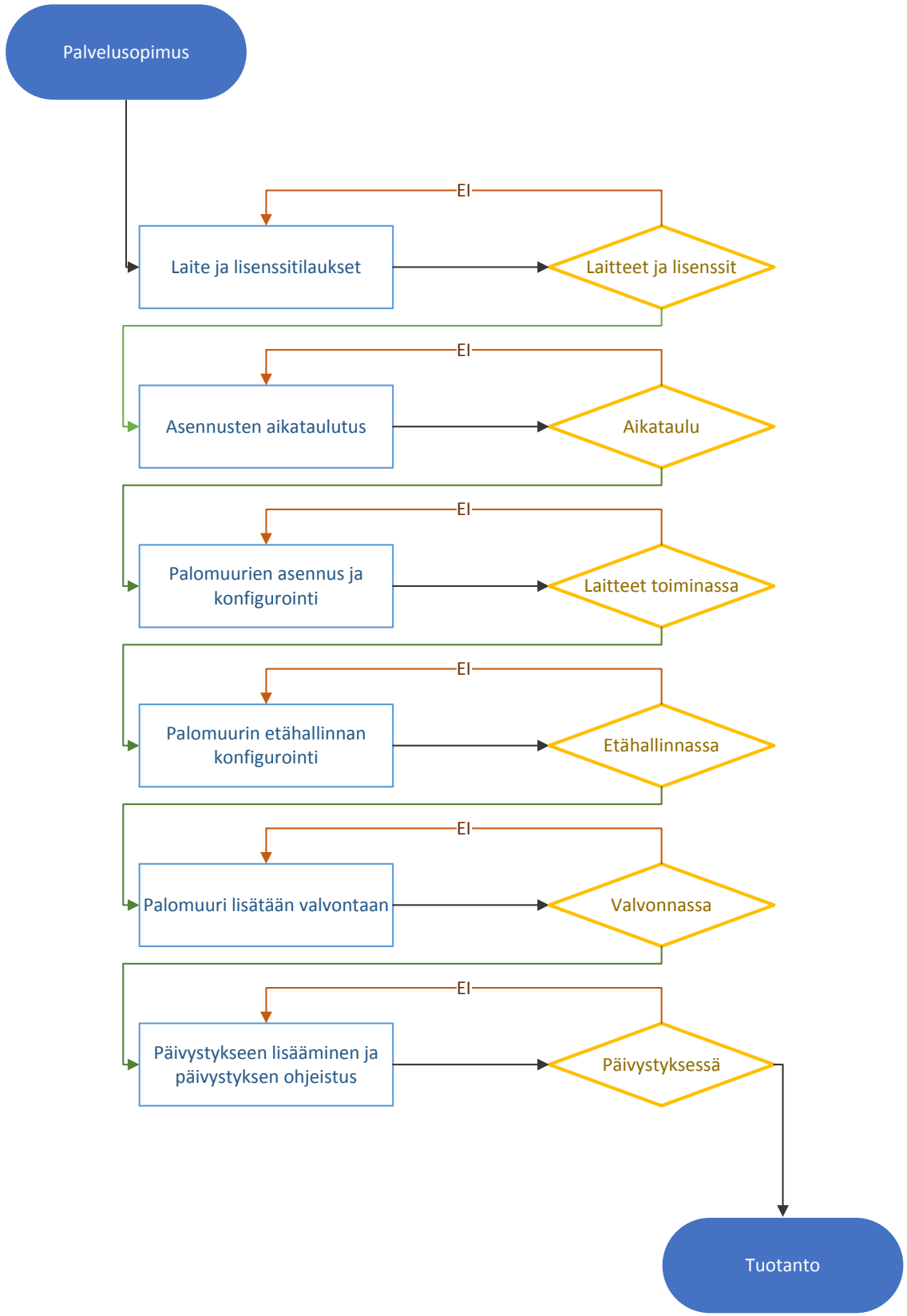
Palomuuripalvelun perusominaisuuksiin kuuluu rajallinen määrä konfiguraation muutoksia yhden työpäivän vasteajalla. Erittäin nopea vaste-aika ja useammat konfiguraation muutokset on mahdollista ottaa lisäpalveluilla. Perusominaisuuksiin kuuluu myös rikkoutuneen laitteen vaihto ja asetusten palautus sekä IP-osoitteisiin ja protokollaan perustuva liikenteen suodatus.

Lisäominaisuuksina palomuuripalvelussa voidaan toteuttaa liikenteen priorisointia, ohjelmakohtaista rajoittamista ja etäyhteyksiä. Turvalliset etäyhteydet voidaan toteuttaa asiakkaan eri toimipisteiden palomuurien välillä VPN-tekniikalla. Asiakkaan työntekijöiden on mahdollista työskennellä toimiston ulkopuolella ja käyttää verkon resursseja, kun päätelaitteilla käytetään VPN-ohjelmaa, jonka yhteys tunneloidaan palomuurille.

5.2 Palveluprosessit

Asiakkaan ottaessa palomuuripalvelun tehdään palvelusopimus. Palvelusopimuksessa määritellään palvelun tilaaja ja tuottaja sekä näiden vastuuhenkilöt. Palvelusopimuksessa määritellään myös sopimusehdot, joita palvelu pitää sisällään, ja vasteajat, joiden puitteissa toimitaan. Palvelusopimus on liitteessä (1).

Palvelusopimuksen jälkeen toimitaan seuraavana esitetyn prosessikaavion mukaisesti.



Kuva 31. Palvelun prosessikaavio

Laite ja lisenssitilaukset on ensimmäinen tehtävä toiminto prosessikaaviossa, kun palvelusopimus on solmittu. Asiakkaan valitseman palvelun mukaiset laitteet tilataan jälleenmyyjältä ja varmistetaan, että valittuja palomuurin ominaisuuksia varten tilataan lisenssit. Kun laitteet ja lisenssit on tilattu ja toimitus päivämäärä on selvillä, voidaan siirtyä seuraavaan vaiheeseen.

Prosessikaavion seuraava vaihe on asennusten aikataulutus. Asiakkaan kanssa neuvotellaan ajankohta fyysisille laiteasennuksille sekä palomuurisääntöjen luomiselle. Jos asiakkaalla on vanha palomuuri käytössä, niin on ensiksi suoritettava vanhojen palomuurisääntöjen läpikäynti. Kun palomuurisäännöt on selvitetty ja ne on luotu palvelupalomuurille, niin asiakkaan kanssa voidaan sopia yliheitosta, eli vanhan palomuurin toiminnan siirtämistä uudelle palomuurille. Yliheiton ajankohdaksi asiakkaan on syytä varata aika, jolloin yrityksen toiminnan kannalta ei ole kriittistä, että kaikki verkon palvelut ja toiminnot eivät toimi. Sovitun ajankohdan jälkeen voidaan siirtyä seuraavan vaiheeseen.

Palomuurin asennus- ja konfiguraatiovaiheessa laite asennetaan fyysisesti asiakkaan tiloihin. Palomuurin käyttöjärjestelmä päivitetään uusimpaan versioon ja tehdään tarvittavat konfiguraatiot verkon muihin laitteisiin, jonka jälkeen määritellään palomuurisäännöt ja muut tarpeelliset ominaisuudet. Palomuurin konfiguraation yhteydessä varmistetaan laitteelle pääsy etäyhteyden avulla.

Kun palomuuri on toimintakunnossa ja etähallinnassa, niin voidaan siirtyä seuraavaan vaiheeseen, joka on palvelu palomuurin lisääminen valvontaan. Valvontaportaali kertoo laitteiden tilan ja lähettää hälytyksiä tarvittaessa.

Valvontaan lisäämisen jälkeen on tehtävä uudet päivystys ohjeet ja ilmoitettava uudesta palvelupalomuurista päivystäjäringin jäsenille. Päivystyksen ohjeistuksessa määritellään toimintaohjeet ja yhteyshenkilöt.

Palveluprosessit läpikäytyä todetaan, että palvelu on tuotannossa. Tuotannossa seurataan, että palvelun laitteet toimivat, kuten pitää, ja tarvittavat asiakaan pyynnöt käsitellään vasteaikojen puitteessa.

5.3 Palvelun kehittäminen

Palomuuripalvelun asiakkailla on tällä hetkellä mahdollisuus muuttaa asetuksia itsenäisesti, koska palomuurin hallintanäkymään ei pääse ilman tunnusten luomista. Palvelun tarkoituksena on, että asiakas ei tee itse muutoksia vaan ne tehdään asiakkaan pyynnöstä. Asiakkaita ei voida tällä hetkellä estää tekemästä muutoksia muuten kuin sopimalla, että muutoksia ei tehdä. Harkinnassa on, jätetäänkö asiakkailta kokonaan pääsy omaan palomuuriinsa, jolloin lisätään raportointia ja sääntömuutoksia.

Tulevaisuudessa palveluun otetaan käyttöön Sophos XG -sarjan palomuurit ja siirrytään pois SG-palomuureista. XG-palomuurien käyttöliittymä ja toimintaperiaate eroavat SG-palomuureista. Migraatio onnistuu tulevaisuudessa SG-palomuureista XG-palomuureille. XG-palomuurien ominaisuuksista puuttuu tällä hetkellä, joitakin tärkeitä ominaisuuksia ja sen takia palvelu toteutetaan tällä hetkellä vielä SG-palomuureilla.

XG-palomuurien tarjoamat uudet ominaisuudet otetaan tulevaisuudessa palomuuripalvelussa käyttöön. Palveluun otetaan mukaan päätelaitteiden tietoturva Sophos Endpoint Security -ohjelman avulla. Päätelaitteille asennetaan ohjelmisto, joka kommunikoi palomuurin kanssa lähettäen tietoa itsestään ja varmistaa, että laite on tietoturvallinen.

Palomuuripalvelu ja MDM-palvelu, jonka avulla hallinnoidaan älypuhelimia ja tabletteja, sulautuvat yhdeksi yhtenäiseksi palveluksi, kun laitteiden hallinta onnistuu yhdestä samasta paikasta.

6 Yhteenveto

Insinöörityöni tavoitteena oli tutustua tietoturvaan ylipäätään ja sen toteuttamiseen käytännössä Sophos-palomuureilla, joita Dustin Finland Oy tarjoaa yrityksille palomuuripalvelullaan. Tarkoitus oli oppia konfiguroimaan ja hallinnoimaan Sophos SG -palomuureja, sekä kehittää valmista palomuuripalvelua ja sen prosesseja.

Tietoturvan määritelmä ja osa-alueet käytiin läpi työn alkuosiossa. Seuraavassa osassa työtä esiteltiin Sophos UTM -palomuurit ja alaotsikoissa pureuduttiin sen ominaisuuksiin. Alaotsikoiden nimet ja järjestys ovat samat kuin palomuurin hallinnassa. Alaotsikoissa esitellään ominaisuuden teoria, tarkoitus ja toiminta. Palomuurin hallintanäkymästä otettujen kuvakaappauksien avulla on pyritty selkeyttämään, miten ominaisuus otetaan palomuurilla käyttöön. Seuraavassa osassa esitellään lyhyesti Sophos ja sen historiaa. Työn loppuosiossa käsitellään Dustin Finland Oy:n palomuuripalvelua. Palomuuripalvelun sisältö ja vaihtoehdot käsitellään alkuun, jonka jälkeen päästään palomuuripalvelun nykytilanteeseen. Palveluprosessista tehtiin työtä varten prosessikaavio, jonka eri vaiheet on selitetty. Lopuksi pohditaan, miten palomuuripalvelu tulee tulevaisuudessa muuttumaan ja kehittymään.

Työn tavoitteet muovautuivat työtä tehdessä ja palvelun kehittämisen tarpeen kasvaessa. Palomuuri palveluna oli valmiiksi olemassa, joten yksi työn tärkeimmistä päämääristä oli kuitenkin kehittää omaa osaamista, jotta työtehtävien hoito palomuuripalvelun parissa onnistuisi. Työn avulla oma osaaminen Sophos SG-palomuureista on kasvanut ja palomuuripalvelun prosessit selkeytyneet. Työssä olisi ollut hyvä käsitellä myös uuden Sophos XG -palomuurilinjan laitteita, mutta meillä ei ole vielä laitteita, joten se ei ollut mahdollista.

Vaikka työssä käsiteltiin vain yhden laitevalmistajan yhtä palomuuri-mallia, niin uskon, että työ on antanut hyvät perusteet muidenkin valmistajien palomuurilaitteiden hallinnoimisille.

Lähteet

1 Tom Thomas. 2005 Verkkojen tietoturva, Helsinki: Edita Prima Oy.

2 Ari Andreasson & Juha Koivisto. 2013 Tietoturvaa toteuttamassa, Tallinna: AS Pakett.

3 Mika Hakala, Mika Vainio & Olli Vuorinen. 2006 Tietoturvallisuuden käsikirja, Porvoo: WS Bookwell.

4 Sophos 2016. Wikipedia. Verkkodokumentti https://en.wikipedia.org/wiki/Sophos Luettu 27.10.2016.

5 Sophos 2010, Naked security. Verkko dokumentti. https://nakedsecurity.sophos.com/2010/11/04/sophos-early-years/ Luettu 27.10.2016.

6 Sophos. Telegraph. Verkkodokumentti. http://www.telegraph.co.uk/finance/newsbysector/banksandfinance/privateequity/11562496/Sophos-founders-to-share-250m-from-upcoming-flotation.html Luettu 27.10.2016

7 Gartner Magic Quadrant for UTM 2016. Verkkodokumentti. https://www.gartner.com/doc/reprints?id=1-3GF1X4X&ct=160830&st=sb . Luettu 20.9.2016.

8 Sophos UTM manual. Verkkodokumentti. https://www.sophos.com/en-us/medialibrary/PDFs/documentation/utm9400_manual_eng.pdf?la=en Luettu 27.10.2016.

9 IETF SMTP-verkkodokumentti. https://www.ietf.org/rfc/rfc2821.txt . Luettu 23.9.2016.