TEKNIIKKA JA LIIKENNE

Tietotekniikka

Tietoverkot

INSINÖÖRITYÖ

CLAVISTER SECURITY GATEWAY JA KÄYTÄNNÖN TOTEUTUS TRANSPARENTTINA PALOMUURINA

Työn tekijä: Hannu Virtanen
Työn valvoja: Janne Salonen
Työn ohjaaja: Matti Nykyri

Työ hyväksytty: 26.2.2009

Janne Salonen
yliopettaja

Metropolia

ALKULAUSE

Tämä insinöörityö tehtiin IT-palvelualan yritys DT-Link Oy:lle. DT-Linkiä kiitän mahdollisuudesta tehdä heille tämä insinöörityö. Kiitän myös työn ohjaajana toiminutta järjestelmäpäällikkö Matti Nykyriä ja valvojana toiminutta koulutusohjelmavastaava Janne Salosta hyvästä yhteistyöstä, joiden ansiosta työ valmistui. Lisäksi kiitän Aleksi Peltosta, jonka ansiosta tutustuin kyseiseen yritykseen ja toimitusjohtaja Heikki Nykyriä rakentavista ideoista koskien tätä työtä.

Helsingissä 8.2.2009

Hannu Virtanen

Metropolia

TIIVISTELMÄ

Työn tekijä: Hannu Virtanen

Työn nimi: Clavister Security Gateway ja käytännön toteutus transparenttina palomuurina

Päivämäärä: 8.2.2009 **Sivumäärä:** 63 s. + liite

Koulutusohjelma: Tietotekniikka

Suuntautumisvaihtoehto: Tietoverkot

Työn valvoja: yliopettaja Janne Salonen

Työn ohjaaja: järjestelmävalvoja Matti Nykyri

Tämän insinöörityön tarkoitus oli tutkia Clavister Security Gatewayn toiminnallisuutta. Työ perustuu kirjallisuustutkimukseen ja käytännön toteutusten suorittamiseen. Tarkoituksena oli kuvailla, mitä työssä tehtiin ja selittää miksi.

Palomuureja on kolmenlaisia: tilattomia ja tilallisia sekä sovellustason yhdyskäytävää käyttäviä. Lisäksi palomuurit voivat yhdistellä näitä ominaisuuksia, kuten Clavister Security Gateway kykenee tekemään.

Security Gatewayn ytimessä on CorePlus, joka toimii Gatewayn ydinkäyttöjärjestelmänä. Security Gateway sisältää paljon muitakin ominaisuuksia kuin vain palomuurina toimimisen. Näitä ominaisuuksia ovat esimerkiksi reititys, NAT, VPN, virustentorjunta, liikenteen hallinta, tunkeutumisen havainnointi ja estäminen, web-sisällönsuodatus, käyttäjän autentikointi ja korkea saatavuus. Clavister Security Gateway onkin ns. xUTM-palomuuri. Security Gatewayn käyttöä voidaan tehostaa erillisillä ohjelmilla, kuten FineTunella, InSightilla ja PinPointilla. Näillä ohjelmilla voi mm. tehokkaasti hallita ja monitoroida CorePlussaa. Clavister Security Gateway -tuoteperhe koostuu monen erilaisen Security Gateway laitetoteutuksen lisäksi ohjelmatoteutuksista tietokoneille ja virtuaalitoteutuksista VMWare ESXi -palvelimelle.

Tässä työssä transparentti palomuuri toteutettiin kahdella tavalla, joista ensimmäinen toteutettiin oikeassa transparentissa tilassa ja toinen Proxy ARP:in avulla. Transparenteilla palomuureilla verkkoliikennettä voidaan tutkia ja suodattaa tarpeen mukaan ilman, että siitä on käyttäjälle haittaa tai verkkoa jouduttaisiin muuttamaan. Työ osoittaa, että molemmilla toteutuksilla on omat etunsa. Esimerkiksi oikea transparentti tila on helppo toteuttaa ja sille on olemassa erityisiä tilalle tarkoitettuja konfiguroitavia parametreja, kun taas Proxy ARP puolestaan mahdollistaa HA-klusteroinnin. Verkon asettamat vaatimukset määrittävät, mikä transparentti palomuuri on verkolle sopivin.

Avainsanat: palomuuri, clavister, transparent, coreplus, security gateway, xUTM, HA

Metropolia

ABSTRACT

Name: Hannu Virtanen

Title: Clavister Security Gateway and Its Implementation As a Transparent Firewall

Date: 8.2.2008 **Number of pages:** 63 + appendix

Department: **Study Programme:**

Information Technology Data Networks

Instructor: Janne Salonen, Principal Lecturer

Supervisor: Matti Nykyri, System Manager

The purpose of this final project was to examine a firewall called Clavister Security Gateway for its functionalities. This study is based on researching current literature and executing practical implementations. The objective was to describe what experiments were made and explain why.

There are three types of firewalls: stateless, stateful and application layer gateways. In addition, firewalls are capable of combining the different types as Clavister Security Gateway is capable of making.

Inside the Security Gateway lies CorePlus which is the core operating system for the device. The Security Gateway contains many more features than the mere firewall function. These features include for example Routing, NAT, VPN, Anti-Virus, Traffic Management, Intrusion Detection and Prevention, Web Content Filtering, User Authentication and High Availability. Clavister Security Gateway is often called xUTM firewall. The use of the Security Gateway can be further improved with programs like FineTune, InSight and PinPoint. With these programs, CorePlus can be managed and monitored more efficiently. The Clavister Security Gateway product family consists of three kinds of Security Gateway series. The series includes both conventional hardware and software appliances as well as a virtual appliance using VMware ESXi.

In this study, a transparent firewall was implemented in two ways, i.e. by using the real transparent mode and with Proxy ARP. With the former, network traffic can be investigated and filtered if needed without the user noticing it and it will not cause any changes to the network infrastructure. The study shows that both implementations have their benefits. For example the real transparent mode is easy to implement and has many specific configurable parameters while Proxy ARP allows the use of HA cluster. The network requirements determine which transparent firewall is better.

Keywords: firewall, clavister, transparent, coreplus, security gateway, xUTM, HA

SISÄLLYS

LYHENTEITÄ JA MÄÄRITELMIÄ

3DES	Triple Data Encryption Standard. Salausmenetelmä, joka käyttää tiedonsalausstandardia kolmesti. Avaimienkäyttö vaihtelevat eri versioissa.
ALG	Application Layer Gateway. Sovellustason yhdyskäytävä
ARP	Address Resolution Protocol. selvittää IP-osoitetta vastaavan MAC-osoitteen.
CA	Certificate Authority. Luotettu digitaalisten sertifikaattien myöntäjä.
CBC	Cipher-Block Chaining. Alueiden ketjutuksessa jokainen alue käydään XOR:illa läpi edellisen salakirjoitetun alueen kanssa ennen salausta.
CHAP	Challenge-Handshake Authentication Protocol. PPP:n päällä toimiva autentikointiprotokolla.
CLI	Command-Line Interface. Komentorivipohjainen käyttöliittymä.
DB	Database. Tietokanta.
DDoS	Distributed DoS. Hajautettu palvelunestohyökkäys.
DHCP	Dynamic Host Configuration Protocol. Käytetään jakaman käyttäjille automaattisesti IP-asetukset.
DNS	Domain Name System. Nimipalvelujärjestelmä, joka muuntaa verkkotunnuksia IP-osoitteiksi.
DMZ	Demiliratized Zone. Demilitarisoitu alue on alue, joka on palomuurilla suojattu ulkomaailmalta, mutta josta ei silti voi ottaa suoria yhteyksiä lähiverkkoon turvallisuuden parantamisen vuoksi.
DoS	Denial of Service. Palvelunestohyökkäys.
DSField	Differentiated Service Field. Kenttä. jossa sijaitsevat paketin DSCP-bitit.
DSCP	Differentiated Service Codepoint. Kenttä IP-paketin tunnisteessa, jota käytetään paketin luokittelemiseen.
DV	Distance Vector. Etäisyysvektori.
ESP	Encapsulation Security Payload. Osa IPsecin protokollapinoa.
GRE	Generic Routing Encapsulation. Ciscon kehittämä IP-tunnelointiprotokolla.
HA	High Availability. Korkea saatavuus.
H.323	ITU-T:n standardi signalointiprotokolla, joka määrittelee videoneuvotteluyhteyksien protokollan pakettiverkkokäyttöön.
HTTPS	Hypertext Transfer Protocol Secure. Salauksella varustettu hypertekstin siirtoprotokolla, jossa tiedot salataan SSL:llä tai TLS:llä ennen lähettämistä.

ICMP	Internet Control Message Protocol. Käytetään kontrolloimaan TCP/IP-pinoa ja tomii IP:n päällä.
IDS	Intrusion Detection System. Tunkeutumisen havainnointijärjestelmä.
IDS	Intrusion Detection Signatures. Tunkeutumisen havaitsemissigneeraukset.
IGMP	Internet Group Management Protocol. TCP/IP-pinon protokolla, joka mahdollistaa liittymisen multicast-ryhmään.
IPS	Intrusion Prevention Signatures. Tunkeutumisen estosigneeraukset.
ISP	Internet Service Provider. Internet-yhteydentarjoaja.
L2TP	Layer 2 Tunneling Protocol. Mikrosoftin ja Ciscon kehittämä tasolla kaksi toimiva tunnelointiprotokolla.
LDAP	Lightweight Directory Access Protocol. Hakemistopalvelujen käyttöön tarkoitettu protokolla.
LS	Link State. Linkin tila.
MD5	Message-Digest Algorithm 5. Kryptograafinen tiivistefunktio.
NAT	Network Address Translation. Dynaaminen verkko-osoitteiden muunnostekniikka, jota käytetään muuntamaan osoitteita sisäverkon ja ulkoverkon välillä.
NAT-T	NAT Traversal. Metodi, jolla IPsecillä suojatut datagrammit saadaan NAT:in ohi.
OSI	Open Systems Interconnection Basic Reference Model. Kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemässä kerroksessa.
OSPF	Open Shortest Path First. Reititysprotokolla.
PAP	Password Authentication Protocol. PPP:n päällä toimiva autentiokointiprotokolla.
PAT	Port Address Translation. Porttien muuntamiseen käytetty tekniikka.
PIM	Protocol Independent Multicast. Protokolla riippumaton ryhmälähetys.
POP3	Post Office Protocol Version 3. Sähköpostin hakuprotokolla.
PPP	Point-to-Point Protocol. Käytetään muodostamaan suora yhteys laitteiden välille.
PPPoE	PPP over Ethernet. Käyttää PPP:tä yhteyden muodostuksessa ethernetin yli.
PPTP	Point-to-Point Tunneling Protocol. Käytetään muodostamaan tunneli laitteiden välille.
QoS	Quality of Service. Palvelun laatu.

RADIUS	Remote Authentication Dial In User Service. Käytetään autentikoinnissa.
RC	Rivest Cipher. Ron Rivestin suunnittelemia salausmenetelmiä, joihin kuuluvat RC2, RC4, RC5 ja RC6.
RIP	Routing Information Protocol. Reititysprotokolla.
RSA	Epäsymmetrinen julkisen avaimen salausalgoritmi.
RST	Reset. Nollata.
SAT	Static Address Translation. Staattinen verkko-osoitteiden muunnostekniikka, jota käytetään muuntamaan osoitteita sisäverkon ja ulkoverkon välillä.
SCP	Secure Copy. Isäntien väliseen tiedostojen siirtoon.
SHA	Secure Hash Algorithm. Kryptograafinen tiivistefunktio.
SIP	Session Initiated Protocol, Signalointiprotokolla, jota käytetään multimediayhteyksissä.
SLB	Server Load Balancing. Palvelimen kuormanjako.
SMTP	Simple Mail Transfer Protocol. Protokolla sähköpostiviestien välittämiseen.
SSL	Secure Socket Layer. Käytetään suojaamaan siirtokerroksen liikennettä.
SSP	Security Service Platform. Turvallisuuspalvelualusta.
TCO	Total Cost of Ownership. Gartnerin TCO-mallia käytetään yritysten IT-hankintojen kustannusten ja palvelutason kokonaisvaltaiseen arvioimiseen.
TCP	Transmission Control Protocol. Tietoliikenneprotokolla yhteyksien luomiseen tietokoneiden välille, joilla on pääsy internetiin.
TFTP	Trivial File Transfer Protocol. Yksinkertainen tiedostonsiirtoprotokolla.
TLS	Transport Layer Security. Käytetään suojaamaan siirtokerroksen liikennettä.
UDP	User Datagram Protocol. Yhteyskäytäntö viestien lähetykseen.
URL	Unified Resource Locator. Käytetään osoittamaan WWW-sivuja.
VLAN ID	Virtual LAN Identification. Virtuaalisen lähiverkon identifikaatti.
VPN	Virtual Private Network. Virtuaalinen yksityisverkko
WebUI	Web User Interface. Web-pohjainen käyttöliittymä.
XAUTH	X Window Authorization. X-ikkunoinnin valtuutustapa.
XOR	Exclusive or. Poissulkeva tai on looginen operaatio.
xUTM	Extended Unified Thread Management. Monipuolisten palomuurien kutsumanimi, jotka lisäksi kykenevät suureen suoritustehoon.

1 JOHDANTO

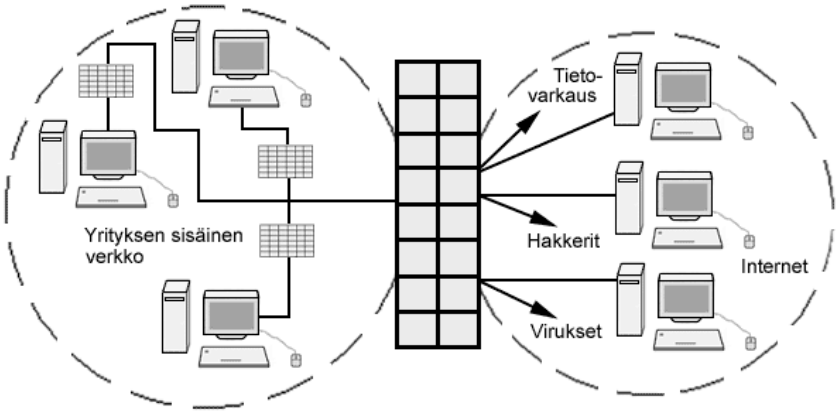
Palomuuri on verkolle lähes pakollinen, jos verkko on yhteydessä ulkoverkkoon ja siitä halutaan turvallinen. Ilman palomuuria verkon käyttäjät ovat hyvin alttiita erilaisille verkkohyökkäyksille, jotka etsivät ja käyttävät haavoittuvuuksia hyväkseen. Palomuuri tuo tätä turvallisuutta verkkoon eliminoimalla näitä erilaisia verkkohyökkäyksiä. Nykyään palomuurilaitteet sisältävät myös muita verkontoimintaan liittyviä ominaisuuksia kuin pelkän palomuuritoiminnon suoritustehon pysyessä silti hyvänä.

Tämä työ koostuu kahdesta osasta, joista ensimmäinen koostuu luvuista kaksi ja kolme sekä jälkimmäinen käsittää luvun neljä. Toisessa luvussa käydään läpi erilaisia palomuurityyppejä ja niiden perustoimintaperiaatteita. Luvussa kolme esitellään tarkemmin käytännöntoteutuksessa käytettävä laite: mikä se on ja mihin se pystyy. Laitteesta esitellään mm. siinä käytettävän ytimen toimintaa ja sen tärkeimpiä ominaisuuksia, siihen saatavilla olevia lisäohjelmia ja saatavilla olevien laitteiden ominaisuudet. Neljännessä luvussa toteutetaan transparentti palomuuri käytännössä Clavister Security Gatewayllä kahdella eri tavalla. Ensimmäisessä toteutuksessa käytetään aitoa transparent-tilaa ja toisessa toteutuksessa transparenttisuus toteutetaan Proxy ARP:in avulla. Proxy ARP toteutuksessa on se hyöty, että voidaan hyödyntää HA-klusterointia, mikä ei onnistu aidossa transparent-tilassa. HA-klusterointi on otettu mukaan toiseen toteutukseen. CorePlussan esittelyssä on käytetty version 9.10 aineistoa ja toteutuksessa käytetyissä laitteissa versiona on 8.90.

2 PALOMUURI JA TIETOTURVA

Palomuuriratkaisu voidaan toteuttaa joko ohjelmallisesti tai sitten erillisellä laitteella. Tietoturvan kannalta ajateltuna on aina riskialtista kytkeä tietokone avoimeen verkkoon ilman, että siinä on palomuuri toiminnassa. Palomuurin päätehtävänä on tutkia ja valvoa verkossa tapahtuvaa liikennettä ja siten suojata sisäverkkoa estämällä ulkoverkosta tulevia hyökkäyksiä. Myös liikennettä sisäverkosta ulkoverkkoon voidaan rajoittaa. Palomuurilla voi lisäksi rajata sisäverkosta haluttuja alueita, kuten kuvassa 1 on tehty. Esimerkiksi sairaaloissa voidaan haluta rajata potilastietokanta muusta verkosta erilleen sen sisältämän luottamuksellisen tiedon takia. Jos kuvan 1 tapauksessa ky-

seessä olisi esimerkin sairaala, ulkoverkon koneet olisi erotettu sisäverkosta palomuurilla, jolloin tuon muurin ohi pääseminen ei vielä antaisi pääsyä potilastietokantaan, koska tiedot olisivat sisäverkossa vielä toisen palomuurin takana.



Kuva 1. Palomuurit estämässä hyökkäyksiä ja segmentoimassa verkkoa. [1.]

Palomuurin täytyy täyttää tietyt vaatimukset ennen kuin siihen voidaan kunnolla luottaa. Lähtökohtana toiminnalle on se, että kaikki liikenne kulkee palomuurin kautta. Palomuurin täytyy olla itsessään immuuni tunkeutujille ja palomuurin saa läpäistä vain ennalta määritelty liikenne. [2.]

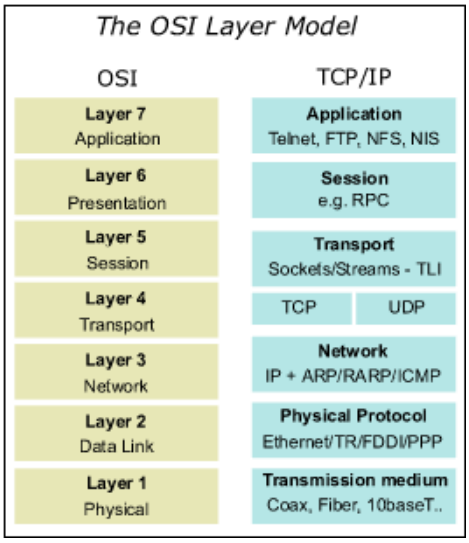
2.1 Palomuurityypit

Palomuureja on kolmea eri tyyppiä

- pakettisuodattimet
- yhteyssuodattimet
- sovellustason yhdyskäytävät (Proxy).

Tehokkaimmat palomuurit käyttävät kaikkia kolmea tekniikkaa hyväkseen päästäkseen parempiin lopputuloksiin. [3.]

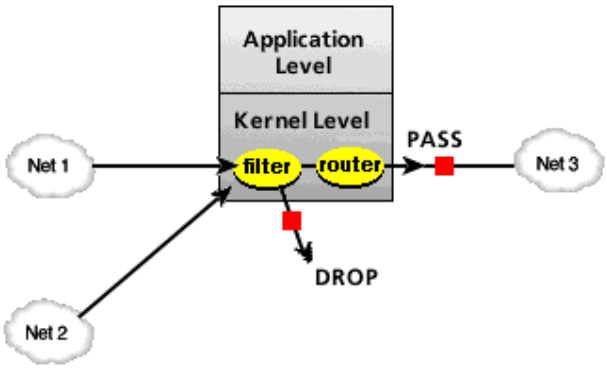
Eri palomuurityypit voidaan jaotella sen mukaan millä OSI-mallin kerroksella ne toimivat (kuva 2). Pakettisuodattimiin perustuva palomuuri toimii kerroksella kolme, yhteyssuodattimiin perustuva palomuuri toimii kerroksella viisi ja sovellustason yhdyskäytävä-tyyppinen palomuuri toimii kerroksella seitsemän. Esimerkiksi reititys tapahtuu kerroksella kolme ja käyttäjän hallinnoimat sovellukset toimivat kerroksella seitsemän. [3.]



Kuva 2. OSI-mallin eri kerrokset. [4.]

2.1.1 Pakettisuodattimet

IP-pakettien suodatus perustuu ehtoihin. Jos paketti ei täytä määrättyjä ehtoja, se hylätään. Kuvassa 3 verkoista net 1 ja net 2 tulevat paketit menevät suodattimen läpi, jossa määrätyt ehdot evaluoidaan. Läpi päässyt paketti jatkaa reitittimen kautta net 3 -verkkoon.



Kuva 3. Pakettisuodatuksen periaate. [3.]

Taulukossa 1 on kuvattu IP-paketin kenttiä, joiden arvoja verrataan pakettisuodattimessa määriteltyihin referenssiarvoihin. Arvojen pysyessä sallituissa rajoissa päästetään paketti läpi. Tämä palomuurityyppi tutkii paketteja vain yksilöinä eikä ota huomioon, mihin kokonaisuuteen paketti kuuluu. Pakettisuodatus ei myöskään ota talteen mitään informaatiota tapahtumista. Tämän vuoksi pakettisuodatinta käyttävää palomuuria sanotaan tilattomaksi palomuuriksi. Pakettisuodatukseen perustuva palomuuri ei ole yhtä turvalli-

nen kuin sovellustason palomuuri, mutta sen etuna on sen nopeus. Pakettisuodatin-tyyppisessä palomuurissa ongelmana on sen sallivuus ja se, että paluupakettien portteja ei voida kaikissa protokollissa tietää tarkasti. Sallivuus tarkoittaa sitä, että joskus ei-sallittuun istuntoonkin kuuluva paketti saattaa päästä läpi. [3.]

Taulukko 1. Pakettisuodatuksen kannalta tärkeimpiä IP-paketin kenttiä. [3.]

IP-PAKETIN KENTTÄ	TARKOITUS
Vastaanottajan IP-osoite	Palveluntarjoajan host-osoite
Lähettäjän IP-osoite	Lähettäjän host-osoite
Ylemmän tason protokolla (UDP tai TCP)	Palvelut riippuvat protokollasta
Vastaanottajan UDP- tai TCP- porttinro	Ilmoittaa palvelun, esim. HTTP tai Telnet
Lähettäjän UDP- tai TCP- porttinro	Normaalisti satunnaisluku > 1024

2.1.2 Yhteyssuodattimet

Yhteyssuodatin valvoo liikennettä jatkuvasti istunnon ajan ja estää yhteyden, jos liikenne ei ole sallittu. Tämän takia yhteyssuodatinta käyttävää palomuuria sanotaan tilalliseksi palomuuriksi. Tilallinen palomuuri pitää kirjaa TCP- ja UDP-yhteyksistä. Tilallisuutensa ansiosta se pystyy määrittelemään, mihin kokonaisuuteen paketti kuuluu tai onko se vioittunut paketti. Jos paketti kuuluu jo olemassa olevaan yhteyteen, se sallitaan. TCP-yhteyttä avattaessa tarkastetaan ensimmäisenä, onko paketti sallittu palomuurin säännöissä. Jos paketti hyväksytään, se lisätään palomuurin yhteyslistaan. Yhteyden katkettua tai tietyn ajan kuluttua tiedot pyyhkiytyvät muistista eikä kyseistä yhteyttä enää automaattisesti sallita. [3.]

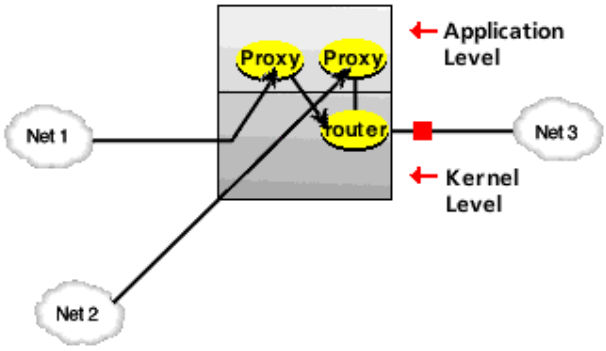
Yhteyssuodatin-tyyppinen palomuuri on rajoittava, mikä tarkoittaa sitä, että paketti ei pääse läpi ellei se kuulu hyväksyttyyn istuntoon. Ei-sallittuun istuntoon kuuluva paketti ei voi siis päästä läpi, kuten pakettisuodatin-tyyppisessä palomuurissa on mahdollista. Tuntemattomien protokollien kanssa paluupaketeilla on sama ongelma kuin pakettisuodattimisissa palomuureissa, mutta tunnetuille protokollille poikkeuksen voi lisätä. [3.]

2.1.3 Sovellustason yhdyskäytävät (Proxy)

Sovellustason palomuurit tunnetaan myös proxy- eli välityspalvelinpohjaisina palomuureina. Sovellustason palomuuri toimii TCP/IP-pinossa nimensä mukaisesti sovellustasolla, johon kuuluvat esimerkiksi WWW, telnet ja FTP-

liikenne. Sovellustason yhdyskäytävä on palvelimella toimiva ohjelma, jonka läpi kaikki tuleva ja lähtevä liikenne ohjataan. Ohjelma tutkii kaikki liikennevirrassa kulkevat paketit. Hyväksyttävät paketit voidaan määritellä melko tarkasti hyödyntäen mm. tiedon salausta päästä päähän, käyttäjän autentikointia ja tiedoston nimeen tai kellon aikaan perustuvaa suodatusta. Jokaiselle sovellukselle on oma proxynsa, esimerkiksi FTP-proxy. Kun sisäverkon kone haluaa muodostaa yhteyden ulkoverkon koneeseen, niin muodostuu tätä yhteyttä varten oma FTP-proxy-esiintymä, joka luodaan vain näiden kahden koneen tarkkailua varten. Yksi proxy-sovellus voi pyörittää montaa prosessia samanaikaisesti. [3.]

Palomuuri voi pysäyttää kaikki sovelluksesta tulevat tai sinne menevät paketit, koska kaiken liikenteen on pakko kulkea proxyn kautta, joten suora kommunikointi sisäverkosta ulkoverkkoon ohi proxyn on mahdotonta. Kuvassa 4 net 1- ja net 2- verkoista tulevat paketit menevät ensin niille tarkoitetuille proxyille, joissa ne hylätään tai niiden matka jatkuu reitittimen kautta net 3 -verkkoon. Periaatteessa sovellustason palomuurit voisivat estää kaiken ei halutun liikenteen pääsemisen suojellulle laitteella, mutta se menisi käytännössä niin monimutkaiseksi mm. sisällön vaihtelevuuden takia, että sitä ei yleensä lähdetä toteuttamaan. [3.]



Kuva 4.Liikennöinti tapahtuu proxyn kautta. [3.]

On olemassa valmiita kaupallisia sovellusyhdyskäytävä ratkaisuja, jotka sisältävät monia eri proxy-sovelluksia. Niitä valitessa kannattaa tutkia ensin, mitä proxy-sovelluksia tarvitsee. Seuraavaksi on listattu muutamia merkittävimpiä proxy-sovelluksia: [3.]

- Telnet-proxy
- WWW-proxy

- FTP-proxy
- Internetin sähköposti proxy.

2.2 Lisäpalvelut ja ongelmat

Koska kaikki liikenne kulkee palomuurin kautta, se tarjoaa mahdollisuuden verkkoliikenteen monitorointiin. Tällöin voi olla mahdollista käyttää hyväksi hälytyspalveluja ja lokitiedostoja verkkotapahtumista. Palomuuri voi myös toimia toisten verkkopalveluiden alustana, kuten NAT:in, VPN:n ja IDS:n. [5.]

Palomuuri on hyödytön, jos se onnistutaan ohittamaan tai kiertämään. Tähän voi olla syynä se, että palomuuri on huonosti konfiguroitu. Tämä voi tarkoittaa esimerkiksi sitä, että oikeasti epäluotettava ohjelma on hyväksytty luotettavaksi tai sitten portteja on avattu liikenteelle tarpeettomasti. Hyökkääjät voivat myös käyttää hyökkäyksessä hyväkseen luotetun sovelluksen mahdollista tietoturva-aukkoa. [5.]

3 CLAVISTER SECURITY GATEWAY

Clavister on ruotsalainen vuodesta 1997 toiminut IT-alan yritys, joka on keskittynyt erityisesti tarjoamaan verkko- ja tietoturvaratkaisuja sekä tuotteita. Clavisterin ja heidän laitteensa tunnistaa logosta, joka sijaitsee laitteiden vasemmassa yläkulmassa ja jonka voi nähdä kuvasta 5. Clavister Security Gateway -tuoteryhmä perustuu heidän omaan tuotemerkkiinsä, turvallisuuspalvelualusta Clavister SSP:hen. Security Gatewaytä voidaan käyttää erikseen tai yhdisteltynä mm. palomuurina, VPN-päätelaitteena, tunkeutumisen estojärjestelmänä, liikenteen hallintaan, virustentorjuntaan ja sisällön suodatukseen. Tällaista palomuuria kutsutaan usein myös xUTM-palomuuriksi sen kyetessä monipuolisuutensa lisäksi suureen suoritustehoon. Security Gatewayn sydämenä toimii CorePlus-ydin. Lisäksi siihen on olemassa joukko käyttöä tehostavia ohjelmia, kuten FineTune, InSight ja PinPoint. FineTune on ohjelma, jolla voidaan hoitaa konfigurointi ja monitorointi. InSight puolestaan on tehty turvallisuus informaation ja tapahtumien hallinnointiin. PinPoint keskittyy tietojen ja tapahtumien monitorointiin ja analysointiin. Security Gatewaystä on tehty erilaisia ratkaisuja, jotka voidaan jakaa kolmeen luokkaan. Järjestelmä toimii joko erillisenä laitteena, ohjelmana tai sitten kokonaan virtuaalisesti virtuaaliympäristössä. [6.]

Kuva 5. Clavister-yhtiön logo. [7, s. 2.]

3.1 CorePlus

CorePlus on firmwarena kaikissa Clavister Security Gateway -tuotteissa ja toimii niiden moottorina. Se on suunniteltu verkon turvallisuuskäyttöjärjestelmäksi ja sillä on korkea luotettavuus. Lisäksi se pystyy käsittelemään suuren määrän liikennettä. CorePlus integroituu saumattomasti alijärjestelmiin ja pystyy tarjoamaan perusteellisen toiminnallisuuden. Mahdollinen hyökkäyspinta on minimoitu, jotta turvallisuushyökkäysten kohteeksi joutumisen riskiä on saatu pienemmäksi. CorePlus käyttää pääasiassa tilalliseksi tarkastukseksi kutsuttua tekniikkaa, johon voi halutessa yhdistellä sovellustason yhdyskäytävän toimintoja. Myös pakettien tilaton välitys onnistuu tarvittaessa. [8, s. 14.]

3.1.1 Pakettivirta

Seuraavassa on alla kuvattuna yksinkertaistettu esimerkki pakettivirran perusperiaatteesta CorePlussassa: [8, s. 18-19.]

1. Ethernet-kehys vastaanotetaan ja validoidaan yhdessä järjestelmän Ethernet-rajapinnoista. Jos kehys ei ole validi, se hylätään.

2. Paketti assosioidaan lähderajapinnan kanssa. Lähderajapinta määritetään seuraavasti:

   - Jos Ethernet-kehys sisältää VLAN ID:n, järjestelmä etsii konfiguroitua VLAN-rajapintaa vastaavan VLAN ID:n. Jos vastaavaa rajapintaa ei löydy, paketti hylätään ja tapahtuma kirjautuu lokiin.

   - Jos Ethernet-kehys sisältää PPP-hyötykuormaa, jäjestelmä etsii vastaavaa PPPoE-rajapintaa. Jos sellainen löytyy, siitä rajapinnasta tulee lähderajapinta. Jos vastaavaa rajapintaa ei löydy, paketti hylätään ja tapahtuma kirjautuu lokiin.

   - Jos mikään yllä olevista ei toteudu, vastaanottavasta rajapinnasta tulee paketille lähderajapinta.

3. Paketin IP-datagrammi välitetään CorePlussan yhteneväisyystarkistukseen. Tarkistuksessa paketin ehjyyttä tutkitaan tarkastamalla mm. tarkistussumma, protokollaliput, paketin pituus jne. Jos yhteneväisyystarkistus epäonnistuu, paketti hylätään ja tapahtuma kirjautuu lokiin.

4. CorePlus yrittää katsoa löytyisikö olemassa olevaa yhteyttä vertailemalla sisään tulevan paketin parametreja. Vertailussa käytetään useita eri parametreja, kuten lähderajapintaa, lähde ja kohde-IP-osoitetta sekä IP-protokollaa.

5. Lähderajapinta tutkitaan, jotta tiedetään, onko rajapinta tietyn reititystaulun jäsen. Sääntöihin perustuvat reitityssäännöt käydään myös läpi , jotta yhteydelle saadaan määritettyä oikea reititystaulu.

6. Pääsysäännöt evaluoidaan, jotta saadaan selville, onko uuden yhteyden lähderajapinnan IP-osoite sallittu vastaanottavassa rajapinnassa. Jos mikään pääsy-sääntö ei täsmää, suoritetaan käänteinen reitin haku. Rajapinta hyväksyy oletuksena vain sellaiset lähde-IP-osoitteet, jotka kuuluvat rajapinnan yli reititettyyn verkkoon. Jos pääsysäännöt tai käänteinen reitin haku huomaa, että lähde-IP-osoite ei ole validi, paketti hylätään ja tapahtuma kirjautuu lokiin.

7. Suoritetaan reitin haku käyttäen siihen sopivaa reititystaulua. Yhteyden kohderajapinta on nyt määritetty.

8. Etsitään IP-säännöistä sääntöä, joka täsmää pakettiin. Seuraavat parametrit ovat osa vertailuprosessia:

    - lähde- ja kohderajapinnat
    - lähde- ja kohdeverkko
    - IP-protokolla (esimerkiksi TCP, UDP ja ICMP)
    - TCP/UDP-portit
    - ICMP-tyypit
    - kohta ajassa referenssinä ennalta määritellylle aikataululle.

Jos vertailu ei tuota tulosta, paketti hylätään.

Jos sellainen sääntö löytyy, joka täsmää uuteen yhteyteen, säännön toimintaparametri päättää, mitä CorePlussan pitäisi tehdä yhteydelle. Jos päätös on hylkää, paketti hylätään ja tapahtuma kirjautuu lokiin.

Jos päätös on hyväksy, paketti hyväksytään läpi järjestelmän. Vastaava tila lisätään yhteystauluun myöhempiä paketteja varten, jotka kuuluvat samaan yhteyteen. Palveluobjekti, joka täsmäsi IP-protokollan ja porttien kanssa, saattoi sisältää viittauksen ALG-objektiin. Tämä tieto on tallennettu tilaan, jotta CorePlus tietää, että yhteydessä täytyy suorittaa sovellustason prosessointia.

Uuden yhteyden avaus kirjautuu lokiin säännön lokiasetusten mukaan.

9. IDP-säännöt evaluoidaan samankaltaiseen tapaan kuin IP-säännötkin. Jos vertailu täsmää, IDP-data tallennetaan tilaan. Tämän ansiosta CorePlus tietää, että IDP-skannaus täytyy toimittaa kaikille kyseiseen yhteyteen kuuluville paketeille.

10. Etsitään liikenteen muokkaussääntö ja kynnysarvo rajasääntöasetuksia.

11. CorePlus tietää tilan antaman informaation ansiosta, mitä tehdä sisään tulevalle paketille:

    - Jos ALG-informaatio löytyy tai IDP-skannaus täytyy suorittaa, paketin hyötykuormasta huolehtii TCP-pseudo-uudelleenkokoamisalijärjestelmä. Analysoidakseen pidemmälle liikenteen muuttumista alijärjestelmä käyttää mm. erilaisia ohjelmistotason yhdyskäytäviä ja tason seitsemän skannausmoottoreita.

      Jos paketin sisältö on kapseloitu (esimerkiksi IPsec:llä, PPTP/L2TP:llä tai jollain muulla tunnelointi protokollalla), rajapintalistat tarkistetaan, jos löytyisi rajapinta, joka täsmää. Jos sellainen löytyy, paketin kapselointi avataan ja hyötykuorma (tavallinen teksti) lähetetään CorePlussalle uudestaan, mutta tällä kertaa

lähderajapinnan ollessa juuri täsmännyt tunnelin rajapinta. Prosessi alkaa uudestaan kohdasta kolme.

Jos liikenteen hallintainformaatio löytyy, paketti voi joutua jonoon tai voi muutoin joutua liikenteen hallintaan liittyvien toimintojen alaiseksi.

12. Paketti lähetetään edelleen kohderajapintaan tilan mukaan. Jos kohderajapinta on tunnelirajapinta tai fyysinen alirajapinta, lisätoimenpiteitä, kuten salaus tai kapselointi, saatetaan suorittaa.

Liitteessä 1 on havainnollistettu kuvien avulla paketin eteneminen CorePlussassa. [8, s. 20-23.]

3.1.2 Hallinta

CorePlussassa ylläpitäjä voi konfiguroida lähes jokaista järjestelmän yksityiskohtaa. Sen takia se sopii myös haastavampiin toimintaympäristöihin. Hallinnointirajapintoja ovat mm. Clavister InControl, WebUI, CLI, Secure Copy ja Console Boot Menu. Oletuksena CorePlussassa on paikallinen käyttäjätietokanta, jossa on kaksi ennalta määriteltyä käyttäjätiliä. [8, s. 25-40.]

Clavister InControl on erillinen tuote, jolla voidaan ylläpitää montaa Clavister Security Gatewaytä. Tuote tarjoaa asiakasohjelman, jota käytetään graafisen käyttöliittymän avulla Windows-koneelta. Yksi tai useampi asiakas kommunikoi InControl-palvelimen kanssa, joka sijaitsee joko samalla tai erillisellä koneella kuin asiakasohjelma. Palvelin toimii säilytyspaikkana kaikelle CorePlus-konfigurointidatalle ja välittää kaikki asiakkaiden lähettämät hallintakomennot. [8, s. 25-40.]

WebUI tarjoaa graafisen käyttöliittymän hallinnointiin ja sitä voi käyttää tavallisella internet-selaimella. Selaimen käyttö mahdollistaa sen, että Security Gatewaytä voi käyttää eri paikoista tarvitsematta erikseen asentaa mitään ohjelmia. WebUI ei tarjoa keskitettyä hallintaa. Uuden Clavister-laitteen sisäinen IP-osoite on oletuksena 192.168.1.1. Kuvassa 6 on oletusrajapinnat, joihin oletus IP-osoite on määritelty. Jos laite ei ole Clavisterin, CorePlus etsiii rajapintoja ja valitsee ensimmäisen vapaana olevan. [8, s. 25-40.]

Hardware Model	Management Interface
SG10/SG50	lan
SG3100	if1
SG3200/SG4200/SG4400	ge1
SG5500/SG	cmm

Kuva 6. Clavister-laitteiden oletusrajapinnat. [8, s. 39.]

CLI:llä pääsee käsiksi Security Gatewayhin joko paikallisesti konsoliportin kautta tai etäyhteydellä käyttäen SSH-protokollaa. CLI tarjoaa yksityiskohtaisimman ja jaotelluimman kontrollin kaikkiin CorePlussan parametreihin. CLI tarjoaa kattavan valikoiman komentoja, jolla voi tutkia konfigurointidataa tai vaikkapa ajonaikaista dataa. Yleisimpiä komentoja ovat add, set, show ja delete. [8, s. 25-40.]

Secure Copy on laajalti käytössä oleva kommunikointiprotokolla tiedostojen siirtoon. CorePlussan mukana ei tule mitään tiettyä SCP-asiakasohjelmaa, mutta niitä on helposti saatavilla ilmaiseksi lukuisia erilaisia eri käyttöjärjestelmille. SCP täydentää CLI:n käyttöä ja tarjoaa turvallisen tavan tiedon siirtoon ylläpitäjän työaseman ja Security Gatewayn välille. Monia eri CorePlussan käyttämiä tiedostoja voidaan ladata SCP:llä, joko laitteeseen tai laitteesta. Kuvassa 7 on esimerkki konfigurointien kopioimisesta. Tiedoston lähetyskomennossa kirjoitetaan aluksi komento scp, sen jälkeen lähetettävän tiedoston nimi ja mihin se lähetetään. Tiedostojen latauksessa komennon scp jälkeen kirjoitetaan, mistä tiedosto ladataan ja minkä niminen se on. Kuvan 7 alareunassa on esimerkki lähde- tai kohdeyhdyskäytävästä, jossa käyttäjänä on ”admin”, jonka yhdyskäytävä on ”10.62.11.10” ja kohdetiedoston nimenä ”config.bak”.

```
Lähetys:   scp <tiedoston_nimi> <kohdeyhdyskäytävä>
Lataus:    scp <lähdeyhdyskäytävä> <tiedoston_nimi>

Esimerkki lähde- tai kohdeyhdyskäytävästä:
<käyttäjänimi>@<yhdyskäytävän_ip_osoite>:<tiedostopolku>
admin@10.62.11.10:config.bak
```

Kuva 7. Konfigurointitiedoston kopiointi. [8, s. 37.]

Console Boot Menu on ylläpitäjän käyttöliittymä CorePlussan kantaohjelmaan firmware-lataajaan. Kyseiseen valikkoon pääse fyysisesti konsoliportin kautta. Ennen laitteen käynnistämistä johdon pitää olla kiinni portissa, CorePlus sammutettuna ja virran pitää olla päällä. Kun laite käynnistetään, niin

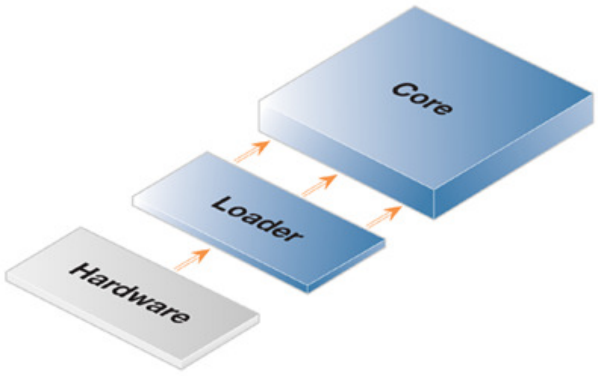
käynnistyksen aikana ennen kuin CorePlus käynnistyy täytyy painaa mitä tahansa näppäintä. [8, s. 25-40.]

Oletuskäyttäjätilit on hyvä muuttaa heti ensimmäisellä kerralla, kun käyttää Security Gatewaytä. Käyttäjänimellä ja salasanalla ”admin” ylläpitäjä saa täydet kirjoitus- ja lukuoikeudet. Käyttäjänimellä ja salasanalla ”audit” ylläpitäjä saa vain lukuoikeuden monitorointia varten. On hyvä huomioida, että Security Gatewayssä on eri salasana fyysisesti otettuun yhteyteen konsoliportin kautta kuin etäyhteyteen esimerkiksi WebUI:n avulla. [8, s. 25-40.]

3.1.3 Ylläpidon toimenpiteet

Toimiakseen oikein jokainen CorePlus vaatii oman lisenssitiedostonsa, joka pitää sisällään laitteen ominaisuudet ja rajoitukset. Ilman lisenssiä se toimii vain kahden tunnin jaksoissa, jonka jälkeen laite pitää käynnistää uudelleen. Tarvittava lisenssinumero koostuu neljästä neljän numeron osasta, jotka on erotettu toisistaan väliviivalla. [8, s. 77-79.]

CorePlus koostuu käytännössä ytimestä ja lataajasta, jolla ytimen päivitykset ladataan käyttöön (kuva 8). Päivityksiä ilmestyy silloin, kun heikkouksia on korjattu tai uusi ydin ilmestyy. Digitaalisesti allekirjoitetut päivitystiedostot löytää internetistä osoitteesta ”https://clientweb.clavister.com”, josta ne voi ladata itselleen. On olemassa pienempiä ja suurempia päivityksiä sekä laitekohtaisia päivityksiä. Oikea päivitys valitaan laite- ja lisenssityypin mukaan. Päivityksen jälkeen High Buffers -asetus kannattaa tarkistaa, että se on asetettu automaattiseksi. Asetus määrää yhteyksien hallintaan käytettävän muistin määrän. Ytimen päivityksen lisäksi CorePlussassa on erilaisia tietokantoja, jotka päivittyvät automaattisesti. [8, s. 77-79.]



Kuva 8. Ytimen päivitysten kulku itse ytimeen. [8, s. 77.]

Ylläpitäjällä on mahdollisuus ottaa ns. tilannekuvia järjestelmästä. Tämän ansiosta järjestelmä voidaan tarvittaessa palauttaa takaisin tilanteeseen, jossa se oli kuvanottohetkellä. Tilannekuvia on kahdenlaisia, joista ”System backup” on koko järjestelmän varmuuskopio ja toinen on kevyempi ”Configuration backup”, joka ei sisällä asennettua CorePlus-versiota. Koko järjestelmän varmuuskopiokaan ei sisällä aivan kaikkea, kuten virus-tietokantoja. Varmuuskopiot voidaan tallentaa lataamalla Security Gatewaystä tiedoston config.bak tai full.bak. Toinen vaihtoehto on ottaa varmuuskopio WebUI:n kautta kohdasta ”Maintenance”. Varmuuskopiot voidaan ottaa milloin tahansa ilman, että CorePlussan toiminta häiriintyy. Järjestelmän palautuksen jälkeen järjestelmä otetaan käyttöön aktivoimalla se uudestaan. Tarvittaessa järjestelmä voidaan myös resetoida tehdasasetuksille. Tosin silloin jää jäljelle vielä dataa, kuten IDP- ja virus-tietokantoja, mutta nekin saadaan halutessa poistettua siihen tarkoitetuilla komennoilla. [8, s. 77-79.]

3.2 CorePlussan olennaisimmat ominaisuudet

CorePlus sisältää paljon ominaisuuksia, joista seuraavaksi on esitelty olennaisimmat. Alla esiteltyjen ominaisuuksien lisäksi CorePlus tarjoaa mm. DHCP-palveluja, suojauksen DoS-hyökkäyksiä vastaan, tuen PPPoE:n, GRE:n, dynaamisen DNS-palvelun jne. [8, s. 16.]

3.2.1 IP-reititys

IP-reititysvaihtoehtoihin kuuluu staattinen, dynaaminen, virtuaalinen ja multicast-reititys. Lisäksi CorePlus tukee sellaisia ominaisuuksia, kuten virtuaali LAN:eja, reitin monitorointia, Proxy ARP:ia ja transparenttisuutta. [8, s. 14.]

Reititys perustuu siihen, että jokaisella reitittimellä on reititystaulu, josta reititin saa tietää, minne se lähettää paketin seuraavaksi (kuva 9). Reititystaulussa on yleensä monia reittejä, joista jokainen sisältää kohdeverkon, lähetysrajapinnan ja mahdollisesti seuraavan yhdyskäytävän IP-osoitteen. Seuraavan yhdyskäytävän IP-osoitetta ei luonnollisesti tarvita, jos kohteeseen on suora yhteys. Kun reititystaulua evaluoidaan, on reittien järjestys tärkeä. Merkittävin reitti evaluoidaan ensin. Tämä tarkoittaa sitä, että jos kahdella reitillä on sama kohdeosoite, kapeampi reitti valitaan ennemmin kuin leveämpi reitti. Esimerkiksi kuvan 9 reititystaulussa osoite 192.168.0.4 täsmää ensimmäiseen ja neljänteen reittiin, mutta ensimmäinen valitaan, koska se on tarkemmin määritelty reitti. CorePlussassa on aina oletusreititystaulu ni-

meltä main, joka on ennalta määritelty ja aina ajan tasalla. Koska CorePlus tukee montaa reititystaulua samaan aikaan, niin muita tauluja voidaan konfiguroida vaihtoehtoista reititystä varten. [8, s. 142.]

Route #	Interface	Destination	Gateway
1	lan	192.168.0.0/24	
2	dmz	10.4.0.0/16	
3	wan	195.66.77.0/24	
4	wan	all-nets	195.66.77.4

Kuva 9. Esimerkki Security Gatewayn reititystaulusta. [8, s. 142.]

Staattinen reititys

Tavallisinta reitityksen muoto on nimeltään staattinen reititys. Staattisuus tarkoittaa sitä, että reitit lisätään reititystauluun käsin ja siitä syystä ne ovat pysyviä. Staattista reititystä käytetään pienemmissä verkoissa, joissa yhteyksiä ei ole kovin montaa. Suuremmissa verkoissa reittien säätäminen käsin on ongelmallista ja vie paljon aikaa. [8, s. 142-175.]

CorePlussassa pakettien uudelleen lähetys perustuu tilaan, joten reitin haku on integroitu CorePlussan tilalliseen tarkastusmekanismiin. Tilallisuuden ansioista vastaanotettu IP-paketti voidaan tarkistaa yhteystaulusta, että onko paketille jo yhteyttä avoinna. Jos on, reititystaulusta ei tarvitse tehdä erikseen reitin hakua. [8, s. 142-175.]

CorePlussan tapa esittää reitit on helppo lukea ja ymmärtää. Tietylle reitille voi määrittää yhdyskäytävän ilman reittiä, joka kattaisi yhdyskäytävän IP-osoitteen. Reittejä sellaisiin kohteisiin voi myös määrittää, jotka ei ole aliverkotettu perinteisin aliverkonpeittein. On täysin hyväksyttävää määrittää reitti alueelle 192.168.0.5-192.168.0.17 ja toinen reitti alueelle 192.168.0.18-192.168.0.254. [8, s. 142-175.]

Dynaaminen reititys

Dynaaminen reititys sopii laajempiin verkkoihin, koska se päivittää automaattisesti verkkotopologian tai verkkokuorman muutokset. CorePlus oppii ensin suoraan yhteydessä olevat reitit, jonka jälkeen se saa muilta reitittimiltä tietoa pidemmälle menevistä reiteistä. Sopivimmat reitit kohteisiin valitaan ja lisätään reititystauluun, josta informaatio levitetään muille reitittimille. Reittien

päivitys lennossa saattaa johtaa kuitenkin ongelmiin, kuten reititys silmukoihin. [8, s. 142-175.]

Dynaamisessa reitityksestä on käytössä kaksi algoritmia, jotka ovat DV- ja LS-algoritmi. Se miten reititin valitsee optimaalisen reitin ja jakaa päivitysinformaatiot riippuu käytetystä algoritmista. DV-algoritmissa jokainen reititin laskee siihen kytkettyjen linkkien arvot ja jakaa tiedon vain naapurireitittimien kanssa. Reititin oppii vähitellen pienimmän arvon saaneet reitit iteratiivisen laskennan ja naapureiden kanssa käydyn tiedonvaihdon avulla. Esimerkiksi RIP on hyvin tunnettu DV-algoritmia käyttävä reititysprotokolla. LS-algoritmissa reitittimet ylläpitävät reititystaulua, joka sisältää koko verkon topologian. Jokainen reititin mainostaa siihen liitetyt linkit ja linkkien arvot kaikille muille verkon reitittimille. Kun reititin saa tällaisen mainostuksen, se ajaa LS-algoritmin ja laskee poluille omat pienimmät arvonsa. Jokainen muutos verkossa lähetetään siis kaikkialle, jotta kaikilla reitittimillä on sama informaatio reititystaulussa. Laajasti käytössä oleva LS-algoritmia käyttävä reititysprotokolla on esimerkiksi OSPF. [8, s. 142-175.]

Virtuaalinen reititys

Virtuaalinen reititys mahdollistaa monen loogisesti erillisen virtuaalijärjestelmän toteuttamisen. Virtuaalisysteemit käyttäytyvät kuten fyysisesti erotetut Security Gatewayt. Ne toimivat lähes samalla tavalla ja niissä pystytään myös ajamaan mm. dynaamista reititystä. Virtuaalireititykseen kuuluvia komponentteja ovat [8, s. 142-175.]

- erillinen sääntöihin perustuva reititystaulu, jokaiselle virtuaalijärjestelmälle erikseen.
- sääntöihin perustuva rajapintakohtainen reititystaulun jäsenyys, jotta rajapinnan IP-osoitteet ovat saavutettavissa vain tiettyä reititystaulua käytettäessä.
- tarvittaessa pari loopback-rajapintoja virtuaalijärjestelmien välistä kommunikointia varten.

Multicast-reititys

Multicast-reititys on tarpeellinen, kun halutaan lähettää sama paketti monelle vastaanottajalle aiheuttamatta kuitenkaan tarpeetonta verkkokuor-

maa. Reitittimet osaavat tehdä sen toistamalla ja edelleen lähettämällä paketteja optimaalista reittiä pitkin kaikille ryhmän jäsenille. IETF:n standardin vaatimukset multicast-reititykselle ovat [8, s. 142-175.]

- luokan D IP-osoite. Jokainen multicast IP-osoite edustaa satunnaista vastaanottaja joukkoa.
- IGMP, joka antaa vastaanottajan kertoa verkolle, että se on tietyn multicast-ryhmän jäsen.
- PIM, jotka ovat ryhmäreititysprotokollia, jotka päättävät multicast-pakettien optimaalisesta polusta.

Toiminnan periaate on se, että vastaanottaja liittyy IGMP:n avulla multicast-ryhmään. PIM-reitittimet voivat sitten monistaa ja edelleen lähettää paketteja kaikille sellaisen multicast-ryhmän jäsenille. Multicastingissa reititin on kiinnostunut erityisesti paketin lähteestä, koska se haluaa edelleen lähettää paketit poispäin lähteestä. Oletuksena CorePlus reitittää CorePlus-paketit ytimeen eli itselleen. SAT-multiplexointisääntöjä voidaan määritellä IP-säännöstöön, joilla voidaan suorittaa edelleenlähetys oikeaan rajapintaan. [8, s. 142-175.]

3.2.2 Palomuurikäytännöt

CorePlus toimii tilallisena palomuurina monille eri protokollille, kuten TCP:lle, UDP:lle ja ICMP:lle. Ylläpitäjä voi määrittää yksityiskohtaisia palomuurisääntöjä perustuen lähde/kohdeverkkoon tai rajapintaan, protokolliin, portteihin, käyttäjiin, kellonaikaan jne. [8, s. 14.]

Ylläpitäjän suunnittelemat CorePlussan turvallisuuskäytännöt ohjaavat, miten liikenteen täytyy kulkea Security Gatewayn läpi. Käytännöt määritetään erilaisilla IP-säännöstöillä. Kyseiset säännöstöt käyttävät suodatusparametreina lähde- ja kohderajapintaa, lähde- ja kohdeverkkoa sekä palveluita. Rajapintana voi olla myös VPN-tunneli. Myös rajapintaryhmiä voidaan määrittää. Verkkoa määriteltäessä voidaan halutessa myös suurempia IP-osoitealueita rajata. Palvelu on protokollatyyppi, johon paketti kuuluu. [8, s. 119-122.]

CorePlussan perussäännöstö, joka määrittää CorePlussan turvallisuuskäytännöt käyttää yllä mainittuja suodatusparametreja ja sisältää seuraavat säännöt. [8, s. 119-122.]

- IP-säännöt määrittävät, mikä liikenne on sallittu.
- Putkisäännöt määrittävät, mikä liikenne laukaisee liikenteen muokkauksen.
- Käytäntöihin perustuvat reitityssäännöt määrittävät reititystaulun, jota liikenne käyttää.
- IDP-säännöt määrittävät, mikä liikenne on aiheena IDP-skannaukselle.
- Autentikointisäännöt määrittävät, mikä liikenne laukaisee autentikoinnin.

Määriteltäessä suodatusparametreja jollekin yllämainituista säännöistä voidaan käyttää hyväksi kolmea ennalta määriteltyä vaihtoehtoa. Lähde- tai kohdeosoitteelle voidaan käyttää ”all-nets”-valintaa, joka on IP-osoitteen 0.0.0.0/0 kanssa yhtenevä ja tarkoittaa sitä, että kaikki IP-osoitteet ovat käypiä. Lähde- tai kohderajapinnalle valinta ”any” tarkoittaa, että käytetyllä rajapinnalla ei ole merkitystä. Kohderajapinta voidaan asettaa coreksi. Tämä tarkoittaa sitä, että liikenne, kuten ICMP Ping kohdistuu itse Security Gatewayhin ja CorePlus vastaa siihen. [8, s. 119-122.]

IP-säännöstö on turvallisuuskäytäntö säännöstöistä kaikista tärkein. On kaksi tapaa, jolla liikennöinti Security Gatewayssä tapahtuu. Joko kaikki kielletään tai kaikki sallitaan, jos ei toisin määrätä. Parempaan turvallisuuteen päästäkseen CorePlus käyttää näistä ensimmäistä. Jos liikennettä halutaan päästää läpi, täytyy luoda IP-sääntöjä sitä varten. Liikenne, joka ei täsmää sääntöön ja jolla ei ole avointa yhteyttä, hylätään automaattisesti. Lokitarkoituksessa on kuitenkin suositeltavaa, että eksplisiittinen IP-sääntö hylkäätoiminnolla suodatusparametreinaan kaikki rajapinnat ja verkot asetetaan viimeiseksi IP-säännöstössä. Kun uusi yhteys muodostuu, säännöt evaluoidaan ylhäältä alas ja ensimmäinen parametreihin täsmäävä sääntö on se, joka määrää miten yhteyttä käsitellään. Poikkeuksen tähän tekee SAT-

säännöt, koska ne tarvitsevat kaksi sääntöä. Ensimmäinen on täsmäys SAT-sääntöön, jonka jälkeen etsintä toiselle säännölle alkaa. [8, s. 119-122.]

IP-säännöstön säännöt koostuvat kahdesta osasta. Edellä mainituista suodatusparametreista ja suoritettavasta toiminnosta, jos parametrit täsmäävät. IP-säännön toteutuessa yksi seuraavista toiminnoista käynnistyy: [8, s. 119-122.]

- Allow-säännössä paketti sallitaan. Kun sääntö otetaan käyttöön, tilapöytään tulee merkintä, että yhteys on päällä.

- FwdFast-sääntö päästää paketin läpi Security Gatewayn tekemättä merkintää tilapöytään. Tilantarkastusprosessi jätetään väliin, joka tekee tästä vähemmän turvallisen kuin NAT- ja Allow-säännöistä. Paketin prosessointi on myös hitaampaa, koska kaikki paketit tarkastetaan erikseen.

- NAT vastaa Allow-sääntöä dynaamisella osoitteenkäännöksellä varustettuna.

- SAT kertoo CorePlussalla, että staattista osoitteenkäännöstä on käytettävä. SAT-sääntö vaatii toimiakseen Allow-, NAT- tai FwdFast-säännön toteutumisen.

- Drop kertoo CorePlussalle, että paketti on heti hylättävä. Tämä on epäkohtelias versio Rejectistä, koska mitään ilmoitusta hylkäyksestä ei lähetetä. Se on siitä syystä suositeltava, koska ei anna mahdolliselle hyökkääjälle tietoa siitä, mitä paketille on tapahtunut.

- Reject vastaa Drop-sääntöä. ”TCP RST” tai ”ICMP Unreachable message” lähetetään lähettävälle tietokoneelle kertomaan, että pakettia ei päästetty läpi.

Yleinen virhe IP-sääntöjä luodessa on tehdä omat säännöt lähtevälle liikenteelle sekä takaisin tulevalle liikenteelle. Kahta sääntöä ei kuitenkaan tarvita, koska kun yhteys on kerran sallittu, liikenne saa mennä kumpaan suuntaan tahansa. Poikkeuksen tähän tekee FwdFast-sääntö. Lähtenyt paketti ei voi palata kohteen kautta lähteeseen, koska paketista ei jää merkintää tilapöytään. [8, s. 119-122.]

Ylläpitäjä voi turvallisuus käytännön yksinkertaistamisen ja joustavuuden lisäämisen vuoksi luoda monia IP-säännöstöjä. Oletus-IP-säännöstö on nimeltään main ja on aina ajan tasalla CorePlussassa. Muita hyötyjä ovat mm. yhden ison IP-säännöstön pilkkominen pienemmiksi säännöstöiksi ja yksittäisen IP-säännöstön assosioiminen reititystauluun. [8, s. 119-122.]

3.2.3 Osoitteenkäännös

CorePlussan tukemia käytäntöpohjaisia osoitteenkäännösmenetelmiä ovat NAT ja SAT. Ne tarjoavat toiminnallisuutta ja turvallisuutta. Osoitteenkäännöksen ansiosta päästään yksityisestä suojatusta verkosta julkiseen. Osoitteenkäännös ei itsessään sisällä mitään erityistä turvallisuusmekanismia, mutta se tekee tunkeutujille suojatun verkon kartoittamisen hankalaksi. Käytäntöpohjaisuus tarkoittaa sitä, että NAT ja SAT voidaan määrittää liikennekohtaisesti sääntöjen avulla. [8, s. 300-312.]

NAT

Dynaamista osoitteenkäännöstä NAT:ia käytetään yleensä silloin, kun ei haluta, että sisäverkon osoitteet näkyvät ulospäin. Sisäverkon osoitteen sijaan ulospäin näkyy Security Gateway. NAT toimii niin, että jokainen NAT-sääntö kääntää erinäisen määrän IP-lähdeosoitteita yhdeksi IP-lähdeosoitteeksi. Istunnon tilatietojen ylläpitämiseksi jokaisen yhteyden dynaamisesti käännettyjen osoitteiden täytyy käyttää yksilöllistä porttinumeron ja IP-osoitteen yhdistelmää lähettäjänään. Tämän takia CorePlus kääntää myös lähdeporttien numerot automaattisesti. Käytettävä lähdeportti on seuraava vapaa portti, joka on numeroltaan yleensä suurempi kuin 32,768. Tämä tarkoittaa sitä, että samaa käännettyä IP-lähdeosoitetta voi käyttää noin 30,000 samanaikaista yhteyttä. [8, s. 300-312.]

CorePlus tukee kahdenlaista lähdeosoitteenkäännösstrategiaa. ”Use Interface Address”-strategiassa uuden yhteyden auettua reititystaulua konsultoidaan, jotta saadaan tietää yhteyden ulosmeno rajapinta. Tuon rajapinnan IP-osoitetta käytetään uutena IP-lähdeosoitteena, kun CorePlus suorittaa osoitteenkäännöksen. ”Specify Sender Address”-strategiassa tietty IP-osoite voidaan määritellä uudeksi IP-lähdeosoitteeksi. Määritellyllä IP-osoitteella täytyy olla täsmäävä ARP-julkistusmerkintä konfiguroituna ulosmenorajapintaan, koska muuten paluuliikennettä ei oteta vastaan Security Gatewayn toimesta. [8, s. 300-312.]

NAT osaa käsitellä oikein TCP-, UDP- ja ICMP-protokollia, koska algoritmi tietää, mitä arvoja täytyy säätää. Muissa IP-tason protokollissa uniikit yhteydet tunnistetaan lähettäjän osoitteen, kohdeosoitteen ja protokollanumeron perusteella. [8, s. 300-312.]

NAT mahdollistaa kommunikoinnin eri yksityisten verkkojen tietokoneiden välillä vain yhden julkisen ulkoisen IP-osoitteen kautta. NAT-poolit tulevat kyseeseen silloin, kun monia julkisia ulkoisia IP-osoitteita on saatavilla. Poolit otetaan yleensä käyttöön, kun tarvitaan suuri määrä yksilöllisiä porttiyhteyksiä. CorePlussan porttien hallinnoinnissa on uniikeista lähde- ja kohde-IP-osoitteiden yhdistelmistä koostuvien yhteyksien määrää rajoitettu noin 65 000 yhteyteen. NAT-pooleja on kolmenlaisia: tilallisia, tilattomia ja fixed-tyyppisiä. [8, s. 300-312.]

Tilallisessa vaihtoehdossa CorePlus varaa uuden yhteyden ulkoiselle IP-osoitteelle, jonka läpi on sillä hetkellä reititetty vähiten yhteyksiä sillä oletuksella, että se on vähiten kuormitettu. CorePlus pitää kirjaa muistissaan kaikista tällaisista yhteyksistä. Sen ansiosta myöhemmät yhteydet, jotka sisältävät saman sisäisen isännän käyttävät samaa ulkoista IP-osoitetta. Hyötynä tilallisuudessa on mahdollisuus tasapainottaa yhteyksiä eri ISP-linkkien kesken ja kuitenkin samaan aikaan varmistaa, että ulkoinen isäntä käyttää samaa IP-osoitetta kommunikoidessaan takaisinpäin. Haittapuolena on lisääntyvä muistinkäyttö. Muistin käyttöä voidaan tehostaa säätämällä State Keepalive - ja Max States -arvoja pienemmiksi. ”State Keepalive” varmistaa sen, että tilapöytä ei sisällä kuolleita merkintöjä kommunikoinneista, jotka eivät ole enää aktiivisia. ”Max States”-arvoilla säädetään itse tilapöydän kokoa. [8, s. 300-312.]

Tilattomassa vaihtoehdossa tilapöytää ei ylläpidetä ja jokaiselle uudelle yhteydellä valittava ulkoinen IP-osoite on se, jolle on vähiten yhteyksiä valmiiksi varattuna. Tämä tarkoittaa sitä, että kaksi yhteyttä sisäisen isännän ja saman ulkoisen isännän välillä voi käyttää kahta erilaista ulkoista IP-osoitetta. Hyötynä tilattomuudessa on se, että uusien yhteyksien jakautuminen ulkoisten IP-osoitteiden välillä ei vie tilapöydästä muistia ja myöhempien yhteyksien käynnistämiseen menee vähemmän aikaa. Haittapuolena on se, että se ei sovellu sellaiseen kommunikointiin, joka vaatii muuttumatonta IP-osoitetta. [8, s. 300-312.]

Fixed-vaihtoehdossa jokaiselle sisäiselle isännälle varataan yksi ulkoisista IP-osoitteista hashing-algoritmin avulla. Vaikka ylläpitäjällä ei ole mahdollisuutta määrätä, mitä ulkoista yhteyttä käytetään, niin yksittäinen sisäinen isäntä kommunikoi aina saman ulkoisen IP-osoitteen kautta. Hyötynä tilattomuudessa on se, että se ei vaadi muistia tilapöydästä ja uusien yhteyksien prosessointi on todella nopeaa. Jonkinlaista kuorman jakoakin tapahtuu ulkoisten yhteyksien valinnassa käytetyn hashing-algoritmin satunnaisuuden ansiosta. [8, s. 300-312.]

SAT

Staattisen osoitteenkäännöksen SAT:in toiminta perustuu siihen, että IP-osoite- tai porttialueet voidaan kääntää niitä vastaaviksi osoitteiksi tai porteiksi uudelle alueelle. Yksinkertaisin SAT:in käyttökohde on yhden osoitteen käännös. Sitä käytetään esimerkiksi silloin, kun halutaan antaa ulkopuoliselle käyttäjälle pääsy suojatulle palvelimelle, jolla on yksityinen IP-osoite. Yksittäistä SAT-sääntöä voidaan käyttää kokonaisten osoitealueiden kääntämiseen, jolloin osoitteet käännetään järjestyksessä niitä vastaaviksi osoitteiksi. Myös monen osoitteen muuntaminen yhdeksi osoitteeksi onnistuu. Lisäksi pelkkien porttiosoitteiden kääntämistä varten on olemassa PAT. [8, s. 300-312.]

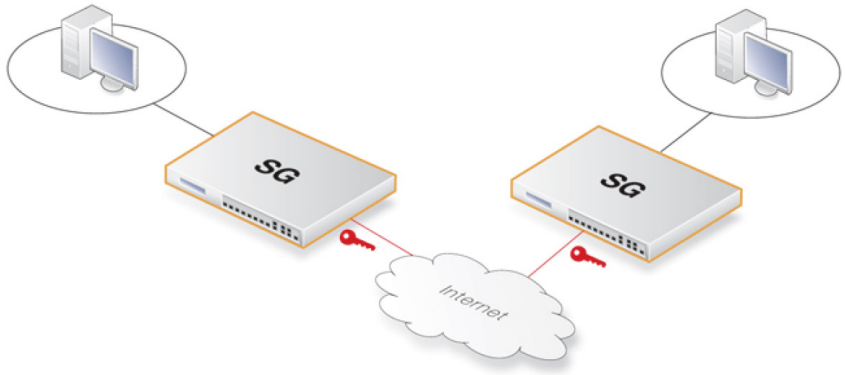
Yleisesti SAT osaa käsitellä kaikkia protokollia, jotka sallivat osoitteenkäännökset. Kuitenkin joitakin protokollia voidaan kääntää vain poikkeustilanteissa ja joitain ei voida kääntää ollenkaan. Protokollat, joita on mahdotonta kääntää SAT:illa, on luultavasti myös mahdotonta kääntää NAT:illa. Myöskään VPN-protokollia ei yleensä voida kääntää ja yleensäkin protokollia, jotka avaavat toisen yhteyden ensimmäisen päälle, on vaikea kääntää. [8, s. 300-312.]

3.2.4 VPN

Internetiä käytetään yhä enemmän tietokoneiden yhdistämisessä toisiinsa, koska se on halpa ja tehokas väline. Kuitenkin tiedon halutaan kulkevan lähettäjältä vastaanottajalle koskemattomana tai siten että kukaan ei esiinny vale-lähettäjänä tai -vastaanottajana. VPN-ratkaisu on syntynyt tyydyttämään tämän tarpeen löytää kustannustehokas keino tarjota turvattu linkki kahden yhteistyötä tekevän tietokoneen välille. VPN-ratkaisussa muodostetaan tunneli kahden laitteen välille, joita kutsutaan päätepisteiksi. Kaikki tun-

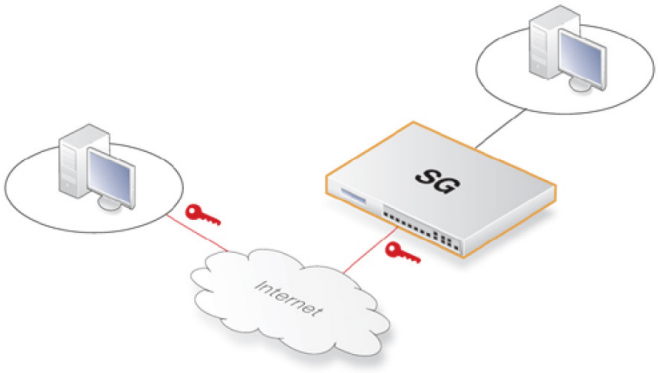
nelin läpi kulkeva data saadaan näin turvattua. CorePlus tukee IPsec-, L2TP- ja PPTP-pohjaisia VPN-ratkaisuja samanaikaisesti sekä voi toimia palvelimena tai asiakkaana kaikille VPN-tyypeille. Se pystyy myös tarjoamaan erilliset turvallisuuskäytännöt jokaiselle VPN-tunnelille. On kahdenlaisia tapauksia, joissa VPN:ää käytetään. [8, s. 329-331.]

- Lähiverkosta lähiverkkoon yhteydessä kaksi sisäverkkoa yhdistetään toisiinsa internetin yli. Tässä tapauksessa jokainen verkko turvataan omalla Security Gatewayllään ja VPN-tunneli luodaan niiden välille (kuva 10). [8, s. 329-331.]



Kuva 10. Yhteys lähiverkosta lähiverkkoon. [8, s. 329.]

- Asiakkaalta lähiverkkoon yhteydessä monet etäasiakkaat voivat ottaa yhteyden sisäiseen verkkoon internetin yli. Tässä tapauksessa asiakas ottaa yhteyden Security Gatewayllä suojattuun sisäverkkoon, joiden välille VPN-tunneli luodaan (kuva 11).



Kuva 11. Yhteys asiakkaalta lähiverkkoon. [8, s. 330.]

VPN-liikenne on salattu käyttäen kryptograafisia menetelmiä. Menetelmät kattavat kolme etua ja tekniikkaa. Näistä ensimmäinen on luottamuksellisuus, joka saavutetaan salauksen avulla. Ainoastaan asiaankuuluvat osapuolet kykenevät vastaanottamaan ja ymmärtämään kommunikointia. Toinen etu, koskemattomuus, saavutetaan autentikoinnilla, jossa yleensä käytetään kryptograafisia tiivistettyjä avaimia. Kolmas etu, kieltämättömyys, on yleensä autentikoinnin sivutuote. Lähettäjä ei voi enää myöhemmin kieltää lähettäneensä dataa, koska siitä on todisteita. [8, s. 329-331.]

Tyypillisesti VPN-yhteyteen hyökkääjä ei yritä murtaa VPN:n salausta, koska se vaatisi paljon työtä. Itse VPN-yhteyden olemassaolo kertoo heille, että toisessa päässä yhteyttä on jotain salaamisen arvoista. Mobiiliasiakkaat ja sivukonttorit ovat haavoittuvuutensa takia kiinnostavampia kohteita kuin yritysten pääverkot. Vaikka VPN-yhteys olisi itsessään turvallinen, turvallisuuden todellinen taso on se, mikä se on tunnelin päätepisteissä. Esimerkiksi tunkeutuja saattaa päästä heikolla suojauksella varustetun kannettavan tietokoneen kautta valmiiksi avattua VPN-yhteyttä pitkin yrityksen verkkoon. Tällaisten tapausten takia VPN-yhteys olisi hyvä laittaa erityiselle DMZ:lle tai yhteydelle tarkoitetulle ulkoiselle porttikäytävälle. Tämän ansiosta voidaan rajoittaa palveluita, joihin VPN:llä päästään käsiksi ja varmistetaan, että palvelut on tunkeutujilta hyvin suojattu. Tapauksissa, joissa yhdyskäytävään on integroitu VPN-ominaisuus voidaan yleensä määrätä, mikä kommunikointi sallitaan. [8, s. 329-331.]

Avaintenjakelun suunnittelussa on hyvä ottaa huomioon esimerkiksi, kuinka avaimet aiotaan jakaa, kuinka monta erilaista avainta tarvitaan, pitäisikö avaimia muuttaa, mitä tapahtuu työntekijän lopettaessa työt tai missä avaimia säilytetään, jos niitä ei suoraan ohjelmoida hallintayksikköön. [8, s. 329-331.]

3.2.5 Sovellustason yhdyskäytävät

Sovellustason yhdyskäytävät eli ALG:it toimivat OSI-mallin korkeimmalla tasolla ja hoitavat siellä suodatuksen tietyissä protokollissa. ALG:it täydentävät alemman tason paketin suodatusta, joka tarkastaa vain pakettien otsikot protokollista, kuten IP, TCP, UDP ja ICMP. CorePlussasta löytyy ALG:eja seuraaville protokollille: HTTP, FTP, TFTP, SMTP, POP3, SIP, H.323 ja TLS. Esimerkiksi pystytään tarkistamaan täsmääkö tiedostotyyppi ladattavaan si-

sältöön ja esimerkiksi SIP ALG pystyy käsittelemään viestien vaihdot vertaisverkon tietojen vaihdon asetustyön aikana. [8, s. 215-216.]

Kun ylläpitäjä on määritellyt ALG-objektin, se otetaan käyttöön assosioimalla ALG-objekti palveluobjektiin, jonka jälkeen palvelu assosioidaan IP-sääntöön CorePlussan IP-säännöstössä (kuva 12). ALG:iin assosioidulla palvelulla on konfiguroitavissa oleva parametri nimeltä ”Max Sessions”, joka määrittää sessioiden maksimi määrän ALG:ia kohti. ALG:ien maksimi sessioiden oletusarvot vaihtelevat ALG-kohtaisesti. Esimerkiksi HTTP ALG:illa maksimi sessioiden määrä on oletuksena 1000 ja vastaavasti H.323 ALG:illa luku on 100. [8, s. 215-216.]

Kuva 12. ALG-objektin käyttöönottaminen. [8, s. 215.]

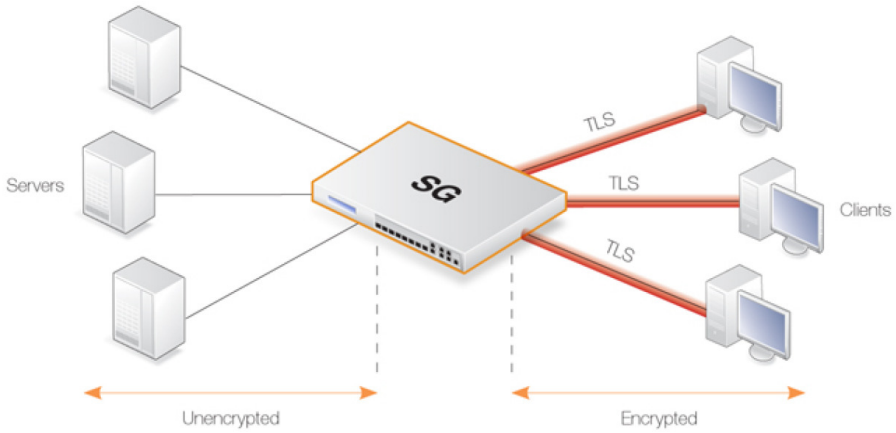
3.2.6 TLS-terminaatio

CorePlus tukee TLS-terminaatiota, joten Security Gateway voi toimia HTTP web-selain asiakkaiden yhteyksien päätepisteenä. TLS on protokolla, joka tarjoaa turvatun yhteyden internetin yli kahden päätepisteen välillä. TLS käyttää siihen salausta sekä tarjoaa päätepisteen autentikoinnin. Tyypillisesti TLS:ää käytettäessä ainoastaan palvelimen identiteetti autentikoidaan ennen kuin salattu yhteys avataan. TLS:ään törmää silloin, kun selaimella otetaan yhteys TLS:ää käyttävään palvelimeen. Esimerkiksi verkkopankkipalveluissa käytetään usein TLS:ää. Tätä kutsutaan toisinaan myös HTTPS-yhteydeksi, jonka tunnistaa usein riippulukosta selaimen navigointipalkissa. [8, s. 257-260.]

TLS:n turvallisuus perustuu digitaalisten sertifikaattien käyttöön. Sertifikaatit sijaitsevat palvelimella, josta ne lähetetään asiakkaalle aina TLS-session alussa. Ne vahvistavat palvelimen identiteetin ja ovat siten salauksen perustana. CA-allekirjoitettuja sertifikaatteja voidaan käyttää palvelimilla tapauk-

sissa, joissa asiakkaan selain automaattisesti tunnistaa sertifikaatin validiuden. Palvelimilla voidaan myös käyttää itse allekirjoitettavia sertifikaatteja. Tällöin selain varoittaa käyttäjää, että sertifikaatin autenttisuutta ei ole tunnistettu ja käyttäjän täytyy itse, valita hyväksyykö sertifikaatin jatkaakseen eteenpäin. [8, s. 257-260.]

TLS voidaan toteuttaa siten, että asiakkaat ovat suoraan yhteydessä palvelimeen tai sitten toinen vaihtoehto on laittaa palvelimet turvaan Security Gatewayn taakse, jolloin CorePlus toimii TLS-päätepisteenä (kuva 13). Tässä tapauksessa CorePlus suorittaa datan TLS-autentikoinnin, salauksen ja salauksen purun. Kuten kuvasta 13 nähdään, data kulkee palvelimilta Security Gatewayhin salaamattomana ja salattuna Security Gatewayltä asiakkaille. Tästä on monia hyötyjä, kuten TLS-tuen ja sertifikaattien hallinnoinnin keskittäminen. Salauksesta purettu TLS-liikenne voidaan ottaa jonkin CorePlussan ominaisuuden aiheeksi, kuten liikenteen muokkauksen tai se voidaan tutkia IDP-skannauksella palvelin uhkien varalta. TLS voi myös olla mukana palvelinten kuorman jaossa, jotta liikenne levittyisi palvelinten kesken. [8, s. 257-260.]



Kuva 13. Palvelimet ovat turvassa Security Gatewayn takana. [8, s. 258.]

Rajoituksia CorePlus TLS:ään ovat tukemattomuus asiakkaan autentikointiin ja uudelleen neuvotteluun sekä palvelinavainten vaihto viestien lähettämiseen. Lisäksi CorePlussan käyttämä sertifikaattiketju voi sisältää enintään kaksi sertifikaattia. [8, s. 257-260.]

CorePlus TLS tukee seuraavia salauksia: [8, s. 257-260.]

- TLS_RSA_WITH_3DES_EDE_CBC_SHA

- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_EXPORT_WITH_RC4_56_SHA (avainkoko 1024:n bittiin asti)
- TLS_RSA_EXPORT_WITH_RC4_40_MD5 (avainkoko 1024:n bittiin asti)
- TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (1024:n bittiin asti)
- TLS_RSA_WITH_NULL_MD5
- TLS_RSA_WITH_NULL_SHA.

3.2.7 Virusten torjunta

Antivirus-ominaisuus on maksullinen ja sen voi ostaa lisäkomponenttina peruslisenssiin. Tilauksen muoto on uusiutuva. Antivirus-moduuli suojaa vahingolliselta koodilta, jota saattaa liikkua tiedostojen latausten yhteydessä. Vahingollisen koodin vaikutus vaihtelee vain hieman ärsyttävistä ohjelmista vahingollisempiin vakoiluohjelmiin, jotka lähettävät salasanoja ja muuta arkaluontoista tietoa tekijälleen. Termiä ”virus” voidaan käyttää tässä yleisenä määritelmänä kaikille vahingollisen koodin muodoille, joita kulkeutuu tiedostoissa. Antivirus-skannaus keskittyy asiakkaiden latauksiin ja se on suunniteltu täydentämään asiakkaan tietokoneen omaa virustentorjuntaohjelmaa. Se ei korvaa asiakkaan omaa torjuntaohjelmaa, mutta toimii hyvänä varmistajana, jos ohjelmaa ei ole jostain syystä asennettu. [8, s. 278-281.]

Ylläpitäjällä on mahdollisuus tehdä listoja, joissa sallitaan tai hylätään halutut tiedostot. Skannattavien tiedostojen kokoa voidaan myös rajoittaa, mutta vapaana oleva muisti voi asettaa rajoituksen samanaikaisten skannausten määrälle. [8, s. 278-281.]

Kun tiedostot siirrettäessä suoratoistetaan Security Gatewayn läpi, CorePlus skannaa data-virran virusten varalta, jos Antivirus-moduuli on laitettu päälle. Koska tiedostot suoratoistetaan, eikä niitä lueta kokonaan muistiin, niin muistia tarvitaan vähemmän. Tarkastusprosessi perustuu kuvion vertailuun viruskuviotietokannan kesken ja voidaan suurella varmuudella määrittää, jos virus on päässyt Security Gatewayn ohi. Kun virus havaitaan tiedoston sisältä, lataus voidaan keskeyttää ennen kuin se päättyy. CorePlus käyttää virustietokantanaan Kasperskyn ylläpitämää SafeStream-tietokantaa, joka sisäl-

tää suojan kaikille tunnetuille virusuhkille. Päivitykset hoituvat automaattisesti, kunhan vain CorePlussan kello on säädetty oikeaan aikaan. [8, s. 278-281.]

Antivirus-skannaus voidaan laittaa päälle ALG-kohtaisesti ja skannata tiedostolatauksia, jotka on assosioitu HTTP, FTP, SMTP ja POP3 ALG:hin. Skannauksen tapaan vaikuttaa kyseessä oleva protokolla. Kun Antivirus-skannausta konfiguroidaan ALG:iin, tietynlaisia parametreja voidaan määritellä. [8, s. 278-281.]

1. Tilan täytyy olla joko Disabled, Audit tai Protect. Disabled-tilassa antivirus toiminto on kytketty pois. Audit-tilassa skannaus on toiminnassa, mutta tapahtumat kirjataan ainoastaan lokiin. Protect-tilassa antivirus on toiminnassa ja epäilyttävät tiedostot hylätään ja kirjataan lokiin. Jos skannaus jostakin syystä epäonnistuu, siirto voidaan hylätä tai sallia tapahtuman kirjautuessa lokiin.

2. Jotkut tiedostotyypit voidaan eksplisiittisesti jättää virusskannauksen ulkopuolelle, jos se on mielekästä. Tällä tavoin saadaan kokonaissuoritustehoa kasvatettua, jos skannaamatta jätetty tiedosto on yleisesti käytössä, kuten kuvatiedostot HTTP-latauksissa. CorePlus suorittaa MIME-sisällön tarkistuksen kaikille tiedostotyypeille, jotka ovat varmistetut MIME-tiedostotyypit listassa todentaakseen tiedoston tiedostotyypin oikeellisuuden, jonka jälkeen sitä tiedostotyyppiä etsitään ulkopuolelle jätettävien listasta. Jos tiedostotyyppiä ei pystytä todentamaan sisällön perusteella, tiedoston nimessä olevaa tiedostotyyppiä käytetään ulkopuolelle jätettävien listaa tarkastettaessa.

3. Skannatessa pakattuja tiedostoja CorePlussan täytyy purkaa pakkaus, jotta sisältö voidaan tutkia. Tiukkaan pakkautuvat tiedostot voivat olla ongelmallisia, koska vievät suoritustehoa suuremman pakkaamisen takia. Tällaisen estämiseksi ylläpitäjä voi määritellä rajoituksen pakkauksen suhdeluvulle. Esimerkiksi rajoitukseksi voi asettaa kahdeksikon. Jos tiedosto on pakkaamattomana kahdeksan kertaa suurempi kuin pakattuna, jokin kolmesta toiminnosta suoritetaan. ”Allow” sallii tiedoston ilman virusskannausta, ”Scan” skannaa tiedoston normaalisti ja ”Drop” hylkää paketin. Kaikista tapauksissa tapahtumat kirjautuvat lokiin.

Antivirus-toiminnon suoritustehoa voidaan parantaa SG50, SG4200 ja SG4400 Security Gatewayssä valinnaisella laitteistonkiihdytyksellä. Montaa suoratoistoa kiihdytetään asynkronisesti, jotta kokonaissuoritustehoa saadaan parannettua. Jos laitteistokiihdytystä ei ole saatavilla, vaihtoehtona saa valita ympäristöön sopivimman skannausmoottorin. AVSW_Engine-asetukselle valittavia vaihtoehtoja ovat Auto, DFA ja NFA. Auto valitsee moottorin automaattisesti, DFA käyttää moottoria maksimoiden skannausnopeuden ja NFA käyttää moottoria minimoiden muistin käytön. [8, s. 278-281.]

3.2.8 IDP

IDP-moduuli on maksullinen lisäkomponentti CorePlussan peruslisenssiin. Se on tilauspalvelu, mikä tarkoittaa sitä, että IDP-signeeraustietokanta voidaan ladata CorePlus-asennukseen. Jatkossa kantaa päivitetään säännöllisesti joko käsin tai automaattisesti. IDP:tä tarvitaan paikkaamaan palveluiden, ohjelmien ja palvelinten haavoittuvuuksista aiheutuvia turvallisuusuhkia. Verkkohyökkäykset, kuten madot, troijalaiset ja takaoven hyödyntämiset yrittävät käyttää näitä haavoittuvuuksia hyväkseen. Näitä hyökkäyksiä voidaan kuvata lyhyesti termillä tunkeutumiset. Tunkeutuminen ilmenee vahingollisena kuviona internet-dataa, joka kohdistuu ohittamaan palvelimen turvallisuusmekanismeja. Tunkeutumiset eivät ole harvinaisia ja ne voivat jatkuvasti kehittyä, jos hyökkääjä on automatisoinut niiden syntymisen. CorePlussan IDP-moduuli on suunniteltu suojaamaan juuri näiltä tunkeutumisyrityksiltä. [8, s. 284-290.]

IDP-säännöt määrittävät, minkälaista liikennettä tai palvelua analysoidaan. IDP-säännöt ovat rakenteeltaan samankaltaiset kuin muutkin CorePlussan turvallisuuskäytännöt, kuten IP-säännöt. IDP-sääntöön määritetään lähde-/kohderajapinnat sekä lähde-/kohdeosoitteet ja se assosioidaan palveluobjektiin, joka määrittelee skannattavat protokollat. Myös aikataulun voi määritellä IDP-säännöllä. Sen jälkeen, kun kuvion vertailu havaitsee tunkeutumisen liikenteessä, joka on IDP-säännön aiheena, niin toimintoon assosioitu sääntö ajetaan. Ylläpitäjän sääntöön assosioimia toimintoja ovat ”Ignore”, ”Audit” ja ”Protect”. Ignore ei tee mitään, vaikka tunkeutuminen havaitaan. Audit pitää myös yhteyden auki, mutta kirjaa tapahtuman lokiin. Protect hylkää yhteyden ja kirjaa tapahtuman lokiin. Protect-toiminnossa voi valinnaisena vaihtoehtona lisätä mustalle listalle IDP-säännön laukaisevan isännän

tai verkon. Tämä tarkoittaa sitä, että jatkossa mustalle listalle laitetusta lähteestä tuleva yhteys hylätään automaattisesti. Sellaista IP-osoitetta, mikä on valkoisella listalla ei voi lisätä mustalle listalle. Siitä syystä on suositeltavaa lisätä itse Security Gateway ja hallintaan käytettävä tietokone valkoiselle listalle, kun IDP on käytössä. Kaikille IDP-säännöille voidaan asettaa monta toimintoa. Esimerkiksi Protect-toimintoa voidaan toistaa. Tällöin jokaiseen toimintoon assosiodaan yksi tai useampi signeeraus tai ryhmä. [8, s. 284-290.]

IDP-prosessoinnin läpi käyvä paketti saapuu ensimmäiseksi yhdyskäytävään, jossa CorePlus suorittaa normaalin tarkistuksen. Jos paketti on osa uutta yhteyttä, IDP-säännöstön evaluointi suoritetaan ennen kuin paketti ohjataan IDP-moduulille. Jos paketti on osa olemassa olevaa yhteyttä, paketti ohjataan suoraan IDP-järjestelmään. Jos paketti ei ole osa olemassa olevaa yhteyttä tai se kielletään IP-säännöstön toimesta, niiin se hylätään. Seuraavassa vaiheessa paketin lähde- ja kohdeinformaatiota verrataan ylläpitäjän määrittelemiin IDP-sääntöihin. Jos vertailu tuottaa tulosta, paketti ohjataan kuvion vertailuun. Paketti hyväksytään, jos vertailu ei tuota tulosta. Paketille ei tehdä enää jatkotoimenpiteitä, jos IP-säännöstössä ei sellaisia ole määritelty. [8, s. 284-290.]

Jotta IDP pystyy identifioimaan hyökkäykset oikein, se käyttää ilmaisimien profiileja tai kuvioita assosioituna eri tyyppisiin hyökkäyksiin. Nämä ennalta määritellyt kuviot tunnetaan myös signeerauksina ja niitä säilytetään yleensä paikallisessa CorePlussan tietokannassa. Jokaisella IDP-signeerauksella on oma numeronsa. Signeeraustyyppejä on kolmenlaisia: IDS, IPS ja Policy. IPS on lähes virheetön. Täsmäys vertailun tuloksena on lähes varma osoitus uhasta. IPS:in kanssa käytettäväksi suositellaan Protect-toimintoa ja se voi havaita ylläpitäjän suorittamat toiminnat sekä turvallisuusskannerit. IDS havaitsee tapahtumat, jotka voivat olla tunkeutumisia. Se ei ole yhtä virheetön kuin IPS ja voi aiheuttaa vääriä hälytyksiä. Tästä syystä on suositeltavaa käyttää ensin Audit-toimintoa ennen kuin päättää Protect-toiminnon käytöstä. Policy-signeeraus havaitsee erilaisia sovellusliikenteen tyyppejä. Niitä voidaan käyttää estämään sovelluksia, kuten tiedostonjakoa. [8, s. 284-290.]

Yleensä tietylle protokollalle löytyy monia eri hyökkäyksiä ja on parasta etsiä ne kaikki samalla, kun liikennettä analysoidaan. Jotta näin voidaan tehdä, tiettyyn protokollaan liittyvät signeeraukset on kerätty ryhmään. Toiminnalli-

suuden kannalta on kuitenkin tarkoituksenmukaista käyttää niin vähän signeerauksia kuin mahdollista. IDP-signeerausryhmät jaetaan kolmeen hierarkkiseen tasoon. Ylimpänä hierarkiassa on signeerauksen tyyppi. Tyyppi voi siis olla, joko IDS, IPS tai Policy. Toisella tasolla on kategoria, joka määrittää sovelluksen tai protokollan tyypin. Näitä ovat esimerkiksi BACKUP, DB, DNS, FTP ja HTTP. Kolmannella tasolla on alikategoria, joka määrittää ryhmän kohteen ja usein myös määrittää sovelluksen. Alikategoria ei ole pakollinen, jos tyyppi ja kategoria riittävät määrittelemään ryhmän. Signeerausryhmä merkitään esimerkiksi tällä tavalla, POLICY_DB_MSSQL. Tasot menevät järjestyksessä vasemmalta oikealle ja ensimmäinen osa vastaa ensimmäistä tasoa jne. Signeerauksien valinnassa voidaan käyttää jokerimerkkejä valitsemaan suurempia määriä signeerauksia kerralla. ?-symboli vastaa mitä tahansa yhtä merkkiä ja *-symboli vastaa minkä tahansa pituista merkkijonoa. [8, s. 284-290.]

IDP-sääntöä määriteltäessä ylläpitäjällä on mahdollisuus ottaa pois käytöstä mahdollisuus suojautua valtaus- ja välttelyhyökkäyksiltä, joka on käytössä oletuksena. Poiskytkennällä voidaan kasvattaa suoritustehoa tai se voi olla väliaikainen ratkaisu, jonka aikana selvitetään epätavallisen suuren väärienhälytysten määrän alkuperää. Kyseiset hyökkäykset käyttävät hyväkseen sitä, että TCP/IP-datasiirrossa datasuoratoisto joudutaan usein uudelleen kokoamaan pienistä datan osista. Valtaushyökkäys perustuu datan lisäämisestä suoratoistoon niin, että IDP-alijärjestelmä hyväksyy paketit, mutta kohdesovellus hylkää ne. Tämä johtaa kahteen erilaiseen datasuoratoistoon. Välttelyhyökkäys on muuten samanlainen kuin valtaushyökkäys, mutta siinä IDP-alijärjestelmä hylkää paketit ja kohdesovellus hyväksyy ne. Esimerkiksi valtaushyökkäyksessä datasuoratoisto jaetaan neljäksi paketiksi p1, p2, p3 ja p4. Hyökkääjä saattaa ensin lähettää paketit p1 ja p3 kohdesovellukselle. IDP-alisysteemi ja kohdesovellus säilyttävät näitä paketteja, kunnes loput paketit saapuvat uudelleenkokoamista varten. Tämän jälkeen hyökkääjä lähettää paketit p2’ ja p3’, jotka kohdesovellus hylkää ja IDP-alijärjestelmä hyväksyy. IDP-alijärjestelmä voi nyt suorittaa kokoamisen, koska luulee pitävänsä hallussaan kokonaista suoratoistoa. Nyt hyökkääjä lähettää paketit p2 ja p3, jotka kohdesovellus hyväksyy ja joka voi nyt suorittaa kokoamisen. Tuloksena on eri datasuoratoiston kuin se, minkä IDP-alijärjestelmä näkee. Hyökkäykseltä suojautumisen ollessa päällä CorePlus korjaa automaattisesti datastreamin ja poistaa siitä ylimääräisen hyökkäykseen assosioidun datan.

Onnistuneesta hyökkäyksen estosta jää lokiin merkintä ”Attack Detected” ja tunnistamattomasta potentiaalisesta hyökkäyksestä jää merkintä ”Unable to Detect”. [8, s. 284-290.]

Kuten antivirus-moduulissa, IDP-moduulin toimintaa voi tehostaa valinnaisella laitteiston päivityksellä, joka on saatavilla laitteisiin SG40, SG4200 ja SG4400. Laitteen kellonaika on myös tärkeä laittaa oikein päivitysten kannalta. [8, s. 284-290.]

3.2.9 Web-sisällönsuodatus

Web-liikenne on yksi suurimmista turvallisuusongelmien aiheuttajista. Huolimattomat internetin selailutavat altistavat verkon monilla turvallisuusuhille. HTTP ALG:n kautta CorePlus tarjoaa kolme työkalua suodattamaan web-sisältöä, jonka on katsottu olevan sopimatonta organisaation tai ryhmän käyttäjille. Työkaluja ovat aktiivinen sisällönkäsittely, staattinen sisällönsuodatus ja dynaaminen sisällönsuodatus. [8, s. 261-265.]

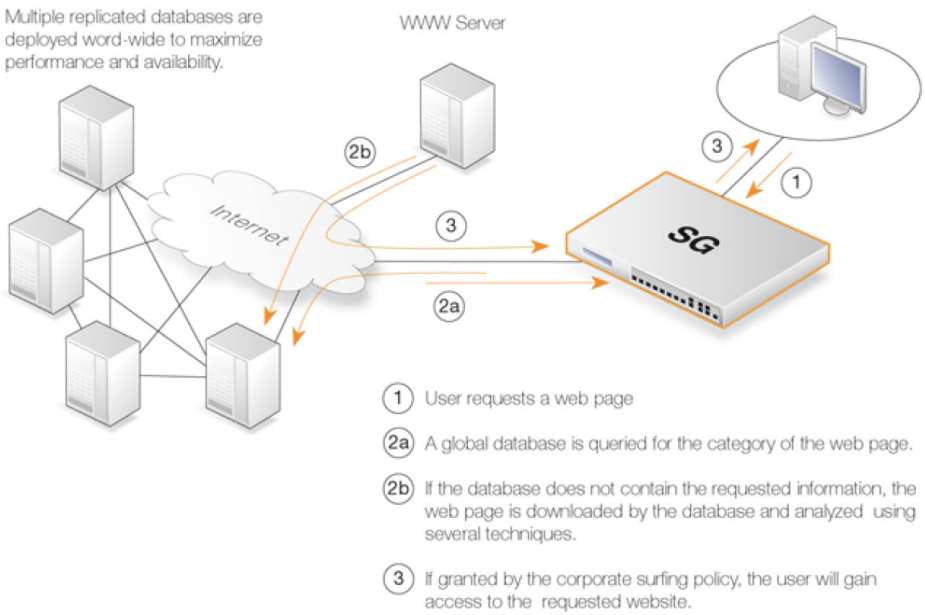
Sisältöä voidaan haluta käsitellä, jotta voitaisiin estää työasemalle ja verkolle vahingollisen koodin leviämisen käyttäjän selaillessa sivustoja internetissä. Tyypillisesti tällainen koodi on sulautettu erilaisiin objekteihin tai tiedostoihin, jotka on puolestaan sulautettu web-sivulle. Aktiivinen sisällönkäsittely pystyy poistamaan web-sivuilta ActiveX-komponentit, Java-sovelmat, Javascript/VBScript-koodin, evästeet ja virheellisesti muotoillut UTF-8-merkit. Poistettavat objektityypit voidaan valita erikseen konfiguroimalla vastaava HTTP ALG niitä vastaavasti. Poistettavien objektien kanssa täytyy olla tarkkana, ettei poistaminen johda vahingossa vääriin tuloksiin. Esimerkiksi jotkut web-sivustot saattavat lakata kokonaan toimimasta. [8, s. 261-265.]

HTTP ALG:n kautta CorePlus pystyy estämään tietyt web-sivustot perustuen konfiguroituihin URL-listoihin, joita kutsutaan mustiksi ja valkoisiksi listoiksi. Tämänkaltaista suodatusta kutsutaan staattiseksi sisällönsuodatukseksi. Sen suurin etu on, että sillä voidaan valita, sallitaanko vai estetäänkö tietyt sivustot. Staattinen sisällönsuodatus suoritetaan aina ennen dynaamista sisällönsuodatusta, joten sillä voi tehdä poikkeuksia dynaamisen sisällönsuodatuksen automaattiseen luokitteluun. Esimerkiksi, jos välttämättä halutaan ostaa tietystä online-kaupasta tarvikkeita ja dynaaminen sisällönsuodatus on asetettu estämään ostossivut estämällä kategoria ”ostosten tekeminen”, silloin voidaan halutun online-kauppasivuston URL lisätä HTTP ALG:n

valkoiseen listaan, jolloin pääsy lisättyyn URL:iin on aina sallittu. Konfiguroitavat URL-listat tukevat jokerimerkkinä *-symbolia, jonka avulla voi mm. määrittää kokonaisia sivustopolkuja. [8, s. 261-265.]

CorePlus tukee web-liikenteen dynaamista sisällönsuodatusta, joka antaa ylläpitäjän sallia tai estää pääsy web-sivuille perustuen kyseisten sivujen sisältöön. Tämä toiminto on automatisoitu eikä sallittavia tai estettäviä URL:eja tarvitse syöttää käsin. Clavister ylläpitää maailmanlaajuista tietokantojen infrastruktuuria, joka sisältää valtavan määrän tämän hetkisiä web-sivujen URL- osoitteita. Osoitteet on jaettu kategorioihin, kuten ostosten tekeminen, uutiset, urheilu, aikuisille suunnattu jne. Näitä tietokantoja päivitetään jatkuvasti poistamalla vanhoja virheellisiä URL:eja ja lisäämällä uusia. [8, s. 261-265.]

Kun käyttäjä lähettää pyynnön web-sivulle, CorePlus lähettää kyselyn tietokantaan saadakseen vastauksena pyydetyn sivun kategorian (kuva 14). Käyttäjän pääsy sivulle riippuu kategoriassa vallitsevasta suodatuskäytännöstä. Jotta prosessi olisi nopeampi, CorePlus ylläpitää paikallisessa välimuistissa viimeisimpänä käytettyjä URL:eja. Tämä voi olla yllättävänkin tehokasta, koska samassa yhteisössä olevilla on tapana käyttää samankaltaisia sivuja. Jos pyydettyä web-sivua ei löydy tietokannasta, sivun sisältö ladataan automaattisesti Clavisterin keskusdatavarastolle, jossa se automaattisesti analysoidaan käyttäen erilaisia tekniikoita. Kategorisoinnin jälkeen URL levitetään maailmanlaajuisesti tietokantoihin, josta CorePlus saa pyytämälleen URL:ille kategorian. On hyvä huomioida, että ainoastaan yksittäisiä sivuja kategorisoidaan, ei kokonaisia sivustoja. [8, s. 261-265.]



Kuva 14. Käyttäjän käynnistämä sisällönsuodatusprosessi. [8, s. 265.]

3.2.10 Liikenteen hallinta

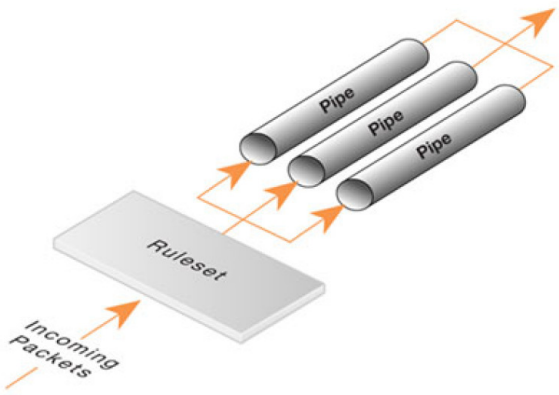
Seuraavaksi kerrotaan neljä tapaa, miten CorePlus pystyy hallitsemaan liikennettä. Tapoja ovat liikenteen muokkaus, kynnysarvosääntö, IDP-liikenteen muokkaus ja palvelimen kuormanjako. [8, s. 385-409.]

Liikenteen muokkaus

TCP/IP:n heikkous on kunnollisen palvelun laadun varmistuksen, QoS:n, puute. Tähän ongelmaan on kehitetty ratkaisuja, kuten esimerkiksi Diffser-arkkitehtuuri, jossa käytetään hyväksi pakettien tunnisteiden sisältämää tietoa. CorePlus tukee DiffServiä edelleen lähettämällä kuusi DSCP:n muodostavaa bittiä kapseloitaviin paketteihin. Bitit kopioidaan Ethernetin VLAN-kehysten prioriteetti QoS-bitteihin ulosmenevään rajapintaan. Sisempien pakettien koko DSField kopioidaan IPsec-tunnelien ESP-pakettien ulompiin IP-tunnisteisiin. Diffserv-arkkitehtuurikin on puuttellinen, koska sovellukset itse tarjoavat verkolle QoS-informaatiota. Parempi on, jos verkkolaitteet tekevät päätökset prioriteettien ja siirtokaistanvarausten perusteella. CorePlus tarjoaa QoS-hallintaa antamalla ylläpitäjän määrätä rajoitukset ja varmistukset Security Gatewayn läpi kulkevalle liikenteelle. Tätä tapaa kutsutaan liikenteen muokkaukseksi ja sitä voidaan soveltaa kaikenlaiseen liikenteeseen, mukaan lukien VPN-tunnelien läpi kulkevaan liikenteeseen. Liikenteen muokkauksessa voidaan asettaa siirtokaistalle rajoituksia ja laittaa paketteja

jonoihin. Ne paketit, jotka ylittävät konfiguroidut rajat, lähetetään myöhemmin siirtokaistan vaatimusten ollessa pienemmät. Muita toimintoja ovat pakettien pudottaminen pakettipuskurien täyttyessä, liikenteen priorisointi ylläpitäjän päätösten mukaan ja vaaditun siirtokaistan takaaminen korkean prioriteetin omaavalle liikenteelle. Priorisoidun liikenteen määrä mitataan ja priorisoimaton liikenne rajoitetaan dynaamisesti, jotta se ei häiritse priorisoidun liikenteen suoritustehoa. [8, s. 385-409.]

CorePlussan liikenteen muokkauksen avaintekijät ovat putket ja putkisäännöt. Putki on liikenteen muokkauksessa keskeinen objekti ja käsitteellinen kanava, jonka läpi data virtaa. Ylläpitäjä voi määritellä niin monta putkea kuin tarvitaan. Putkista voi myös tehdä putkiketjuja, jotka voivat koostua enintään kahdeksasta putkesta. Putki on yksinkertainen eikä se välitä liikenteen tyypistä tai suunnasta. Se vain mittailee dataa ja toimeenpanee ylläpitäjän konfiguroimia rajoituksia. Putki myös ottaa huomioon etuarvojärjestykset ja ryhmät. Putkisäännöt muodostavat putkisäännöstön (kuva 15), jossa sääntöjen määrittäminen on samankaltainen kuin muissakin CorePlussan käytännöissä. Kun uusi yhteys on IP-säännöstön puolesta sallittu, suoritetaan aina putkisäännöstön vertailu täsmäävän säännön varalta. Putkisääntöä määriteltäessä myös kaikki säännön kanssa käytettävät putket määritellään, jonka jälkeen sääntö laitetaan joko lähtevien tai saapuvien ketjuun. [8, s. 385-409.]



Kuva 15. Putkisäännöstö jakaa paketit putkiin. [8, s. 387.]

Kynnysarvosääntö

Kynnysarvosäännön on tarkoituksena havaita epänormaali liikenne ja reagoida siihen. Esimerkki epänormaalista toiminnasta voisi olla sisäisen isän-

nän altistuminen virukselle, joka ottaa toistuvia yhteyksiä ulkoisiin IP-osoitteisiin. Vaihtoehtoisesti joku ulkoinen lähde voisi yrittää avata suuren määrän yhteyksiä sisäänpäin. Kynnysarvosääntö on kuin normaali käytäntöpohjainen sääntö. Jokaiseen sääntöön voi assosioida yhden tai useamman toiminnon, jotka määrittävät, kuinka eri kynnysarvotiloja täytyy käsitellä. Kynnysarvolla on parametreinaan [8, s. 385-409.]

- Action, toimintoreaktio rajan ylittämiseen, joko seuraa tai suojaa.
- Group By, joko isäntä- tai verkkopohjainen.
- Threshold, numeerinen kynnysarvo, jonka ylittäminen laukaisee reaktion.
- Threshold Type, rajoittaa yhteyksiä sekuntikohtaisesti tai rajoittaa kokonaismäärän samanaikaisista yhteyksistä.

Yhteyden nopeuden rajoittaminen sallii ylläpitäjän rajoittaa uusien Security Gatewayhin avattavien yhteyksien määrää sekuntia kohden, kun taas koko yhteyksien rajoittamisessa voidaan asettaa rajoitus yhteyksien kokonaismäärän perusteella. Jälkimmäinen on erityisen kätevä silloin, kun paljon NAT-pooleja tarvitaan vertaisverkkokäyttäjien takia. [8, s. 385-409.]

Ryhmittely voidaan järjestää joko perustuen isäntään tai verkkoon. Isäntään perustuvassa ryhmittelyssä kynnysarvo laitetaan yhteyksiin, jotka on eroteltu IP-osoitteilla. Verkkoon perustuvassa ryhmittelyssä kynnysarvo laitetaan kaikkiin yhteyksiin, joihin säännöt täsmäävät. Kun kynnysarvo ylittyy, yhteyttä auditoidaan tai ylittymisen aiheuttava yhteys pudotetaan. Sääntötoimintojen nimet ovat ”Audit” ja ”Protect”. Ylittymisen aiheuttaja voidaan laittaa suoraan mustalle listalle identifioituna IP-osoitteella tai verkolla. Jos useampi sääntötoiminto täytyy suorittaa, toiminnot suoritetaan siinä järjestyksessä kuin ne ilmestyvä käyttäjän rajapintaan. Jos useat samaan tyyppi ja ryhmittely-yhdistelmään kuuluvat toiminnot ylittävät kynnysarvon samanaikaisesti, ainoastaan korkeimman kynnysarvon omaava toiminto kirjautuu lokiin. [8, s. 385-409.]

IDP-liikenteen muokkaus

IDP-liikenteen muokkaus ominaisuus perustuu CorePlus IDP-alijärjestelmästä tulevaan informaatioon. Pääasiassa IDP-liikenteen muok-

kausta käytetään liikenteen hallintaongelmien, kuten paljon siirtokaistaa vievien sovellusten kanssa toimimiseen. Tyypillisiä tällaisia sovelluksia ovat esimerkiksi vertaisverkko-ohjelmat, kuten Direct Connect ja Bit Torrent. Vertaisverkkojen tuottamilla suurilla verkkokuormilla voi olla huono vaikutus toisten verkon käyttäjien palveluiden laatuun. ISP:n tai yrityksen verkon ylläpitäjä voi sellaisissa tapauksissa rajoittaa suuren kuorman aiheuttavien sovellusten saamaa siirtokaistaa mm. IDP-liikenteen muokkaus sovelluksella. Tärkeä osa tätä järjestelmää on kontrolloitavan liikenteen tunnistaminen muusta liikenteestä. CorePlussassa IDP:n signeeraustietokanta tarjoaa tähän tehokkaan keinon ja lisäksi tunnistamisen jälkeen liikenne voidaan viedä nopeasti liikenteen muokkausalijärjestelmän läpi. IDP-liikenteen muokkaus on näiden kahden ominaisuuden yhdistelmä, jossa IDP-alijärjestelmän tunnistettua liikennevirran automaattisesti asetetaan liikenteen muokkausputket kontrolloimaan virtoja. [8, s. 385-409.]

IDP-liikenteen muokkaus asetukset laitetaan toimintaan määrittelemällä ensin IDP-sääntö, joka laukeaa tietyn liikenteen takia. Sitten valitaan sääntötoiminto putkivaihtoehdoksi ja siirtokaista-arvo säännölle. Tämän jälkeen voidaan valinnaisesti määrittää aikaikkuna sekunneissa ja vielä lopuksi voitaisiin määrittää haluttu verkko. [8, s. 385-409.]

Koko IDP-liikenteen muokkauksen prosessiketju alkaa siitä, kun uusi yhteys isännältä isännällä avataan läpi Security Gatewayn. CorePlus kirjaa itselleen yhteyden lähde- ja kohde-IP-osoitteet. Yhteyden liikennevirta laukaisee IDP-säännön, jolla on putki toimintonaan. Tästä syystä yhteyden liikenne on nyt IDP-säännössä määritellyn putken liikenteen kaistanleveyden muokkauksen aiheena. Sitten avataan uusi yhteys, joka ei laukaise IDP-sääntöä. Yhteydellä pitää kuitenkin olla joko sama lähde- tai kohde-IP-osoite kuin aikaisemmin säännön laukaisseella yhteydellä oli. Jos IP-osoite kuuluu verkoksi määriteltyyn IP-alueeseen, yhteyden liikenne sisältyy putkeen, joka suorittaa liikenteen muokkauksen myös alkuperäiselle säännön laukaisevalle yhteydelle. Vaikka verkkoa ei olisi määritelty, uusi yhteys sisältyisi silti säännön laukaisevan yhteyden putken liikenteeseen, jos vain lähde tai kohde täsmää. [8, s. 385-409.]

Palvelimen kuormanjako

Palvelimen kuormanjako, SLB, on CorePlussan ominaisuus, jolla voidaan parantaa verkon suorituskykyä, skaalautuvuutta, luotettavuutta ja ylläpidon hoitoa. SLB sallii verkkopalveluiden tarpeiden jakamisen monen palvelimen kesken. Tämä lisää suorituskykyä ja skaalautuvuutta, koska palvelinfarmit pystyvät käsittelemään suuremman määrän pyyntöjä kuin yksittäinen palvelin. SLB lisää verkkosovellusten luotettavuutta monitoroimalla kuormaa jakavia palvelimia aktiivisesti. Se havaitsee, jos palvelin menee tukkoon, eikä enää ohjaa sille pyyntöjä ennen kuin sen toiminta normalisoituu. Ylläpitäminen helpottuu, kun palvelimille voidaan suorittaa huoltotoimenpiteitä keskeyttämättä palveluita. Yksittäiset palvelimet voidaan päivittää, käynnistää uudelleen, poistaa tai korvata. Myös uusia palvelimia ja sovelluksia voidaan lisätä häiritsemättä palvelun toimintaa. CorePlus SLB voidaan ottaa käyttöön IP-säännöstön SLB_SAT-sääntöjen kautta ja nämä säännöt antavat mahdollisuuden valita kuormanjakoon sopivan algoritmin tarpeen mukaan. SLB:tä käytettäessä neljää asiaa pitäisi harkita: kuormanjakoon osallistuvat palvelimet, kuorman levitystila, käytetty SLB-algoritmi ja monitorointitapa. [8, s. 385-409.]

3.2.11 Käyttäjän autentikointi

Ylläpitäjä voi vaatia käyttäjien autentikointia käyttäjien ottaessa yhteyttä suojattuun lähteeseen Security Gatewayn läpi, jossa onnistunut autentikointi takaa pääsyn lähteeseen. Autentikointi perustuu käyttäjän identiteetin todistamiseen. Todisteena siitä voidaan käyttää jotain, mitä käyttäjä on, käyttäjällä on tai käyttäjä tietää. Näitä ovat esimerkiksi sormenjäljet, digitaaliset passit ja salasanat. Yleisimmin käytetään kahta jälkimmäistä todisteryhmää ja niiden yhdistelmiä turvallisuuden parantamiseksi. Esimerkiksi digitaalinen passi voi vaatia salasanaksi PIN-koodin toimiakseen. [8, s. 316-326.]

Seuraavaksi käsitellään käyttäjän autentikointia salasanan ja käyttäjänimen yhdistelmällä. Tähän menetelmään tarvitaan autentikointisäännön käyttämiä tietokantoja, joista se tarkastaa käyttäjän salasana ja nimi yhdistelmät, joita ovat paikallinen tietokanta sekä RADIUS- ja LDAP-palvelimet. Myös käyttäjän autentikointisääntöjä tarvitaan, jotka kuvailevat autentikoitavan liikenteen ja autentikaatiolähteen sekä IP-objekteja tarvitaan autentikoitavien asiakkaiden IP-osoitteille. Lisäksi tarvitaan IP-sääntöjä sallimaan autentikoinnin tapahtuminen ja pääsy haluttuun paikkaan. [8, s. 316-326.]

Paikalliset käyttäjätietokannat ovat ylläpitäjän CorePlussaan määrittämiä rekistereitä, jotka sisältävät valtuutettujen käyttäjien ja ryhmien profiilit. Käyttäjänimi/salasana yhdistelmät kirjoitetaan niihin ja salataan käänteisellä salauksella. Yksittäisen käyttäjän voi halutessa lisätä yhden tai useamman ryhmän jäseneksi. Autenkikointiryhmillä ei ole riippuvuutta autentikointisääntöihin, mutta ne ovat assosioitu IP-objekteihin, joita sitten käytetään IP-säännöstössä. Käyttäjän määrittelemää IP-objektia voidaan käyttää määriteltäessä lähdeverkkoa IP-sääntöön ja ryhmä voidaan assosioida kyseiseen IP-objektiin. Tällöin IP-sääntö astuu voimaan vain niillä sisään kirjautuneilla käyttäjillä, jotka kuuluvat myös lähdeverkon ryhmään. Tämän tarkoituksena on estää niiden pääsy tiettyihin ryhmiin, jotka eivät kuulu samaan ryhmään kuin säännön lähdeverkon ryhmä. [8, s. 316-326.]

Suuremmissa verkkotopologioissa voidaan keskusautentikointitietokanta ylläpidon työmäärän vähentämiseksi laittaa siihen tarkoitetulle tietylle palvelimelle. Ulkoinen autentikointipalvelin voi validoida käyttäjänimen ja salasanan yhdistelmiä vastaamalla CorePlussan pyyntöihin. Tämän mahdollistaa RADIUS-protokolla. CorePlus toimii RADIUS-asiakkaana lähettäen RADIUS-viestissä käyttäjän suosituksia ja yhteyden paramteri-informaatiota nimitetylle RADIUS-palvelimelle. Palvelin prosessoi pyynnöt ja lähettää vastauksena joko hyväksyvän tai kielteisen vastauksen. Yhden tai useamman ulkoisen palvelimen voi määritellä. Molemmille, RADIUS-asiakkaalle ja palvelimelle, konfiguroidaan jaettu avain. Jaettu avain salaa RADIUS-asiakkaalta palvelimelle lähetettävät viestit. Avain voi sisältää enintään 100 merkkiä ja on merkkikokoriippuvainen. RADIUS käyttää PPP:tä käyttäjänimen ja salasanan siirtoon asiakkaan ja palvelimen välillä ja käyttää PPP-autentikointeja PAP:ia ja CHAP:ia. Viestit lähetetään UDP-viesteinä portin 1812 kautta. [8, s. 316-326.]

Ulkoisia LDAP-palvelimia voi käyttää CorePlussan kanssa myös autentikointilähteenä. Tämä toteutetaan niin, että Security Gateway toimii asiakkaan yhdelle tai useammalle LDAP-palvelimelle. Voi olla järkevä konfiguroida monta palvelinta tarjoamaan redundanssia, jotta aina olisi palvelin saavutettavissa. Kun käyttäjän autentikointi määritellään LDAP-palvelinten kanssa, täytyy CorePlussaan aluksi määrittää LDAP-palvelinobjekti käyttäjän autentikointia varten ja määritellä lista näistä palvelinobjekteista käyttäjä-autentikointi-sääntöön. Yhden tai useamman LDAP-palvelinobjektin voi mää-

ritellä CorePlussassa. Ne kertovat palvelimelle, mitkä LDAP-palvelimet ovat saatavilla ja kuinka niihin päästään käsiksi. Yleisiä parametreja palvelinten konfigurointiin ovat palvelimen nimi ja IP-osoite, portin numero, autentikoinnin aikakatkaisu, reititystaulu, palvelimen tyyppi ja toimialueen nimi. Palvelinautentikointi on automaattisesti konfiguroitu toimimaan käyttäen LDAP-yhdistämispyyntöautentikointia. Tämä tarkoittaa sitä, että autentikointi onnistuu, jos yhteys LDAP-palvelimelle onnistuu. Yksittäisiä asiakkaita ei erotella toisistaan. Kun vähintään yksi palvelinobjekti on määritelty, täytyy hankkia niihin viittaava käyttäjä autentikointisääntö. Yhden tai useamman palvelinobjektin voi assosioda listaksi käyttäjä autentikointisäännön kanssa. Palvelinten järjestys listalla osoittaa, missä järjestyksessä palvelimiin otetaan yhteyttä. Ylimpänä listassa olevat käydään aiemmin läpi kuin alempana olevat. Kun LDAP-palvelimelle lähetetään käyttäjä autentikointikysely, seurauksena on mahdollisesti palvelimen positiivinen vastaus ja käyttäjän onnistunut autentikointi, palvelimen negatiivinen vastaus ja käyttäjän epäonnistunut autentikointi tai palvelin ei vastaa aikakatkaisuun mennessä. Jos viimeisessä kohdassa ei ole muita palvelimia, autentikointia voidaan pitää epäonnistuneena. Palvelimia voidaan myös monitoroida reaaliajassa. Monitorointi vaihtoehtoja ovat onnistuneet/epäonnistuneet autentikointipyynnöt, autentikointien kokonaismäärä, montako autentikointia toteutuu sekunnissa sekä väärien tunnusten ja salasanojen määrä. [8, s. 316-326.]

Autentikointisääntöön määritellään säännön aiheena oleva liikenne. Säännöt rakentuvat muuten samankaltaisesti kuin muut CorePlussan turvallisuuskäytännöt, mutta se ei ole kiinnostunut kohde rajapinnasta eikä verkosta. Autentikointisäännöllä on käytössään parametrit, jotka koskevat rajapintaa, IP-lähdeosoitetta, autentikointilähdettä ja liikenteen autentikointitapaa. Autentikointitapa voi olla HTTP/HTTPS, L2TP/PPP tai XAUTH. Autentikointisääntö voi määritellä kahdenlaisia aikakatkaisuja perustuen, joko yhteyden enimmäisolemassaoloaikaan tai yhteyden toimettomana olo aikaan. Lisäksi autentikointisääntö voi määritellä miten yhteyksien käsitellään, jos monesta eri IP-lähdeosoitteesta yritetään kirjautua samoin tunnuksin. [8, s. 316-326.]

Kätevä autentikointityyli on HTTP-autentikointi web-selaimella, jossa käyttäjä kirjoittaa HTML-sivulle tarvittavat tiedot. Sitä käytettäessä täytyy ottaa huomioon, että HTTP-autentikointi ja WebUI käyttävät samaa TCP-porttia 80, joten se kannattaa WebUI:lta vaihtaa vaikkapa portiksi 81. Autentikointiin on

olemassa valmiita valintoja kirjautumistyypiksi. Lisäksi CorePlussassa on valmiita muokattavia banneri-tiedostoja, joista käyttäjälle näytettävä banneri riippuu kirjautumisen menestyksestä. [8, s. 316-326.]

3.2.12 Korkea saatavuus

Korkea saatavuus toiminto, HA, saadaan käyttöön lisäämällä yhden Security Gatewayn orjaksi olemassa olevan herra, Security Gatewayn rinnalle. Orja ja herra ovat yhteydessä toisiinsa ja muodostavat loogisen HA-klusterin. Klusterissa toinen yhdyskäytävä on aktiivisessa tilassa ja toinen on valmiustilassa. Aluksi orja on valmiustilassa ja monitoroi herraa. Jos orja havaitsee, että herra ei vastaa, niin vian korjaus käynnistyy ja orjasta tulee aktiivinen. Vaikka herra myöhemmin taas palautuisi kuntoon, pysyy orja silti aktiivisena siihen asti kunnes jotakin vikaa ilmenee. Osat siis muuttuvat vaihdon jälkeen ja nyt herra monitoroi orjaa. Yhdyskäytävien herra ja orja nimet ovat pysyviä ja vain aktiivisuustila muuttuu. Jotta yhteys orjan ja herran välillä toimii oikein, on ne yhdistettävä toisiinsa ristikytkentäpiuhalla. Käytettäväksi rajapinnaksi täytyy valita yksi normaaleista rajapinnoista kummaltakin laitteelta. Niiden välistä synkronisointi yhteyttä kutsutaan CorePlussassa sync-rajapinnaksi. Paketteja, joita kutsutaan sydämenlyönneiksi, lähetetään jatkuvasti sync:in ja muiden rajapintojen yli laitteesta toiseen. Näin toisen kuntoa voidaan monitoroida. Paketteja lähetetään molempiin suuntiin, jotta molemmat yksiköt tietävät toistensa kunnon. [8, s. 417-418.]

HA-klusteri lisää verkon redundanssia, koska kahdella laitteella on pienempi todennäköisyys mennä toimintakyvyttömäksi kuin yhdellä. Täytyy kuitenkin muistaa pitää huolta muiden verkonlaitteiden redundanttisuudesta. Itse klusteria hallitaan niin kuin se olisi erillinen laite ja sillä on uniikki klusterinimi, joka näkyy hallintarajapinnassa yksittäisenä loogisena Security Gatewaynä. Ylläpitäjän tekemät toimenpiteet, kuten IP-säännöstön sääntöjen muutokset suoritetaan normaalisti muutosten päivittyessä automaattisesti sekä orjaan että herraan. Mitään kuormanjakoa HA-klusteri ei voi tarjota, koska valmiustilassa oleva yhdyskäytävä voi vain tarkkailla aktiivisen yhdyskäytävän tilaa ja päivittää itselleen viimeisimmät tiedot. Lisäksi klusterin voi muodostaa ainoastaan kaksi Clavister Security Gatewaytä. Käytettävissä laitteissa on oltava identtiset lisenssiavaimet ja olisi hyvä, jos laitteissa olisi identtiset konfiguraatiot. [8, s. 417-418.]

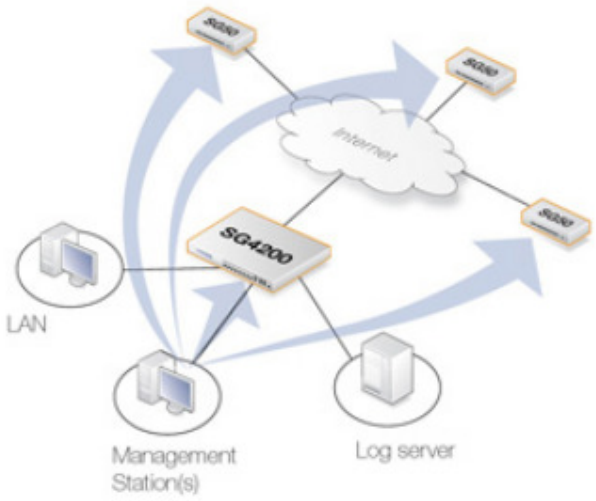
CorePlussassa on linkin monitorointi ominaisuus, jolla voidaan monitoroida tiettyjen verkkopolkujen toimivuutta lähettämällä ICMP-pyyntöjä tietyille isännille. Jos isännät eivät vastaa, polkua voidaan pitää toimimattomana. Siinä tapauksessa voidaan vian korjaus aloittaa, koska valmiustilassa ollut laite saattaa käyttää toista polkua, jolloin liikenne voi taas virrata. [8, s. 417-418.]

3.3 Clavisterin käyttöä tehostavat ohjelmat

Clavisteriin on olemassa erilaisia lisäohjelmia, jotka tuovat uusia ulottuvuuksia Security Gatewayn hallintaan. Alla on esitelty kyseisistä ohjelmista kolme.

3.3.1 FineTune

FinteTune toimii Windows-ympäristössä ja on graafisella käyttöliittymällä varustettu ohjelma, jolla voi keskitetysti etähallita monia CorePlus-laitteita (kuva 16). Ohjelmalla voi konfiguroida, monitoroida ja jopa suorittaa firmware päivityksiä. Yhteys on salattu 128-bittisellä salauksella ja autentikoinnilla. [9.]



Kuva 16. FineTunella voi etähallita monia CorePlus-laitteita. [9.]

Järjestelmän tiedostoturvalliset tarkastukset estävät virheellisen konfiguroinnin pysäyttämästä CorePlussaa tai lukitsemasta ylläpitäjää ulos. Nämä valinnat suunnittelussa auttavat pitämään TCO:n alhaisena. [9.]

Kaikki CorePlus-konfiguroinnit on turvallisuussyistä keskitetysti arkistoitu. Tämän ansiosta käytössä olevan CorePlussan voi vaihtaa muutamassa mi-

nuutissa. Myös vanhemmat konfigurointi versiot säilytetään, jotta ylläpitäjällä on mahdollisuus ottaa takaisin käyttöön haluamansa vanhempi konfiguraatio. Lokitiedot kaikista laitteista lähetetään yhdelle tai useammalle lokitietojen vastaanottajalle, joka on joko Clavister Logger -ohjelma tai yleinen syslog-vastaanottaja. Se, mitä tietoja lokiin kirjoitetaan, on pitkälle itse määriteltävissä. Lokitiedot voidaan analysoida FineTuneen integroitavalla advanced log analyzer -työkalulla tai sitten lokitiedot voi siirtää toisiin ohjelmiin jatkotutkimuksia varten. [9.]

3.3.2 InSight

InSight tarjoaa reaaliaikaista turvallisuustekoälyä auttaakseen selvittämään hakkerin tai viruksen käyttäytymisen voittaakseen turvallisuusuhat ja noudattaakseen verkon sääntöjä. InSight voidaan asentaa, joko erillisesti tai jaetusti. InSightin pääominaisuuksia ovat keskitetty lokien hallinta, reaaliaikainen monitorointi ja varoitukset, kattava raportointi ja tekninen analysointi. [10.]

Lokien hallinta on keskitetty ja on skaalautuva tuhansiin laitteisiin. Se automaattisesti kerää, normalisoi, kokoaa yhteen, pakkaa, salaa ja arkistoi lokitietoja eri valmistajien laitteista, kuten reitittimistä, kytkimistä, palomuureista ja IDS/IPS:stä. Organisaatiot voivat siten tehokkaammin identifioida turvallisuusmurroksia sekä hakkeri-, tunkeutumis- ja virusaktiviteettia. [10.]

Monitorointi ja varoitusjärjestelmä toimii reaaliaikaisesti ja saa tietoja koko verkon turvallisuustapahtumista. Ohjelma korreloi turvallisuustapahtumia, joka vähentää vääriä hälytyksiä. Sen kojetaulusta voi helposti nähdä verkossa tapahtuvat turvallisuusongelmat. Siten epäilyttäviä tapahtumia voidaan seurata ja tehdä oikeat päätökset ennen kuin kukaan pääsee salaisiin tietoihin käsiksi tai virus pääsee leviämään. [10.]

Raportointijärjestelmä tuottaa informaatiota, jonka avulla organisaatiot voivat analysoida ja kehittää toimenpiteitään turvallisuusoperaatioissa. Raportoinnin ohella järjestelmä mm. antaa pääsyn yli 1500:n raporttiin ja korreloi raportteja. [10.]

Tekninen analysointi mahdollistaa tapahtumien tutkimisen pitkänkin ajan päästä välikohtauksen jälkeen. Tämä on siksi tärkeää, koska turvallisuus informaation tutkimisessa kehitytään koko ajan. InSightilla pystytään tutkimaan satoja gigoja tämän hetkistä sekä vanhaa lokitietoa. Tekninen analysointi

mahdollistaa miljoonien verkkotapahtumien tehokkaan läpikäymisen, joka varmistaa, että sääntöjä on noudatettu oikein. [10.]

3.3.3 PinPoint

PinPoint näyttää monitoroimansa ja analysoimansa tiedot kojetaulutyyppisessä näkymässä (kuva 17). Se näyttää visuaalisesti CorePlussan tilan ja antaa tarvittaessa tarkentaa syvemmälle haluttuun yksityiskohtaan. Esimerkiksi mittareista voisi helposti nähdä, jos internetin käyttö nousisi epäilyttävän korkealle. PinPointissa tulee valmiina ennalta määriteltyjä malleja yleisimpiin monitorointi skenaarioihin. Ohjelma soveltuu niin yksittäisen kuin useammankin CorePlussan seuraamiseen. [11.]

Kuva 17. PinPointin kojetaulu. [11.]

3.4 Tuoteperhe

Tuoteperhe perustuu Security Gatewayhin, joka voi toimia erilaisissa ympäristöissä. Kolme ryhmää, joihin toteutukset jaetaan, ovat laite-, ohjelma- ja virtuaalitoteutus.

3.4.1 Laitetoteutus

Security Gateway -laitteita on kevyeen liikenteeseen tarkoitetusta SG10-sarjasta raskaalle liikenteelle tarkoitettuun SG5500-sarjaan. Alla olevista kuvista 18, 19 ja 20 voi nähdä mm. laitteiden mallit, datankäsittely nopeudet salauksella ja ilman, samanaikaisesti tuettujen yhteyksien määrät ja tuetut rajapinnat. [12.]

SG 10 -sarja on tarkoitettu laajan verkon haarakonttoreihin ja keskushallittuihin kotitoimistoihin. SG 50 -sarja on suunnattu pienille ja keskisuurille organisaatioille sekä etätoimistoihin ja haarakonttoreihin (kuva 18). [12.]

	SG 10		SG 50			
						
System Performance	**12**	**15**	**51**	**53**	**55**	**57**
Plaintext Throughput (Mbps)	50	50	50	75	100	200
AES/3DES Throughput (Mbps)	25/25	25/25	20/20	20/20	40/40	40/40
Concurrent Connections	4,000	4,000	4,000	8,000	16,000	32,000
Concurrent VPN Tunnels	2	2	25	50	100	200
Ethernet Interfaces	2x100BASE-TX 4x100BASE-TX	2x100BASE-TX 4x100BASE-TX	3x100BASE-TX 7x100BASE-TX	3x100BASE-TX 7x100BASE-TX	3x100BASE-TX 7x100BASE-TX	3x100BASE-TX 7x100BASE-TX
Virtual Interfaces (VLAN)	4	4	4	8	32	64
Virtual Systems & Virtual Routers	-	-	5	5	5	5
Users	10	25	Unlimited			

Kuva 18. SG 10 - ja SG 50 -sarjan laitteiden alasarjat ja ominaisuudet. [12.]

SG 3200 -sarja on tehty pienien ja keskisuurten yritysten käyttöön sekä keskusyhdyskäytäväksi keskisuurille VPN-verkoille. SG 4200 -sarja sopii mm. suurten yritysten pääkonttoreihin, finanssilaitoksiin, keskusyhdyskäytäväksi suuriin VPN-verkkoihin, datakeskuksiin, teleteollisuuteen ja palvelun tarjoajille monigigabittistä verkkokuormaa varten (kuva 19). [12.]

	SG 3200			SG 4200		
						
System Performance	**3210**	**3230**	**3250**	**4210**	**4230**	**4250**
Plaintext Throughput (Mbps)	350	500	1000	750	1,500	2,500
AES/3DES Throughput (Mbps)	100	150	250	250/250	400/400	1.000/1.000
Concurrent Connections	32,000	128,000	256,000	256,000	512,000	1,000,000
Concurrent VPN Tunnels	250	400	600	1,000	2,000	5,000
Ethernet Interfaces	6 x 1000BASE-TX			8xSFP (Mini-GBIC) 2x1000BASE-TX 4x100BASE-TX	8xSFP (Mini-GBIC) 2x1000BASE-TX 4x100BASE-TX	8xSFP (Mini-GBIC) 2x1000BASE-TX 4x100BASE-TX
Virtual Interfaces (VLAN)	64	128	256	512	1,024	2,048
Virtual Systems & Virtual Routers	5 + up to 25 additional			10 + up to 500 additional		
Users	Unlimited			Unlimited		

Kuva 19. SG 3200 - ja SG 4200 -sarjan laitteiden alasarjat ja ominaisuudet. [12.]

SG 4400 ja SG 5500 -sarja soveltuu keskusyhdyskäytäväksi korkean kuorman VPN-verkkoihin, teleteollisuuteen, kantoaaltoverkkoihin ja datakeskuksiin, joissa on käytössä IPsec VPN -palvelut (kuva 20). [12.]

	SG 4400				SG 5500
					
System Performance	**4410**	**4430**	**4450**	**4470**	**5500 blade**
Plaintext Throughput (Mbps)	750	1,500	2,500	4,000	3000
AES/3DES Throughput (Mbps)	350/350	500/500	1,000/1,000	1,000/1,000	2000
Concurrent Connections	256,000	512,000	1,000,000	5,000,000	10.000.000
Concurrent VPN Tunnels	1,000	2,000	5,000	10,000	50.000
Ethernet Interfaces	2x1000BASE-TX 4x100BASE-TX	8xSFP (Mini-GBIC) 2x1000BASE-TX 4x100BASE-TX	8xSFP (Mini-GBIC) 2x1000BASE-TX 4x100BASE-TX	8xSFP (Mini-GBIC) 2x1000BASE-TX 4x100BASE-TX	4x1000BASE-TX + 2x1000BASE-TX
Virtual Interfaces (VLAN)	512	1,024	2,048	4,096	4.096
Virtual Systems & Virtual Routers	10 + up to 1,000 additional				up to 1000
Users	Unlimited				Unlimited

Kuva 20. SG 4400 - ja SG 5500 -sarjan laitteiden alasarjat ja ominaisuudet. [12.]

Lisäksi kaikissa Security Gateway -laitteissa on ominaisuudet, jotka on listattu taulukossa 2. Mainittuja ominaisuuksia voidaan sanoa Clavisterin ns. perusominaisuuksiksi, koska ne löytyvät jokaisesta laitteesta. Kaikista löytyy erilaisia valittavia toimintatiloja ja palomuuritoimintoja. Valittavia toimintatiloja ovat virtuaalinen IP, transparenttisuus ja reititys sekä käytäntöihin perustuvat NAT/PAT ja palvelimen kuormanjako. Palomuurissa on verkko-, DoS- ja DDoS-hyökkäysten havaitsemis- ja estojärjestelmä. Tuettuja VPN-salauksia ja -tekniikoita on monia AES:ista CAST-128:aan ja IPsecistä L2TP:n. Valittavia sovellustason yhdyskäytäviä ovat HTTP, FTP/TFTP, SIP/H.323 ja SMTP/POP3. Lisäksi tarjolla on eri vaihtoehtoja liittyen sisällön turvallisuuteen, siirtokaistan hallintaan, lokien pitämiseen, monitorointiin ja yleiseen hallintaan. Reitityksessä ja osoitteidenhallinnassa tuettuja ovat mm. staattinen IP, OSPF, DHCP-palvelut ja GRE. Myös korkean saatavuuden tarjoamat edut ovat melkein kaikkien saatavilla.

Taulukko 2. Security Gatewayn ominaisuuksia [12.]

Mode of Operation	**Logging/Monitoring**
Layer 2 Mode (Transparent Mode)	Clavister Syslog
Layer 3 Mode (Route Mode)	Real-time Log Viewer
Policy-based NAT/PAT	Real-time Performance Monitoring
Policy-based Server Load Balancing	SNMP Polling/Traps
Virtual IP	Clavister InSight™ Compatible
Firewall	**Management**
Network Attack Detection/Prevention	Web Based Management
DoS and DDoS Detection/Prevention	Local Console RS232/SSH
VPN – Virtual Private Networking	Command-line based Remote Management
AES, 3DES, DES, Twofish, Blowfish, CAST-128	Remote Fail-safe Operation
Authentication SHA-1, MD5	User Authentication
X.509 Certificates, Pre-Shared Keys	LDAP Authentication
Self-Signed Certificates	External RADIUS User Database , multiple servers
IPsec NAT Traversal (NAT-T)	CHAP, PAP
VPN Tunnel Keep-alive	VPN IKE XAuth
L2TP and PPTP Client/Server (LNS/PNS) Client only	**Addressing and Routing**
Application Layer Gateways	Static IP
FTP/TFTP	Policy-based Routing (PBR)
SIP/H.323	OSPF
HTTP	Proxy ARP (Transparent Mode)
SMTP/POP3	DHCP Client, Server and Relay
Content Security	PPPoE
Intrusion Detection & Prevention (IDP)	GRE
Web Content Filtering	Multicast - IGMP
Anti-Virus	**High Availability***
Anti-Spam	Firewall and VPN State Synchronization
Bandwidth Management	Dead Link, Gateway & Interface Detection
IDP Traffic Shaping	Route Failover, Interface Failover
Policy-based Bandwidth Management	Average Failover Time < 800ms
Guaranteed/Maximum Bandwidth	
Dynamic Bandwidth Balancing	* Limited to Route/Port Failover in SG12 and SG15

3.4.2 Ohjelmatoteutus

SG 30-sarja on ominaisuuksissa löytyy yhdistelmää laitepuolen SG 10 ja SG 50 -sarjasta. Mm. salaamattoman liikenteen siirtonopeus ja samanaikaiset yhteydet vastaa SG 10 -sarjan vastaavia sekä VPN-tunneleiden määrä vastaa SG 50 -sarjan alkupuolen vastaavia (kuva 21). [13.]

SG 30-Series	SG33	SG35	SG36	SG37
Plaintext Throughput (Mbps)	50	50	50	50
Max nr. Ethernet Interfaces	3	3	4	4
Concurrent connections	4,000	4,000	4,000	4,000
Concurrent VPN Tunnels	25	50	25	50
Virtual Systems & Routers	5	5	5	5
VLAN	4	4	4	4

Kuva 21. SG 30 -sarjan ominaisuuksia. [13.]

SG 200 -sarja on ominaisuuksiltaan hyvin samankaltainen laitepuolen SG 57:män kanssa. Esimerkiksi salaamattoman liikenteen siirtonopeus, samanaikaisten yhteyksien ja VPN-tunneleiden määrä sekä VLAN:ien lukumäärät ovat samoja (kuva 22). [13.]

SG 200-Series	SG230	SG240	SG250
Plaintext Throughput (Mbps)	200	200	200
Max nr. Ethernet Interfaces	3	4	5
Concurrent connections	32.000	32.000	32.000
Concurrent VPN Tunnels	100	100	100
Virtual Systems & Routers	5	5	5
VLAN	32	64	64

Kuva 22. SG 200 -sarjan ominaisuuksia. [13.]

Ohjelmatoteutuksen tehokkaimmat neljä Security Gatewaytä edustavat omia sarjojansa yksilöinä. Tehokkaimman toteutuksen salaamattoman liikenteen siirtonopeus on 2000 Mbps ja samanaikaisia VPN-tunneleita voi olla enintään 1000 kappaletta. Kaikissa ohjelmatoteutuksissa virtuaalijärjestelmien ja reitittimien määrä on rajoitettu viiteen (kuva 23).

	SG360	SG680	SG1110	SG2160
Plaintext Throughput (Mbps)	300	600	1000	2000
Max nr. Ethernet Interfaces	6	8	10	16
Concurrent connections	64.000	128.000	256.000	512.000
Concurrent VPN Tunnels	200	600	600	1000
Virtual Systems & Routers	5	5	5	5
VLAN	64	128	128	128

Kuva 23. Tehokkaimpien SG-ohjelmatoteutuksien ominaisuuksia. [13.]

3.4.3 Virtuaalitoteutus

Virtuaalitoteutukset ovat räätälöity virtuaaliympäristön tarpeisiin. Toteutuksia on neljä, joten ominaisuudet heikommasta tehokkaampaan kasvaa luonnollisesti harppauksittain. Harppauksia lyhentää kuitenkin se, että tehokkain toteutus on rajoitettu suorituteholtaan 1000 Mbps:ään salaamattoman liikenteen siirron osalta (kuva 24). Virtuaalitoteutuksia ajetaan VMware ESXi -virtuaaliympäristössä. [14.]

	VSG21	VSG110	VSG510	VSG1010
Plaintext Throughput (Mbps)	50	200	500	1000
Maximum Number of Ethernet Interfaces	3	5	7	10
Concurrent Connections	4000	16000	64000	256000
Concurrent VPN Tunnels	25	200	700	1000
VLAN	4	64	128	512

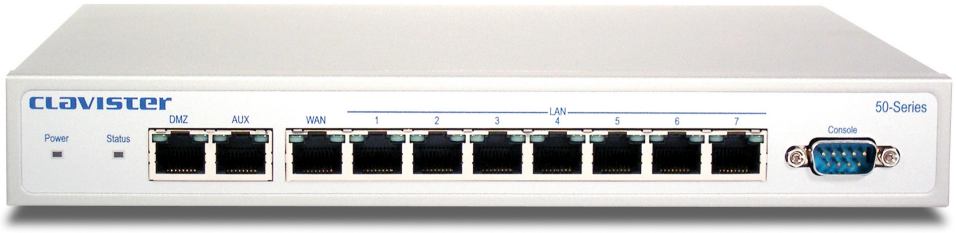
Kuva 24. SG-virtuaalitoteutuksien ominaisuuksia. [14.]

4 TRANSPARENTTI PALOMUURI

Coreplussan transparent-ominaisuuden tarkoitus on mahdollistaa Security Gatewayn liittäminen verkkoon ilman verkon uudelleen konfigurointia ja ilman, että isännät tiedostavat sen olemassaoloa. Security Gatewayllä voi normaalisti monitoroida ja hallita sen läpi kulkevaa liikennettä, mikä lisää verkon turvallisuutta ja kontrolloitavuutta. Seuraavissa kappaleissa kerrotaan miten transparentti palomuuri toteutetaan kahdella eri tavalla. Ensimmäisessä toteutuksessa Security Gateway konfiguroidaan transparenttisuudelle tarkoitettuun transparenttiin tilaan. Toisessa toteutuksessa transparenttisuus toteutetaan käyttäen Proxy ARP:ia ja siinä hyödynnetään lisäksi HA-klusterointia.

4.1 Alkutoimet

Toteutuksessa käytettiin SG-57-mallista Clavister Security Gatewaytä (kuva 25). Laitteen edestä löytyy sarjaportti, seitsemän LAN-porttia, WAN-, AUX- ja DMZ-portti sekä merkkivalot virralle ja tilalle. Laitteen takana on paikka virtapiuhalle ja resetoinnissa käytettävä nappula.



Kuva 25. SG-50-sarjan Clavister Security Gateway. [15.]

Valtaosa Security Gatewaytä koskevia konfigurointeja tehdään tässä työssä FineTunen Security Editorin kautta valitsemalla sieltä konfiguroitava Security Gateway. Konfiguroidut tiedot aktivoidaan Security Gatewayhin kirjoittautumalla sisään klikkaamalla ensin ”Check In” kuvaketta (Nuoli paperista disketti kohden.), jonka jälkeen klikataan ”Deploy Configuration” -kuvaketta (kuva 26). Sisään kirjoittautuneina ollessa konfigurointeihin ei voi tehdä mitään muutoksia vaan ensin täytyy kirjoittautua ulos painamalla ”Check Out” -kuvaketta (Nuoli disketistä paperia kohden.) (kuva 26). Konfiguraatiot saa myös ladattua laitteisiin näppäinyhdistelmällä ”CTRL-ALT-U”, jolloin näkyville tulee valikko laitteista, joihin konfiguraatio voidaan ladata.

Kuva 26. Kuvasta rajattu Check In ja Out -kuvakkeet sekä Deploy Configuration.

Koska laite oli ollut aikaisemmin muussa käytössä, se kannatti ensimmäiseksi resetoida. Aluksi kytkettiin sarjakaapeli tietokoneen sarjaportista Clavisterin sarjaporttiin konsoli yhteyttä varten, jotta resetoinnin onnistuminen nähtiin välittömästi laitteen käynnistyessä. Konsoliyhteys muodostettiin PuTTY-ohjelmalla. Resetointi tapahtui pitämällä laitteen takana olevaa reset-nappia pohjassa ennen laitteen käynnistämistä ja noin 30 sekuntia sen käynnistämisen jälkeen.

Laitteen käynnistyttyä resetoinnin jälkeen täytyi siihen määritellä haluttu hallintarajapinta ja IP-osoite (kuva 27). Hallintarajapinnaksi valittiin LAN-portit, mikä tarkoittaa sitä, että mikä tahansa seitsemästä LAN-portista voi toimia hallintarajapintana. IP-osoitetta syötettäessä on huomioitava, että nollia täytyy lisätä numeron eteen tarvittaessa, jotta pisteellä erotetuista numerosarjoista tulee kolminumeroisia.

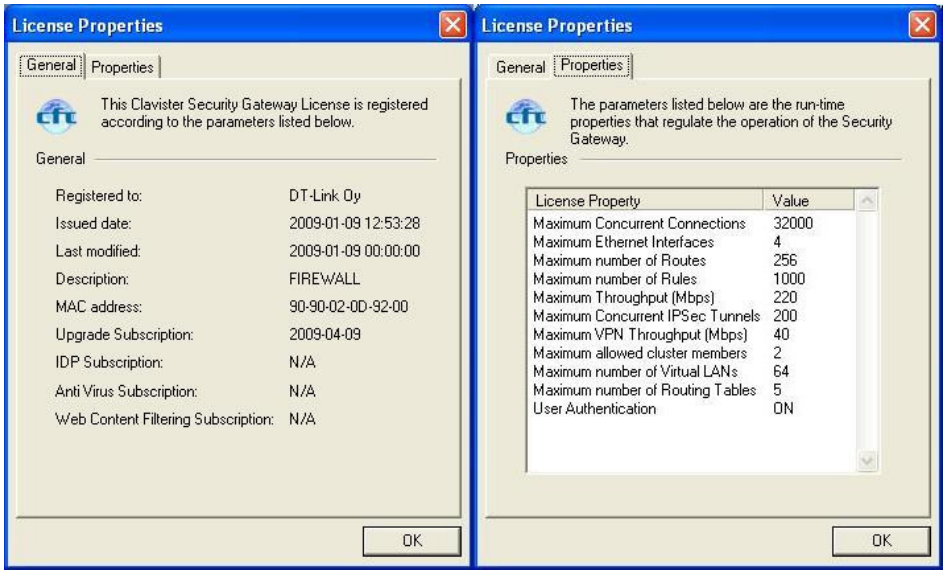
```
LAN: Switched interfaces Port 1-7
WAN: Fast Ethernet interface 10/100
AUX: Fast Ethernet interface 10/100
------------------------------------------------------------------
ESC Return to previous menu

==================================================================
 Base IP configuration
==================================================================
Management Interface:
LAN: Switched interfaces Port 1-7

Use DHCP:             [ ]
Use PPPoE:            [ ]

IP Address:           [010.000.002.252]
Netmask:              [255.255.255.0  ]
Gateway Address:      [010.000.002.254]   (Leave blank for none)
Allowed Mgmt Net:     [   .   .   .   ]   (Leave blank for local network)
Netmask:              [#  .   .   .   ]
```

Kuva 27. Hallintarajapinnan valinta ja IP-asetukset.

Edellisen kohdan asetusten ollessa kunnossa ladattiin Clavisterin sivuilta demo-paketti [16.], joka sisältää mm. FineTunen, jota tässä toteutuksessa käytettiin konfigurointiin. Hallintakone ja Clavister kytkettiin tässä välissä toisiinsa ristiinkytkentäkaapelilla.

Jotta Security Gatewaytä päästiin hallitsemaan, täytyi se lisätä käyttöön napsauttamalla FineTunen vasemmasta sivupalkista kuvaketta ”Security Editor” ja seuraamalla ohjeita. Jos ohjelmassa on jo olemassa yksi tai useampi Security Gateway, saadaan uusi lisättyä klikkaamalla oikeata hiiren nappia kohdassa ”Security Gateways” ja valitsemalla ”New”. Tässä vaiheessa laitettiin Security Gatewaylle salasana, jonka sai asetettua Security Editorissa ollessa napsauttamalla kohtaa ”Security Gateway”. Tämän jälkeen yläpalkkiin tuli valinta ”Action”, josta päästiin vaihtamaan salasanaa seuraamalla polkua ”Communication -> Change Security Gateway Password”.

Seuraavaksi laitettiin lisenssi paikoilleen yläpalkin kohdasta ”Tools” ja sieltä ”Licenses”, jotta laitetta ei tarvitse käynnistää uudelleen kahden tunnin päällä olon jälkeen. Lisenssin tiedoista näkee mm. voimassaoloajan, käytettävissä olevat ominaisuudet sekä tilattavien lisäpalvelujen tilan (kuva 28).



Kuva 28. Lisenssin tiedot sekä General- että Properties-välilehdiltä.

4.2 Oikean transparentin tilan hyödyntäminen

Security Gatewayssä on kaksi toimintatilaa, joissa se voi toimia. Näistä toinen on reititystila ja toinen transparent-tila. Reititystilassa käytetään normaaleja reittejä ja Security Gateway pystyy suorittamaan kaikki toiminnot, joita OSI-tason kolme reititinkin pystyy tekemään. Transparent-tila aktivoidaan määrittelemällä reititystauluun kytketty reitti normaalin reitin sijaan. Kytketylle reitille määritellään yleensä verkoksi ”all-nets”, mutta tarvittaessa verkolle voi määrittää tietyn alueenkin. Transparent-tilassa Security Gatewayn pakettien

välitystä voi verrata OSI-tason kaksi kytkimeen, joka välittää paketteja oikeisiin rajapintoihin muuttamatta mitään paketin osoitetietoja IP- tai Ethernet-tasoilla. Reititys- ja transparent-tiloja voi yhdistellä sillä rajoituksella, että yksi rajapinta ei voi toimia kuin yhdessä tilassa kerrallaan.

4.2.1 Toimintaperiaate

Kommunikointia aloitettaessa isäntä paikantaa kohdeisännän fyysisen osoitteen mainostamalla kaikille ARP-pyyntöä. CorePlus sieppaa tämän ARP-pyynnön ja mainostaa sitä kaikille muille kytkettyyn reittiin kuuluville rajapinnoille paitsi sinne, mistä pyyntö otettiin vastaan. Jos CorePlus saa ARP-vastauksen ennen määriteltävissä olevaa aikakatkaisua, se välittää vastauksen takaisin pyynnön lähettäjälle käyttäen informaatiota, jonka se on aikaisemmin tallettanut ARP-toimituksentilaan. ARP-toimituksen aikana CorePlus saa itselleen lähdeosoitetiedot pyynnön ja vastauksen ansiosta yhteyden molemmille päille. CorePlus ylläpitää CAM-pöytää ja tason kolme välimuistipöytää. CAM-pöytä jäljittää annetusta rajapinnasta saatavilla olevan MAC-osoitteen ja tason kolme välimuisti - pöytä kartoittaa MAC-osoitteille ja rajapinnoille kuuluvat IP-osoitteet. Koska tason kolme välimuistia käytetään vain IP-liikenteelle, tason kolme välimuistimerkinnät talletetaan yksittäisinä isäntä-merkintöinä reititystauluun. Jokaiselle paketille, joka kulkee Security Gatewayn läpi suoritetaan reitintarkistus kohdetta varten. Jos reitti täsmää kytkettyyn reittiin, CorePlus tietää, että sen pitää käsitellä paketti transparenttiin tapaan. Jos kohderajapinta ja MAC-osoite on saatavilla reitillä, CorePlussalla on tarvittavat edellytykset paketin edelleen lähettämiselle kohteesee. Reitin ollessa kytketty reitti eikä kohteesta ole tietoa saatavilla, täytyy yhdyskäytävän selvittää ne. Löytääkseen tiedot CorePlus lähettää ARP- ja ICMP-pyyntöjä kytkettyyn reittiin kuuluville rajapinnoille esittäen alkuperäistä IP-paketin lähettäjää. Jos saadaan takaisin ARP-vastaus, CorePlus päivittää edellä mainitut pöydät ja edelleen lähettää paketin kohteeseen.

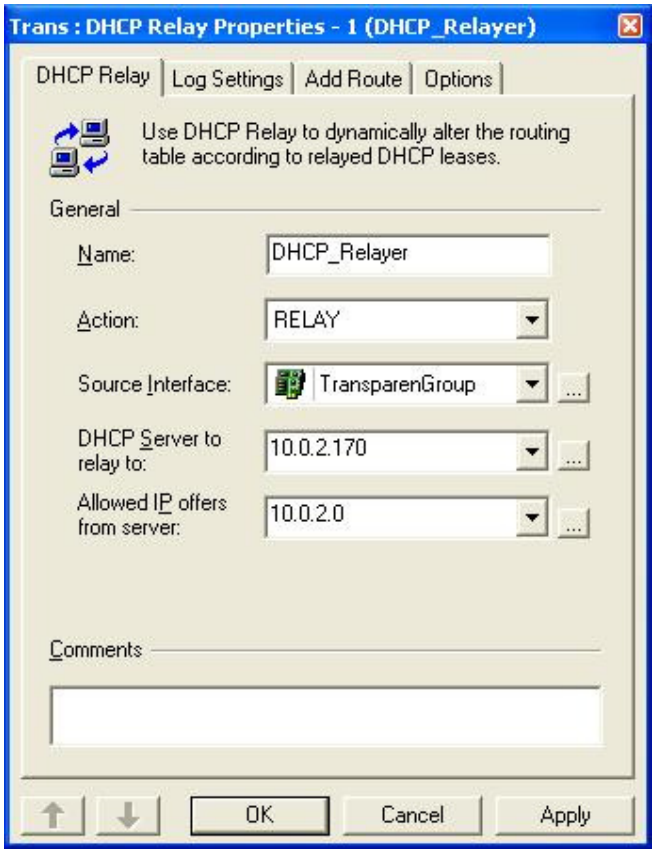
4.2.2 Transparent-tilan aktivoiminen

Aluksi suoritettiin kappaleessa 4.1 mainitut alkutoimet, jonka jälkeen muokattiin wan- ja lan-objekteja, jotka löytyivät kohdasta ”Interfaces -> Ethernet”. Molempiin laitettiin IP-osoitteeksi 10.0.2.252 ja mainostus osoitteeksi saman verkon osoite 10.0.2.255.

Tämän jälkeen mentiin kohtaan ”Interfaces -> Interface Groups -> New Interface Group”, jossa uudelle rajapintaryhmälle annettiin nimeksi ”TransparenGroup” ja kontrolloitaviksi rajapinnoiksi lisättiin lan ja wan.

Kytketty reitti lisättiin kohdasta ”Routing -> Routes -> New Switch Route -> Main”, jolle annettiin nimeksi ”SwitchRoute”. Rajapinnaksi laitettiin edellisessä kohdassa luotu ”TransparenGroup”, verkoksi ”all-nets” ja etäisyysarvoksi 0. Saman ikkunan välilehdeltä ”Proxy ARP” laitettiin vielä rasti TransparenGroupin riville. Tämän jälkeen klikattiin OK ja poistettiin reititystaulun käytöstä kaikki lan- ja wan-rajapintoja koskevat reitit luonnollisesti lukuun ottamatta juuri luotua SwitchRoutea.

IP-osoitteiden jako laitettiin DHCP-palvelimen tehtäväksi. Jos DHCP-palvelin sijaitsee Clavisterin takana niin ongelmia ei tule, mutta jos jostain syystä DHCP-palvelin halutaan sijoittaa reitittimen ja Clavisterin väliin, niin tällöin tarvitaan ”DHCP Relayer” välittämään DHCP-viestejä. Lisääminen tapahtuu kohdasta ”Routing -> Routes -> DHCP Relay -> New DHCP Relay”. Välittäjälle voidaan antaa parametreja esimerkiksi kuvan 29 mukaisesti. Parametreja ovat nimi, toiminto, lähderajapinta, DHCP-palvelimen osoite ja sallitut IP-tarjoukset.



Kuva 29. DHCP-Relayer asetukset.

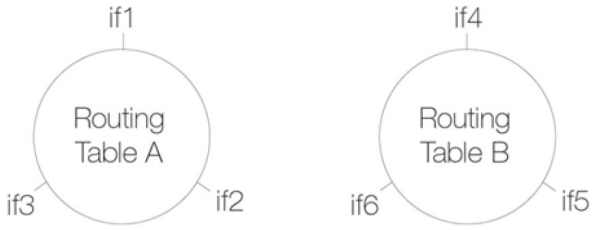
Seuraavaksi halusimme lisätä liikenteelle sääntöjä, kuten sallia DNS-viestinnän, HTTP/HTTPS-liikenteen, pingin CorePlussalle ja muita verkon käyttötarkoitusta palvelevia sääntöjä. Sääntöjä lisättiin kohdasta ”Rules -> Main -> New Rule”. Säännöille määriteltiin verkko- ja rajapintaparametrit sekä palvelu-objekti johon se liitettiin. Palveluita on ennalta määriteltyjä ja niitä voi myös itse määritellä tarkemmin. Lisäksi voimassaoloaikataulun olisi voinut halutessa määrittää. Alimpana sääntönä on hyvä pitää DropAll-sääntöä. Tämäkin toteutus, niin kuin useat muutkin toteutukset lähtee siitä, että kaikki liikenne kielletään oletuksena (kuva 30).

	Name	Action	Rule Set	Log	Source Interface	Source Network	Destination Interface	Destination Network	Service
1	DropNetBIOS	Drop		☑	any	all-nets	any	all-nets	smb-all
2	MgmtPing	Allow		☑	TransparenGroup	lannet	core	all-nets	ICMP ICMP Params...
3	allowdns	Allow		☑	TransparenGroup	lannet	any	all-nets	dns-all
4	HTTP_S_Allow	Allow		☑	TransparenGroup	lannet	any	all-nets	http-all
5	DropAll	Drop		☑	any	all-nets	any	all-nets	All

Kuva 30. Säännöstö, josta näkee mm. verkot ja rajapinnat.

4.2.3 Muuta huomioitavaa

Yhden kytketyn reitin ja rajapintaryhmän sijaan voidaan laittaa yksittäisiä kytkettyjä reittejä erillisille rajapinnoille. Lopputulos on kuitenkin sama, koska kaikki reititystauluun määritellyt kytketyt reitit yhdistetään toisiinsa CorePlussan toimesta. Se, miten rajapinnat on assosioitu kytkettyihin reitteihin, ei vaikuta niiden transparenttiseksi tulemiseen. Tämä toimii silloin, kun kaikki rajapinnat on assosioitu samaan reititystauluun. Monella reititystaululla voidaan tehdä monta eri transparent-tilassa toimivaa verkkoa. Esimerkiksi käytössä voisi olla reititystaulut A ja B, joihin olisi assosioitu rajapintoja kuvan 31 tapaan. Reititystaulut konfiguroidaan sitten tavalliseen tapaan. Se, minkä reititystaulun jäsen rajapinta on, määrittää PBR-jäsenyysparametri, joka määritetään jokaiselle rajapinnalle erikseen. Transparent-tilaa toteutettaessa täytyy rajapintojen PBR-jäsenyydet laittaa kuntoon. [17, s. 141-154.]



Kuva 31. Eri reititystauluissa sijaitsevat kytketyt reitit ovat erilliset. [17, s. 144.]

HA-klusterointia ei voida toteuttaa oikeassa transparent-tilassa, koska HA:n kanssa ei voida käyttää kytkettyjä reittejä. Myös NAT:ia ei pidä laittaa CorePlussan tehtäväksi, koska transparent-tilassa Security Gateway toimii, kuten OSI-tason kaksi kytkin ja osoitteenkäännös tehdään korkeammalla kerroksella. [17, s. 141-154.]

4.2.4 Lisäominaisuudet

CorePlussassa on lisäksi lukuisia transparent-tilaan liittyviä asetuksia. Seuraavaksi on esitelty niitä ja niiden oletusasetuksia. [17, s. 141-154.]

- Decrement TTL. Laitetaan päälle, jos halutaan, että TTL-arvoa pienennetään aina, kun paketti kulkee yhdyskäytävän läpi. Oletus: ei päällä.

- CAM Size. Jos CAM-koko asetusta ei ole laitettu dynaamiseksi, tämä määrittää CAM-pöydän enimmäiskoon. Oletus: 8912.

- Dynamic L3C Size. Tason kolme välimuistin dynaaminen varaus. Oletus: päällä.

- L3 Cache Size. Tason kolme välimuistille käsin asetettava varaus. Oletus: dynaaminen.

- Transparency ATS Expire. Määrittelee vastaamattoman ATS merkinnän elinajan sekunneissa. Oletus: 3 sekuntia.

- Transparency ATS Size: Määrittelee enimmäismäärään ATS merkinnöille. Valittavat arvot ovat väliltä 128-65536. Oletus: 4096.

- Null Enet Sender. Määrittelee mitä tehdään, kun lähettäjän MAC-osoite on asetettu nollaksi ethernet-tunnisteeseen. Vaihtoehtoja ovat Drop, joka hylkää paketin ja DropLog, joka hylkäyksen lisäksi kirjaa tapahtuman lokiin. Oletus: DropLog.

- Broadcast Enet Sender: Määrittelee mitä tehdään, kun lähettäjän MAC-osoite on asetettu mainostusosoitteeksi ethernet-tunnisteeseen. Vaihtoehtoina ovat alla listatut kolme vaihtoehtoa, joista jokaisesta on toinen lokiin kirjoittava Log-päätteinen vaihtoehto. Oletus: DropLog.

    - Accept. Hyväksyy paketin.

    - Rewrite. Korvaa MAC:in lähettävän rajapinnan MAC:illä.

    - Drop. Hylkää paketin.

- Multicast Enet Sender. Määrittelee mitä tehdään, kun lähettäjän MAC-osite on asetettu multicast-osoitteeksi ethernet-tunnisteeseen. Vaihtoehdot ja oletusasetus ovat samat kuin ”Broadcast Enet Sender” tapauksessa yllä.

- Relay Spanning-tree BPDUs. Kun asetettu Ignore-asetukselle, kaikki sisääntulevat STP, RSTP ja MSTP BPDU:t ohjataan kaikille saman reititystaulun transparenteille rajapinnoille lukuun ottamatta sisääntulo rajapintaa. Oletus: Drop.

- Ignore. Antaa pakettien kulkea, mutta ei kirjaa tapahtumaa. lokiin.
- Log. Antaa pakettien kulkea ja kirjaa tapahtuman lokiin.
- Drop. Hylkää paketit.
- DropLog. Hylkää paketit ja kirjaa tapahtuman lokiin.

- Relay MPLS. Kun asetettu Ignore-asetukselle, kaikki sisääntulevat paketit välitetään transparent-tilassa. Vaihtoehdot ja oletusasetus ovat samat kuin ”Relay Spanning-tree BPDUs” tapauksessa yllä.

4.3 Transparenttisuus Proxy ARP:illa

Proxy ARP:illa toteutetussa transparentissa tilassa verkko jaetaan kahteen osaan Security Gatewayllä. Tällöin itse CorePlus vastaa verkon välillä kulkeviin ARP-pyyntöihin. Esimerkiksi toisen verkon isäntä A lähettää ARP-pyynnön selvittääkseen toisessa verkossa sijaitsevan isännän B IP-osoitteelle kuuluvan MAC-osoitteen. CorePlus vastaa tähän ARP-pyyntöön isännän B sijaan lähettämällä vastauksena oman MAC-osoitteensa esittäen isäntä B:tä. Vastauksen saatuaan isäntä A lähettää jatkossa kaiken datan suoraan CorePlussalle, joka edelleen lähettää datan isäntä B:lle. Näin CorePlus voi tutkia ja tarvittaessa suodattaa dataa. Tässä toteutuksessa hyödynnetään HA-klusterointia, joka esiteltiin aikaisemmin kappaleessa 3.2.12.

4.3.1 Proxy ARP:in konfigurointi

Aluksi suoritettiin kappaleessa 4.1 mainitut alkutoimet, jonka jälkeen muokattiin wan- ja lan-objekteja, jotka löytyivät kohdasta ”Interfaces -> Ethernet”. Molempiin laitettiin IP-osoitteeksi 10.0.2.252 ja mainostus osoitteeksi saman verkon osoite 10.0.2.255.

Reititystaulusta asetettiin reitit ja tarvittaviin reitteihin Proxy ARP:aus. Muokattava reititystaulu löytyi kohdasta ”Routing -> Routes -> Main”. Tauluun lisättiin oletusreitti, jossa rajapinta wan on kaikkien verkkojen yhdyskäytävä maailmalle. Rajapinnalle wan asetettiin myös reitit verkon osoitteista 10.0.2.254, 10.0.2.1 - 10.0.2.100 ja 10.0.2.201 - 10.0.2.253, joihin laitettiin Proxy ARP:aus lan rajapintoihin. Rajapinnalle lan asetettiin vastaavasti verkon osoitteista 10.0.2.101 - 10.0.2.200 koostuva reitti, johon laitettiin Proxy

ARP:aus wan rajapintaan. Näiden konfigurointien jälkeen sisäverkon osoitteista väliltä 101-200 pääsee ulkoverkkoon ja osoitteista 1-100 ja 201-253 pääsee vastaavasti sisäverkkoon. Reititystaulu on näillä asetuksilla kuvan 32 näköinen.

	Interface	Network	Gateway	Local IP	Proxy ARP
1	wan	all-nets	gw-world		
2	wan	gw-world			lan
3	wan	10.0.2.1 - 10.0.2.100			lan
4	lan	10.0.2.101 - 10.0.2.200			wan
5	wan	10.0.2.201 - 10.0.2.253			lan

Kuva 32. Reititystaulu, jossa reitit käyttävät Proxy ARP:ia.

4.3.2 HA-klusteroinnin käyttöönotto

HA-klusterointia varten toiseksi Security Gatewayksi otettiin samanlainen laite kuin, mikä ensimmäinenkin oli. Laitteeseen suoritettiin kappaleen 4.1 mukaiset alkutoimet lukuun ottamatta kahta poikkeusta. IP-osoitteeksi konfiguroitiin 10.0.2.253 sekä IP-asetusten laiton jälkeen mentiin Boot Menuun vastaamalla ytimen latausta koskevaan kysymykseen kieltävästi ja painamalla mitä tahansa näppäintä ennen kuin automaattinen ytimen lataus käynnistyy. Valikosta valittiin kohta ”System” ja sieltä ”Set type to High Availability Slave”. Tämän jälkeen käynnistettiin ytimen lataus.

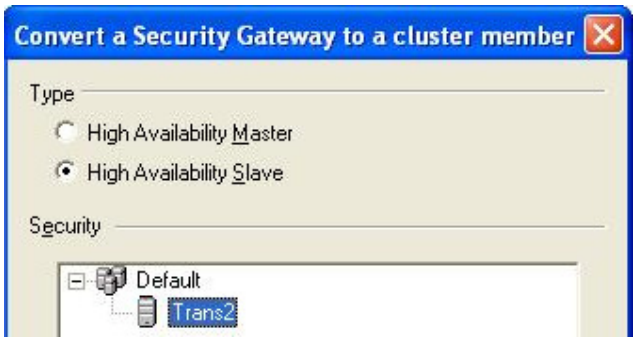
Ennen HA-klusterin luomista tarkastettiin, että ytimien versiot täsmäävät. Nämä tiedot löytyivät klikkaamalla kohtaa ”Security Gateways” (kuva 33). Jos versiot eivät täsmää, on suositeltavaa päivittää versiot samoiksi valitsemalla yläpalkista ”Action -> Communication -> Upgrade -> Core”.

	DB cfg	Core cfg	Core ver	Uptime	Last Modified	Subscription valid until	Comments
1	2	2	8.90.05.10-8223	0 hours	2009-02-07 18:54	2009-04-09	Master
2	3	2	8.90.05.10-8223	-	2009-02-07 19:15	2009-05-06	Slave

Kuva 33. Ytimien versiot täsmäävät.

Tässä vaiheessa luotiin HA-klusteri klikkaamalla hiiren oikeaa nappia kohdassa ”Security Gateways” ja klikkaamalla sieltä ”New -> High Availability Cluster”. Klusteri nimettiin hadt:ksi, jonka jälkeen sille asetettiin Master ja Slave Security Gateway olemassa olevista laitteista. Masterin ja Slaven lisääminen tapahtui klikkaamalla oikeaa hiiren nappia kohdassa ”Cluster Members” ja valitsemalla ”Make a Security Gateway a cluster Member”. Ku-

vassa 34 tehdään Trans2-nimisestä Security Gatewaystä Slave. Synkronointirajapinnaksi valittiin molemmille aux, koska se ei ollut vielä käytössä.



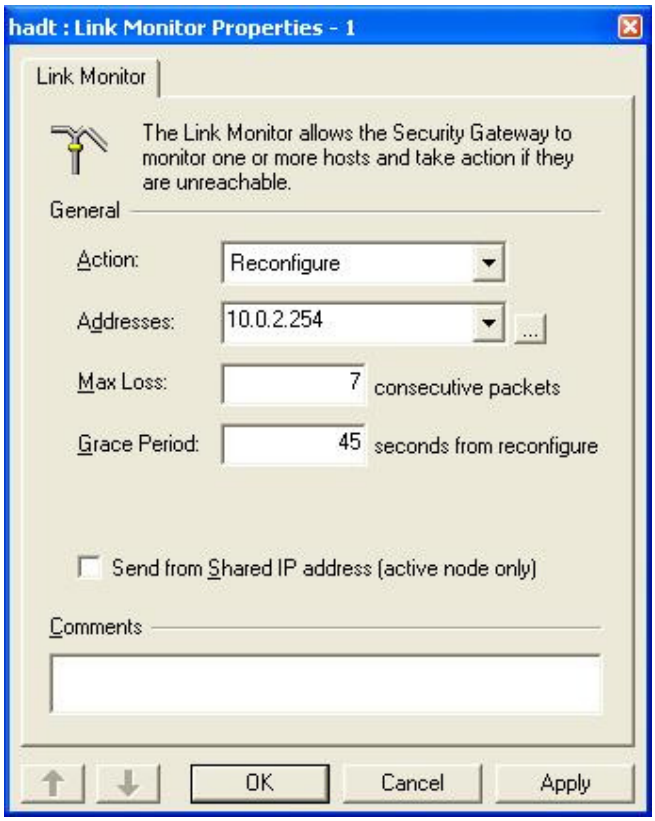
Kuva 34. Security Gatewayn lisääminen klusterin jäseneksi.

Ennen kuin konfiguroinnit aktivoitiin laitteisiin, tarkistettiin asetukset. Reititystauluun oli ilmestynyt oikein sync-rajapinta verkolla 127.0.3.0/24. Rajapintojen osoitteita piti muokata, jotta ne vastasivat tarkoitusta. Lan- ja wan-rajapinnan Master IP:ksi laitettiin 10.0.2.252, Slave IP:ksi 10.0.2.253 ja Shared IP:ksi 10.0.2.251. Lisäksi Master connect -kentän tiedot täytyi lisätä käsin, koska ne olivat menneet jostain syystä Nulleiksi eli tyhmiksi kaiken liikenteen hylkääviksi rajapinnoiksi. Kentän tiedot olivat siis samat kuin kentän Slave connect -tiedot, koska käytetyt laitteet ja portit olivat samoja. Dmz-rajapinnan tietoja ei muokattu, koska se ei ollut käytössä. Kuvassa 35 rajapinnat ja niiden IP-osoitteet. Kohdasta ”Advanced Settings -> HA” asetettiin vielä Cluster ID -arvoksi 40. Arvoa ei tarvitse muuttaa, jos verkossa ei ole muita HA-klustereita, mutta sen voi varmuuden vuoksi muuttaa haluamakseen tulevaisuuden varalta. Tarkistusten ja muutosten jälkeen konfiguraatio aktivoitiin laitteisiin normaaliin tapaan. HA-klusterin masterin ja slaven tilan voi kätevästi tarkistaa mm. Remote Consolella tai sarjaportti-yhteydellä kirjottamalla sinne komennon ”ha”. Vastauksena saadaan tietoa, onko laite master vai slave, aktiivisuustilasta, aktiivisesta ajasta ja klusterin toisen laitteen tilasta. Jos yhteydessä ilmenee ongelmia kannattaa kokeilla kytkeä päälle asetus ”HAUseUniqueSharedMacAddressPerInterface”, joka antaa jokaiselle rajapinnalle oman MAC-osoitteen. Joitain kytkimiä saattaa häiritä, jos rajapinnat käyttävät jaettua MAC-osoitetta.

	Name	Master c	Master IP	Slave connect	Slave IP	Shared IP	Broadcast
1	lan	IXP4N...	10.0.2.252	ixp4npe [Bus: 0 Slot: 0 Port 1 auto auto]	10.0.2.253	10.0.2.251	10.0.2.255
2	wan	IXP4N...	10.0.2.252	ixp4npe [Bus: 0 Slot: 0 Port 2 auto auto]	10.0.2.253	10.0.2.251	10.0.2.255
3	sync	R8139...	127.0.0.2	r8139 [Bus: 0 Slot: 1 Auto Auto]	127.0.0.3	127.0.0.254	127.0.0.255
4	dmz	Null	Master_ip_dmz	r8139 [Bus: 0 Slot: 2 Auto Auto]	Slave_ip_dmz	127.0.0.3	Broadcast_ip_dmz

Kuva 35. HA-klusterin rajapinnat ja IP-osoitteet.

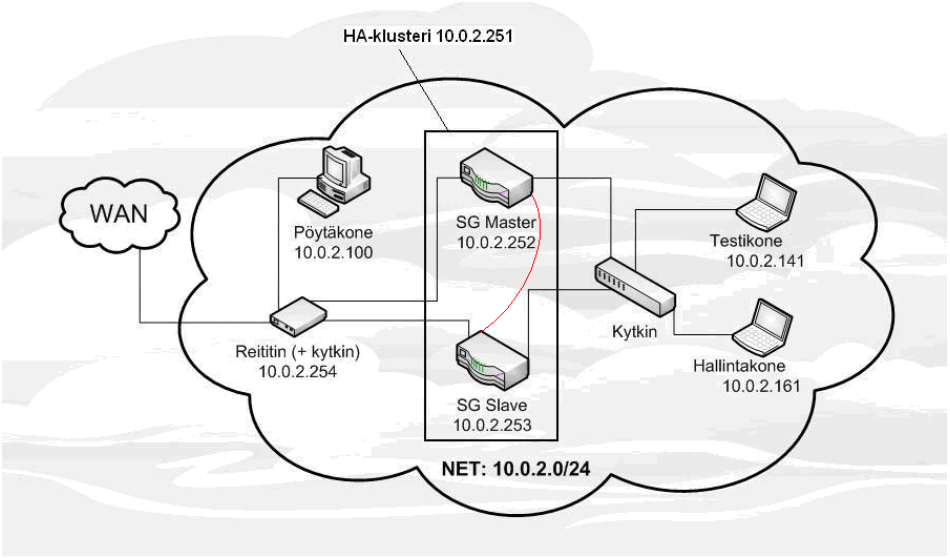
Linkin monitorointi on järkevää laittaa päälle, jotta aktiivinen laite vaihtuu yhteyden katketessa ennalta määriteltyyn osoitteeseen tai osoitteisiin. Etenkin silloin monitorointi on hyödyllinen, kun pääsy WAN:iin on järjestetty pitkin kahta eri reittiä. Jos pääsy WAN:iin järjestetään samaa reittiä pitkin, hyödyksi jää esimerkiksi kaapelin irtoamisen aiheuttama linkin katkeaminen. Linkin monitorointi kytketään päälle klikkaamalla hiiren oikeaa nappia kohdasta ”Miscellaneous -> Link Monitor” ja valitsemalla ”New Link Monitor”. Parametreina on valittava toiminto, seurattavat osoitteet, maksimi hävikki ja odotettava armon aika uudelleen konfiguroinnin jälkeen (kuva 36).



Kuva 36. Linkin monitoroinnin säädettävät parametrit.

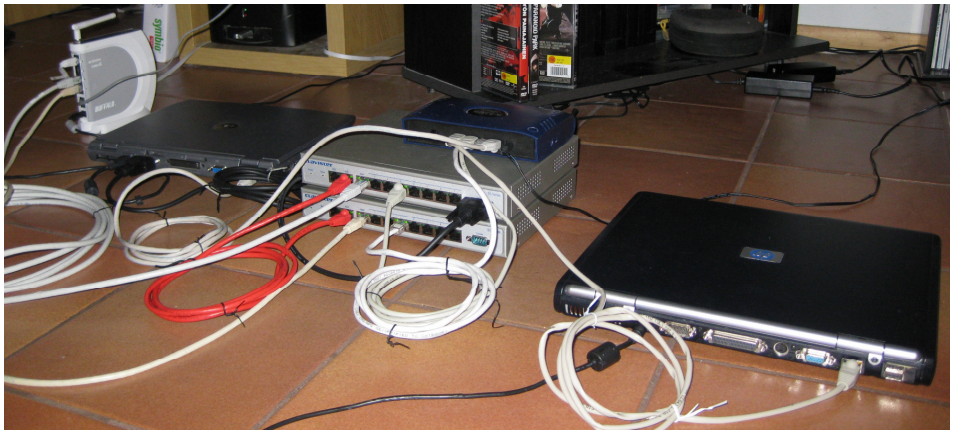
Ennen systeemin käyttöönottoa testaaminen suoritettiin kuvan 37 ympäristössä. Klusterin käyttämä IP-osoite on siis virtuaalinen 10.0.2.251, joka on aina käytössä, kunhan vain vähintään toinen Security Gatewaystä on toi-

minnassa. Laitteiden omia osoitteita käytetään vain hallinnointiin. Kuvassa 37 Clavistereiden oikea puoli on siis lania ja vasen puoli wania Clavistereista katsottuna. Testauksen ajaksi sääntöihin laitettiin kaiken salliva sääntö, jotta toiminta ei jäisi säännöistä kiinni. Tarkempia sääntöjä ja muita hienosäätöjä ei käydä tässä yksityiskohtaisesti läpi. IP-osoitteet päätettiin tällä kertaa laittaa kiinteinä. Jos DHCP-palvelinta kuitenkin käytettäisiin tässä konfiguroinnissa, olisi järkevintä, että se sijaitsisi lanin puolella ja jakaisi lanin puolen osoitteita ja tarpeen vaatiessa Clavisterista katsottuna wanin puolen osoitteet olisivat kiinteitä. Jos palvelin sijaitsisi Clavisterista katsottuna wanin puolella, DHCP-Relayer täytyisi konfiguroida Clavisterille, jotta osoitteiden jako laniin onnistuisi. Tällöin välittäjän asetuksiin tulisi määrittää, että lanin puolen koneet saisivat vain lanin puolelle tarkoitettuja osoitteita, jotka tässä mallissa ovat siis 10.0.2.101 - 10.0.2.200.



Kuva 37. Testausympäristön kaavio.

Toteutuksen testauksessa käytetyt laitteet ja kytkennät näkyvät kuvasta 38. Kaikki käytetyt piuhat ovat tavallisia kategorian viisi ja kuusi RJ45-liitäntäisiä verkkopiuhoja, paitsi että synkronointirajapintojen välissä käytettiin ristiinkytkettyä piuhaa.



Kuva 38. Testausympäristön laitteisto.

5 YHTEENVETO

Palomuuri on oltava olemassa, jos vaatii verkolta turvallisuutta. Palomuurilaitteet, jotka tukevat monia palomuuritekniikoita ja tarjoavat sen lisäksi tukun muitakin verkontoiminnan kannalta hyödyllisiä ominaisuuksia, ovat omiaan alentamaan yrityksen verkontoimintaan liittyviä kustannuksia. Aina ei tarvitse ostaa erillistä laitetta, jos haluaa lisää ominaisuuksia.

Transparenteissa toteutuksissa on omat hyvät puolensa. Oikeassa transparent-tilassa on mm. valittavana valmiita transparenttisuuteen liittyviä ominaisuuksia sekä sen konfiguroiminen on nopeaa. Transparentin tilan toteutus Proxy ARP:illa on järkevää, kun halutaan hyödyntää HA-klusterointia. Tämän konfigurointi on hieman työläämpää, koska käytettät osoitteet täytyy konfiguroida käsin Proxy ARP:ille. Yleisesti näistä kahdesta toteutustavasta suositellaan käytettäväksi oikeaa transparent-tilaa, mutta käytettävä tapa määräytyy luonnollisesti tarvittavien ominaisuuksien mukaan.

VIITELUETTELO

[1] Kuva palomuurista. Oulun seudun ammattikorkeakoulu. [Verkkodokumentti] [Viitattu 7.12.2008] Saatavissa: http://www.ratol.fi/opensource/lahiverkot/images/palomuuri_.gif.

[2] Firewall. Wikipedia. [Verkkodokumentti] 6.12.2008 [Viitattu 7.12.2008] Saatavissa: http://en.wikipedia.org/wiki/Firewall_(networking)#Function.

[3] Palomuurityypit. TKK Tietoverkkolaboratorio. [Verkkodokumentti] 8.12.2000 [Viitattu 7.12.2008]. Saatavissa: http://www.netlab.tkk.fi/opetus/s38118/s00/tyot/30/ptyypit.shtml.

[4] The 7 Layer OSI Model. Mironov Rich. [Verkkodokumentti] 28.02.2003 [Viitattu 7.12.2008] Saatavissa: http://www.mironov.com/assets/images/osi-layers.gif.

[5] Palomuuri. Viestintävirasto. [Verkkodokumentti] 27.09.2007 [Viitattu 7.12.2008] Saatavissa: http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/palomuuri.html.

[6] Yhtiö. Clavister. [Verkkodokumentti] [Viitattu 29.12.2008] Saatavissa: http://www.clavister.com/company/index.html.

[7] clavister-brand_guide.pdf. Clavister. [Verkkodokumentti] [Viitattu 29.12.2008] Saatavissa: http://www.clavister.com/company/press_logos.html.

[8] Clavister_CorePlus_Admin_Guide_9_10.pdf. Clavister. [Verkkodokumentti] [Viitattu 29.12] Saatavissa: http://www.clavister.com/support/documents.html.

[9] FineTune. Clavister. [Verkkodokumentti] [Viitattu 27.12.2008] Saatavissa: http://www.clavister.com/products/finetune.html.

[10] InSight. Clavister. [Verkkodokumentti] [Viitattu 27.12.2008] Saatavissa: http://www.clavister.com/products/insight.html.

[11] PinPoint. Clavister. [Verkkodokumentti] [Viitattu 28.12.2008] Saatavissa: www.clavister.com/products/pinpoint.html.

[12] clavister-dts-sg_series.pdf. Clavister. [Verkkodokumentti] [Viitattu 9.12.2008] Saatavissa: http://www.clavister.com/products/documentation.html.

[13] Software. Clavister. [Verkkodokumentti] 29.12.2008] Saatavissa: http://www.clavister.com/products/security_software_overview.html.

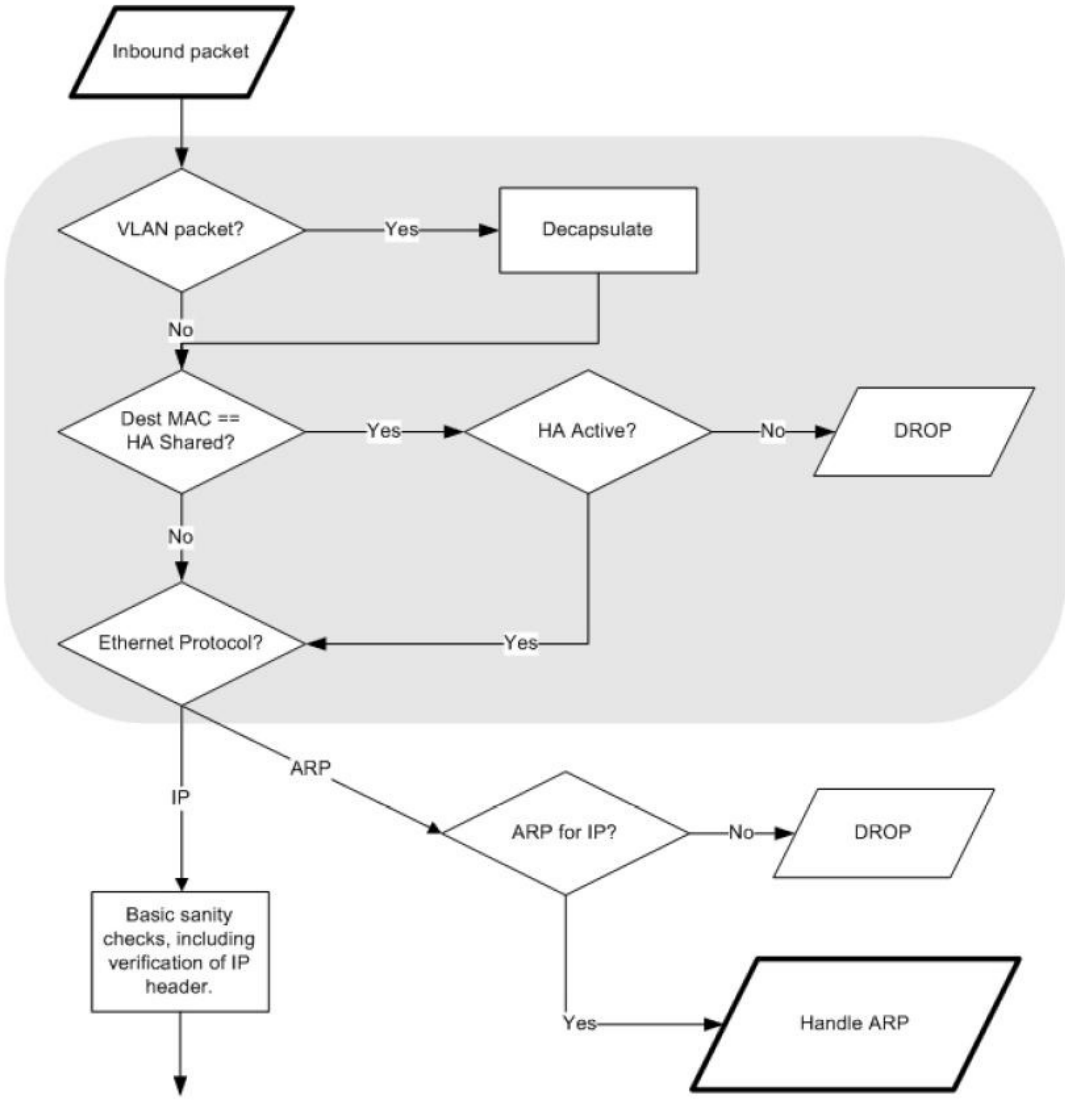
[14] Virtual. Clavister. [Verkkodokumentti] [Viitattu 29.12.2008] Saatavissa: http://www.clavister.com/products/virtual_security_gateway_specifications.html.

[15] Clavister. SG-50 [Verkkodokumentti] [Viitattu 15.01.2008] Saatavissa: http://www.clavister.com/images/product_images/sg50_front_large.jpg.

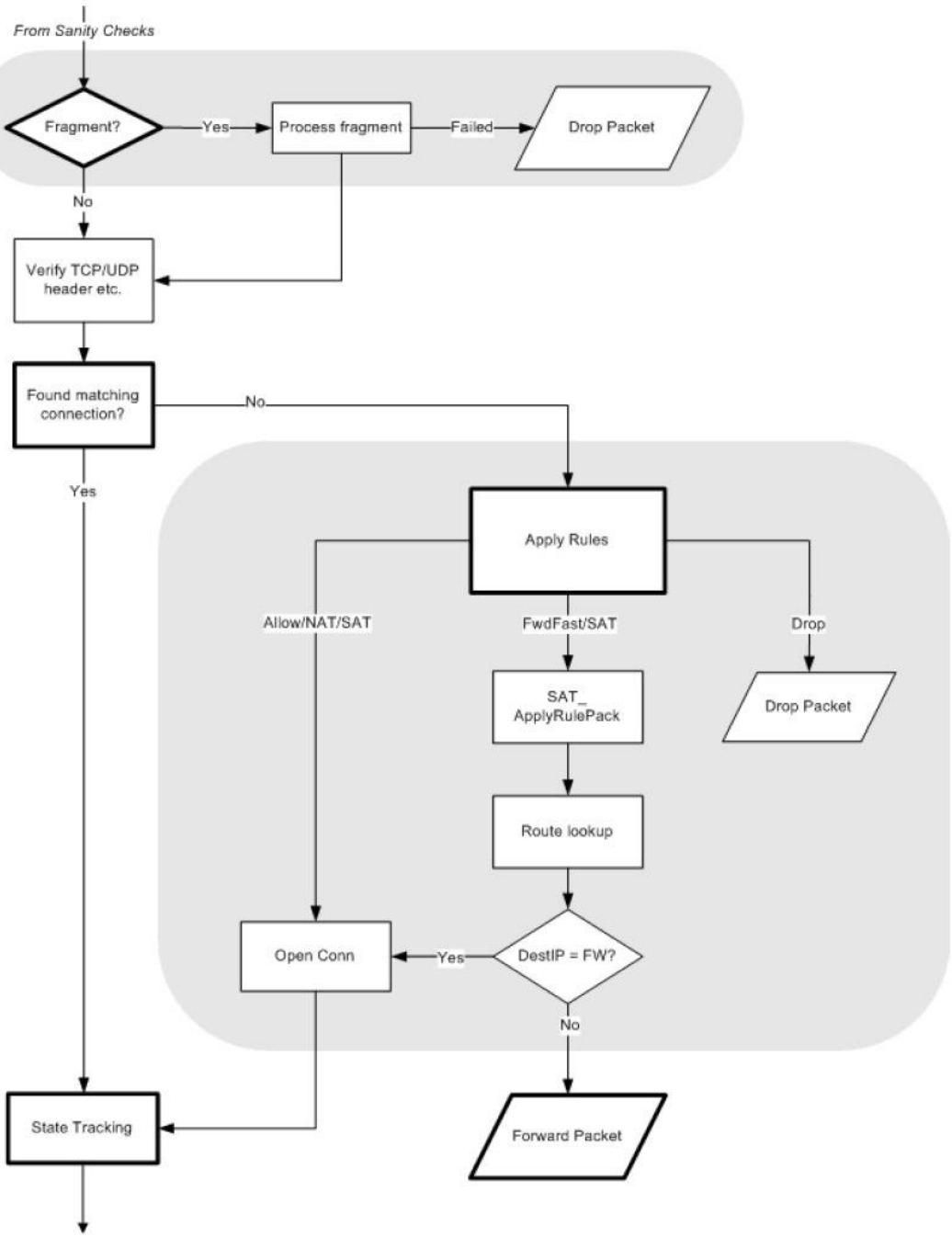
[16] Ohjelmia. Clavister. [Verkkodokumentti] [Viitattu 15.01.2008] Saatavissa: http://www.clavister.com/products/demo2.html.

[17] Clavister_CorePlus_Admin_Guide_8_90_04.pdf. Clavister. [Verkkodokumentti] [Viitattu 16.01.2008] Saatavissa: http://www.clavister.com/support/documents.html.

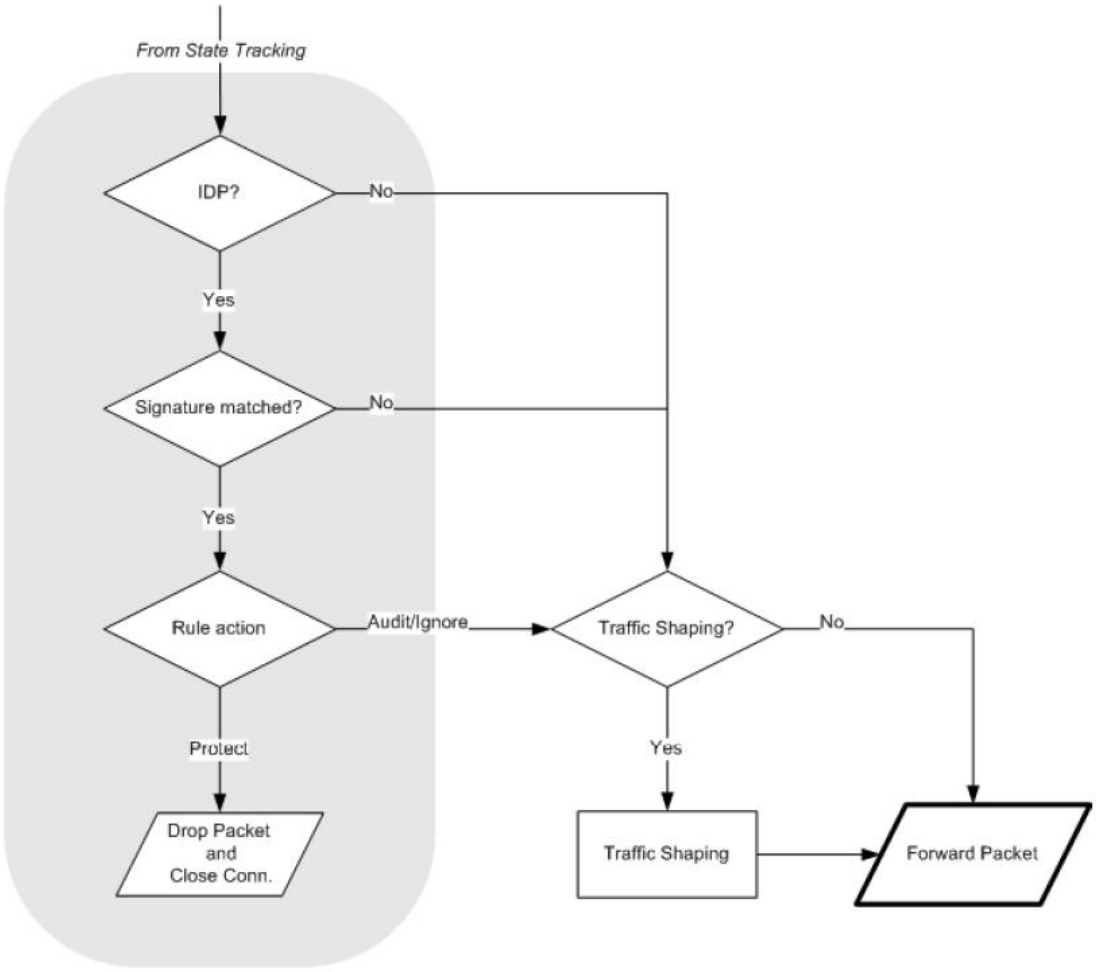
Pakettivirran eteneminen CorePlussassa.



Pakettivirran eteneminen CorePlussassa (jatkoa edelliseen).



Pakettivirran eteneminen CorePlussassa (jatkoa edelliseen).



Liitteen sivun kaksi laatikko ”Apply Rules” yksityiskohtaisemmin.