Mika Töyrylä

Jouni Ylärakkola

SEURAAVAN SUKUPOLVEN PALO-MUURI JA SEN KONFIGUROINTI

Opinnäytetyö

Tietotekniikka

Kesäkuu 2016

KYAMK
University of Applied Sciences

KYAMK
University of Applied Sciences

Tekijä/Tekijät	Tutkinto	Aika
Mika Töyrylä Jouni Ylärakkola	Insinööri	Kesäkuu 2016

Opinnäytetyön nimi

Seuraavan sukupolven palomuuri ja sen konfigurointi

47 sivua

Toimeksiantaja

LPOnet Oy Ab

Ohjaaja

Yliopettaja Martti Kettunen

Tiivistelmä

Opinnäytetyön aiheena oli Firepowerin eli Ciscon valmistaman seuraavan sukupolven palomuurin ominaisuuksien tutkiminen ja sen soveltuvuus toimitettavaksi palveluna usealle asiakkaalle. Tavoitteena oli myös Firepowerin käyttöönottaminen Kymenlaakson ammattikorkeakoulun ICTLAB-opetusympäristössä.

Opinnäytetyössä käytiin läpi Firepoweriin liittyvä teoria ennen käytännön osuutta. Teoriaosuudessa käsiteltiin palomuurien, IDPS:ien, SSL:n ja Firepowerin toimintoja yleisellä tasolla.

Käytännön osuus aloitettiin asentamalla Firepower Management Center virtuaalisena versiona ICTLAB:n ESXi-palvelimelle. Tämän jälkeen Firepower-ominaisuus asennettiin kahteen eri Cisco ASA 5515-X laitteeseen, joista toinen on tarkoitettu laboratoriotestikäyttöön ja toinen tuotantoverkkoon. Asennuksen jälkeen ne liitettiin osaksi management centeriä, jossa varsinainen hallinta tapahtui.

Management centerissä luotiin pääsynhallinta-, SSL-, AMP-, NGIPS- ja identiteettikäytännöt ja niihin tarkoituksenmukaiset säännöt. Kaikki käytännöt liitettiin osaksi pääsynhallintakäytäntöä, joka liitettiin ASA-laitteeseen. Järjestelmän luomasta informaatiosta luotiin verkkokohtaisia raportteja, joista selvisi esimerkiksi mahdolliset haittaohjelmat, hyökkäykset ja niiden määrä. Lopussa testattiin myös korrelaatioiden toimintaa ja konfiguroitiin käyttöön ulkoinen autentikointi LDAP-menetelmällä.

Työ onnistui hyvin ja järjestelmä jäi käyttöön ICTLAB-opetusympäristöön. Työtä tehtäessä kävi ilmi, että Firepower soveltuu myös tarjottavaksi palveluna asiakkaille, mutta karsituin ominaisuuksin. Hyödyllisiä ominaisuuksia nousi myös esille, kuten raportoinnin automatisointi. Jatkokehitettäväksi jäi luotujen sääntöjen optimointia.

Asiasanat

palomuuri, firepower, IPS, SSL, NGFW

KYAMK
University of Applied Sciences

Author (authors)	Degree	Time
Mika Töyrylä Jouni Yläräkkola	Bachelor of Engineering	June 2016

Thesis Title

Next-Generation Firewall and How to Configure It

47 pages

Commissioned by

LPOnet Oy Ab

Supervisor

Martti Kettunen, Principal Lecturer

Abstract

The subject of this thesis was to investigate features of Cisco's next-generation firewall called Firepower and to find out if it can be used as a service delivered to multiple customers. Another goal was to implement this system to ICTLAB of Kymenlaakso University of Applied Sciences.

The theoretical framework around the subjects connected to Firepower was explored before the practical part of the work. The theoretical framework included basic theory about features of firewall, IDPS, SSL and Firepower.

The practical part was started by installing a virtual version of Firepower Management Center into ESXi server of ICTLAB. After this, Firepower feature was installed in two different Cisco's ASA 5515-X devices, one for testing and the other for production network. After the installation, the devices were connected to be a part of the management center where the actual controlling happened.

Access control, SSL, AMP, NGIPS and identity policies and appropriate rules were created in the management center. All created policies were linked as part of the access control policy, which was linked to the ASA device. Reports defined by networks were created from system generated information. Reports included information such as possible malwares, intrusions and amount of intrusions. In the end, correlations were also tested and external authentication was configured with LDAP.

The thesis was successful and the system was left running in the ICTLAB. During the thesis process it was found out that it is possible to deliver Firepower as a service but the features are limited. Useful features such as automatic reports were also found. The work can be continued by optimizing the rules created.

Keywords

firewall, firepower, IPS, SSL, NGFW

SISÄLLYS

SANASTO JA LYHENTEET 6
1 JOHDANTO 7
2 PALOMUURIT 8
2.1 Perinteiset palomuurit 8
2.1.1 Pakettisuodattimet 8
2.1.2 Yhteyssuodattimet 8
2.1.3 Sovellustason yhdyskäytävät 9
2.2 Seuraavan sukupolven palomuurit 9
2.3 Palomuurien liitännät: Inside, Outside ja DMZ 9
2.4 Virtuaaliset erillisverkot 10
3 TUNKEUTUMISEN HAVAITSEMIS- JA ESTOJÄRJESTELMÄT 10
3.1 IDPS-järjestelmien käyttötarkoitukset 11
3.2 IDPS-järjestelmien toiminnot 12
3.3 IDPS-järjestelmien havaitsemistyypit 13
3.3.1 Tunnisteperusteinen 13
3.3.2 Poikkeavuusperusteinen 14
3.3.3 Protokollaperusteinen 14
3.4 IDPS-tyypit 15
4 SSL-SALAUS 16
4.1 SSL-salauksen toiminta 16
4.2 Salauksen haavoittuvuus 17
5 FIREPOWER MANAGEMENT CENTER 18
5.1 Hallittavat laitteet 19
5.1.1 7000- ja 8000-sarjan laitteet 20
5.1.2 NGIPSv 20
5.1.3 Cisco ASA with FirePOWER Services 21
5.2 Järjestelmän hallinta 22
5.2.1 Käyttäjien hallinta 22

5.2.2 Lisenssit 23
5.2.3 Toimialueet 23
5.3 Pääsynhallinta 24
5.4 Salatun liikenteen hallinta 27
5.5 Haittaohjelmasuojaus ja tiedostonhallinta 29
5.6 Tunkeutumisen estojärjestelmät 31
5.7 Verkon havainnointi ja identiteetti 33
5.8 Korrelaatiot 34
5.9 Raportointi 34
5.10 Hälytykset 35
6 KÄYTÄNNÖN TOTEUTUS JA TESTIT 35
6.1 Firepower Management Centerin asennus 35
6.2 Firepower-moduulin asennus 37
6.3 Järjestelmänhallinta 39
6.3.1 Käyttäjät 39
6.3.2 Sähköpostiasetukset 40
6.3.3 Verkon havainnointi 40
6.3.4 Hälytykset 40
6.3.5 Päivitykset ja varmuuskopiointi 40
6.4 Pääsynhallinta 41
6.5 SSL 41
6.6 AMP ja tiedostonhallinta 42
6.7 NGIPS 43
6.8 Käyttäjien tunnistus 44
6.9 Korrelaatio 45
6.10 Raportointi 45
7 LOPPUPÄÄTELMÄT 46
LÄHTEET 47

SANASTO JA LYHENTEET

AD	Active Directory
AMP	Advance Malware Protection
ASA	Advanced Security Appliance
ASDM	Cisco Adaptive Security Device Manager
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IOS	Ciscon laitteiden käyttämä ohjelmisto
IPS	Intrusion Prevention System
ISE	Identity Services Engine
NAT	Network Address Translation
NBA	Network Behavior Analysis
NGIPS	Next Generation Intrusion Prevention System
PKI	Public Key Infrastructure
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
Syslog	Lokitiedostojen tallennuspalvelin
TCP	Transport Control Protocol
Telnet	Yhteysprotokolla
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VLAN	Virtuaalilähiverkko
VPN	Virtual Private Networking

1 JOHDANTO

Kun nykyisin ajatellaan verkon tietoturvaa, pelkkä palomuuri ei enää yksin aja asiaansa. Kyberuhan koko ajan kasvaessa tarvitaan rinnalle muita verkon suojaamiseen kehitettyjä työkaluja. Tämän opinnäytetyön tarkoituksena onkin tutustua Cisco Systemsin kehittämään seuraavan sukupolven palomuuriin, Firepower, joka sisältää näitä tärkeitä ominaisuuksia. Työssä kerrotaan myös perusteoria laitteen eri osa-alueista.

Työn toimeksiantajana toimii itäuusmaalainen tietoliikenneyhtiö LPOnet Oy AB, joka on Puhelinosuuskunta LPO:n tytäryhtiö. Yhtiö tarjoaa internet-, tv- ja puhepalveluja niin kuluttajille kuin yrityksillekin. Yhtiö kuuluu valtakunnalliseen Finnet-ryhmään ja se palvelee asiakkaitaan Loviisan ja Porvoon myymälöissä.

Tavoitteena on tutkia Firepowerin soveltuvuutta palveluntarjoajan käytössä sekä perehtyä laitteen tarjoamiin ominaisuuksiin. Tärkeitä testattavia aiheita ovat esimerkiksi, kuinka palveluntarjoajan eri asiakkaat pystytään rajaamaan ja miten heille pystytään tarjoamaan yrityskohtaisia raportteja. Toinen tavoite on saada järjestelmä käyttöön Kymenlaakson ammattikorkeakoulun ICTLAB-opetusympäristössä.

Aiheeseen liittyen on aiemmin tehty opinnäytetyö *Seuraavan sukupolven palomuuri* Satakunnan ammattikorkeakoulussa, tekijänä Jani Roukka. Kyseisessä työssä esitellään yleisluontoisesti seuraavan sukupolven palomuureja ja niiden vertailuja keskenään. Tämä opinnäytetyö eroaa aiemmasta siten, että se keskittyy tiettyyn seuraavan sukupolven palomuuriin, sen eri ominaisuuksiin ja hallintaan. Työssä käytettävä palomuuri on Cisco ASA 5515-X with FirePOWER Services.

Kaikki käytännön testaukset suoritetaan ICTLAB-opetusympäristössä. Ensimmäiset testit toteutetaan erillisessä laboratorioympäristössä, joka ei ole yhteydessä muuhun verkkoon. Täten estetään konfiguraatiovirheiden aiheuttamat ongelmat aiheen ollessa vielä vieras. Järjestelmän tullessa paremmin tutuksi siirretään tuotos ICT-laboratorion tuotantoverkkoon pysyvään käyttöön ja se konfiguroidaan verkkoon sopivaksi.

2 PALOMUURIT

Termi palomuuri on saanut nimensä toimitilojen arkkitehtuurisesta maailmasta. Rakennuksissa palomuuri on tulenkestävästä materiaalista, kuten betonista, valmistettu muuri, jonka tarkoitus on hidastaa tulen leviämistä läpi rakennuksen. Samalla tavoin palomuurin tehtävä tietoverkossa on estää sinne kuulumaton liikenne verkosta toiseen. Yleisimmin palomuuri sijoitetaan luotetun verkon ja luottamattoman, tavallisesti Internetin, väliin. (Osipov, Sweeney & Sajavaara 2002, 17.)

Menneisyydessä oli tavallista, ettei organisaatioilla ollut lainkaan käytössä palomuuria, vaan luotettiin ainoastaan päätelaitteiden tietoturvaan tiedon suojaamiseksi. Verkkojen kasvaessa riittävän tietoturvatason ylläpitämisestä tuli kömpelöä ja riskialtista, etenkin hakkerointiuhan koko ajan kasvaessa. (Osipov ym. 2002, 17.)

2.1 Perinteiset palomuurit

2.1.1 Pakettisuodattimet

Pakettisuodattimet (Packet Filters) tekevät reitityspäätöksen ainoastaan OSI-mallin siirto- tai verkkokerroksesta löytyvän tiedon perusteella. Ne käsittelevät joka pakettia yksitellen eivätkä siten pysty seuraamaan koko TCP-istuntoa. Näin ollen ne eivät pysty tunnistamaan ulkoverkosta saapuvia käsiteltyjä paketteja, jotka ovat merkitty olemaan osa olemassa olevaa istuntoa. Pakettisuodattimet konfiguroidaan niin, että ne sallivat tai estävät liikenteen lähde- tai kohdeosoitteiden, -porttien tai eri protokollien perusteella. (Osipov ym. 2002, 20.)

Pakettisuodattimien suurin hyöty onkin niiden nopeus. Koska ne eivät tarkista sovelluskohtaista tietoa, voivat ne toimia lähes yhtä nopeasti kuin reitittimet. (Osipov ym. 2002, 20.)

2.1.2 Yhteyssuodattimet

Tilallisten yhteyssuodattimien (Stateful Inspection Packet Filters) kehittäminen alkoi halusta parantaa tavallisten pakettisuodattimien kyvykkyyttä ja tietoturvaa, silti hyödyntäen pakettisuodattimien nopeutta. Yhteyssuodattimet pystyvät seuraamaan käynnissä olevia istuntoja ja näin ne voivat tarkastaa ACK-

pakettien laillisuuden verraten pakettia yhteystaulukon merkintöihin. Palomuuri luo näitä merkintöjä aina sen nähdessä ensimmäisen SYN-paketin, joka aloittaa TCP-yhteyden. Merkinnät poistuvat automaattisesti käyttäjän määrittelemän ajan jälkeen. (Osipov ym. 2002, 21.)

Tilallisuutta pystytään hyödyntämään myös näennäisesti UDP-liikenteessä, jolla ei normaalisti ole käsitystä tilasta. Palomuuri luo merkinnän yhteystaulukkoon, kun ensimmäinen UDP-paketti lähetetään. UDP-paketti turvattomammasta verkosta (vastaus) sallitaan vain, mikäli vastaava merkintä löytyy yhteystaulukosta. (Osipov ym. 2002, 21–22.)

2.1.3 Sovellustason yhdyskäytävät

Sovellustason yhdyskäytävät (Application Proxies) toimivat välittäjinä verkkoistunnoissa. Käyttäjän yhteys päättyy välipalvelimeen ja vastaavanlainen erillinen yhteys aloitetaan palvelimelta kohdelaitteelle. Yhteydet analysoidaan OSI-mallin sovelluskerrokselle saakka ja päätetään sallitaanko ne. Tästä syystä välipalvelimia voidaan pitää turvallisempina kuin pakettisuodattimia. Näihin verrattuna tämä prosessi on kuitenkin toiminnaltaan vaativampaa ja heikentää suorituskykyä. (Osipov ym. 2002, 22.)

2.2 Seuraavan sukupolven palomuurit

Seuraavan sukupolven palomuuri, Next Generation Firewall, on joustavasti käytetty termi uusista palomuureista, joihin on sisällytetty myös muita verkon tietoturvaan liittyviä ominaisuuksia. Näitä ovat mm. identiteetin tunnistaminen, integroitu tunkeutumisen estojärjestelmä ja sovellusten tunnistaminen. Tarkemmin näistä ominaisuuksista kerrotaan työssä myöhemmin. (Wilkins. 2014.)

2.3 Palomuurien liitännät: Inside, Outside ja DMZ

Perustilassa palomuurilla on vain kaksi verkkoliitäntää, inside ja outside. Nämä nimet kuvastavat luottosuhdetta liitettyihin verkkoihin: outside-liitäntä verkolle johon ei luoteta (yleisimmin Internet) ja inside-liitäntä luotetulle verkolle. (Osipov ym. 2002, 23.)

Kun käytössä on vain kaksi liitäntää, muodostuu ongelmaksi esimerkiksi asiakkaille tarkoitetun WWW-palvelimen sijoittaminen. Jos se sijoitetaan palomuurin ulkopuolelle, on se täysin altis hyökkäyksille ja vain oman tietoturvansa varassa. Mikäli se puolestaan sijoitetaan palomuurin sisäpuolelle, on palo-

muuri konfiguroitava sallimaan WWW-liikenne (portit 80 ja 443) palvelimelle. Mikäli hyökkääjä nyt kykenisi kaappaamaan WWW-palvelin etäyhteydellä hallintaansa käyttäen porttia 80, pystyisi hän käynnistämään sieltä hyökkäyksiä minne tahansa sisäverkossa. (Osipov ym. 2002, 23.)

Vastaus tähän ongelmaan on kolmas verkkoliitäntä, joka ei ole sisä- eikä ulkopuolella vaan pikemminkin niiden välissä. Kyseistä verkkoa kutsutaan nimellä DMZ ja tänne on sijoitettavissa Internetyhteyttä vaativat palvelimet, kuten aiemmin esimerkkinä ollut WWW-palvelin. Näin sekin on suojattu palomuurilla, mutta sillä ei enää ole vapaata pääsyä sisäverkkoon. (Osipov ym. 2002, 23.)

2.4 Virtuaaliset erillisverkot

Koska kiinteä yhteys arkaluontoista tietoa toisilleen lähettävien toimipaikkojen välillä olisi kallista, kehitettiin ratkaisuksi virtuaalinen erillisverkko eli VPN. Tiedonsiirron yksityisyys läpi julkisen verkon, kuten Internetin, saavutetaan tyypillisesti käyttäen salausmenetelmiä. (Osipov ym. 2002, 29.)

Aiemmin organisaatioiden oli käytettävä kalliita menetelmiä, kuten päästä päähän vuokrattuja yhteyksiä tai kehysvälitysverkkoja, saavuttaakseen tiedonsiirron toimipaikkojen välillä. Kalleudesta huolimatta VPN:t yleistyivät hitaasti niiden vaikean hallittavuuden ja konfiguroinnin sekä Internetin epäluotettavuuden takia. (Osipov ym. 2002, 30.)

Internetin sittemmin muututtua luotettavaksi siirtotieksi ja hallinnan optimoinnin myötä VPN:ien adoptoijat keskittyivät yhteentoimivuuden ja tietoturvan parantamiseen. Yksi näistä kehityksistä oli esimerkiksi IPsec-protokollastandardi. Kehityksen johdosta VPN:iä käytetäänkin nykyisin laajalti moniin eri tarkoituksiin, kuten yhteysratkaisuna yrityksien asiakkaille, liikkeille tai yhteistyökumppaneille. (Osipov ym. 2002, 30–31.)

3 TUNKEUTUMISEN HAVAITSEMIS- JA ESTOJÄRJESTELMÄT

Tunkeutumisen havaitseminen on prosessi, jolla monitoroidaan tapahtumia tietokonejärjestelmässä tai verkossa mahdollisten tapahtumien varalta, jotka rikkovat tai ovat välitön uhka tietoturvapolitiikalle. Tapahtumilla on monia aiheuttajia, kuten haittaohjelmat, hyökkääjän laiton pääsy järjestelmään internetistä tai käyttäjät, jotka väärinkäyttävät oikeuksiaan tai yrittävät saada lisä oi-

keuksia. Vaikka monet tapahtumat ovat haitallisia, eivät kaikki kuitenkaan ole. Esimerkiksi käyttäjä saattaa kirjoittaa osoitteen väärin, jolloin hän saattaa yrittää yhdistää järjestelmään, johon hänellä ei ole käyttöoikeutta. (Scarfone & Mell. 2007, 15.)

Tunkeutumisen havaitsemisjärjestelmä (IDS) on sovellus, joka automatisoi tunkeutumisen havaitsemisen. Tunkeutumisen estojärjestelmä (IPS) on sovellus, jolla on tunkeutumisen havaitsemisjärjestelmän ominaisuudet, mutta se voi myös yrittää pysäyttää mahdolliset tapahtumat. IDS ja IPS tarjoavat monia samoja ominaisuuksia, ja käyttäjä voi halutessaan ottaa IPS:n esto-ominaisuuden pois päältä tehden siitä havaitsemisjärjestelmän. Järjestelmistä, jotka sisältävät molemmat ominaisuudet, käytetään yleensä yhteisnimitystä IDPS. (Scarfone & Mell. 2007, 15.)

3.1 IDPS-järjestelmien käyttötarkoitukset

IDPS:n tarkoitus on havaita mahdolliset tapahtumat. Se voi esimerkiksi havaita, kun hyökkääjä on onnistuneesti vaarantanut järjestelmän hyötykäyttäen haavoittuvuutta järjestelmässä. Sen jälkeen IDPS voi ilmoittaa tapahtumasta järjestelmänvalvojalle, joka voi puuttua tapahtumaan minimoidakseen mahdolliset vahingot. IDPS voi myös kerätä tietoa tapahtumista, joita voidaan myöhemmin käyttää tapahtumien analysointiin. Monet IDPS:t voidaan myös konfiguroida havaitsemaan mahdolliset tietoturvarikkomukset. Esimerkiksi IDPS voidaan konfiguroida palomuurin tapaisilla asetuksilla, jotka sallivat sen havaita verkkoliikenteen, joka rikkoo yrityksen tietoturvapolitiikkaa. Jotkut IDPS:t voivat myös monitoroida tiedostojen siirtoa ja havaita epäilyttäviä tapahtumia, kuten suuren tietokannan kopiointi kannettavalle tietokoneelle. (Scarfone & Mell. 2007, 15.)

Monet IDPS:t voivat myös havaita tiedustelut, jotka saattavat viitata mahdolliseen hyökkäykseen. Esimerkiksi jotkut hyökkäystyökalut ja haittaohjelmat suorittavat tiedustelua, kuten käyttäjä- ja porttiskannaukset, tunnistaakseen hyökkäyksen kohteet. IDPS voi estää tiedustelun ja ilmoittaa siitä verkon ylläpitäjälle, joka voi tehdä mahdolliset muutokset estääkseen hyökkäyksen. Koska tiedustelu on niin yleistä internetissä, tiedustelun havaitseminen tehdään yleensä vain suojatussa sisäverkossa. (Scarfone & Mell. 2007, 15.)

Tapahtumien havaitsemisen lisäksi yritykset ovat löytäneet monia muita käyttötarkoituksia IDPS:ille:

- **Havaitsee mahdolliset tietoturvaongelmat.** IDPS:ään voidaan tehdä samat säännöt kuin palomuurissa ja näin havaita mikäli liikenne pääsee palomuurin läpi, vaikka sen ei pitäisi.
- **Uhkien dokumentointi.** IDPS kirjaa tietoa uhista, joita se havaitsee. Uhkien määrän ja tyyppien ymmärtäminen voi auttaa tarvittavien tietoturvatoimenpiteiden tekemisessä.
- **Estää yksilöitä rikkomasta tietoturvapolitiikkaa.** Jos käyttäjät tietävät olevansa monitoroinnin alaisia, eivät he todennäköisemmin tee rikkomuksia. (Scarfone & Mell. 2007, 16)

Tietojärjestelmäriippuvuuden noustessa ja mahdollisten hyökkäysten yleistyessä niitä kohtaan, on IDPS:istä tullut tarpeellinen osa lähes jokaisen yrityksen tietoturvainfrastruktuuria. (Scarfone & Mell. 2007, 16.)

3.2 IDPS-järjestelmien toiminnot

IDPS:iä on olemassa monia erilaisia ja ne eroavat toisistaan siten, että kuinka ja minkälaisia tapahtumia ne huomaavat. Monitoroinnin ja analysoinnin lisäksi kaiken tyyppiset IDPS:t suorittavat seuraavanlaisia toimintoja:

- **Tallentaa tietoa tapahtumista.** Tieto tallennetaan usein paikallisesti, mutta voidaan myös lähettää erillisiin järjestelmiin.
- **Ilmoittaa tärkeistä tapahtumista.** Hälytysilmoituksia lähetetään esimerkiksi syslogiin, sähköpostiin tai SNMP-trap viesteillä. Niissä on usein vain perustiedot ja tarkemmat tiedot on tarkistettava IDPS:stä.
- **Luo raportteja.** Tekee raportteja monitoroiduista tapahtumista ja antaa tarkempia tietoja halutuista tapahtumista. (Scarfone & Mell. 2007, 16.)

Jotkut IDPS:t voivat myös muuttaa profiiliaan havaitessaan uusia uhkia. Esimerkiksi IDPS saattaa alkaa kerätä tarkempaa dataa tietyntyyppisen haitallisen tapahtuman jälkeen. Se voi muuttaa asetuksia tietyntyyppisten hälytysten tapahtuessa tai muuttaa mihin prioriteettiluokkaan tapahtumat sijoitetaan. (Scarfone & Mell. 2007, 16.)

IPS ja IDS eroavat toisistaan siten, että IPS voi pysäyttää mahdolliset hyökkäykset. Ne käyttävät useita tekniikoita, jotka jaetaan seuraaviin ryhmiin:

- **IPS pysäyttää hyökkäyksen.** Katkaisee yhteyden, jota käytetään hyökkäykseen tai estää liikenteen hyökkäyksen kohteeseen.
- **Muuttaa tietoturvaympäristöä.** Muokkaa muiden verkkolaitteiden konfiguraatiota niin että se estää hyökkäyksen.

- **Muuttaa hyökkäyksen sisältöä.** Poistaa tai muokkaa osaa hyökkäyksestä. Esimerkiksi poistaa haitallisen liitteen sähköpostista. (Scarfone & Mell. 2007, 16–17.)

IDPS ei voi taata täysin varmaa tunnistusta. Tämä aiheuttaa vääriä positiivisia ja negatiivisia tapahtumia. Järjestelmissä ei ole mahdollista poistaa kaikki vääriä positiivisia ja negatiivisia hälytyksiä, sillä yleensä toisen vähentäminen lisää toisia. Suurimmassa osassa yrityksistä pyritään vähentämään vääriä negatiivisia hälytyksiä, joka tarkoittaa että havaitaan enemmän haitallisia tapahtumia. Tämä aiheuttaa sen että tarvitaan myös lisää prosessointitehoa erottaakseen väärät positiiviset oikeista hyökkäyksistä. (Scarfone & Mell. 2007, 17.)

Suurin osa IDPS:istä tarjoaa myös tunnetuimpien väistötekniikoiden havaitsemista. Hyökkääjät käyttävät näitä tekniikoita välttääkseen IDPS:ää havaitsemasta hyökkäystä. Tämä tapahtuu esimerkiksi muokkaamalla sisältö niin että se pääsee IDPS:n läpi siten, että kohde vielä ymmärtää sisällön. Suurin osa IDPS:istä pystyy kuitenkin näkemään sisällön samalla tavalla kuin kohde, jolloin IDPS:n ohittaminen ei onnistu. (Scarfone & Mell. 2007, 17.)

3.3 IDPS-järjestelmien havaitsemistyypit

IDPS:t voidaan jakaa kolmeen eri tyyppiin: tunniste- (Signature-Based), poikkeavuus- (Anomaly-Based) ja protokollaperusteinen (Stateful Protocol Analysis). Suurimmassa osassa IDPS:iä käytetään useampaa tyyppiä yhdessä, jotta saavutetaan tehokkaampi ja tarkempi havaitseminen. (Scarfone & Mell. 2007, 17.)

3.3.1 Tunnisteperusteinen

Tunnisteperusteinen tunnistus on prosessi, joka vertaa tunnisteita valvottuihin tapahtumiin tunnistaakseen hyökkäyksiä. Tunniste on kaava, joka vastaa jotain tunnettua uhkaa. Esimerkkejä tunnisteista:

- Telnet yhteys nimellä ”root”, joka rikkoo yrityksen tietoturvapolitiikkaa.
- Sähköposti, jonka aiheena on ”Free pictures!” ja liitteenä on ”free-pics.exe”, jotka ovat tunnetun haittaohjelman piirteitä.
- Käyttöjärjestelmän lokimerkintä status-koodin arvon ollessa 645, mikä tarkoittaa että käyttäjän tarkastus on pois päältä. (Scarfone & Mell. 2007, 18.)

Tunnisteperusteinen tunnistus on hyvin tehokas valmiiksi tunnettujen uhkien havaitsemiseen, mutta tehoton ennestään tuntemattomia uhkia havaittaessa. Esimerkiksi jos hyökkääjä muuttaa edellisten esimerkkien liitteen nimeksi ”freepics2.exe”, ei sitä enää tunnisteta, koska järjestelmä etsii vain ”freepics.exe” tiedostoa. (Scarfone & Mell. 2007, 18.)

Tunnisteperusteinen tunnistus on yksinkertaisin havaitsemistekniikka, koska se vain vertaa nykyistä aktiviteettia, kuten pakettia tai lokitiedostoa, valmiiseen listaan. Tunnisteperusteinen tunnistus ei ymmärrä monimutkaisia kommunikaatioita, joka aiheuttaa sen, että se ei tunnista hyökkäyksiä jotka sisältävät useita tapahtumia. (Scarfone & Mell. 2007, 18.)

3.3.2 Poikkeavuusperusteinen

Poikkeavuusperusteinen tunnistus vertaa normaalia verkon toimintaa havaittuihin tapahtumiin suurien eroavaisuuksien varalta. Tämä metodi käyttää profiileita, jotka ovat luotu monitoroimalla verkon normaalia toimintaa tietyllä aikavälillä. Tämän jälkeen IDPS vertaa nykyistä verkon aktiviteettia tyypilliseen liikenteeseen profiilissa. Poikkeavuusperusteinen tunnistus voi olla hyvin tehokas havaitsemaan ennestään tuntemattomia uhkia. Yleisiä ongelmia puolestaan ovat esimerkiksi: profiiliin saattaa sisältyä valmiiksi haitallisia aktiviteetteja, profiilit jotka eivät ole riittävän monimutkaisia oikean maailman liikenteeseen tai useat väärät hälytykset. (Scarfone & Mell. 2007, 22.)

3.3.3 Protokollaperusteinen

Protokollaperusteinen tunnistus vertaa valmiiksi luotuja profiileja nykyisiin protokollatiloihin. Toisin kuin poikkeavuusperusteinen tunnistus, joka käyttää käyttäjä- tai verkkokohtaisia profiileja, protokollaperusteinen tunnistus käyttää laitevalmistajan globaaleja profiileja. Ne määrittävät millaisia protokollia tulisi käyttää. Se kykenee seuraamaan ja ymmärtämään protokollien tilaa, mikä mahdollistaa monien uhkien tunnistamisen, joita muut tekniikat eivät tunnista. Protokollaperusteisen tunnistuksen ongelmia ovat seuraavat: täysin tarkkaa mallia protokollista on vaikea tai mahdoton valmistaa, se käyttää hyvin paljon resursseja ja se ei tunnista hyökkäyksiä, jotka eivät riko yleisesti hyväksyttyjen protokollien ominaisuuksia. (Scarfone & Mell. 2007, 22.)

3.4 IDPS-tyypit

IDPS-tyyppejä on monenlaisia. Ne voidaan jakaa neljään ryhmään: verkkoperusteinen (Network-based), langaton (Wireless), käyttäytymisperusteinen (Network Behavior Analysis) ja isäntäperusteinen (Host-based). Jako tehdään sen mukaan, millaisia tapahtumia ne valvovat ja miten ne on toteutettu. (Scarfone & Mell. 2007, 20.)

Verkkoperusteinen

Verkkoperusteinen IDPS monitoroi verkon osaa tai laitteita, ja analysoi verkkoa sekä sovellus protokollien toimintaa havaitakseen epäilyttävää toimintaa. Se voi myös tunnistaa monia erityyppisiä tapahtumia. Se sijoitetaan usein verkon reunalle, kuten reunapalomuurien tai -reitittimien, VPN-palvelimien, etäyhteyspalvelimien ja langattomien verkkojen läheisyyteen. (Scarfone & Mell. 2007, 20.)

Langaton

Langaton IDPS monitoroi langatonta verkkoliikennettä ja analysoi langattomia verkkoprotokollia hyökkäyksien varalta. Se ei tunnista hyökkäyksiä sovelluksissa tai korkeamman tason verkkoprotokollissa (esim. TCP tai UDP), jota verkkoliikenne kuljettaa. Yleensä se sijoitetaan sinne, missä yrityksen langaton verkko on, mutta se voidaan myös sijoittaa paikkaan, jossa luvaton verkko liikenne on mahdollista. (Scarfone & Mell. 2007, 20–21.)

Käytösperusteinen (NBA)

Käytösperusteinen IDPS tutkii verkkoliikennettä tunnistaen uhkia, jotka liittyvät epätavalliseen verkkoliikenteeseen, kuten palvelunestohyökkäys, tietynlaiset haittaohjelmat tai sääntörikkomukset. NBA valvoo yleensä yrityksen sisäisen verkon liikennettä, mutta se voidaan tehdä myös yrityksen sisä- ja ulkoverkon välille. (Scarfone & Mell. 2007, 21.)

Isäntäperusteinen

Isäntäperusteinen IDPS monitoroi yksittäisen laitteen ominaisuuksia epätavallisten tapahtumien varalta. Tyypillisesti sillä valvotaan yhden koneen liikennettä, lokeja, prosesseja, sovelluksia ja tiedostoja. Isäntäperustein IDPS sijoite-

taan yleensä kriittisiin laitteisiin, kuten palvelimiin, joissa on tärkeää tietoa. (Scarfone & Mell. 2007, 21.)

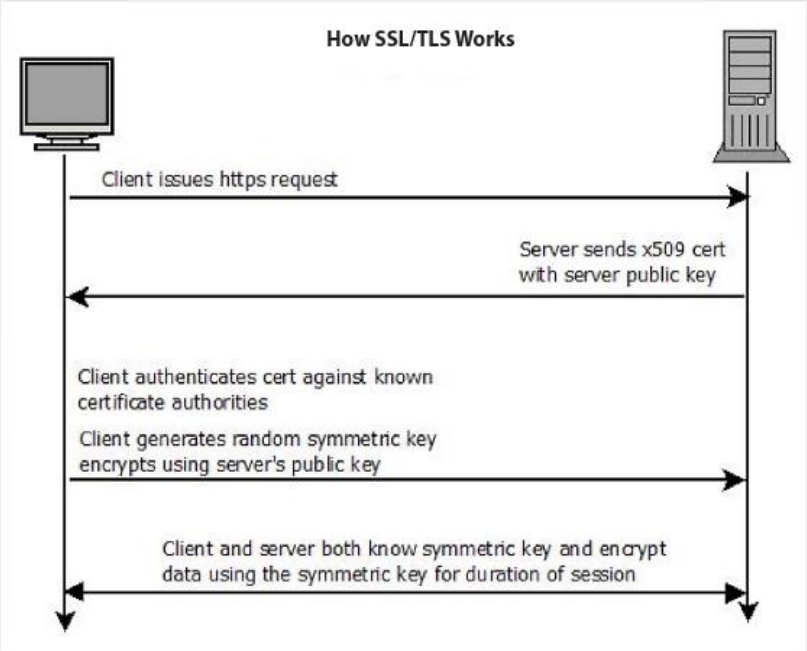
4 SSL-SALAUS

SSL-salaus on tärkeä osa datan suojaamista verkkoliikenteessä esim. verkko-ostoksissa, sähköposteissa ja mobiilisovelluksissa. SSL-salattu data voi kulkea koko yrityksen tietoturvan läpi ilman tarkastusta. Sen takia SSL-liikenteestä on tullut hyökkääjien työkalu. (Butler. 2013, 4.)

4.1 SSL-salauksen toiminta

SSL, toiselta nimeltään TLS, on PKI-salausprotokolla. SSL toimii siirtoprotokollan (TCP) ja sovelluksen, jonka dataa yritetään suojata, välillä. Se voi olla osa mitä tahansa sovellusta, joihin sisältyy selaimet tai sähköpostisovellukset, ja se suojaa dataa tekemällä siitä lukukelvotonta ulkopuolisille. (Butler. 2013, 4.)

SSL sisältää julkisten avainten vaihtamista. Niitä käytetään symmetrisen avaimen salaamiseen ja sen voi avata vain toisen käyttäjän yksityisellä avaimella. Kuvassa 1 SSL yksinkertaisessa muodossa. (Butler. 2013, 4.)



Kuva 1 SSL:n toiminta (Butler. 2013, 4)

SSL:n edut ovat muutakin kuin salaus ja datan suojaaminen. Niihin sisältyvät tiedon eheys ja luotettavuus, jotka ovat avainasemassa riskien hallinnassa. On tärkeää kuitenkin muistaa, että SSL:ää voi käyttää myös ilman todellista

varmennusta, kuten itse allekirjoitettujen sertifikaattien kanssa. (Butler. 2013, 4.)

SSL on sen julkaisun jälkeen muuttunut entistä turvallisemmaksi esim. nostamalla salausavaimen pituutta. Vielä turvallisempi vaihtoehto on käyttää *Diffie-Hellman Exchange* (DHE) -algoritmia RSA-avaimien sijaan. (Butler. 2013, 5.)

4.2 Salauksen haavoittuvuus

Salauksen haavoittuvuus ei ole jäänyt hyökkääjiltä huomaamatta. Vaikka SSL yrittää tehdä internetistä turvallisemman, saattaa se luoda sokeita kohtia, jotka oikeastaan vähentävät tietoturvaa. (Butler. 2013, 6.)

Vaikka kaikki tietoturvalaitteet olisivat kunnossa, eivät ne välttämättä kykene näkemään muuta kuin kohdelaitteen, ja paketin muu sisältö jää tuntematto-maksi. Tämä on ongelmallista, sillä siihen voi olla piilotettu haitallista dataa. (Butler. 2013, 6.)

Hyökkääjät voivat piilottaa haitallisia toimia ja laitonta datansiirtoa monilla eri tavoilla esim. lähettämällä dataa palomuurin sallituista porteista, peittämällä haittaohjelman kommunikaatio hyökkääjän kanssa tai tekemällä tietojenkalas-teluyrityksistä entistäkin luotettavamman näköisiä. (Butler. 2013, 6.)

Alkuperäinen tartunta, joka tulee sallitusta portista, on yleisin tapa saada tar-tunta järjestelmään, palomuurin tai IPS:n huomaamatta. Keskiverto käyttäjä-kään ei tavallisesti huomaa hyökkäystä, sillä verkkosivulla näkyy salaukseen viittaava lukko (Miller. 2014, 14). Liikenteen salaus luo täydellisen suojan hyökkäyksille. (Butler. 2013, 6.)

Cross-site scripting mahdollistaa evästeiden varastamisen. Evästeitä voidaan käyttää esim. käyttäjän varastamiseen, istunnon kaappaukseen, asetusten muuttamiseen, *cookie poisoningiin* ja väärään mainontaan. Kaikki tämä voi-daan toteuttaa SSL-salatun liikenteen alaisena. (Butler. 2013, 6.)

Haittaohjelmaperheet, kuten *Zeus*, ovat tunnettuja siitä, että ne käyttävät sa-lausta ja muita metodeja salatakseen komennon ja hallinnan. Yhtenä esi-merkkinä *Gameover*-pankkitroijalainen, joka avaa SSL-yhteyden saastuneelta verkkosivulta ja käyttää sitä komento- ja hallintatoimiin. Alkuperäinen tartunta lähetetään roskapostin avulla. Kun käyttäjän selain menee saastuneelle sivul-le, luodaan yhteys automaattisesti. (Butler. 2013, 7.)

5 FIREPOWER MANAGEMENT CENTER

Firepower Management Center on Ciscon tietoturvalaitteiden keskitetty hallintakeskus. Se tarjoaa palomuurien hallintaa, sovellusten hallintaa, tunkeutumisen eston, URL-suodatuksen sekä AMP:n. Management center on keskitetty tapahtumien ja sääntöjen hallintasovellus seuraaville ratkaisuille:

- Cisco Firepower Next-Generation Firewall (NGFW)
- Cisco ASA with FirePOWER services
- Cisco Firepower Next-generation IPS (NGIPS)
- Cisco FirePOWER threat Defence for ISR
- Cisco Advanced Malware Protection (AMP) (Cisco Systems, Inc. 2016b.)

Management center tarjoaa laajaa tietoa käyttäjistä, sovelluksista, laitteista, uhista ja haavoittuvuuksista, jotka sijaitsevat tietoverkossa. Se käyttää näitä tietoja käytössä olevan verkon haavoittuvuuksien analysoimiseen ja tarjoaa suosituksia siitä, millaisia tietoturvasääntöjä kannattaa käyttää ja mitä tapahtumia tulisi tutkia. (Cisco Systems, Inc. 2016b.)

Management center tarjoaa helppokäyttöisiä hallintaikkunoita, joista voidaan säätää tietoturva-asetuksia. Se on integroitu AMP:n kanssa ja hyödyntää hiekkalaatikkoteknologiaa sekä sisältää työkalut haittaohjelmien seuraamiseen verkossa. Kaikki tämä voidaan toteuttaa helposti yhdessä käyttöliittymässä. Kuvassa 2 näkyy erilaisia hallintaikkunoita. (Cisco Systems, Inc. 2016b.)

Kuva 2. Erilaisia hallintaikkunoita (Cisco Systems, Inc. 2016b)

Firepower Management Center voidaan toteuttaa fyysisenä laitteena tai virtuaalisena sovelluksena VMware-ympäristössä. Fyysiset laitteet tarjoavat enemmän sensoreita ja suurempaa tallennustilaa kuin virtuaaliset. Virtuaalinen sovellus puolestaan on helppo sisällyttää jo valmiiseen virtualisointiympäristöön. (Cisco Systems, Inc. 2016b.)

Fyysisten management center -laitteiden malleja on useita erilaisia. Malli tulee valita sen mukaan, kuinka paljon tarvitaan sensoreita, käyttäjämäärien ja odotetun tapahtumamäärän mukaan. Kaikki mallit sisältävät samanlaiset laitteidenhallintamahdollisuudet. Kuvassa 3 nähdään eri mallien ominaisuuksia. (Cisco Systems, Inc. 2016b.)

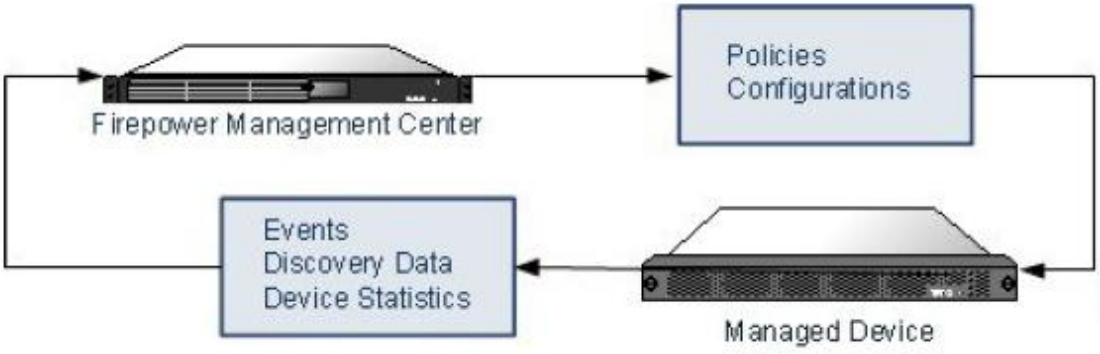
				
Feature	**FS 750**	**FS 2000**	**FS 4000**	**FS -VMW-SW**
Maximum number of sensors managed	10	70	300	25 10 2
Maximum number of IPS events	20 million	60 million	300 million	10 million
Event storage	100 GB	1.8 TB	3.2 TB	250 GB
Maximum network map (hosts/users)	2,000/2,000	150,000/150,000	600,000/600,000	50,000/50,000
Maximum flow rate (flows per second)	2,000 fps	12,000 fps	20,000 fps	Varies*
Network interfaces	2 x 1 Gbps	2 x 1 Gbps 2 x 10 Gbps (optional SFPs available in Cisco Commerce)	2 x 1 Gbps 2 x 10 Gbps (optional SFPs available in Cisco Commerce)	1 x 1 Gbps
High availability	Lights-out management (LOM)	RAID 5, LOM, high-availability pairing	RAID 5, LOM, high-availability pairing	No

Kuva 3. Management centerin eri mallit (Cisco Systems, Inc. 2016b)

5.1 Hallittavat laitteet

Verkkoon asennetut hallittavat laitteet monitoroivat liikennettä management centerissä analysointia varten. Ne keräävät yksityiskohtaista tietoa mm. organisaation päätelaitteista, käyttöjärjestelmistä, sovelluksista, käyttäjistä, lähete-

tyistä tiedostoista ja haavoittuvuuksista. Firepower yhdistää nämä tiedot verkon ylläpitäjälle, jolloin hänellä on mahdollisuus tarkkailla millaisilla sivustoilla käyttäjät vierailevat, mitä sovellusta he käyttävät, arvioida verkkoliikenteen kulkua ja vastaanottaa ilmoituksia mahdollisista hyökkäyksistä. Firepower Management Centerin kanssa yhteensopivia hallittavia laitteita on useita eri malleja eri tuotesarjoista, niin fyysisiä kuin virtuaalisiakin yksilöitä. Kuvassa 4 on nähtävissä kuinka laitteet ja management center kommunikoivat keskenään. (Cisco Systems, Inc. 2015, 72)



Kuva 4. Firepower Management Centerin ja lisätyn laitteen kommunikointi (Cisco Systems, Inc. 2015, 72)

5.1.1 7000- ja 8000-sarjan laitteet

Cisco Firepower 7000- ja 8000-sarjan laitteet ovat juuri Firepower-järjestelmää varten luotuja fyysisiä yksilöitä. Laitteet vaihtelevat suoritustehoittain, mutta jakavat suurimman osan ominaisuuksistaan. Yleisesti ottaen 8000-sarjan laitteet ovat tehokkaampia kuin 7000-sarjan ja niissä on erillisiä lisäominaisuuksia, kuten *fast-path*-säännöt, linkkien yhdistäminen tai useamman laitteen yhdistäminen yhdeksi tehokkaammaksi laitteeksi. (Cisco Systems, Inc. 2015, 72)

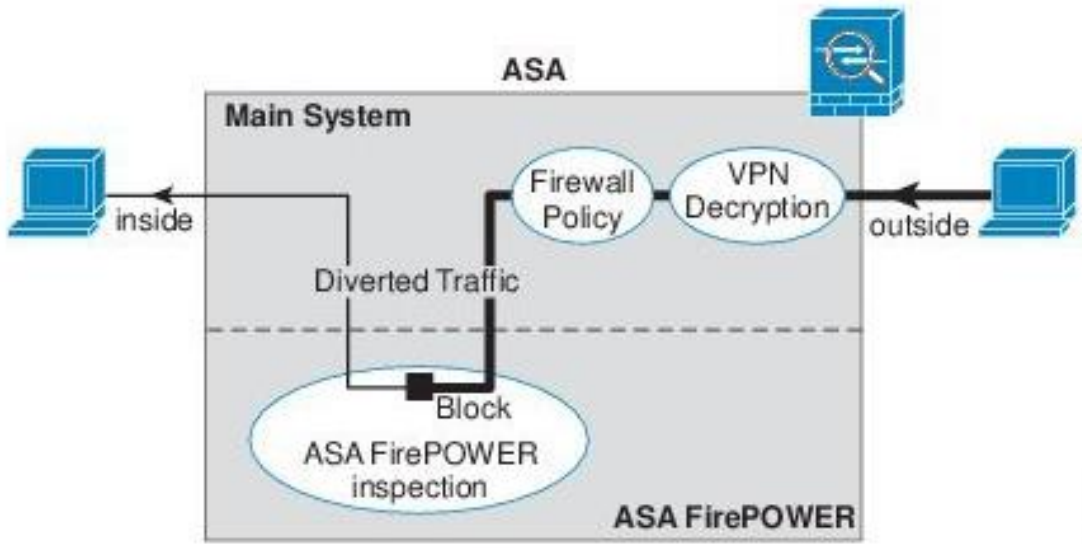
5.1.2 NGIPSv

NGIPSv on mahdollista asentaa 64-bittisenä ESXi-virtuaalilaitteena käyttäen VMwaren vSphere Hypervisoria tai vCloud Director -ympäristöä. Oletuksena NGIPSv käyttää gigan nopeudella toimivia *e1000*-portteja, mutta ne ovat muutettavissa kymmenen gigan nopeudella toimiviksi *vmxnet3*-porteiksi. Lisensseistä riippumatta NGIPSv ei tue fyysisten laitteiden ominaisuuksia, kuten redundanttisuutta ja resurssien jakamista, välitystä tai reititystä. (Cisco Systems, Inc. 2015, 72–73.)

5.1.3 Cisco ASA with FirePOWER Services

Kolmas vaihtoehto on laite Ciscon perinteisistä ASA-palomuureista. Uusimpiin 5500-X-sarjan laitteisiin on sisällytetty ohjelmistopohjainen Firepower-moduuli, poikkeuksena malli 5585-X, joka sisältää laitteistopohjaisen moduulin (Cisco Systems, Inc. 2016a). Tämä moduuli on yhteensopiva vain uusimpien IOS-versioiden kanssa ja tämä on otettava huomioon ennen sen käyttöönottoa.

Kuvassa 5 on nähtävissä kuinka ASA:n ja Firepowerin ohjelmistot keskustelevat keskenään. ASA analysoi liikenteen ensin omien käytäntöjen ja sääntöjen perusteella ja siirtää vasta hyväksytyn liikenteen Firepowerille. Nyt vuorostaan Firepower vertaa liikennettä omiin sääntöihinsä ja palauttaa vain hyväksytyn liikenteen takaisin ASA:lle lähetettäväksi eteenpäin. Firepower on kuitenkin mahdollista asettaa passiiviseen tilaan, jolloin se ei puutu liikenteeseen vaan pelkästään monitoroi sitä. (Cisco Systems, Inc. 2016a.)



Kuva 5. ASA:n ja moduulin kommunikointi (Cisco Systems, Inc. 2016a)

Mikäli ASA itse estää ja pudottaa verkkoliikenteen, ei tästä siirry minkäänlaista tietoa moduulille. Näin ollen palomuurin estämän liikenteen analysointi ei ole mahdollista management centerissä.

NGIPSv:n tapaan moduulipohjaisen Firepowerin ominaisuudet eivät ole yhtä laajat kuin 7000- ja 8000-sarjan fyysisissä laitteissa. ASA itsessään kuitenkin sisältää joitakin näistä puuttuvista ominaisuuksista, kuten VPN:n, joten näiden puuttuminen ei ole yhtä merkittävää. (Cisco Systems, Inc. 2015, 73.)

5.2 Järjestelmän hallinta

5.2.1 Käyttäjien hallinta

Firepower mahdollistaa käyttöoikeuksien jakamisen käyttäjäroolien perusteella. Analyytikolle voidaan esimerkiksi määrittää *Security Analyst* ja *Discovery Admin*. *Administrator* rooli voidaan antaa järjestelmän ylläpitäjälle, joka hoitaa Firepower-konfiguraation. (Cisco Systems, Inc. 2015, 113.)

Järjestelmän asetuksista voidaan määrittää oletusrooli kaikille ulkoista varmennusta käyttäville. Kun ulkoista varmennusta käyttänyt käyttäjä kirjautuu järjestelmään ensimmäistä kertaa, voidaan käyttäjän oikeuksia muokata. Jos käyttäjän oikeuksia ei muokata, jäävät ne perustasolle. Paikallisia käyttäjiä tehdessä määritetään käyttäjärooli jo niitä tehdessä. (Cisco Systems, Inc. 2015, 113.)

Jos järjestelmä on konfiguroitu käyttämään LDAP-varmennusta, käyttöoikeudet jaetaan sen mukaan, mihin LDAP-ryhmään käyttäjä kuuluu. Käyttäjät saavat oikeudet siihen ryhmään, missä heillä on korkein käyttöoikeus. Jos käyttäjä ei kuulu mihinkään ryhmään, saavat he oletusroolin, joka on määritetty. Mikäli LDAP on käytössä, se kumoaa oletusroolit. Samalla tavalla voidaan myös luoda RADIUS-varmennusobjekti. (Cisco Systems, Inc. 2015, 113–114.)

Useamman toimialueen järjestelmässä voidaan käyttäjäroolit jakaa toimialueen mukaan. Voidaan esimerkiksi antaa käyttäjälle vain lukuoikeus globaaliin toimialueeseen, mutta *Administrator*-oikeudet alitoimialueeseen. (Cisco Systems, Inc. 2015, 114.)

Firepower sisältää kymmenen valmiiksi määritettyä käyttäjäroolia:

- Access Admin
- Administrator
- Discovery Admin
- External Database User
- Intrusion Admin
- Maintenance User
- Network Admin
- Security Analyst
- Security Analyst (Read Only)
- Security Approver

Järjestelmässä on myös mahdollista luoda omia käyttäjärooleja, joiden pohjana voidaan käyttää valmiiksi luotuja rooleja tai luoda kokonaan uusia. (Cisco Systems, Inc. 2015, 114–115.)

Käyttäjät voivat konfiguroida henkilökohtaisia asetuksia, kuten kotisivu, salasana, aikavyöhyke ja tapahtumien näyttötavat. Jos käyttäjä kirjautuu RADIUS- tai LDAP-käyttäjällä, salasanan vaihto ei ole mahdollista. Useamman toimialueen järjestelmässä käyttäjän asetukset ovat samat kaikissa toimialueissa. (Cisco Systems, Inc. 2015, 101.)

5.2.2 Lisenssit

Firepower Management Center vaatii viisi eri lisenssiä: *protection*, *control*, *malware*, *URL-filtering* ja *VPN*, tarjotakseen täydet ominaisuudet. Ne syötetään yksi kerrallaan management centerissä ja ne ovat laite- ja management center -kohtaisia. Esimerkiksi *protection*-lisenssin avaamia ominaisuuksia laitteelle Firepower 8250 ei voida käyttää laitteella 8140. Huomioitavaa on, ettei ilman laitteelle aktivoitua *protection*-lisenssiä pystytä aktivoimaan muitakaan lisenssejä, sillä *protection*-lisenssi on aina syötettävä ensimmäisenä. Laitteelle aktivoituja lisenssejä voidaan vapaasti ottaa käyttöön tai poistaa käytöstä. (Cisco Systems, Inc. 2015, 175–176.)

Eri lisenssien avaamat toiminnot management centerissä ovat:

- **Protection:** IDS- ja IPS-toiminnot, tiedostojen hallinta (file controll) ja *security intelligence filtering*.
- **Control:** Käyttäjä- ja ohjelmistohallinta. 7000- ja 8000-sarjan laitteissa aukeaa myös high availability- sekä NAT-toiminnot.
- **Malware:** AMP
- **URL-filtering:** Kategoria- ja mainepohjainen URL-suodatus
- **VPN:** 7000- ja 8000-sarjan laitteissa VPN-ominaisuudet (Cisco Systems, Inc. 2015, 176.)

5.2.3 Toimialueet

Management centerissä olevia toimialue-asetuksia käyttäen yrityksen on mahdollista päästää asiakkaitansa hallitsemaan ja monitoroimaan heidän omia verkkojaan. Asiakkaat eivät näe toistensa alitoimialueita tai niihin liitettyjä laitteita. Mikäli käyttäjä ei erikseen muuta ko. asetuksia, kuuluvat kaikki laitteet, konfiguraatiot ja tapahtumat järjestelmän luomaan globaaliin toimialuee-

seen. Alitoimialueita voidaan luoda korkeintaan 50, kahdessa tai kolmessa tasossa. (Cisco Systems, Inc. 2015, 333–334.)

Kahden tason konfiguraatiossa yritys hallitsee globaalia toimialuetta ja sen alaisia, asiakkaille hallittavaksi tarkoitettuja, alitoimialueita. Kolmen tason konfiguraatiossa yrityksellä on edelleen hallintaoikeus kaikkeen, mutta alitoimialueisiin on mahdollista luoda vielä omia alitoimialueita, joita voi esimerkiksi antaa asiakkaan asiakkaiden hallittaviksi. Ainoastaan alin eli ns. *leaf*-toimialue voi pitää sisällään hallittavia laitteita. (Cisco Systems, Inc. 2015, 334.)

5.3 Pääsynhallinta

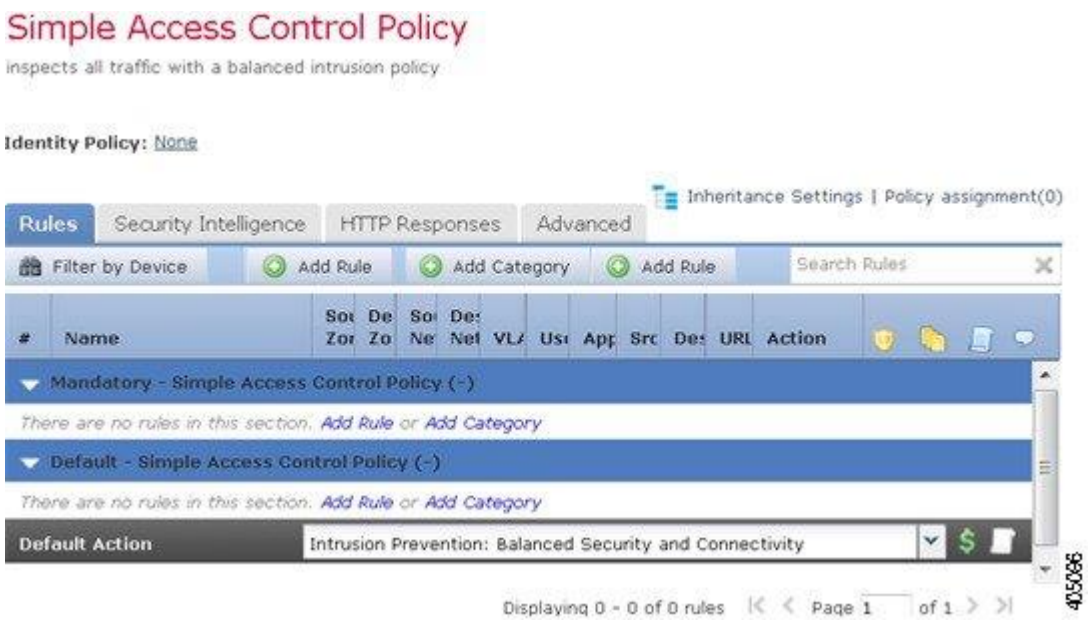
Pääsynhallinta (Access control) on hierarkkinen käytäntöperusteinen ominaisuus, joka sallii verkkoliikenteen tutkimisen. Se on erittäin hyödyllinen usean toimialueen ympäristöissä, joissa jokainen käytäntö voi periä säännöt ja asetukset pohjakäytännöstä. Tämä periminen voidaan joko pakottaa tai pienemmän tason käytännöt voivat ylittää pohjakäytännön. Jokaisella hallittavalla laitteella on käytössä vain yksi pääsynhallintakäytäntö. (Cisco Systems, Inc. 2015, 673.)

Dataa, jota käytäntö kerää hallittavista laitteista, voidaan käyttää liikenteen suodatukseen ja hallintaan perustuen:

- Yksinkertaisiin verkko- ja siirtokerroksen ominaisuuksiin, kuten kohde ja lähde, portti ja protokolla
- Viimeisin sisältöön liittyvä tieto, johon sisältyy ominaisuuksia, kuten maine, riski, merkitys työelämässä, sovellus ja sivun URL
- Alue, käyttäjä, käyttäjäryhmä tai ISE-attribuutti
- Salatun liikenteen ominaisuudet – liikenteen salaus voidaan myös purkaa tarkempaa tarkastelua varten.
- Sisältääkö liikenne haittaohjelmia tai tunkeutumisen yrityksiä. (Cisco Systems, Inc. 2015, 673.)

Jokainen liikenteen tutkimisen ja kontrollin tyyppi tapahtuu siellä, missä siinä on eniten järkeä joustavuuden ja toimivuuden kannalta. Esimerkiksi maineperusteinen musta lista käyttää vain lähde- ja kohdedataa, joten se voi estää liikenteen jo varhaisessa vaiheessa. Tunkeutumisen ja hyötykäytön estäminen taas ovat viimeinen osa puolustusta. (Cisco Systems, Inc. 2015, 674.)

Uusi pääsynhallintakäytäntö ohjaa kaikkia sen kohdelaitteita hallitsemaan liikennettä oletusasetuksella. Kuvassa 6 nähdään pääsynhallintaikkuna. (Cisco Systems, Inc. 2015, 674.)



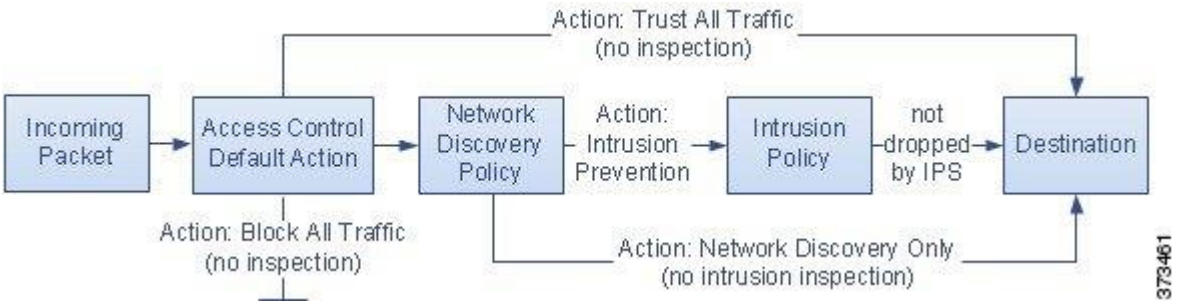
Kuva 6. Pääsynhallintasääntöikkuna (Cisco Systems, Inc. 2015, 674)

Seuraavalla listalla on mahdolliset asetukset, joita voidaan muokata käytännön luomisen jälkeen:

- **Nimi ja kuvaus:** Jokaisella laitteella tulee olla uniikki nimi. Laitteen kuvaus on vapaaehtoinen.
- **Asetusten perintä:** Asetusten perintä mahdollistaa hierarkkiset pääsynestokäytännöt. Pääkäytäntö määrittää perusasetukset sen alaisille, joka on erittäin käytännöllistä usean toimialueen toteutuksissa
- **Käytännön valinta:** Jokainen pääsynhallintakäytäntö tunnistaa käytössä olevat laitteet. Jokaisessa laitteessa voi olla käytössä vain yksi käytäntö
- **Säännöt**: Määrittävät sallitun liikenteen. Säännöt pääsynhallinnassa ovat numeroitu alkaen numerosta 1. Järjestelmä vertaa liikennettä pääsynhallintakäytäntöön aloittaen ylimmästä.
- **Oletuskäytäntö:** Määrittää kuinka järjestelmä hoitaa liikenteen, joka ei osu mihinkään muuhun pääsynhallinta listan sääntöön.
- **Security Intelligence:** On ensimmäinen osa puolustusta hyökkäyksiä vastaan. Tämä ominaisuus mahdollistaa yhteyksien estämisen IP-osoitteen, URL:n ja toimialueen perusteella.
- **HTTP-vastaus:** Määrittää millainen sivu estetylle verkkosivulle mentäessä käyttäjälle näytetään
- **Kehittyneet asetukset:** Tarvitsevat usein vähän tai eivät ollenkaan muokkausta. Yleensä perusasetukset ovat riittävät. Kehittyneistä asetuksista voidaan muokata liikenteen ennaltakäsittelyä, SSL-tarkastelua, identiteettiä ja muita suoritustehoasetuksia. (Cisco Systems, Inc. 2015, 674–675.)

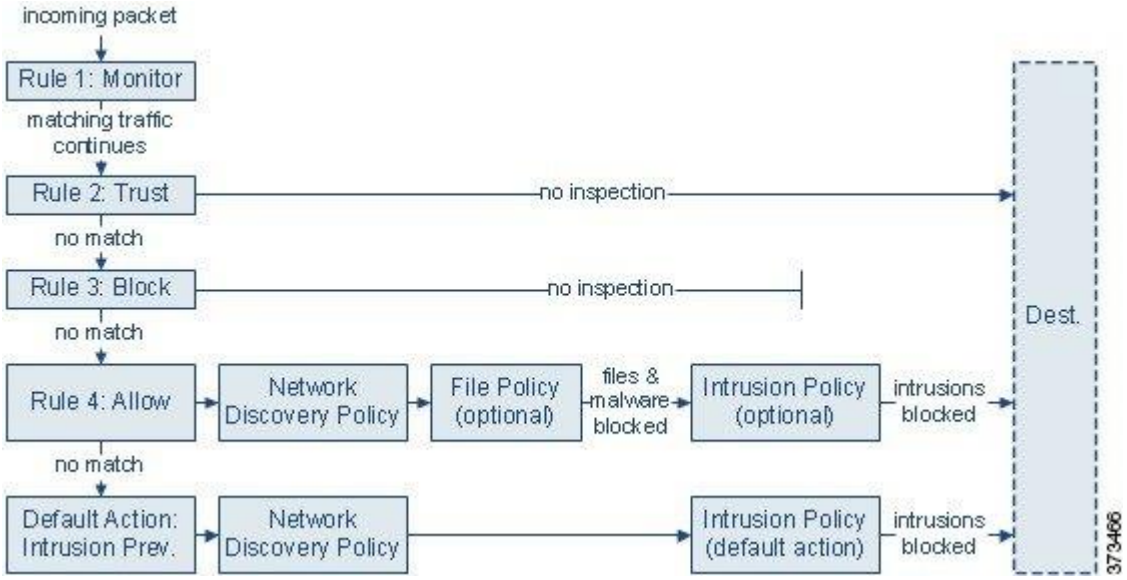
Yksinkertaisessa konfiguraatiossa oletustoiminto päättää, miten liikennettä käsitellään. Monimutkaisemmassa konfiguraatiossa oletustoiminto käsittelee liikenteen, jos se ei ole mustalla listalla tai estetty SSL-tarkastelussa, käytä

luotettua sovellusta tai ei vastaa mihinkään käytännön sääntöön. Kuvassa 7 nähdään pääsynhallinnan oletuskäytäntö. (Cisco Systems, Inc. 2015, 676.)



Kuva 7. Oletuskäytännön toiminta (Cisco Systems, Inc. 2015, 677)

Jokaisessa säännössä on toiminta, joka päättää monitoroidaanko, luotetaanko, estetäänkö vai sallitaanko liikenne. Liikenteen sallittaessa on mahdollista toteuttaa syvempää tarkastelua tunkeutumisen eston ja tiedostojen tarkastelun avulla mahdollisten haittaohjelmien ja hyökkäysten varalta. Kuvassa 8 nähdään pääsynhallinnan neljä eri vaihtoehtoa toiminnassa. (Cisco Systems, Inc. 2015, 709.)



Kuva 8. Pääsynhallinnan toiminta (Cisco Systems, Inc. 2015, 710)

Pääsynhallintasäännöissä on myös monia muita asetuksia. Sääntöjä on mahdollista ottaa pois käytöstä, sekä määrittää niiden sijainti ja kategoria. Tapahtumia voidaan lajitella alueen, verkon, portin, VLAN:n, sovelluksen, URL:n, käyttäjän, ryhmien tai ISE-attribuutin perusteella. Tapahtumien tallentaminen tapahtuu tietokantaan, syslogiin tai SNMP-palvelimeen. Sääntöihin voi myös tehdä omia kommentteja. (Cisco Systems, Inc. 2015, 712–713, 717–718.)

5.4 Salatun liikenteen hallinta

Oletuksena Firepower ei voi tutkia liikennettä, joka on salattu SSL tai TLS protokollilla. Osana pääsynhallintaa SSL-tarkastelu mahdollistaa salatun liikenteen estämisen tarkistamatta sitä, tai tarkastella salattua tai purettua liikennettä pääsynhallinnan kanssa. Kun järjestelmä käsittelee salattua tapahtumaa, se kirjaa tietoja liikenteestä. Salatun liikenteen tarkastelu yhdessä salatun liikenteen datan analysoinnin kanssa mahdollistaa suuremman tietämyksen ja kontrollin salatauista sovelluksista ja liikenteestä. (Cisco Systems, Inc. 2015, 801.)

Jos järjestelmä tunnistaa SSL- tai TLS-kättelyn TCP-yhteydessä, se määrittää pystyykö se purkamaan havaitun liikenteen. Jos se ei pysty, se suorittaa jonkun seuraavista toimista: estää salatun liikenteen, estää liikenteen ja nollaa TCP-yhteyden tai ei pura liikennettä. (Cisco Systems, Inc. 2015, 801.)

Jos järjestelmä pystyy purkamaan liikenteen, se estää liikenteen ilman muita tarkastuksia, arvioi purkamattoman liikenteen pääsynhallinnan kanssa tai purkaa liikenteen käyttämällä jotain seuraavista metodeista:

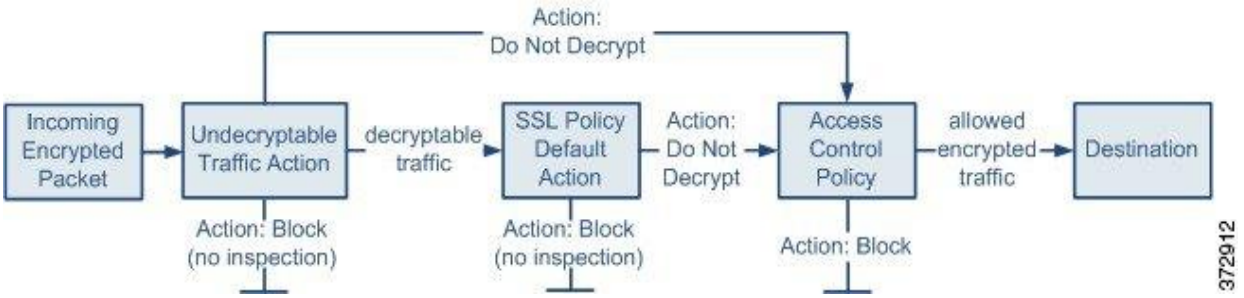
- **Decrypt with a known private key:** Kun ulkopuolinen laite aloittaa SSL-kättelyn omasta verkosta löytyvän palvelimen kanssa, järjestelmä vertaa vaihdettua sertifikaattia aikaisemmin lisättyyn palvelimen sertifikaattiin. Sen jälkeen se käyttää ladattua yksityistä avainta liikenteen purkamiseen.
- **Decrypt by re-signing the server certificate:** Kun laite omassa verkossa aloittaa SSL-kättelyn ulkoisen palvelimen kanssa, järjestelmä uudelleen allekirjoittaa sertifikaatin aikaisemmin lisätyllä sertifikaatilla, jonka jälkeen se purkaa liikenteen ladatulla yksityisellä avaimella. (Cisco Systems, Inc. 2015, 801–802.)

Purettu liikenne kulkee saman liikenteenhallinnan ja -analyysin läpi kuin salaamaton liikenne. Näihin tarkasteluihin kuuluu verkko-, maine- ja käyttäjäperusteinen pääsynhallinta, IPS, AMP ja havainnointi. Jos järjestelmä ei estä liikennettä, se uudelleen salataan ennen sen lähettämistä kohteeseen. (Cisco Systems, Inc. 2015, 802.)

SSL-käytäntö määrittää miten järjestelmä hallitsee salattua liikennettä verkossa. SSL-käytäntöjä voidaan konfiguroida yksi tai useampia. SSL-käytäntö määritetään pääsynhallintakäytäntöön, jonka jälkeen se lisätään hallittavaan laitteeseen. Kun laite havaitsee TCP-kättelyn, pääsynhallinta tutkii ensin liikenteen. Jos se havaitsee SSL-salatun liikenteen TCP-yhteydessä, SSL-

käytäntö jatkaa liikenteen käsittelyllä ja purkamisella. (Cisco Systems, Inc. 2015, 818–819.)

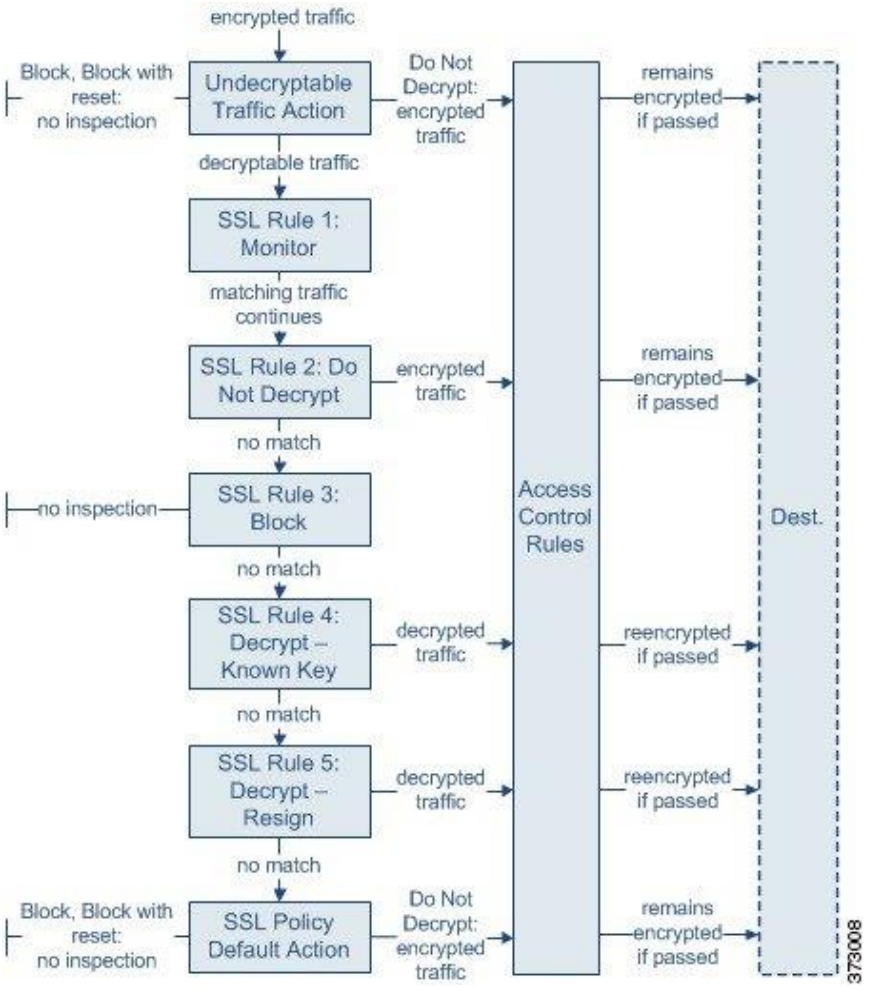
Yksinkertaisin SSL-käytäntö, joka näkyy kuvassa 9, kertoo laitteelle miten salattua liikennettä käsitellään yhdellä oletustapahtumalla. Oletusasetukseksi voidaan valita liikenteen estäminen tai tutkia salattua, purettavissa olevaa, liikennettä pääsynhallinalla. Tämän jälkeen järjestelmä voi joko estää tai sallia liikenteen. Jos järjestelmä havaitsee liikennettä, jota se ei pysty purkamaan, se joko estetään ilman tarkastelua, tai sitä ei pureta ja käytetään pääsynhallintaa tutkimiseen. (Cisco Systems, Inc. 2015, 819.)



Kuva 9. SSL-käytäntö (Cisco Systems, Inc. 2015, 819)

Järjestelmä yhdistää liikenteen SSL-sääntöihin määrätyllä tavalla. Useimmissa tapauksissa järjestelmä käsittelee liikennettä ensimmäisen SSL-säännön mukaan, jossa ehdot täyttyvät. Ehdot voivat olla yksinkertaisia tai monimutkaisia. Liikennettä voidaan hallita alueen, verkon, maantieteellisen sijainnin, VLAN:n, portin, sovelluksen, URL:n, käyttäjän, sertifikaatin, salauspaketin (cipher suite) tai salausprotokollan mukaan. (Cisco Systems, Inc. 2015, 827.)

Jokainen sääntö myös määrittää mitä liikenteelle tehdään. Sääntö määrittää monitoroidaanko, estetäänkö vai tutkitaanko salattu tai purettu paketti pääsynhallinnan kanssa. Järjestelmä ei tutki paketteja, jotka se on estänyt. Järjestelmä tutkii kuitenkin salatut paketit pääsynhallinnassa. Pääsynhallinta ei kuitenkaan voi suorittaa kaikkia toimenpiteitä salattuihin paketteihin, joten salattu liikenne vastaa vain muutamiin sääntöihin. Oletuksena IPS ei tarkasta salattuja paketteja. Kuvassa 10 nähdään miten SSL-säännöt käsittelevät liikennettä. (Cisco Systems, Inc. 2015, 827.)



Kuva 10. SSL-säännöt (Cisco Systems, Inc. 2015, 828)

5.5 Haittaohjelmasuojaus ja tiedostonhallinta

Haitalliset ohjelmat voivat päästä yrityksen verkkoon monia eri reittejä. Auttaakseen tunnistamaan ja estämään haittaohjelmien vaikutukset, Firepowerin kehittynyt haittaohjelmilta suojautuminen (Advanced Malware Protection) -ominaisuus tunnistaa, seuraa, analysoi ja estää haittaohjelmien liikennöinnin verkossa. (Cisco Systems, Inc. 2015, 879.)

AMP ja tiedostonhallinta voidaan konfiguroida osaksi pääsynhallintaa. Tiedostonhallinta mahdollistaa tiedostojen kontrolloinnin tyypin mukaan riippumatta siitä sisältävätkö ne haittaohjelmia. Luodut tiedostokäytännöt voidaan yhdistää pääsynhallintaan. Tunnistetut tiedostot voidaan ladata paikallista haittaohjelmien tunnistusta varten. Tiedostot voidaan myös lähettää AMP-pilveen, joka määrittää dynaamisella analyysillä onko tiedosto haitallinen. (Cisco Systems, Inc. 2015, 879.)

Tiedosto- ja haittaohjelmatapahtumista sekä tallennetuista tiedostoista luodaan automaattisesti lokimerkintä. Kun jokin näistä merkinnöistä tapahtuu, jär-

jestelmä merkkaa kyseisen tapahtuman lopetuksen lokiin. (Cisco Systems, Inc. 2015, 879.)

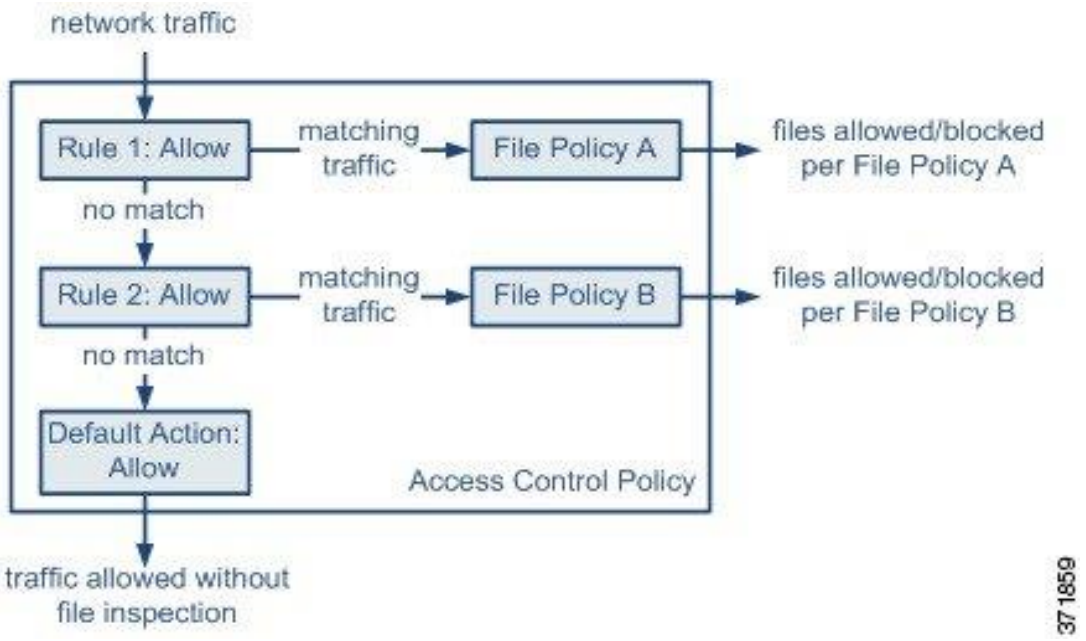
Järjestelmä käyttää monia metodeja tiedostojen analyysiin, määrittääkseen sisältävätkö ne haitallisia ohjelmia. Riippuen siitä mitkä vaihtoehdot ovat valittu, tarkistukset suoritetaan seuraavassa järjestyksessä:

- **Spero Analysis:** Jos kyseessä on exe-tiedosto, järjestelmä analysoi tiedoston ja lähettää sen AMP-pilveen. Pilvi käyttää tunnisteita määrittääkseen onko tiedosto haitallinen.
- **Local Malware Analysis:** Käyttää paikallista haittaohjelman tunnistusta. Laite tutkii yhteensopivan tiedoston estäen sen, jos se sisältää haittaohjelmia ja sääntö on niin konfiguroitu.
- **Dynamic Analysis:** Järjestelmän määrittäessä tiedoston mahdolliseksi haittaohjelmaksi, se lähetetään AMP-pilveen analyysia varten. AMP-pilvi suorittaa tiedoston hiekkalaatikkoympäristössä ja määrittää onko tiedosto mahdollisesti haitallinen. Se palauttaa vastauksena uhka-arvion, joka näyttää todennäköisyyden sille onko tiedosto haitallinen. (Cisco Systems, Inc. 2015, 880–881.)

Perustuen tiedostoanalyysin tuloksiin, tallennettuja tiedostoja ja tapahtumia voidaan tarkastella jälkikäteen. Tiedostojen kulkua voidaan myös seurata *Network file trajectory* -ominaisuudella, joka näyttää millä laitteilla tiedostoa on havaittu. Se näyttää myös monia muita tiedoston ominaisuuksia. (Cisco Systems, Inc. 2015, 881.)

Järjestelmä kykenee tunnistamaan pakattuja tiedostoja, kuten zip tai rar. Jos yksikin tiedosto pakkauksessa tunnistetaan haitalliseksi, koko paketti estetään. Järjestelmä voidaan myös määrittää estämään tiedostot, jotka ylittävät määritetyn pakkaustason tai joiden sisältöä se ei kykene tarkistamaan. (Cisco Systems, Inc. 2015, 881.)

Tiedostokäytäntö suorittaa AMP:n ja tiedostonhallinnan osana pääsynhallintaa. Tämä yhtenäisyys varmistaa, että ennen kuin tiedosto pääsee eteenpäin pääsynhallinnasta, sille suoritetaan tiedoston tarkistus. Kuvassa 11 nähdään tiedostokäytännön toiminta. (Cisco Systems, Inc. 2015, 885.)



Kuva 11. Yksinkertainen tiedostokäytäntö (Cisco Systems, Inc. 2015, 886)

Kuten pääsynhallinnassa myös tiedostokäytännöissä on sääntöjä, jotka määrittävät miten tiedostoja käsitellään. Sääntöjä voidaan luoda useita ja ne reagoivat eri tavalla eri tiedostomuotoihin, protokolliin ja tiedostojensiirron suuntiin. Kun tiedosto vastaa jotain sääntöä, se voidaan estää, sallia, tallentaa tai lähettää analysoitavaksi. Tiedostokäytäntö voi määrittää tiedostot automaattisesti puhtaaksi tai haittaohjelmiksi oman tunnistuslistan avulla. Tiedosto voidaan myös määrittää haitallisiksi uhka-arvion ollessa liian korkea. (Cisco Systems, Inc. 2015, 890–891.)

5.6 Tunkeutumisen estojärjestelmät

Verkkoanalyysi ja tunkeutumisen estokäytännöt toimivat osana Firepowerin tunkeutumisen havaitsemista ja estoa. Tunkeutumisen havaitsemisella tarkoitetaan passiivista verkon tarkkailua ja tunkeutumisen esto puolestaan pystyy myös estämään mahdolliset hyökkäykset. (Cisco Systems, Inc. 2015, 911.)

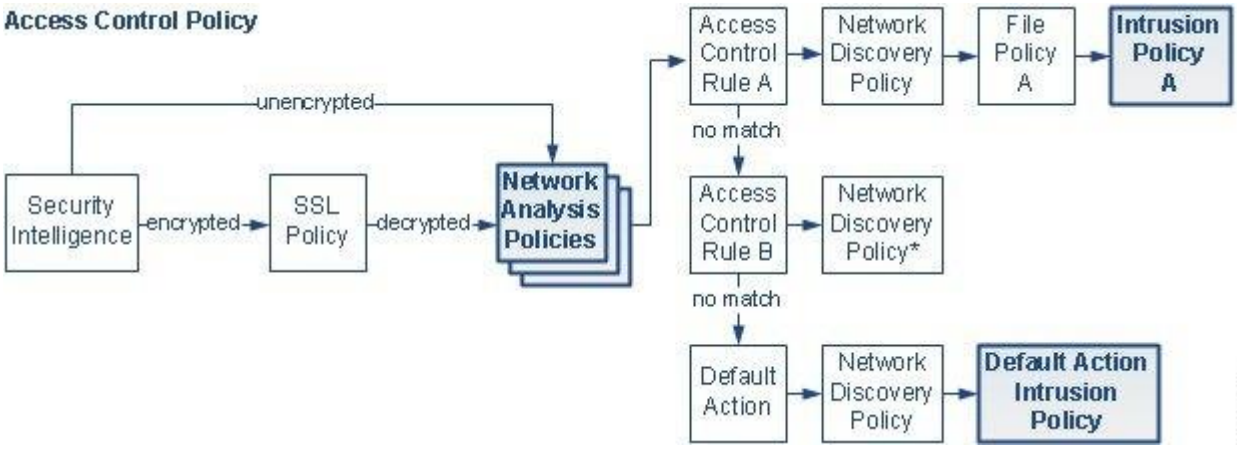
Tunkeutumisen esto toteutuksessa, kun järjestelmä tutkii paketteja: verkkoanalyysikäytäntö kattaa sen kuinka liikenne tulkitaan ja alkukäsitellään, jotta sitä voidaan tarkemmin tutkia. Tunkeutumisen estokäytäntö käyttää tunkeutumisen estosääntöjä tutkiakseen kaavoihin perustuvien hyökkäysten paketteja. Tunkeutumiskäytännön parina on muuttujia, jotka mahdollistavat nimellistenarvojen käytön tarkan tunnistuksen saavuttamiseksi. (Cisco Systems, Inc. 2015, 911.)

Verkkoanalyysi ja tunkeutumisen estokäytännöt toimivat molemmat käytönhallintasäännön alaisena, mutta eri aikoihin. Ensin suoritetaan verkkoanalyysi, jonka jälkeen tunkeutumisen estokäytännöt. Yhdessä verkkoanalyysi ja tunkeutumisen esto tarjoavat laajan ja tarkan pakettien tarkastelun. Ne auttavat tunnistamaan, hälyttämään ja suojaamaan verkkoliikennettä vastaan, joka uhkaa saatavuutta, eheyttä ja luotettavuutta järjestelmissä ja niiden datassa. (Cisco Systems, Inc. 2015, 911.)

Firepowerin mukana tulee useita valmiita tunkeutumisen estokäytäntöjä. Käyttämällä järjestelmän tarjoamia käytäntöjä voidaan käyttää hyödyksi Cisco Talos Security Intelligence and Research Group (Talos) kokemusta. (Cisco Systems, Inc. 2015, 912.)

Tunkeutumisen estokäytäntöjä voidaan myös luoda itse. Näiden käytäntöjen asetuksia voidaan muokata juuri omalle yritykselle sopivaksi. Tämä lisää hallittavien laitteiden suorituskykyä ja mahdollisuutta vastata käytäntöjen muodostamiin tapahtumiin tehokkaasti. (Cisco Systems, Inc. 2015, 912.)

Kun järjestelmä analysoi liikennettä osana pääsynhallintaa, verkkoanalyysi tapahtuu erikseen ennen tunkeutumisen estokäytäntöä. Kuvassa 12 on esitetty yksinkertaisessa muodossa missä vaiheessa eri käytännöt toimivat. (Cisco Systems, Inc. 2015, 912.)



Kuva 12. Tunkeutumisen estokäytännön toiminta (Cisco Systems, Inc. 2015, 912)

Järjestelmässä on mahdollista luoda myös omia tunkeutumisen estosääntöjä. Säännöt on jaettu kahteen ryhmään, objekti- ja tekstisäännöt. Objektisäännöt ovat Talos ryhmän sääntöjä, jotka voivat tunnistaa uhkia joita tavalliset tekstisäännöt eivät tunnista. Objektisääntöjä ei pysty itse luomaan. Kaikki itse luodut säännöt ovat tekstisääntöjä. (Cisco Systems, Inc. 2015, 1005.)

Säännöt ovat kokoelma avainsanoja ja väitteitä, joita järjestelmä käyttää havaitakseen haavoittuvuuksien hyötykäytön järjestelmässä. Järjestelmän analysoidessa liikennettä se vertaa paketteja sääntöihin, ja jos paketti täsmää niihin, sääntö aktivoituu. Sääntöjen aktivoituessa on kolme mahdollista tapaa reagoida: hälytys, liikenteen salliminen tai estäminen. (Cisco Systems, Inc. 2015, 1005.)

5.7 Verkon havainnointi ja identiteetti

Firepower käyttää verkon havainnointi- ja identiteettikäytäntöjä kerätäkseen verkosta laite-, sovellus- ja käyttäjädataa. Tietyntyyppistä havainnointi- ja identiteettidataa voidaan käyttää verkon kartoittamiseen, hyökkäysten analysointiin, verkkokäytöksen profilointiin, pääsynhallintaan ja vastaamaan haavoittuvuuksiin verkossa. (Cisco Systems, Inc. 2015, 1271.)

Laitedatan keräämiseksi Firepower monitoroi verkon läpi kulkevaa liikennettä. Se vertaa paketin otsikkokentän arvoa ja muita liikenteen ominaisuuksia määritettyihin arvoihin, selvittääkseen tietoa laitteista. Näihin tietoihin sisältyvät laitteiden määrä sekä tyyppi, perustopologia data, käyttöjärjestelmä ja sovellukset sekä niiden käyttäjät. Jos järjestelmä ei kykene automaattisesti määrittämään laitteen käyttöjärjestelmää, voidaan luoda uusi tunnistusmääritelmä. (Cisco Systems, Inc. 2015, 1285.)

Sovellusdataa järjestelmä yrittää tunnistaa analysoimalla IP-liikennettä yleisesti tunnettujen ohjelmien varalta. Järjestelmä kykenee tunnistamaan kolmen tyyppisiä sovelluksia: sovellus protokollat, kuten HTTP tai SSH, asiakasohjelmat, kuten selain tai sähköpostisovellus, ja web-sovellukset, kuten MPEG-video tai Facebook. Tunnistuksessa voidaan käyttää järjestelmän omia tunnistussääntöjä tai luoda omat tunnistussäännöt. (Cisco Systems, Inc. 2015, 1325–1326.)

Identiteetin tunnistamiseksi Firepower hyödyntää neljää erilaista identiteettilähdettä: liikenneperusteinen tunnistus, user agent, ISE ja captive portal. Data näistä identiteettilähteistä tallennetaan management centerin tietokantaan. Järjestelmä voidaan konfiguroida lataamaan käyttäjätietokanta automaattisesti. (Cisco Systems, Inc. 2015, 1345.)

5.8 Korrelaatiot

Korrelaatioiden avulla käyttäjän on mahdollista luoda käytäntöjä, joiden perusteella järjestelmä toimii erikseen määritellyissä tilanteissa. Havaitessaan määrittelyjä vastaavan tilanteen järjestelmä aktivoi korrelaation, ja toimii jälleen määritysten mukaisesti. Korrelaatiot koostuvat valkoisesta listasta, säännöistä ja vastauksista.

Valkoisessa listassa on kaksi osaa, kohteet ja laiteprofiilit. Kohteet rajaavat verkon laitteet, joko osan tai kaikki niistä, jotka valitaan arvioitaviksi. Laiteprofiilit määrittelevät mitä käyttöjärjestelmiä, sovelluksia ja protokollia valitut kohteet voivat käyttää. (Cisco Systems, Inc. 2015, 1407.)

Korrelaatiosääntöihin voidaan luoda monia erilaisia sääntöjä. Järjestelmän korrelaatio voidaan esimerkiksi määrittää aktivoitumaan, jos tietystä osoitteesta alkanut verkkoliikenteen määrä ylittää kymmenen megatavua tai verkossa havaitaan uusi laite.

Vastaukset määrittelevät kuinka järjestelmä toimii tietyn korrelaation aktivoituessa. Se voi vaihtoehtoisesti luoda merkinnän tapahtumalokiin, ilmoittaa ylläpitäjälle vaikkapa sähköpostitse ja estää vastedes kohdeosoitteesta saapuvan liikenteen.

Korrelaatioihin kuuluu myös *traffic profiling*, joka voidaan määrittää keräämään tietoa verkon liikenteestä tietyllä aikavälillä ja eri ehdoilla. Tietoa voidaan esimerkiksi kerätä tietyn kohdeosoitteen perusteella. Mikäli mitään tarkempia määrityksiä ei anneta, tutkii se koko verkkoa ja kaikkea liikennettä. Tästä liikenteestä järjestelmä piirtää erilaisia kuvioita käyttäjän määrittelemien asetusten mukaisesti.

5.9 Raportointi

Firepower tarjoaa joustavan raportointijärjestelmän, joka mahdollistaa nopeasti ja helposti moniosaisten raporttien luomisen järjestelmän tapahtumista. Järjestelmässä on myös mahdollista luoda omia kustomoituja raporttipohjia. (Cisco Systems, Inc. 2015, 1489.)

Raportti on dokumentti pdf-, html- tai csv-muodossa halutulla sisällöllä. Raporttipohja määrittää millaista dataa etsitään ja minkälainen raportti on. Järjestelmään kuuluu tehokas automatisoitu raporttisuunnittelija joka tekee raportti

pohjat. Raportteihin voidaan kopioida kaikki taulukot ja tapahtuma listat jotka näkyvät web-liittymässä. (Cisco Systems, Inc. 2015, 1489.)

Raporttipohjia voidaan luoda niin monta kuin niitä tarvitaan. Jokainen raporttipohja määrittää tarvittavat osat, etsintä parametrit joista dataa haetaan, esitys muodon ja ajanjakson. Pohja määrittää myös millainen kansilehti ja sisällysluettelo raportille luodaan. Raporttipohjat on mahdollista myös siirtää toiseen management centeriin. (Cisco Systems, Inc. 2015, 1489.)

Raportteihin voidaan myös määrittää syötettävät parametrit, jotka lisäävät sen käytettävyyttä. Parametrit mahdollistavat räätälöityjen raporttien luonnin samasta pohjasta. Kun luodaan raporttia joka sisältää parametreja, ohjelma pyytää syöttämään vaaditut tiedot. Esimerkkinä järjestelmä voi pyytää vaikka kohteen IP-osoitetta tai verkkoa. Näin ollen saadaan tietoa vain halutusta käyttäjästä tai verkosta. (Cisco Systems, Inc. 2015, 1489.)

5.10 Hälytykset

Vaikka Firepower tarjoaa monia näkymiä tapahtumista web-liittymässä, saattaa ulkoisten hälytysten konfiguroiminen kriittisten järjestelmien kohdalla olla tarpeellista. Firepower voidaan konfiguroida luomaan hälytyksiä, jotka ilmoittavat tapahtumista syslogiin, sähköpostiin tai SNMP-trap viesteillä. Hälytys voidaan luoda seuraavista tapahtumista: tietyn tasoiset tunkeutumistapahtumat, tietyn tyyppiset havaitsemistapahtumat, haittaohjelmatapahtumat, korrelaatiotapahtuma, yhteystapahtuma tai moduulin tilan muuttuminen. (Cisco Systems, Inc. 2015, 1519.)

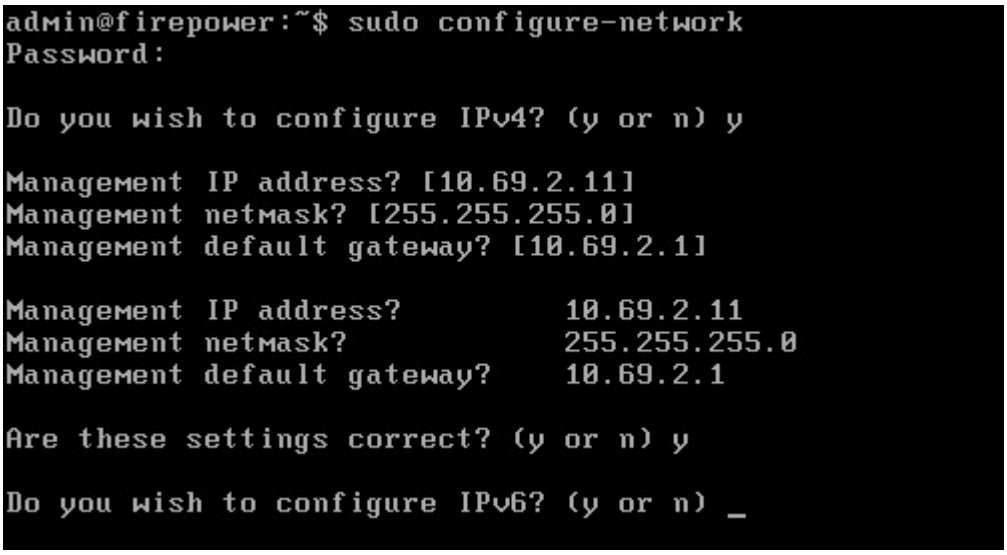
6 KÄYTÄNNÖN TOTEUTUS JA TESTIT

Kaikki käytännön testit suoritettiin ICTLAB-ympäristössä käyttäen hyödyksi jo valmiiksi asennettuja verkon järjestelmiä, kuten Microsoft AD ja VMware ESXi palvelin. Alustavat testit tehtiin erillisessä laboratorioverkossa ennen tuotantoverkkoon siirtymistä.

6.1 Firepower Management Centerin asennus

Firepower Management Center asennettiin cyberlabin ESXi-palvelimelle. Asennus tehtiin VMware vSphere clientillä valitsemalla *Cisco_Firepower_Management_Center_Virtual_VMware-ESXi-6.0.0-1005* OVF template -tiedosto. Kun järjestelmä käynnistyi, kirjauduttiin komentorivillä si-

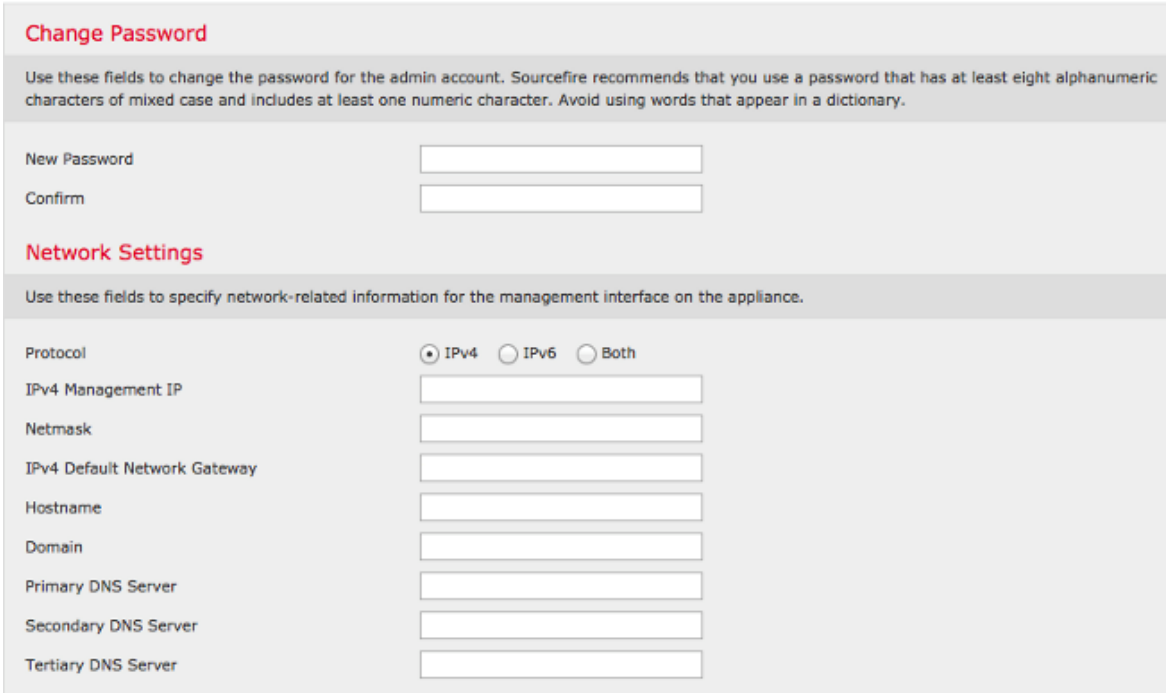
sään käyttäjällä admin:Admin123. Tämän jälkeen määriteltiin verkon perusasetukset komennolla ***sudo configure-network*** kuvan 13 esimerkin mukaisesti.



Kuva 13. Management center verkkoasetukset

Kun verkkoasetukset oli määritelty, ei komentoriviä tarvinnut enää muiden asetusten määrittämiseen. Tästä eteenpäin hallinta tehtiin selaimella laitteelle määritetyssä osoitteessa. Hallintayhteys salli vain salatun liikenteen (HTTPS).

Ensimmäisellä kirjautumisella oli vaihdettava salasana ja hyväksyttävä käyttöehtosopimus. Myös muiden perusasetusten, kuten laitenimen sekä DNS- ja NTP-palvelimen, muuttaminen oli mahdollista kuvassa 14 näkyvästä valikosta. Kaikkia näitä asetuksia voitiin kuitenkin muokata käyttöliittymässä myöhemmin *System>Configuration* valikosta. Myös kaikki vaaditut lisenssit syötettiin tässä vaiheessa tai ne olisi voitu syöttää myöhemmin *System>Licenses* valikosta.



Kuva 14. Perusasetukset ensimmäisen kirjautumisen yhteydessä

6.2 Firepower-moduulin asennus

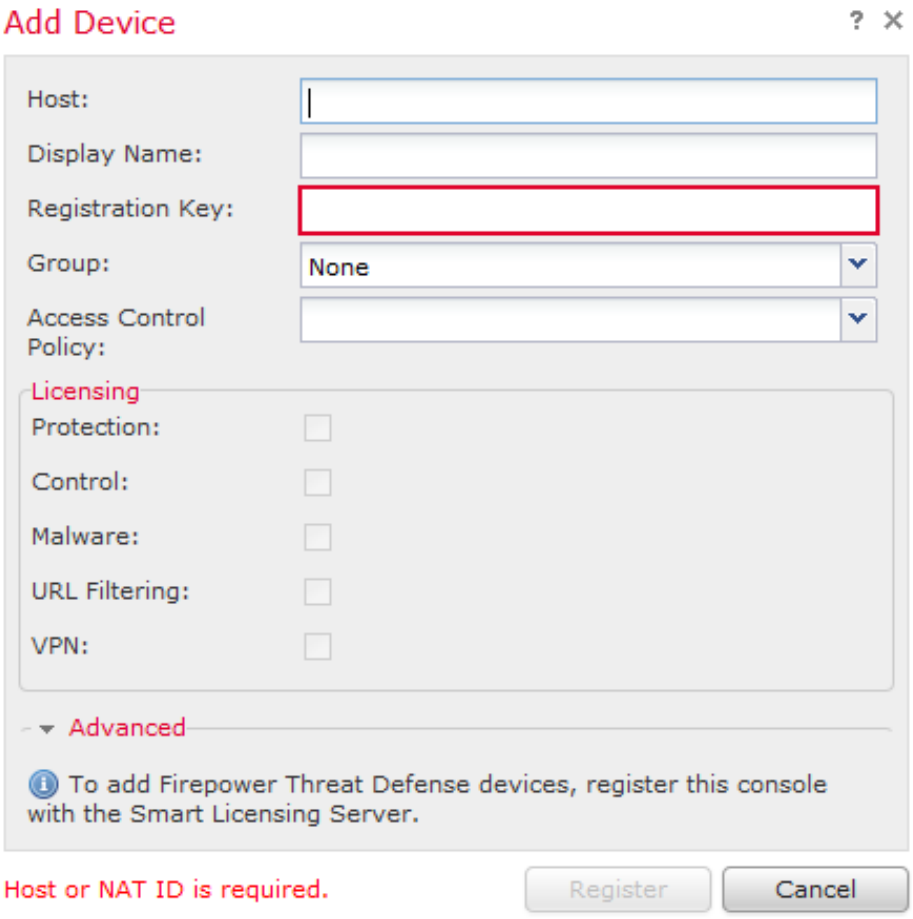
Firepowerin asennukseen vaadittiin käynnistystiedosto ja järjestelmätiedosto, jotka olivat ladattavissa Ciscon latauskeskuksesta. Käynnistystiedosto siirrettiin ASA:n sisäiselle levylle ja järjestelmätiedosto oli siirrettävä HTTP- tai FTP-palvelimelle myöhempää käyttöä varten. Ennen Firepower-ominaisuuden asentamista ASA:aan, oli käytössä ollut IOS-versio päivitettävä, sillä kyseinen versio ei ollut yhteensopiva uuden Firepower version (6.0) kanssa.

Kun ASA oli päivitetty vaadittuun versioon, aloitettiin Firepower-moduulin asentaminen kahdella komennolla: ***sw-module module sfr recover configure imagedisk0:asasfr-5500x-boot-6.0.0-1005.img*** ja ***sw-module module sfr recover boot***. Tämän jälkeen oli odotettava noin kymmenen minuuttia moduulin käynnistymistä. Moduulin tila oli nähtävissä komennolla ***show module sfr.*** Kun moduuli oli käynnistynyt, siirryttiin konfiguroimaan moduulin sisäiseen istuntoon komennolla ***session sfr console***. Tässä vaiheessa järjestelmä pyysi käyttäjätunnusta ja salasanaa, jotka ovat oletuksena admin:Admin123.

Firepower-moduulissa syötettiin komento ***setup*** ja määritettiin verkkoasetukset. Näiden määritysten jälkeen syötettiin komento ***system install http://10.69.2.10/asa/asasfr-sys-6.0.0-1005.pkg*** ja vahvistettiin se syöttämällä ***y***. Jälleen oli odotettava noin kymmenen minuuttia asennuksen valmistumista.

Asennuksen valmistuttua siirryttiin jälleen moduulin päätteeseen komennolla ***session sfr*** ja kirjauduttiin sisään. Moduuli vaati oletussalasanan vaihtoa ennen muita määrityksiä. Vaihtamisen jälkeen määritettiin halutut verkkoasetukset järjestelmän niitä pyytäessä. Viimeisenä moduulissa annettiin komento ***configure manager add 10.69.2.11 avain***, joka vaadittiin Firepowerin liittämiseksi management centeriin. Tämän jälkeen moduulissa ei tarvinnut tehdä muuta.

Seuraavana siirryttiin management centerin puolelle, jossa ASA:n yhdistämisen viimeinen vaihe suoritettiin. Tämä tapahtui *Device>Device Management>Add Device* valikon alla kuvassa 15 näkyvässä ikkunassa. Ikkunassa syötettiin Firepowerin osoite, haluttu nimi ja annettiin viimeisessä komennossa käytetty rekisteröintiavain. Laitteeseen liitetty pääsynhallintakäytäntö oli valittava tai luotava ennen laitteen rekisteröimistä. Myös laitteen käyttämät lisenssit oli mahdollista antaa tässä vaiheessa tai ne voitiin antaa myöhemmin *Device>Device Management* valikosta.



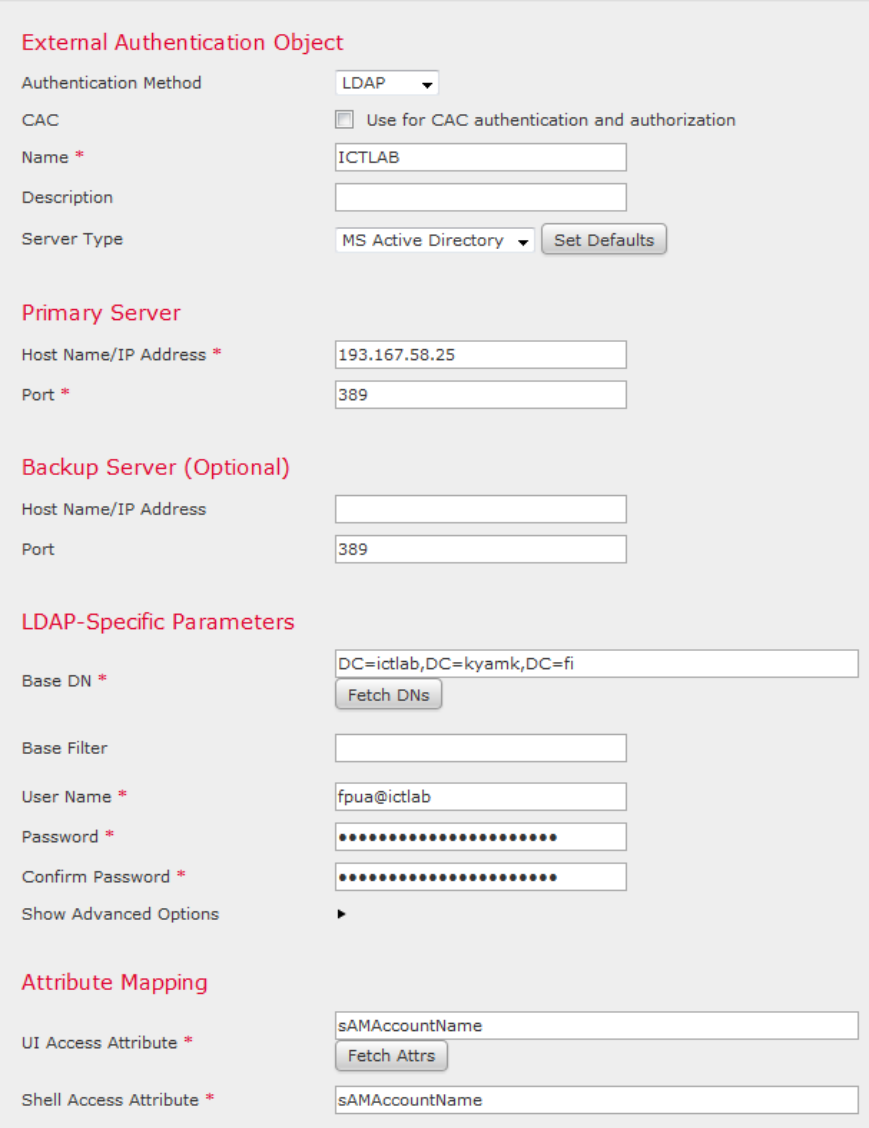
Kuva 15. Laitteen lisäys management centeriin

Laitteen lisäyksen jälkeen oli viimeisenä vaiheena määritettävä verkkoliikenne kiertämään ASA:ssa Firepower-moduulin kautta. Tämä tehtiin ASDM:llä luomalla uusi *Service Policy Rule* ja tähän sääntöön valittiin kohta *Enable ASA FirePOWER for this traffic flow* aktiiviseksi.

6.3 Järjestelmänhallinta

6.3.1 Käyttäjät

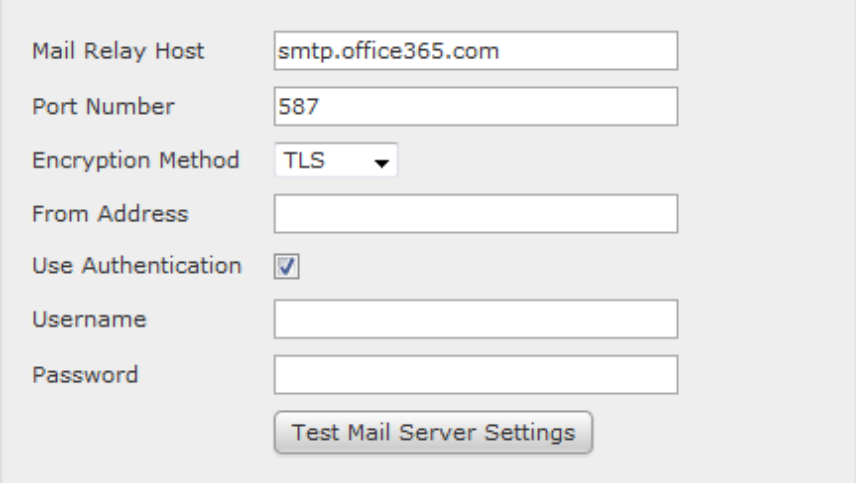
Ensimmäisenä luotiin toinen paikallinen järjestelmänvalvoja-tunnus *System>Users* valikossa, sillä käyttäjiä oli kaksi. Samanaikaisessa konfiguroinnissa on kuitenkin aina vaaransa, joten pääasiassa hallintaan käytettiin vain yhtä tunnusta. Myös ulkoinen autentikointi otettiin käyttöön LDAP-menetelmällä kuvan 16 mukaisesti.



Kuva 16. LDAP-autentikointi

6.3.2 Sähköpostiasetukset

Management center käyttää sähköpostiviesteissä SMTP-välityspalvelinta. Tämä määritettiin *System>Configuration>Email Notification* valikosta. Näissä asetuksissa käytettiin koulun Office 365 -sähköpostipalvelua. Kuvassa 17 on nähtävissä Office 365:den vaatimat asetukset.



Kuva 17. SMTP Office 365

6.3.3 Verkon havainnointi

Verkon havainnointi määritettiin siten, että havainnoin kohteina oli ainoastaan ICTLAB:n sisäverkon. Oletuksena havainnointi tutki koko IPv4-liikennettä, mikä lisäsi verkkolaitelistaan myös internetistä löytyviä laitteita. Tämä teki listasta vaikeasti luettavan, kun haluttiin tutkia juuri oman verkon laitteita. Määritykset tehtiin *Policies>Network Discovery>Add Rule* valikosta ja havainnoin tuloksia pystyi seuraamaan *Analysis>Hosts* valikon alta.

6.3.4 Hälytykset

Hälytysmääritykset löytyivät *Policies>Acions>Alerts* valikosta ja tänne määritettiin järjestelmä ilmoittamaan syslogiin ja sähköpostiin, kun se havaitsi haittaohjelman tai vakavuusasteen yksi tunkeutumistapahtuman. Myös korrelaatioiden vastauksiin liittyvät hälytykset luotiin tässä valikossa.

6.3.5 Päivitykset ja varmuuskopiointi

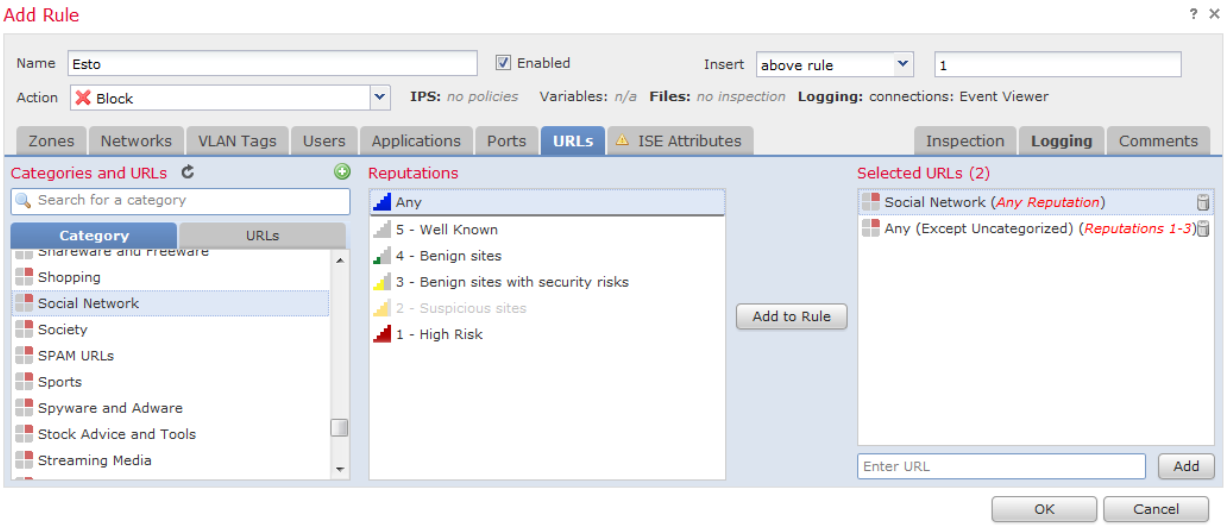
Järjestelmän päivitykset tarkastettiin *System>Updates* valikosta ja niitä asennettiin päivityskohtaisesti. Sääntöpäivitykset ja *geolocation* päivitykset asetettiin päivittymään automaattisesti.

Varmuuskopioita tehtiin *System>Tools>Backup/Restore* valikossa. Varmuuskopioitaviksi valittiin koko management centerin tietokanta. Vaihtoehtona olisi ollut laittaa järjestelmä varmuuskopioimaan itsensä automaattisesti tietyin välein *System>Tools>Scheduling* valikosta.

6.4 Pääsynhallinta

Pääsynhallintakäytäntö on verkonhallintaa ajatellen avainasemassa. Kaikki muut käytännöt korrelaatioita lukuun ottamatta sisällytetään myöhemmin siihen. Pääsynhallinnan alle luotavat säännöt luetaan pääsylistojen tapaan ylhäältä alas. Sääntöihin lisättiin testimielessä erilaisia estoja ja ehtoja:

- estettiin tietyn verkon, osoitteen tai portin liikenne
- estettiin tietyn käyttäjän liikenne
- sallittiin vain tiettyjen sovellusten käyttö
- estettiin sosiaalinen media
- estettiin pääsy huonomaineisille sivustoille (kuva 18)



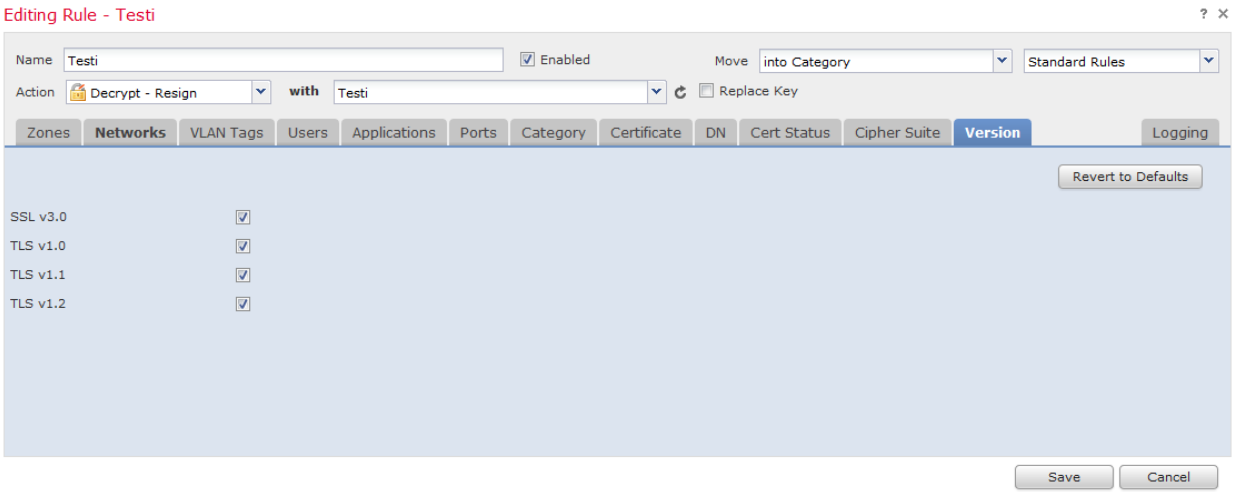
Kuva 18. Esimerkki pääsylistaan luotavasta säännöstä

Joihinkin näistä säännöistä aktivoitiin loki ominaisuus, joka kirjaa tapahtumat ylös tarkasteltaviksi. Näitä tapahtumia päästiin tarkastelemaan *Analysis>Connections>Event* valikon alta. Tapahtumia voidaan etsiä monin eri ehdoin, kuten protokolla tai kohde- ja lähdeosoite, tai rajata ajan mukaan.

6.5 SSL

Salauksen purkaminen tapahtui *Policies>Access Control>SSL* valikosta. Ensimmäisenä luotiin uusi SSL-käytäntö, jossa määritettiin perustoiminnoksi *do not decrypt*. Tätä pystyi kuitenkin muuttamaan helposti pudotusvalikosta. Ennen säännön luomista tehtiin *Objects>Object Management* valikon alle itse al-

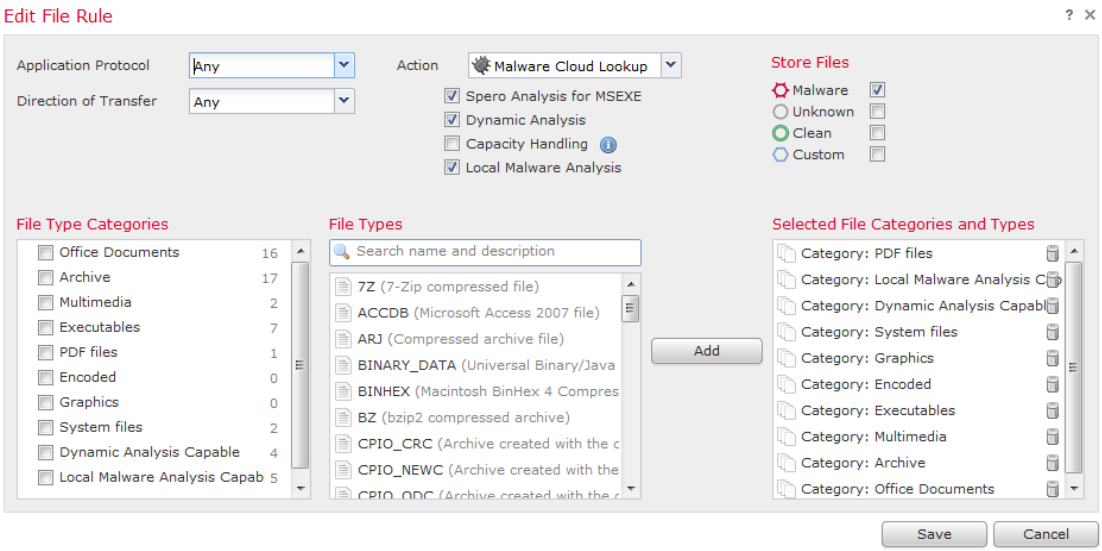
lekirjoitettu sertifikaatti. Tämän jälkeen luotiin SSL-sääntö kuvassa 19 näkyvästä valikosta. Säännölle annettiin nimi Testi, toiminnoksi valittiin *Decrypt-Resign* ja käytettäväksi valittiin aiemmin luotu sertifikaatti. Kun sääntö oli valmis, käytiin SSL-käytäntö liittämässä pääsynhallintaan. Tämä kuitenkin vaikutti verkon suorituskykyyn huomattavasti, joten ominaisuutta ei jätetty käyttöön.



Kuva 19. SSL-sääntö

6.6 AMP ja tiedostonhallinta

Tiedostojen hallintaa ja tarkastelua koskevat asetukset löytyivät *Policies>Access Control>Malware & File* valikosta. Ensimmäisenä luotiin tiedostokäytäntö, jonka alle määriteltiin mm. kuvassa 20 näkyvät säännöt. Valvottavaksi valittiin kaikki tiedosto- ja analysointityypit. Kaikkien näiden toimivuutta oli vaikea todentaa, sillä haittaohjelmien tahallinen lataaminen ei ollut houkutteleva vaihtoehto. Järjestelmä kuitenkin havaitsi Eicar-testiviruksen.

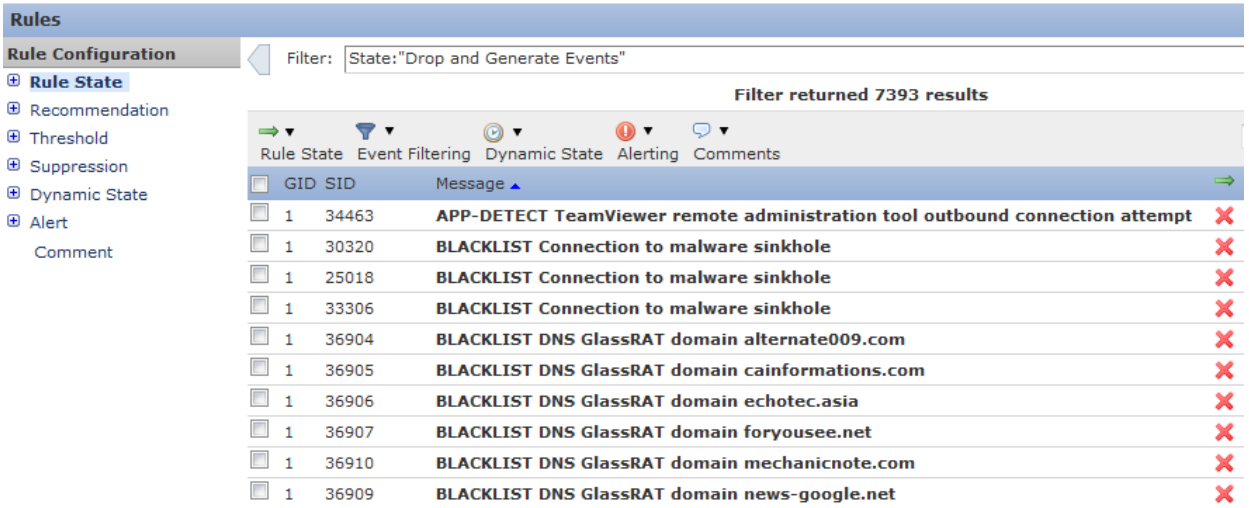


Kuva 20. Tiedostonhallinta

Tiedostonhallinta on tarkoitettu myös tiedostomuotojen estämiseen tai sallimiseen riippumatta siitä, sisältääkö tiedosto haittaohjelman. Esimerkiksi exe-tiedostomuotojen lataaminen voidaan estää. Kaikista tiedostohallinnan tapahtumista tehdään lokimerkintöjä, joita voi tutkia *Analysis>Files* valikosta.

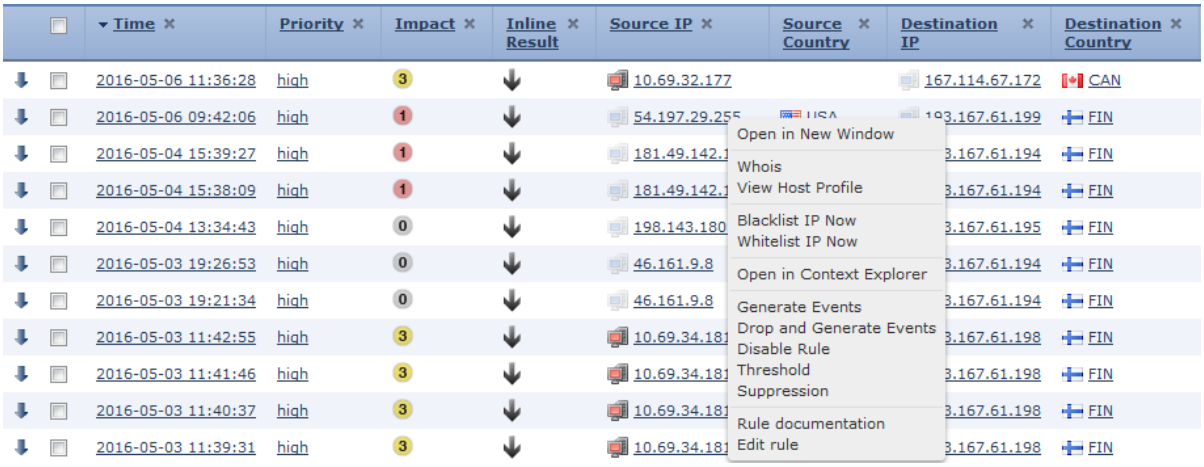
6.7 NGIPS

Tunkeutumisen estojärjestelmän hallinta tapahtui *Policies>Access Control>Intrusion* valikosta. Ensin luotiin käytäntö, johon valittiin pohjaksi *balanced security and connectivity* ja määritettiin käytäntö estämään hyökkäykset. Käytännön alta oli valittavissa mitkä säännöt olivat aktiivisena ja mikä niiden toiminto on. Kuvassa 21 on nähtävissä esimerkkejä estettävistä tapahtumista. Sääntöjä voidaan muokata *Objects>Intrusion Rules* valikosta. Myös uusien sääntöjen luominen on mahdollista.



Kuva 21. NGIPS-käytännön määritys

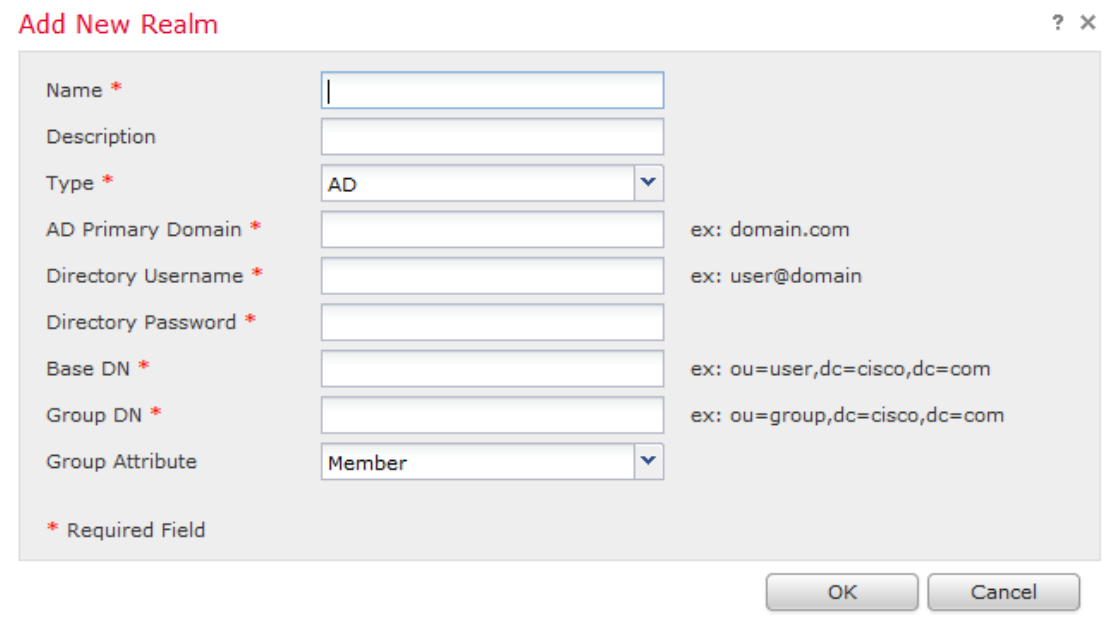
Tapahtumia voidaan seurata *Analysis>Intrusions>Events* valikon alta. Kuvassa 22 nähdään estettyjä hyökkäysyrityksiä. Näistä tapahtumista on saatavissa enemmän tietoa hiiren oikealla painikkeella ja valitsemalla *rule documentation*. Aukeavalta sivulta nähdään sääntö, joka aiheutti tapahtuman ja tapahtumakohtaisesti eri linkkejä mm. haavoittuneen sovelluksen tekijän sivuille, joilta voi löytyä mahdollisia korjausehdotuksia.



Kuva 22. Estetty liikenne

6.8 Käyttäjien tunnistus

Käyttäjien tunnistaminen aloitettiin luomalla *System>Integration>Realms* alle uusi alue. Tässä käytettiin ICTLAB:n valmiiksi konfiguroitua AD-palvelinta ja sen tiedot lisättiin kuvassa 23 näkyvään valikkoon. Kun alue oli luotu, ladattiin AD:n käyttäjäryhmät. Seuraavana lisättiin user agent, joka mahdollisti käyttäjien kirjautumisten seuraamisen, *System>Integration>Identity Sources* valikkoon.



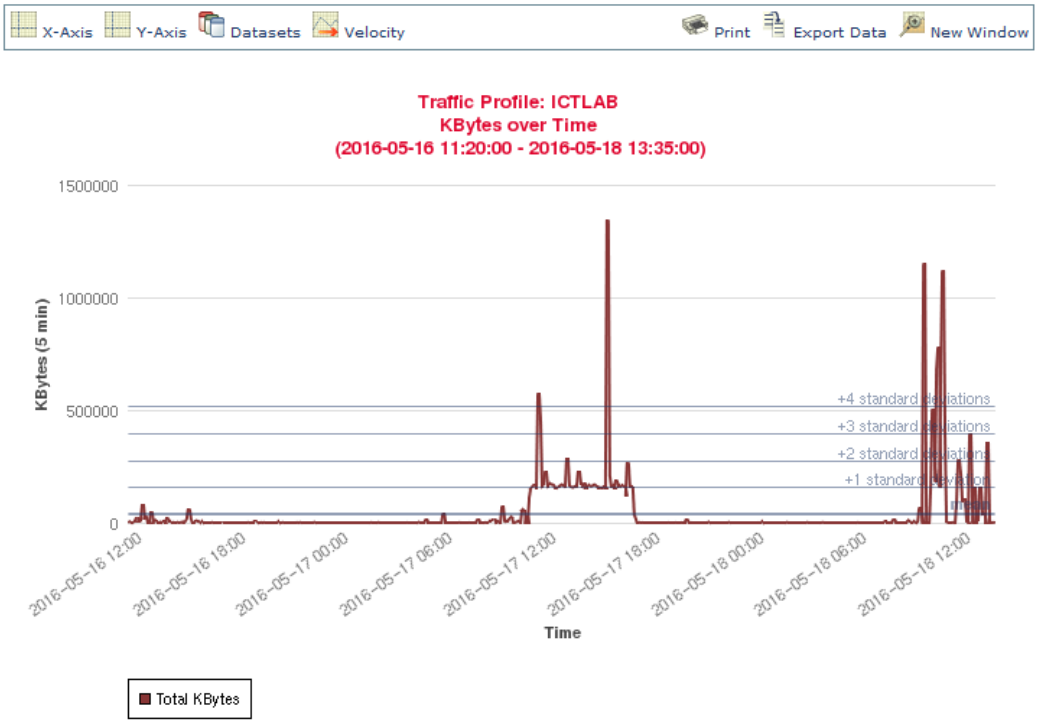
Kuva 23. Uuden alueen lisääminen

User agent -sovellus asennettiin väliaikaisesti kannettavalle tietokoneelle, josta se siirrettiin myöhemmin pysyvämpään sijaintiin. Sovellukseen määritettiin AD:n ja management centerin osoite. AD:n lisääminen vaati käyttäjän, jolla oli oikeus lukea AD:n kirjautumistietoja.

Seuraavana mentiin management centerin *Policies>Access Control>Identity* valikkoon, jossa luotiin uusi käytäntö. Käytäntöön lisättiin passiivinen autentikointi -sääntö, johon liitettiin aiemmin luotu alue. Viimeisenä vaiheena käytiin identiteettikäytäntö lisäämässä osaksi pääsynhallinnan käytäntöä.

6.9 Korrelaatio

Korrelaatioita päästiin luomaan *Policies>Correlation* valikosta. Korrelaatiota testattiin luomalla sääntö, joka tarkasteli yhden verkon liikennettä. Sääntö lisättiin osaksi korrelaatiokäytäntöä ja käytännön vastaukseksi määritettiin syslog-viesti. Korrelaatiotapahtumia voidaan tarkastella *Analysis>Correlation* valikosta. Korrelaatioihin luotiin myös *traffic profile* ja se määritettiin tarkkailemaan koko ICTLAB:n verkkoliikennettä. Tuloksena järjestelmä antoi kuvassa 24 näkyvän kuvaajan. Kuvaaja on nähtävissä samassa paikassa, jossa *traffic profile* luotiin.



Kuva 24. Verkon liikenne

6.10 Raportointi

Erilaisia raportteja verkon tapahtumista päästään luomaan *Overview>Reporting* valikosta. Mallipohjia ei haluttu sotkea, joten *malware*-raporttipohjasta kopiointiin käyttöön uusi raporttipohja. Raporttipohjaan rajattiin halutut aliverkot ja määritettiin luotu raportti lähetettäväksi sähköpostiin.

7 LOPPUPÄÄTELMÄT

Kokonaisuutta ajatellen työ onnistui hyvin ja tavoitteet saavutettiin. Firepowerin tärkeimmät ominaisuudet, kuten IPS ja AMP, saatiin pysyvään käyttöön ICTLAB-opetusympäristössä. Firepoweria pystytään myös tarjoamaan yrityksen asiakkaille palveluna, mutta kaikkia ominaisuuksia ei pystytä hyödyntämään. Jos asiakasyrityksellä on esimerkiksi käytössä NAT, ei Firepower pysty tunnistamaan verkossa olevia laitteita vaan ainoastaan asiakkaan käyttämän julkisen osoitteen. Firepoweria voidaan yhtälailla käyttää ASA:n ollessa single-/multiple- tai transparent-/routed -tilassa.

Raportointia ajatellen järjestelmästä löytyi hyödyllinen ominaisuus liittyen automatisointiin. Yritys pystyy määrittämään automaattisen raportoinnin eri asiakkaillensa, esimerkiksi kuukauden ensimmäisenä päivänä, käyttäen eri raporttipohjia. Nämä raporttipohjat luodaan asiakaskohtaisiksi ja niihin rajataan asiakkaan osoiteavaruus sekä asiakkaan haluama sähköpostiosoite. Näin järjestelmä lähettää automaattisesti raportin kuukausittain jokaiselle halutulle asiakkaalle.

Firepower Management Centeriä voidaan kaiken kaikkiaan pitää helppokäyttöisenä järjestelmänä. Online tuki -ominaisuus on erittäin hyödyllinen ja sen apuun pystytään turvautumaan ongelmatilanteissa. Järjestelmän suurin ongelma on sen hitaus, ainakin oletustehoja käytettäessä. Suorituskykyä pystyisi mahdollisesti parantamaan lisäämällä muistia ja virtuaalisia prosessoreja.

Järjestelmästä löytyy edelleen ominaisuuksia, joita työssä ei käytetty. Myös monien käytettyjen ominaisuuksien asetuksia, kuten IPS:n tiukkuutta, voidaan optimoida verkkoon sopivammaksi. Lisäksi salatun liikenteen purkaminen voidaan yrittää ottaa käyttöön, ilman että se romauttaa verkon toiminnan. Tämä mahdollistaa jatkokehittämisen, ainakin ICTLAB-ympäristössä.

LÄHTEET

Butler, J. M. 2013. Finding Hidden Threats by Decrypting SSL. Saatavissa: http://www.sans.org/reading-room/whitepapers/analyst/finding-hidden-threats-decrypting-ssl-34840 [viitattu 2.5.2016]

Cisco Systems, Inc. 2015. Firepower Management Center Configuration Guide, Version 6.0. Saatavissa: http://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60.pdf [viitattu 2.5.2016]

Cisco Systems, Inc. 2016a. Cisco ASA FirePOWER Module Quick Start Guide. Saatavissa: http://www.cisco.com/c/en/us/td/docs/security/asa/quick_start/sfr/firepower-qsg.html [viitattu 9.5.2016]

Cisco Systems, Inc. 2016b. Cisco Firepower Management Center Data Sheet. Saatavissa: http://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheet-c78-736775.html [viitattu 2.5.2016]

Miller C. L. 2014. Mobile Security for Dummies. Hoboken, NJ: John Wiley & Sons, Inc.

Osipov, V., Sweeney, M. & Weaver, W. 2002. Cisco Security Specialists Guide to PIX Firewall. 1. painos. Rockland, MA: Syngress.

Scarfone, K & Mell, P. 2007. Guide to Intrusion Detection and Prevention Systems (IDPS). Saatavissa: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf [viitattu 2.5.2016]

Wilkins, S. 2014. A Guide to Choosing a Next-Generation Firewall. Saatavissa: http://www.tomsitpro.com/articles/next-generation-firewall-vendors,2-847.html [viitattu 9.5.2016]