TIETOVERKON PÄÄSYNHALLINTA

Toteutus avoimilla ohjelmilla

Oskari Peura

Opinnäytetyö
Joulukuu 2013

Tietotekniikan koulutusohjelma
Tekniikan ja liikenteen ala

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖN
KUVAILULEHTI

Tekijä(t) PEURA, Oskari	Julkaisun laji Opinnäytetyö	Päivämäärä 11.12.2013
	Sivumäärä 51	Julkaisun kieli SUOMI
	Luottamuksellisuus ( ) saakka	Verkkojulkaisulupa myönnetty (X)
Työn nimi TIETOVERKON PÄÄSYNHALLINTA, Toteutus avoimilla ohjelmilla		
Koulutusohjelma Tietotekniikka		
Työn ohjaaja(t) RANTONEN Mika, HÄKKINEN Antti		
Toimeksiantaja(t) Jyväskylän ammattikorkeakoulu, teknologiayksikkö, ICT		

Tiivistelmä

Tämän opinnäytetyön päämääränä oli tutustua avoimilla ja vapailla ohjelmistoilla toteutettuun tietoverkon pääsynhallintaan (NAC, network access control) ja tutkia sen soveltuvuutta opetuskäyttöön.

Työn toimeksiantajana oli Jyväskylän ammattikorkeakoulun teknologiayksikkö, joka myös antoi valmiin ehdotuksen käytettäväksi ohjelmistoksi. Työssä tutkittava ohjelmisto oli PacketFencen versio 3.4.1 ja sen virtualisoitu ZEN-versio (zero effort nac).

Teoriaosuudessa tutustuttiin ohjelmiston dokumentaatioon ja rakenteeseen. Muiden avoimen lähdekoodin ohjelmistojen ja projekteiden tapaan perinteisiä kirjallisia lähteitä oli vaikea löytää tai ne olivat vanhentuneita. Verkosta taas löytyikin laajasti erilaisia käyttökelpoisia lähteitä, tosin niihin tuli suhtautua varsin kriittisesti. Joukosta valikoituikin vain itse PacketFencen omat dokumentaatiot ja isompien yritysten www-sivuilta löytyviä artikkeleita.

PacketFence osoittautui varsin monipuoliseksi ja helposti mukautettavaksi ohjelmistoksi. Sen käyttöönotto uudessa ympäristössä oli varsin mutkatonta, ja vanhaan ympäristöön sovittaminen osoittautui varsin helpoksi. Toiminta monien laitevalmistajien ja erityyppisten ja -merkkisten asiakaslaitteiden verkossa mahdollistuu käytännössä juuri avoimiin ja laitteistoriippumattomiin ohjelmiin.

PacketFence osoittautui monipuoliseksi ja helposti mukautettavaksi kohteeksi myös opetuskäyttöä ajatellen. Sen avulla monien eri tekniikoiden opettaminen tietoverkon pääsynhallintaan liittyen olisi mahdollista.

Avainsanat (asiasanat)
Tietoverkko, pääsynhallinta, NAC, PacketFence, avoin lähdekoodi

Muut tiedot

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

Author(s)	Type of publication	Date
PEURA, Oskari	Bachelor´s / Master's Thesis	11.12.2013
	Pages 51	Language FINNISH
	Confidential ( ) Until	Permission for web publication (X)

Title
NETWORK ACCESS CONTROL, Open source implementation

Degree Programme
Information Technology

Tutor(s)
RANTONEN Mika, HÄKKINEN Antti

Assigned by
JAMK University of Applied Sciences, School of Technology, Department of ICT

Abstract

The purpose of this study was to explore network access control, NAC, which consists of open and free software and to investigate its suitability for teaching.

The thesis was assigned by JAMK University of Applied Sciences, School of Technology, which also gave the software to be used for this project. The software studied was PacketFence version 3.4.1 and its virtualized ZEN version (zero effort NAC).

In the theoretical part of the thesis the structure of the software and its documentation were examined. As in cases of other open-source software and projects traditionally, the written sources were difficult to find or they were outdated. The internet was found useful in a wide range of sources, however, they had to be dealt with very critically. Only PacketFence's own documentation and articles found on web pages of larger companies were selected for this thesis.

PacketFence proved to be very versatile and easily customizable. The implementation in new environment was quite straightforward, and adaptation to old environment proved to be quite easy. Operation in a network of different manufacturers and various types of clients was made possible using open source and not manufacturerspecific software.

PacketFence proved to be very useful in the educational use and it allows teaching many different techniques as far as network access control is concerned.

Keywords
Computer network, NAC, PacketFence, open source

Miscellaneous

SISÄLTÖ

KUVIOT

LYHENTEET

PC	Personal computer
WLAN	Wireless local area network
BYOD	Bring your own devices
NAC	Network access control/controller
ESX	Elastic Sky X (VMwaren projektin nimi)
JAMK	Jyväskylän ammattikorkeakoulu
IT	Informaatioteknologia
GNU	GNU's not unix
GPL	Generall public license
ZEN	Zero effort network access control/controller
USB	Universal serial bus
OVF	Open virtualization format
IPFIX	Internet protocol flow information export
SNMP	Simple network management protocol
MAC	Media access control
DHCP	Dynamic host control protocol
LDAP	Lightweight directory access protocol
RADIUS	Remote authentication dial in user service
ACS	Access control server
NPS	Network policy server
SQL	Structured query language
P2P	Point to point
IDS	Intrusion detection system
IPS	Intrusion prevention system
VoIP	Voice over internet protocol
WWW	World wide web
RFC	Request for comments
IE	Internet explorer
OpenVAS	Open Vulnerability Assessment System
WAN	Wide area network
VLAN	Virtual local area network
SoH	State of health
XP	Experience
NAP	Network access protection
OSI	Open systems interconnection
MAB	MAC authentication bypass
EAP	Extensible authentication protocol

WPA	Wireless fidelity protected access
SSID	Service set identifier
IOS	Internetwork operating system
ADSL	Asymmetric digital subscriber line
DNS	Domain name system
BIND	Berkeley internet name domain
AMD	Advanced micro devices
GHz	Gigahertsi
GB	Gigabyte
MB	Megabyte
UI	User interface
SSH	Secure shell
DES	Data encryption standard
AES	Advanced encryption standard
OS	Operating system
HTTP	Hypertext transfer protocol
FTP	File transfer protocol

1 PÄÄSYNHALLINNALLA LISÄÄ TURVALLISUUTTA

Tietoverkkojen määrä on moninkertaistunut nykyaikana. Verkkoja, suuria ja pieniä, löytyy yrityksistä, yhteisöistä ja myös useista kodeista. Tavallinen kotikäyttäjä tosin harvoin mieltää muutaman multimedialaitteen ja PC:n (personal computer) yhdistelmän tietoverkoksi.

Verkkojen ja laitteiden, etenkin mukana kulkevien ja WLAN-tekniikkaa (wireless local area network) käyttävien, määrän kasvun myötä niiden asiallinen suojaaminen on muuttunut aina tärkeämmäksi. Vastuu on toisaalta laitteiden käyttäjillä, mutta toisaalta verkon haltijalla ja omistajalla. Moni päätelaitteen omistaja saattaa usein, jopa tietämättään, olla saastuneen laitteen kanssa toisen verkossa altistaen verkon muut laitteet ja palvelut esimerkiksi haittaohjelmille. Yhä useammissa verkoissa sallitaan niin sanottu BYOD (bring your own devices) käytäntö, eli käyttäjä saa tuoda omat laitteensa ja liittyä verkkoon. Varsinkin yhteisöjen ja kotien verkoissa tämä on pikemmin sääntö kuin poikkeus.

Etenkin edellä kuvatuissa tilanteissa verkon omistaja ehkä haluaisi, tai pikemminkin tämän tulisi, suojata oma verkkonsa etenkin vierailijoiden päätelaitteiden uhkia silmällä pitäen. Tällöin vastuu aktiivisesta suojaamisesta on yksinomaan verkon omistajan tai haltijan vastuulla. Yksi tekniikka jolla tätä ongelmaa voidaan lähestyä, on tietoverkon pääsynhallinta eli NAC (network access control/controller).

Tässä opinnäytteessä tutustuttiin yhteen avoimen lähdekoodin vaihtoehtoon ja sen ominaisuuksiin. Tarkoituksena oli myös tutkia perusominaisuuksien lisäksi ESX-virtuaaliversion (Elastic Sky X) soveltuvuutta opetuskäyttöön. Toimeksiantajana tällä työllä oli JAMK (Jyväskylän ammattikorkeakoulu).

2 PACKETFENCE

2.1 Historiaa

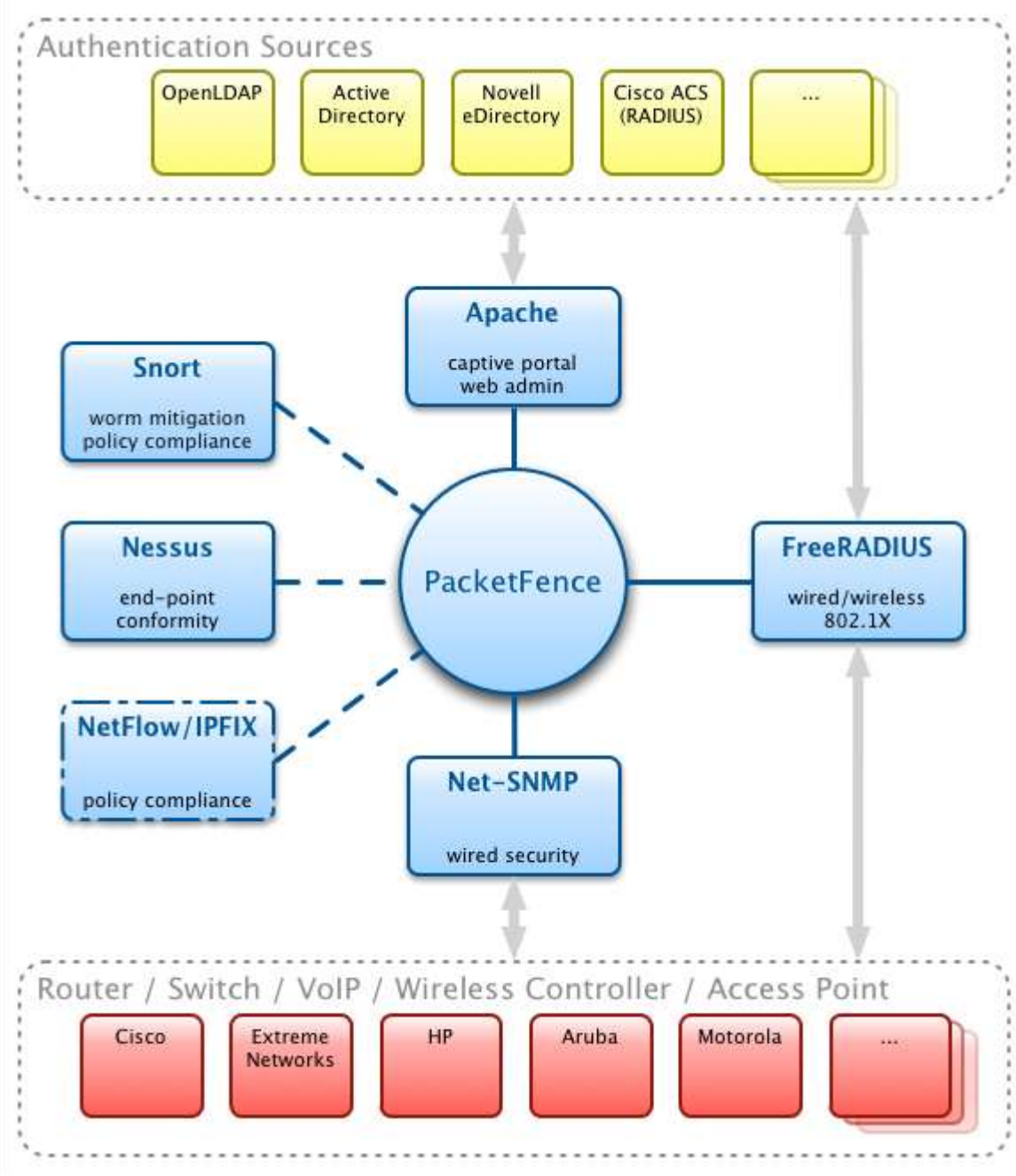
PacketFence on alun perin kahden Harvardin yliopiston IT-työntekijän (informaatio teknologia), Dave LaPorten ja Kevin Amorin, kehittämä avoimen lähdekoodin vaihtoehto tietoverkon pääsynhallinnan toteuttamiseksi. He kehittivät aluksi PacketFenceä omiin tarkoituksiinsa vapaa-aikanaan, mutta huomasivat pian että kaupallisille sovelluksille tarvittaisiin vaihtoehtoja. Kaupalliset toteutukset käyttävät usein rajoittuneita tekniikoita, ja niiden mukauttaminen monipuolisiin ympäristöihin voi olla työlästä tai jopa mahdotonta. PacketFence tarjoaa käyttäjien tunnistamiseen monia eri tekniikoita ja on siten sovellettavissa helposti useiden eri laitevalmistajien laitteista rakentuvaan verkkoon. Lisäksi GNU/GPL (GNU's not unix/general public lisence) lisenssin alla julkaistava projekti on kunkin käyttäjän vapaasti muokattavissa omiin tarkoituksiinsa sopivaksi. (Cram session n.d.)

Alkuvuodesta 2008 asti PacketFencen kehittämisestä on vastannut kanadalainen Inverse Inc. (New Leadership! 2008). Yhtiö tarjoaa myös kaupallista tukea eritasoisten sopimusten mukaan ylläpidossa ja käyttöönotossa (Commercial support 2013). Pääkehittäjän vaihtumisen myötä on kehitystahti nopeutunut. Laaja yhteisöllinen kehittäminen jatkuu yhä tiiviisti Inversen kehitystyön rinnalla. Tämä malli onkin eittämättä kustannustehokkain tapa edistää avoimen lähdekoodin ohjelmistoja.

2.2 Yleistä

PacketFence on vapaa avoimen lähdekoodin sovellus tietoverkon pääsynhallintaan. Itse asiassa se on kokoelma hyväksi havaittuja ja jatkuvasti kehittyviä sovelluksia LINUX ympäristössä lisättynä keskitetyllä selainpohjaisella hallinnalla (ks. Kuvio 1).

Ominaisuuksia voidaan ottaa käyttöön verkon laitekannan ja käyttötarkoituksen mukaan. PacketFence soveltuu helposti niin pienen paikallisen verkon vierailijoiden hallintaan, kuin myös suuren, globaalin verkon kaiken kattavaan laite- ja käyttäjähallintaankin. (PacketFence overview 2013)



Kuvio 1. PacketFence rakentuu useista tunnetuista ohjelmistoista (PacketFence overview 2013)

PacketFence on saatavilla joko paketoituina LINUX sovelluksina, jolloin asennuksesta ja integraatiosta käytettävään käyttöjärjestelmään vastaa käyttöönottaja, tai sitten valmiina LINUX jakeluna jossa on kaikki tarvittava valmiiksi mukana. (PacketFence releases 2013). Tätä paketointia kehittäjä kutsuu nimellä ”The ZEN edition of PacketFence”. Lyhenne ZEN tulee englanninkielisistä sanoista zero effort NAC, eli vapaasti käännettynä se voisi tarkoittaa ”tietoverkon pääsynhallintaa ilman ponnisteluja”. Tämä kuvaakin hyvin käyttöönoton suoraviivaisuutta ja yksinkertaisuutta.

Opinnäytetyön valmistumisajankohtana oli PacketFencen vakaaksi todettu ajantasainen tuotantoversio 4.0.6. Se on julkaistu 13.9.2013. (PacketFence releases 2013) Lisäksi PacketFence on saatavilla kahtena eri ZEN-jakeluna. Toinen on USB-muistilta (universal serial bus)suoritettava live-jakelu versiona 4.0.5, ja toinen on eri virtuaalialustoja varten julkaistu OVF-paketti (open virtualization format) versiona 4.0.2. (Zero effort NAC 2013.)

Opinnäytetyön aloitusajankohdasta (syksy 2012) johtuen tässä työssä käytettiin kuitenkin ZEN-jakelun VMWaren ESX-alustalle tarkoitettua versiota 3.4.1. Se rakentuu CentOS (operating system) version 5.8 päälle.

2.3 Käyttötarkoituksia ja ominaisuuksia

2.3.1 PacketFencen rakenteesta

PacketFencectä on moneksi. Ominaisuuksia on runsaasti johtuen PacketFencen käyttämistä ohjelmistoista. Ominaisuudet ovat myös laajasti muokattavissa ja sopeutettavissa kulloisenkin ympäristön ja käyttötarkoituksen mukaisiksi.

PacketFence rakentuu muun muassa seuraavista ohjelmistoista

- Apache
- Snort

- Netflow/IPFIX
- Net-SNMP
- FreeRADIUS
- Nessus / OpenVAS

Joitakin käyttötarkoituksia mainitakseni, PacketFence soveltuu vierailijatunnusten ja -laitteiden hallintaan, langattomien tukiasemien ylläpitoon, haittaohjelmien tunnistamiseen ja estämiseen verkkoliikenteen perusteella, erilaisten verkon toiminnan kannalta haitallisten ohjelmien suorittamisen estämiseen, virustorjunnan ja valittujen ohjelmien versioiden ajantasaisuuden tarkastamiseen, erilaisten käyttäjäagenttien ja laitteiden tunnistamiseen ja käytön estämiseen jne. (PacketFence käyttöopas 2012, 2.) Lisää ominaisuuksia löytyy PacketFencen kotisivuilta www.packetfence.org/about/advanced_features.html.

2.3.2 Käyttäjien tunnistus

PacketFence voi tunnistaa verkkoon pyrkivän käyttäjän useita eri tekniikoita käyttäen. Järjestelmä voi toimia täysin itsenäisesti käyttäen sisäistä käyttäjätietokantaa tai se voidaan integroida olemassa olevaan ympäristöön käyttäen jo olemassa olevaa käyttäjätunnistusta. Käyttäjä voidaan tunnistaa myös liittyvän laitteen perusteella ja pääsy verkkoon voidaan automatisoida tietylle edeltä määritellylle laitejoukolle. Automaattinen rekisteröinti voi perustua verkkolaitteeseen, jolloin kaikki ko. kytkimen oppimat MAC-osoitteet (media access control) kirjataan rekisteröityneeksi. Tämä helpottaa PacketFencen käyttöönottoa valmiissa ympäristössä. Rekisteröinti voi perustua myös DHCP-sormenjälkeen (dunamic host configuration protocol) tai MAC-osoitteeseen. (PacketFencen ominaisuudet 2013)

Käytössä on muun muassa seuraavat tekniikat

- LDAP
    - Microsoft Active Directory
    - Novell eDirectory
    - OpenLDAP

- RADIUS
    - Cisco ACS
    - RADIUS (FreeRADIUS, Radiator)
    - Microsoft NPS
- Paikallinen käyttäjätietokanta, esim Apache htpasswd tai SQL-tietokanta
- Uusimmissa PacketFence versioissa OAuth2-tekniikka
    - Facebook
    - Google
    - GitHub

(PacketFencen ominaisuudet 2013)

2.3.3 Normaalista poikkeavan verkkoliikenteen tunnistus

Epänormaalin tai epäilyttävän verkkoliikenteen, kuten esimerkiksi madot, virukset, vakoiluohjelmat tai etukäteen kielletyksi määritelty liikennetyyppi, vaikka P2P (point to point), havainnointiin käytetään Snort-sovellusta. Snort on avoimen lähdekoodin IDS/IPS-järjestelmä (intrusion detection/prevention system). Snorttia julkaisee ja kehittää Sourcefire, joka on nykyään osa Ciscoa. Alun perin Snort on julkaistu vuonna 1998, ja nykyään siitä on tullut ns. de facto-standardi IPS-järjestelmänä yli 400000 rekisteröityneen käyttäjän ja miljoonien latausten kautta (Snort 2013.)

Snort on täysin integroitu käyttöliittymään, ja sääntöjen päivittäminen Snortin tietokannoista onnistuu automaattisesti. Epäilyttävät ohjelmat ja liikenne tunnistetaan suoraan tietovirrasta ilman kohteeseen asennettavia lisäosia. (PacketFence käyttöopas 2012, 39.)

Estämällä esimerkiksi ei toivottu P2P-liikenne vapautetaan verkon kapasiteettia hyötyliikenteen käyttöön. Näin toimimalla saatetaan välttyä tarpeettoman lisäkaistan hankkimiselta, ja samalla säästyy resursseja muihin verkon tarpeisiin.

PacketFence sisältää runsaasti valmiita sääntöjä, mutta käyttäjällä on halutessaan mahdollisuus tehdä omia sääntöjä tunnistamiseen omien tarpeidensa mukaisesti.

2.3.3.1 DHCP-sormenjälkitunnistus

Lähes jokaisella käyttöjärjestelmällä on uniikki ja erilainen DHCP-sormenjälki. Pyytäessään järjestelmältä osoitetta DHCP-protokollaa (dynamic host configuration protocol) käyttäen, PacketFence vertaa Snortin avulla laitteen, eli käyttöjärjestelmän sormenjälkeä omaan tietokantaansa ja sen perusteella joko sallii tai estää liikenteen kohdeverkkoon ennakkoon asetetun säännön mukaisesti. DHCP-sormenjälkien hallinta onnistuu WWW-käyttöliittymän kautta. Tällä mekanismilla voidaan verkosta eristää laitteita, joiden ei haluta pääsevän käyttämään verkon resursseja. Ne voivat olla esimerkiksi

- Sony Playstation tai vastaavat muun merkkiset pelikonsolit
- VoIP puhelimet mallin ja merkin mukaan
- Langattomat tukiasemat
- Matkapuhelimet
- Eri PC-käyttöjärjestelmät jne.

(PacketFencen ominaisuudet 2013)

PacketFence käyttää Inversen ylläpitämää DHCP-sormenjälki tietokantaa osoitteesta www.fingerbank.org. (Fingerbank 2013)

2.3.3.2 User-agent tunnistus

PacketFence kykenee tunnistamaan liikenteen perusteella esimerkiksi käytettävän internet selaimen, eli User-Agentin (RFC 2616 2013). User-Agent sisältää tiedon esimerkiksi selaimen ja käyttöjärjestelmän versioista. Tunnistuksen perusteella voidaan estää ei toivotun laitteen tai sovelluksen pääsy suojattavaan kohdeverkkoon. Estetty kohde voi olla esimerkiksi:

- Apple iPod tai iPhone laitteet
- Android laitteiden eri versiot
- Vanhat versiot internetselaimista, kuten esimerkiksi IE6

(PacketFencen ominaisuudet 2013.)

2.3.3.3 Tunnistus MAC-osoitteen perusteella

Tunnistussääntö voi perustua myös MAC-osoitteeseen. Jokaisella laitevalmistajalla on oma MAC-osoitealueensa. Tämän perusteella voidaan sulkea kohdeverkosta tietyn laitevalmistajan laitteet. Tosin ns. MAC-spoofing tekniikalla on mahdollista kiertää MAC-osoitteisiin perustuva suodatus. (PacketFencen ominaisuudet 2013)

2.3.4 Haavoittuvuuksien tutkiminen

Haavoittuvuuksien etsimisellä ja havaitsemisella pyritään ennalta poistamaan jonkin jo tunnetun uhan pääseminen verkkoon. Uhan voivat muodostaa esimerkiksi vanhat käyttöjärjestelmäversiot, puutteelliset päivitykset tai puuttuva virussuojaus.

PacketFence voi käyttää havaitsemiseen kahta eri ohjelmistoa. Suljetun lähdekoodin Nessus tai avoimen lähdekoodin vaihtoehtona OpenVAS. Kummatkin ohjelmistot on täysin integroituja PacketFencen käyttöliittymään, ja sääntöjen hallinta onnistuu kokonaisuudessaan PacketFencen web-käyttöliittymän kautta. Nessuksen käyttö vaatii joko ilmaisen rekisteröitymisen yksityiskäyttöön tai maksullisen lisenssin kaupallisessa käytössä. OpenVAS ei vaadi rekisteröintiä tai lisenssiä käyttöönottaessa (PacketFence käyttöopas 2013, 44).

Haavoittuvuuksien skannaus eli etsintä voidaan asettaa suoritettavaksi uuden laitteen rekisteröinnin yhteydessä, ennalta asetetuin määräajoin tai esimerkiksi Snor-havainnon perusteella uhkan ilmentyessä (PacketFence käyttöopas 2013, 46).

Suuren prosessorikuormituksen takia on suositeltavaa asettaa haavoittuvuuksien havaitsemiseen käytettävät sovellukset eri alustoille varsinaisen PacketFence palvelun kanssa. Tämä on suositeltava toimintatapa varsinkin jos kyseessä on hajautettu verkko. Silloin haavoittuvuudet kannattaa etsiä samassa fyysisessä paikassa ja lähiverkossa, jossa liittyvät asiakaskoneet sijaitsevat. Muutoin verkkoliikenteen määrä WAN-yhteyden yli kasvaa tarpeettomasti hidastaen verkon toimintaa (PacketFence käyttöopas 2013, 46).

2.3.5 Kaistan käytön valvonta

PacketFence voidaan määritellä valvomaan tietyn laitteen tai asiakkaan kaistan käyttöä. Valvonta perustuu siirrettyyn datamäärään tietyllä aikavälillä. Kun määritelty datamäärä täyttyy siirretään ko. asiakas esimerkiksi eristys VLAN-verkkoon josta on rajoitettu pääsy joko kohdeverkkoon tai internettiin. Määritellyn ajan kuluttua asiakas voidaan palauttaa takaisin normaaliin VLAN-verkkoon.

Rajoitus toteutetaan RADIUS Accounting-toiminnolla. Rajoitus voi perustua tulevaan, lähtevään tai kokonaisliikenteeseen. Tämä ominaisuus on hyödyllinen etenkin pienen organisaation vierailuverkon käytössä, jossa usein internetyhteys on nopeudeltaan rajallinen. Näin verkon omille käyttäjille taataan riittävät resurssit verkossa (PacketFence käyttöopas 2013, 47).

2.3.6 Statement of Health

SoH eli Statement of Health on Microsoftin lanseeraama ja käyttämä tekniikka Windows XP2-käyttöjärjestelmästä eteenpäin. Se liittyy tietokoneen tilaa valvovaan NAP-palveluun (Network Access Protection). Palvelu lähettää tietoja virustunnisteiden tilasta, Windows Updaten ajantasaisuudesta jne. joko RADIUS- tai DHCP-palvelimelle. PacketFencen tapauksessa käytetään integroitua RADIUS-palvelinta freeradius2 paketista.

Web-käyttöliittymän kautta luodaan säännöt eri käyttöjärjestelmille ja niiden versioille. Tämän perusteella puutteelliset asiakkaat voidaan captive-portal toiminnolla ohjata päivitysten ja täydennysten vaatimille www-sivuille. (PacketFence käyttöopas 2013, 54-55.)

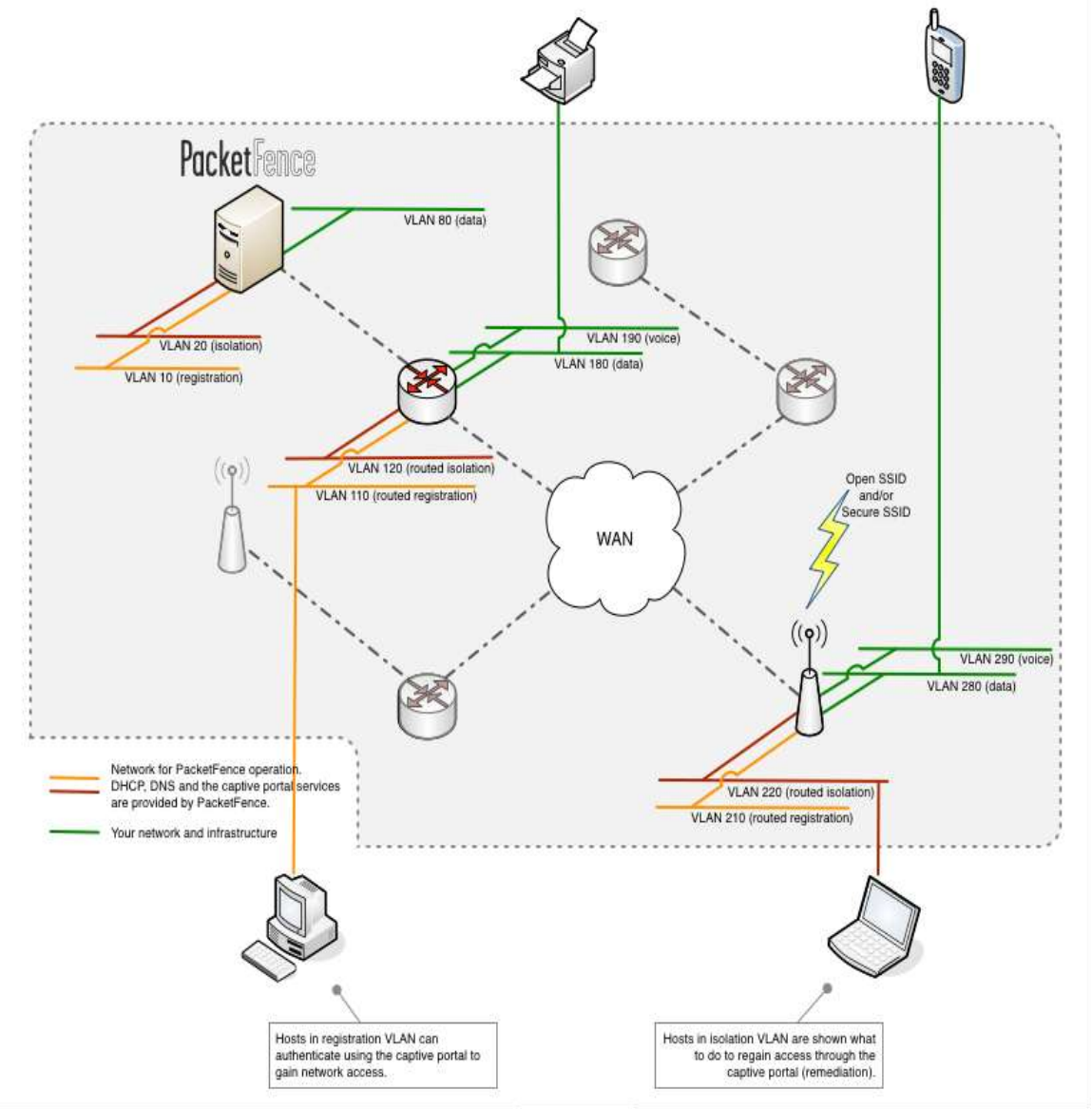
2.3.7 Toimintamallit

PacketFence voi toimia kahdella eri toimintaperiaatteella tai niiden yhdistelmällä.

Ensimmäinen toimintatapa on ns. Inline, jossa nimen mukaisesti kaikki liikenne kulkee PacketFence järjestelmän kautta. Toimintamuoto tarvitsee yksinkertaisimmillaan kaksi verkkoliitäntää, toinen kohdeverkkoon ja toinen valvottaville laitteille. PacketFence käyttää verkkoliikenteen ohjaamiseen verkkojen välillä IPTables-sovellusta (PacketFence käyttöopas 2012, 76.) Tämä toimintamuoto soveltuu erittäin hyvin pieniin ympäristöihin ja hallitsemattomien verkkolaitteiden, kuten yksinkertaisten kytkinten tai WLAN-tukiasemien kanssa käytettäväksi. Suuremmilla liikennemäärillä saattaa PacketFencen suorituskyky heikentyä, ellei sitä ole otettu huomioon palvelimen suorituskykyä suunniteltaessa. Inline-malli ei sovellu myöskään käytettäväksi tapauksissa, joissa yhden PacketFence sovelluksen avulla täytyy hallita useita fyysisesti erillään sijaitsevia verkkolaitteita.

Toinen toimintatapa on ns. Out-of-band joka on esitetty kuviossa 2. Tässä mallissa PacketFencen tehtäväksi jää verkkolaitteiden ohjaaminen. Tällöin PacketFence palvelin ja hallittavat verkkolaitteet voivat sijaita toisistaan riippumattomissa paikoissa. Kokonaisuutta on helppo laajentaa tarvittaessa ja ylläpito on helppo keskittää esim. suuryrityksen yhteen toimipisteeseen. Haittapuolena tässä mallissa on joidenkin ominaisuuksien vaatima ylimääräinen yhteys verkkolaitteeseen liikenteen monitorointia varten. Tämä vaatii PacketFence palvelimelta ylimääräisen verkkoliitännän monitorointia varten sekä hajautetun infran verkkolaitteisiin yhteyden ko. verkkoliitynnästä.

Kolmas malli on kahden aiemmin mainitun yhdistäminen, jolloin voidaan käyttää sekä hallittavia että yksinkertaisia verkkolaitteita ympäristön toteuttamiseen.



Kuvio 2. Out-of-band toteutus hajautetussa ympäristössä. (PacketFence overview 2013)

2.3.8 Kaapelikytkentäiset verkkolaitteet

2.3.8.1 Yleistä

PacketFencen toteutus päätelaitteiden ohjaamiseen oikeisiin verkon osiin sekä haitallisten tai epämääräisten ja tuntemattomien laitteiden eristäminen perustuu virtuaalisten lähiverkkojen (VLAN) käyttöön. PacketFence valitsee ennalta määritettyjen sääntöjen perusteella kulloiseenkin tilanteeseen määritellyn VLAN

verkon, jonka se asettaa kulloisenkin verkkolaitteen portin käyttämään asiakaslaitteesta riippuen. Tällä tekniikalla eristäminen ja verkkojen välinen kytkeminen tapahtuu OSI-mallin kerroksella 2. Tämä takaa suuren luotettavuuden verkon turvallisuudelle ja vaikean kierrettävyyden eristetyn päätelaitteen näkökulmasta. Virtuaalisten lähiverkkojen käyttö myös helpottaa PacketFencen käyttöönottoa tuotantoympäristössä, joissa yleensä VLAN tekniikka on jo monesti otettu käyttöön.

VLAN-verkkojen osoittamiseen PacketFencellä on käytössään kolme tekniikkaa: SNMP trapit, 802.1X ja MAC authentication bypass (MAB). Näistä jälkimmäisiä kahta käytetään yleensä yhdessä vaihtoehtoisina tekniikoina. (PacketFencen tekninen esittely 2013)

Ajantasainen lista tuetuista verkkolaitteista ja käytettävistä olevista tekniikoista löytyy osoitteesta http://www.packetfence.org/about/supported_switches_and_aps.html.

2.3.8.2 SNMP trapit

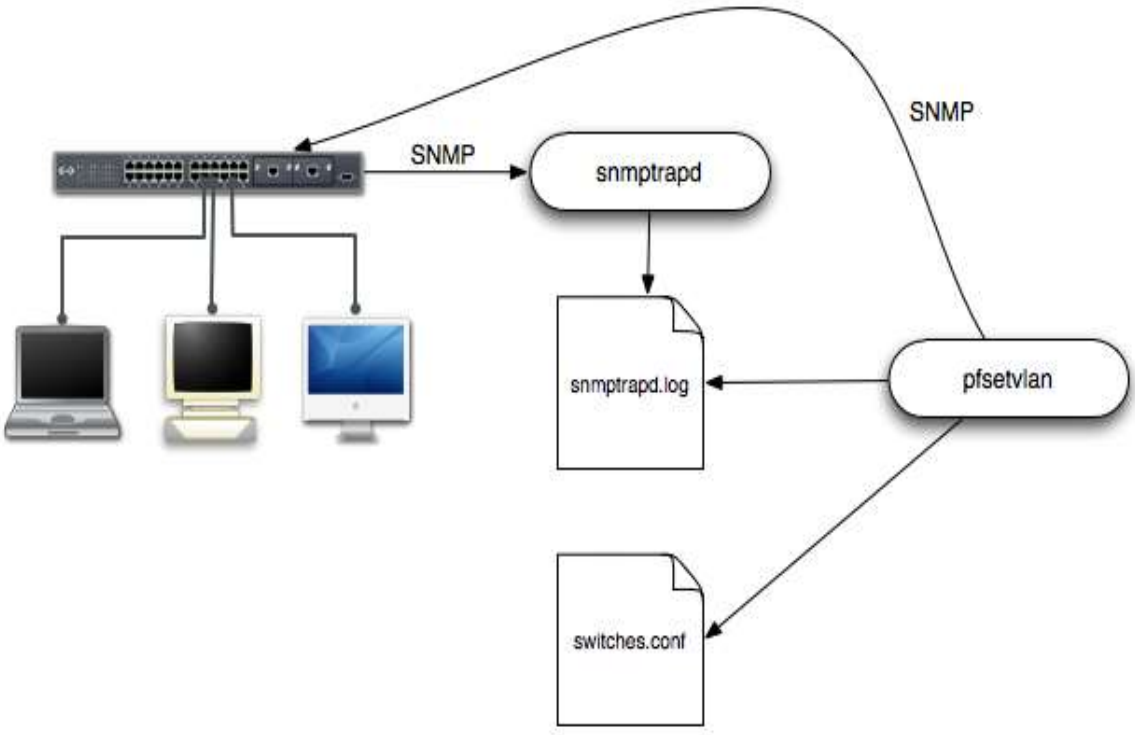
Käytettäessä SNMP-trappeja (simple network management protocol) VLAN-verkkojen osoittamiseen on kaikki kytkimen portit, joissa aiotaan käyttää kyseistä tekniikkaa, asetettava lähettämään SNMP-viestejä PacketFence palvelimelle (ks. Kuvio 3).

SNMP trappeja käytettäessä PacketFence tukee kolmea eri vaihtoehtoa päätelaitteen havaitsemiseksi ja tunnistamiseksi. Seuraavassa on esitetty tekniikat järjestyksessä heikoimmasta suositeltavimpaan:

- Kytkimen portin tilan muutos (LinkUp/LinkDown)
- MAC osoitteen huomioiva kytkinportti (MAC learnt/MAC removed)
- Port Security (kytkin muistaa MAC osoitteen)

Linkin tilan muutokseen perustuva tunnistus on kaikkein yksinkertaisin ja se löytyy lähes kaikista kytkimistä. Tekniikan heikkous perustuu useisiin tilan muutoksiin esimerkiksi tietokoneen käynnistyessä tai sähkökatkon sattuessa laajassa verkossa. PacketFencen on reagoitava tällä tekniikalla jokaiseen linkin muutokseen, jolloin se saattaa aiheuttaa verkon saavuttamisessa suuria viiveitä. Lisäksi tekniikka vaatii kytkimeen ylimääräisen VLANin. Tätä virtuaaliverkkoa käytetään MAC-osoitteen oppimiseen. Se on tyhjä verkko, johon asiakas lähettää DHCP-pyyntöjä, kunnes portti oppii asiakkaan MAC-osoitteen. PacketFence lähettää toistuvia kyselyitä kytkimelle, kunnes ko. portti on oppinut asiakkaan MAC-osoitteen. Tämä liikenne lisää verkon overhead-liikennettä syöden hyötyliikenteen kaistaa. Lisäksi vikatapaukset, esimerkiksi sähkökatko, lisää vain palvelimen kuormitusta.

Jos kytkin tukee lisäksi SNMP viestiä jolla se ilmoittaa opitun MAC-osoitteen, ottamalla se käyttöön vähenee SNMP viestien ja sen myötä turhan liikenteen määrä oleellisesti.

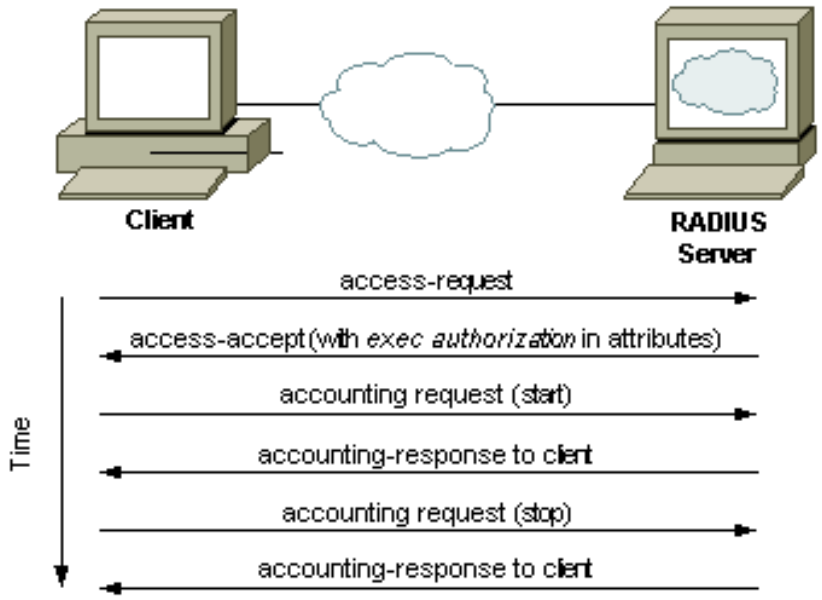


Kuvio 3. SNMP-viestien kulku ja VLAN-verkkojen osoitus. (PacketFence käyttöopas 2012, 74)

Kolmas, ja suositelluin, tekniikka perustuu Port Securityyn. Tällä tekniikalla on huomattava vaikutus ns. turhan ohjausliikenteen (overhead) määrään kytkimen ja PacketFence palvelimen välillä. Etenkin hitaiden yhteyksien varassa olevat hajautetut verkot, joissa on paljon asiakaslaitteita, tulisi liittää käyttäen tätä tekniikkaa. Näin estetään pitkät viiveet kohdeverkkoon liityttäessä. Port Security tekniikalla hallittava kytkin hoitaa myös asiakaslaitteen/portin eristämisen MAC-osoitteen vaihtuessa nopeasti. (PacketFencen käyttöopas 2012, 72)

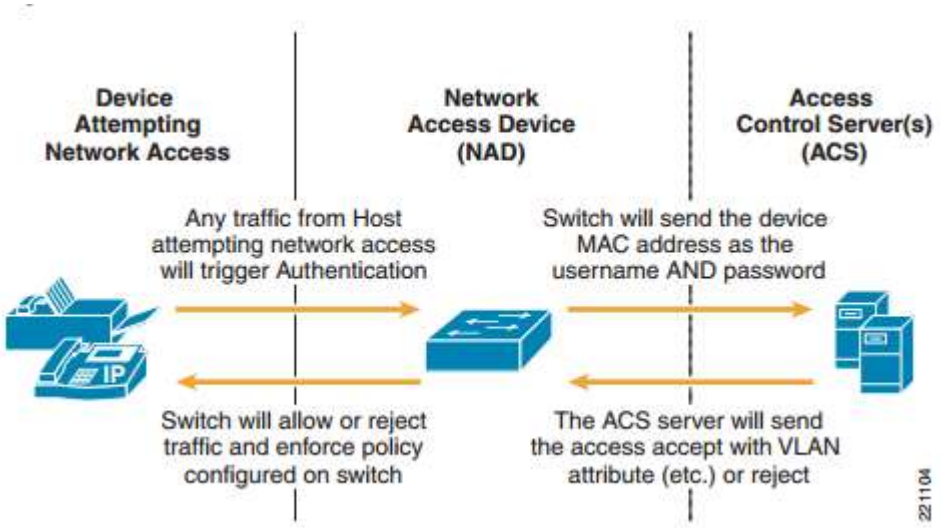
2.3.8.3 802.1X + MAC authentication bypass (MAB)

Käytettäessä 802.1X protokollaa saavutetaan porttikohtainen käyttäjän tunnistus. Asiakaslaite toimii tunnistuksen pyytäjänä (supplicant), kytkin toimii pyynnön välittäjänä (authenticator) ja tunnistus tapahtuu usein esimerkiksi RADIUS-tietokantaa (Remote authentication dial in user service) vastaan. Esimerkki RADIUS autentikoinnista on esitetty kuviossa 4. Myös muita hakemistoja, kuten Active Directoria, voidaan käyttää käyttäjien tunnistautumiseen. Tällöin täytyy pitää huoli siitä että kumpikin osapuoli käyttää samaa Extensible Authentication Protocol:n (EAP) versiota. EAP-protokollan avulla varmistetaan myös se, että kumpikin osapuoli vaihtaa tietoja luotettavan osapuolen kanssa (EAP, protokollan toiminta 2004). PacketFencen tapauksessa yksinkertaisimmillaan käyttäjän tunnistamisen hoitaa järjestelmän sisäänrakennettu FreeRADIUS palvelin.



Kuvio 4. Esimerkki RADIUS autentikoinnista. (Autentikointiportokollat 2008)

Varjopuoli tämän tekniikan käytössä on tarvittava tuki 802.1X protokollalle, jota ei kaikissa laitteissa ole. Tällöin voidaan nämä laitteet tunnistaa käyttäen MAB mekanismia hyväksi käyttäen (ks. Kuvio 5). MAB toimintoa käytetään 802.1X:n epäonnistuttua tunnistamisessa, näin laitteet joista puuttuu tuki 802.1X protokollalle voivat tällaisessa ympäristössä saavuttaa oikean VLAN verkon. Tätä MAB toiminnallisuutta tarjoaa vain harva laitevalmistaja.



Kuvio 5. MAB mekanismin toiminta. (MAC Authentication Bypass 2007)

2.3.9 Langaton ympäristö

Langattomassa ympäristössä käytetään myös 802.1X protokollaa yhdessä WPA2-Enterprise salauksen kanssa takaamaan luotettava ja turvallinen tapa muodostaa langaton verkko myös yrityskäyttäjille. PacketFence voi olla yhteydessä langattomiin tukiasemiin joko suoraan tai WLAN-kontrollerin välityksellä. Jälkimmäisessä tapauksessa riittää että kontrolleri on tuettujen laitteiden listalla. Jos halutaan ohjata suoraan langatonta tukiasemaa ilman kontrolleria, tulee tukiaseman täyttää seuraavat vaatimukset:

- Useita SSID:tä, useita VLAN:eja SSID:ssä
- Autentikointi RADIUS palvelimeen
- Dynaaminen VLAN osoitus
- SNMP deautentikointi trapit

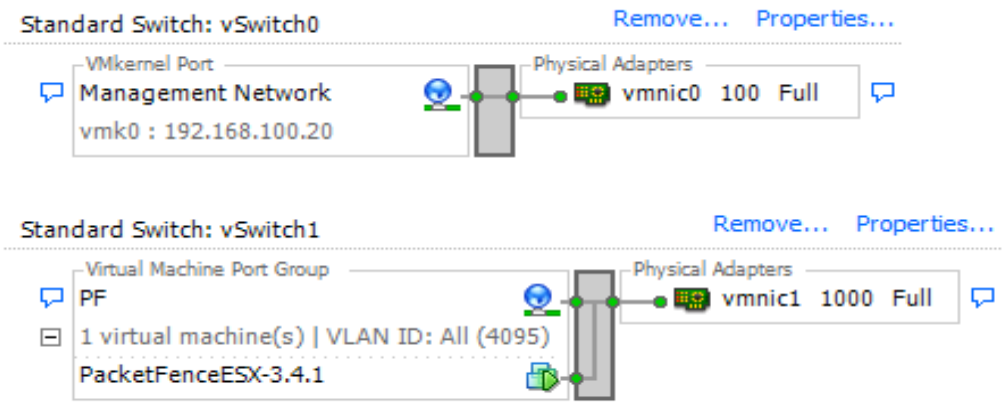
Tässä työssä ei toteutettu langattomia järjestelmiä.

2.4 Testausympäristö

Tässä opinnäytetyössä oletetaan että lukija osaa käyttää VMWaren virtuaalialustoja, tuntee yleisimmät tietoverkon käsitteet hyvin ja LINUX:in peruskäyttö on hallussa. Myös Ciscon IOS:in peruskomennot on osattava. Näitä asioita ei käydä syvällisemmin ympäristön rakentamisessa, konfiguroinnissa ja testaamisessa läpi.

Opinnäytetyötä varten rakennettiin oma testausympäristö, jossa kohdeverkkoa kuvataan yksinkertaisella ADSL-kytkin yhdistelmällä. Tästä laitteesta on yhteys myös internettiin. Lisäksi asennettiin PC-tietokoneeseen VMWaren ESXi versio 5.0.0 virtuaalialustaksi testattavaa PacketFence ZEN virtuaalikonetta varten. ESXi rautaan lisättiin yksi verkkokortti, jolloin kokonaislukumääräksi saatiin kaksi verkkoliityntää. Toista liityntää, vmnic0, käytetään virtuaalialustan hallintaan kohdeverkosta käsin.

Verkkoliitynnän IP-osoitteeksi asetettiin kiinteä osoite 192.168.100.20/24. Toinen liittymä, vmnic1, on käytössä ainoastaan PacketFencen liikennettä varten. Se on asetettu ns. trunk tilaan asettamalla VLAN ID:ksi 4095. Virtuaalikoneen verkkoasetukset on esitetty kuviossa 6.

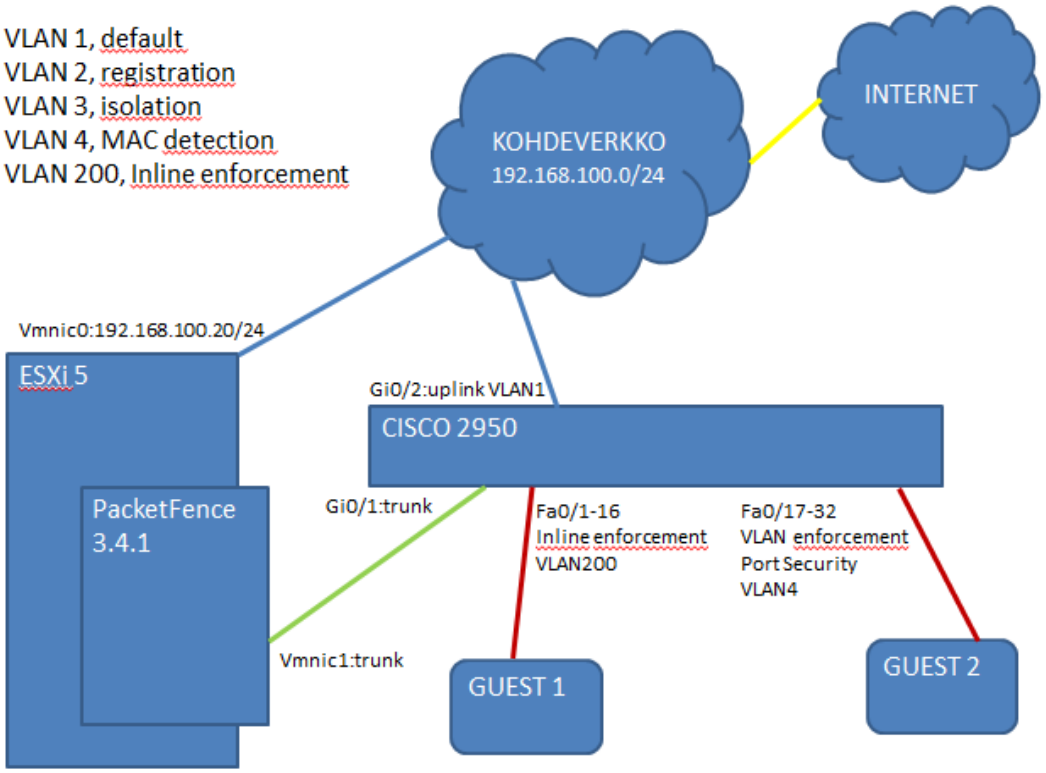


Kuvio 6. Virtuaalikoneen verkkoliitynnät.

Tämän lisäksi ympäristössä käytetään Ciscon 48-porttista access-tason kytkintä malliltaan 2950. Tämä kytkin valikoitui JAMK:in laboratorio ympäristössä käytössä olevan tyypin mukaisesti.

2.4.1 Testiympäristön rakenne

Kuviossa 7 on esitetty testiympäristön topologia.



Kuvio 7. Testiympäristön topologia.

Kuvasta ilmenee testiympäristön komponenttien väliset ethernet-kaapeloinnit. Sininen väri kuvastaa kohdeverkon sisäistä liikennettä, liikennöinti tapahtuu VLAN1 verkossa. Vihreä väri kertoo liikenteen olevan PacketFence järjestelmän ja kytkimen välistä ohjausliikennettä sekä Inline liikennettä virtuaalisten verkkoliityntöjen välillä. Tällä välillä liikkuu VLAN 1,2,3 ja 200 verkkojen liikennettä. VLAN4 on ainoastaan kytkimen sisäinen VLAN verkko käytettäessä MAC tunnistusta. Punainen väri kuvaa liittyvien vierailijoiden tunnistamatonta liikennettä ennen tunnistautumista ja rekisteröintiä.

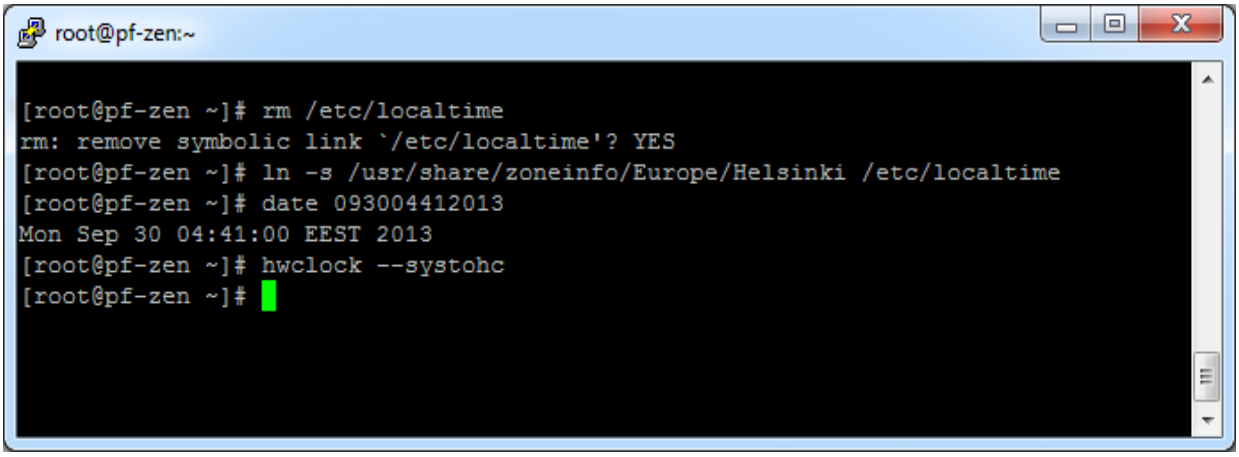
2.4.2 Virtuaalikoneen valmistelu

Virtuaalikone on alun perin rakennettu englanninkieliseen ympäristöö ja käytössä on amerikan-englantilainen näppäinasettelu. Se kannattaa vaihtaa käytössä olevan näppäimistön mukaiseksi, tässä suomalaiseksi. Näppäimistö asettelun muuttaminen tapahtuu muokkaamalla tiedostoa /etc/sysconfig/keyboard. Sieltä kohta

KEYTABLE=”xx” tulee muuttaa muotoon KEYTABLE=”fi”. Uudellenkäynnistyksen jälkeen käytössä tulisi olla suomalainen näppäimistöasettelu.

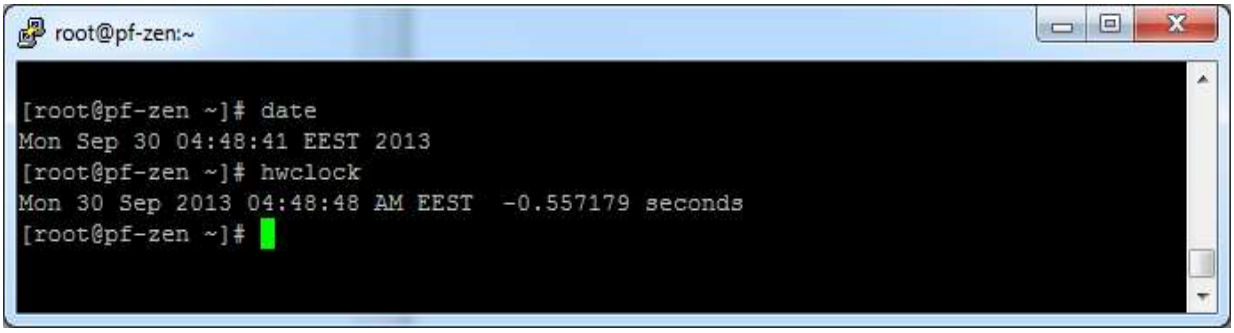
Toinen asia mikä kannattaa ottaa huomioon, on aikavyöhykkeen valinta. Tämä helpottaa ainakin vianhakua, koska lokitietojen aikaleimat ovat muuten eri ajassa.

Aika asetetaan alla olevan kuvan mukaisesti. Ajan muotona on MMDDhhmmYYYY. Komennolla hwclock --systohc asetetaan käyttöjärjestelmän ja raudan kellot samaan aikaan.



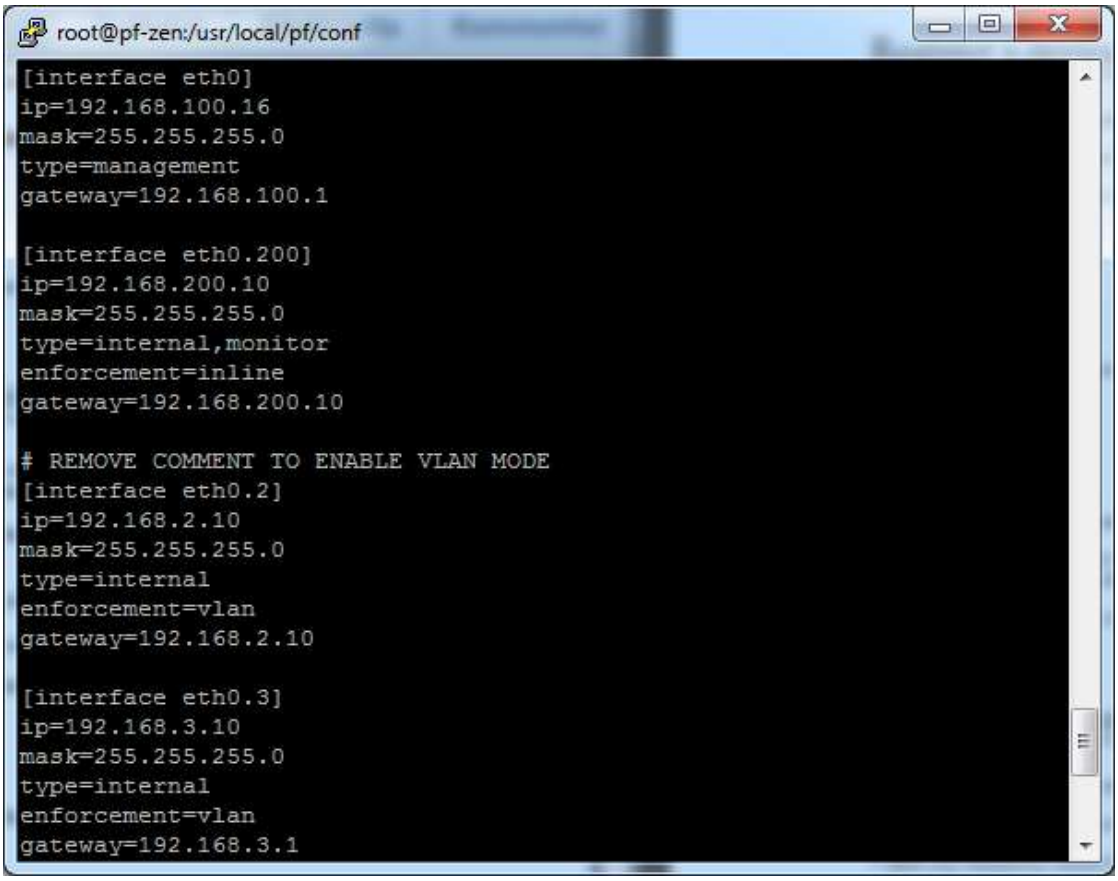
Kuvio 8. Ajan asettaminen virtuaalikoneessa.

Asetuksen onnistumisen voit tarkastaa kuviossa 9 käytetyillä komennoilla.



Kuvio 9. Ajan asetuksen tarkastaminen.

Tämän lisäksi virtuaalikoneen verkkokortille kannattaa antaa kiinteä osoite. Se tapahtuu muokkaamalla tiedostoa /usr/local/pf/conf/pf.conf alla olevan kuvio 10:n mukaisesti. Tässä asetetaan kiinteäksi osoitteeksi 192.168.100.16/24. Muihin kuin eth0 liitynnän asetuksiin ei tule tässä vaiheessa koskea.



Kuvio 10. IP-osotteiden asettaminen.

Näiden valmistelujen jälkeen virtuaalikone on valmiina otettavaksi käyttöön asetusten mukaisessa ympäristössä.

3 TOTEUTUS

3.1 Yleistä

Opinnäytetyössä testattiin PacketFencen ESXi virtuaalikoneelle soveltuvaa valmista jakelua. Ympäristön topologiana on aiemmin kuvatunlainen yksinkertainen rakenne, joka koostuu käytännössä yhdestä kytkimestä ja virtuaalisesta PacketFence palvelimesta. Virtuaalipalvelimen yhteen verkkoliityntään (vmnic1) on lisätty tarvittavat VLAN verkot sekä Inline että VLAN enforcement käyttöä ajatellen. Näin saadaan minimaalisella kokoonpanolla käyttöön molemmat PacketFencen toimintatavat. Tämän lisäksi kytkimelle tuodaan yhteen porttiin ns. uplink kohdeverkkoon. Tämä portti asetetaan toimimaan VLAN 1 verkossa, jolloin sitä kautta saadaan yhetys kohdeverkkoon, ja sieltä internettiin asti.

3.2 PacketFence ZEN 3.4.1

Käytettävä versio on 3.4.1 ZEN eli Zero Effort NAC. Alla olevassa kuviossa on esitetty käytössä olevat ohjelmaversiot. (PacketFence käyttöopas 2012. 6.)

MySQL server	MySQL 4.1 or 5.1
Web server	Apache 2.2
DHCP server	DHCP 3
DNS server	BIND 9
RADIUS server	FreeRADIUS 2.1.12
Snort	Snort 2.8 or 2.9

Kuvio 11. Käytössä olevat ohjelmat ja versiot.

Suositeltavat vähimmäisvaatimukset raudan osalta ovat:

- Intel tai AMD suoritin, 3 GHz
- 2048 MB keskusmuistia
- Vähintään 20 GB levytilaa
- 1 verkkokortti

3.2.1 Oletusasetukset

Tässä opinnäytetyössä seuraavat konfiguraatiot ja olettamukset ovat käytössä ellei muuta mainita.

3.2.1.1 Verkko kokoonpano

Käytössä on alla olevan kuvion 12 mukainen kokoonpano verkko-osoitteista ja VLAN ID:stä käyttötarkoituksineen, lukuun ottamatta VLAN 5 ja 10. Hallinta verkko VLAN 1 toimii tässä toteutuksessa myös tuotanto- ja kohdeverkkona.

VLAN ID	VLAN Name	Subnet	Gateway	PacketFence Address
1	Management	DHCP		DHCP
2	Registration	192.168.2.0/24	192.168.2.10	192.168.2.10
3	Isolation	192.168.3.0/24	192.168.3.10	192.168.3.10
4	Mac Detection			
5	Guests	192.168.5.0/24	192.168.5.10	192.168.5.10
10	Normal	192.168.1.0/24	192.168.1.1	192.168.1.10
200	Inline	192.168.200.0/24	192.168.200.10	192.168.200.10

Kuvio 12. Verkkoparametrit.

3.2.1.2 DHCP/DNS

PacketFencen sisäänrakennettua DHCP-palvelinta käytetään jakamaan osoitteet VLAN verkoille 2,3 ja 200. VLAN 1 verkko saa osoitteensa kohdeverkon DHCP-palvelimelta.

VLAN verkoille 2 ja 3 osoitteenselvittämiseen käytetään PacketFencen sisäistä DNS-palvelinta. (PacketFence ZEN asennusopas 2012)

Nämä asetukset määritellään tiedostossa /usr/local/pf/conf/networks.conf, josta niitä voi tarvittaessa muuttaa.

3.2.1.3 Käyttäjätunnukset ja salasanat

Virtuaalikoneen käyttöön tarvitaan useita eri käyttäjätunnus salasanapareja eri toiminallisuuksiin. Oletukset on esitelty PacketFence ZEN asennusoppaan sivulla 8 ja alla olevassa kuviossa 13.

Management (SSH/Console) and MySQL

- Login: root
- Password: p@ck3tf3nc3

Administrative UI

- URL: https://dhcp_ip:1443
- Login: admin
- Password: p@ck3tf3nc3

Captive Portal / 802.1X Registration User

- Login: demouser
- Password: demouser

Kuvio 13. Oletuskäyttäjät ja salasanat.

3.3 Käyttöönottaminen

Edellä esitetyn virtuaalikoneen mukauttamisen lisäksi käyttöönotossa ainoa tehtävä on lisätä PacketFencen konfiguraatioon käytettävä verkkolaite. PacketFencen alkuasetukset käyttöönoton yhteydessä kannattaa tehdä muokkaamalla kahta

tarvittavaa tiedostoa polussa /usr/local/pf/conf/. Nämä tiedostot ovat pf.conf ja switches.conf.

Pf.conf pitää sisällään yleisen toimintaan vaikuttavan konfiguraation, esimerkiksi toimintatavan valinta määritellään tässä tiedostossa (PacketFencen käyttöopas 2012. 13).

Switches.conf tiedostossa määritellään hallintaan otettavat kytkimet, tukiasemat tai WLAN-kontrollerit. Tämä tiedosto koostuu yleisestä osasta, jossa on kaikille verkkolaitteille yhteiset asetukset, sekä laitekohtaisesta osasta, jossa määritellään jokaisen ohjattavan laitteen parametrit (PacketFencen käyttöopas 2012. 15). Tätä tiedostoa ei tarvitse ottaa huomioon jos toimintatavaksi valitaan ainoastaan Inline.

Näiden konfiguraatiotiedostojen muokkaamisen jälkeen uudelleenkäynnistys vaaditaan muutosten voimaanastumiseksi (PacketFencen käyttöopas 2012. 15).

Tässä toteutuksessa käytössä olleet konfiguraatiot on kokonaisuudessaan esitetty liitteissä 1 ja 2.

3.4 Verkkolaitteiden lisääminen

Jos Inline toiminnallisuuden lisäksi otetaan käyttöön VLAN verkkoihin perustuva kytkimen hallinta, on PacketFencen konfiguraatiota muokattava. Switches.conf tiedostoon määritellään liikenne palvelimelta kytkimeen ja kytkimeltä palvelimeen toisistaan riippumatta. Tämä mahdollistaa esimerkiksi eri SNMP version käytön eri suuntiin. Tässä toteutuksessa kuitenkin käytetään SNMP:n versiota 3. Se on ainoa versio joka siirtää ohjausviestit salattuna, ja käytössä oleva kytkinkin tukee versio 3:n käyttöä sillä erotuksella että käytettävä salaus on DES AES:n sijaan.

3.4.1 PacketFence palvelimen määrittely

Muokataan switches.conf tiedoston PF to switch osio alla olevan kuvion 14 mukaiseksi muuttaen AES DES:iksi.

```
SNMPVersion = 3
SNMPUserNameRead = readUser
SNMPAuthProtocolRead = MD5
SNMPAuthPasswordRead = authpwdread
SNMPPrivProtocolRead = AES
SNMPPrivPasswordRead = privpwdread
SNMPUserNameWrite = writeUser
SNMPAuthProtocolWrite = MD5
SNMPAuthPasswordWrite = authpwdwrite
SNMPPrivProtocolWrite = AES
SNMPPrivPasswordWrite = privpwdwrite
```

Kuvio 14. Switches.conf, PF to switch. (PacketFence käyttöopas 2012. 16.)

Liikenne kytkimeltä palvelimelle määritellään switches.conf tiedoston kohdassa switch to PF seuraavasti huomioiden jälleen salaus, AES > DES (ks. Kuvio 15).

```
SNMPVersionTrap = 3
SNMPUserNameTrap = readUser
SNMPAuthProtocolTrap = MD5
SNMPAuthPasswordTrap = authpwdread
SNMPPrivProtocolTrap = AES
SNMPPrivPasswordTrap = privpwdread
```

Kuvio 15. Swiches.conf, switch to PH. (PacketFence käyttöopas 2012. 17.)

3.4.2 Kytkimen konfigurointi

Koska tässä toteutuksessa otetaan käyttöön sekä Inline enforcement että VLAN isolation enforcement toiminnallisuudet, joudutaan osa kytkimen porteista konfiguroimaan toimimaan ikään kuin ne olisivat suoraan yhetydessä PacketFence palvelimeen. Tämä onnistuu käyttäen tarkoitukseen varattua VLAN verkkoa ID:llä 200. Portin konfiguraatio on muutoin yksinkertainen. Tässä tapauksessa portit Fa0/1-16 on määritelty toimimaan Inline portteina.

```
interface FastEthernet0/1
 description INLINE ENFORCEMENT
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
```

Spanning-tree portfast toiminto nopeuttaa huomattavasti portin toimintaa poistaen 30 sekunnin viiveen portin tilan vaihtuessa (Spanning tree portfast 2013).

Kytkimen portit Fa0/17-32 on määritetty toimimaan VLAN verkkojen avulla tapahtuvaan päätelaitteen hallintaan. Aiemmin esitellyitä SNMP toiminnallisuuksista valittiin Port Secutity parhaana vaihtoehtona testikäyttöön.

```
interface FastEthernet0/17
 description VLAN ENFORCEMENT PORT SECURITY
 switchport access vlan 4
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address 0200.0000.0017
```

Portti asetetaan lähtökohtaisesti tyhjään VLAN verkkoon 4, jolloin siihen liittyvä laite on eristetty kaikista muista verkon laitteista. Tässä verkossa ei myöskään ole mitään palvelua josta asiakas saisi osoitteen. Asetetaan portti port security tilaan ja rikkeen tapahduttua hylätään sisääntulevat paketit sekä ilmaistaan rike (Port-security violation). Jotta portti voi havaita jo ensimmäisen kytkeytyvän laitteen MAC-osoitteen muuttuessa, on portille annettava jokin teennäinen MAC-osoite lähtökohdaksi.

Seuraavaksi täytyy yksi portti määrittää PacketFencen ohjausliikennettä ja Inlinen toista verkkoliityntää varten. Tämän portin täytyy kyetä liikennöimään useilla eri VLAN ID:llä, joten portti täytyy asettaa trunk tilaan.

```
interface GigabitEthernet0/1
 description PF TRUNK
 switchport mode trunk
```

Vielä tarvitaan yksi ns. uplink portti, josta on yhteys tuotantoverkkoon. Portti asetetaan toimimaan oletus VLAN:issa ID 1. Kun PacketFence nyt asettaa jonkin

rekisteröityneen laitteen portin normaaliin liikennöintitilaan, pääsee se tämän uplink portin kautta kohdeverkon resursseihin, kunhan on saanut osoitteen tämän verkon DHCP-palvelimelta.

Seuraavaksi täytyy määrittää kytkin samaan SNMP tilaan kuin PacketFence palvelin aiemmin määriteltiin. Tarvittava esimerkki konfiguraatio on esitetty alla olevassa kuviossa 16. Taas tulee huomata, että vaihdetaan algoritmiksi kytkimen IOS:in tukema DES. Lisäksi SNMP-serverin osoitteeksi tulee valita oman PacketFencen osoite, tässä 192.168.100.16.

```
snmp-server engineID local AA5ED139B81D4A328D18ACD1
snmp-server group readGroup v3 priv
snmp-server group writeGroup v3 priv read v1default write v1default
snmp-server user readUser readGroup v3 auth md5 authpwdread priv aes 128
 privpwdread
snmp-server user writeUser writeGroup v3 auth md5 authpwdwrite priv aes 128
 privpwdwrite
snmp-server enable traps port-security
snmp-server enable traps port-security trap-rate 1
snmp-server host 192.168.0.50 version 3 priv readUser  port-security
```

Kuvio 16. Kytkimen SNMP konfiguraatio.

Jotta kytkintä voidaan hallita verkosta käsin, täytyy sille antaa hallintaa varten IP-osoite. Tämä tapahtuu antamalla osoite Vlan1 rajapinnalle seuraavasti:

```
interface Vlan1
 ip address 192.168.100.22 255.255.255.0
```

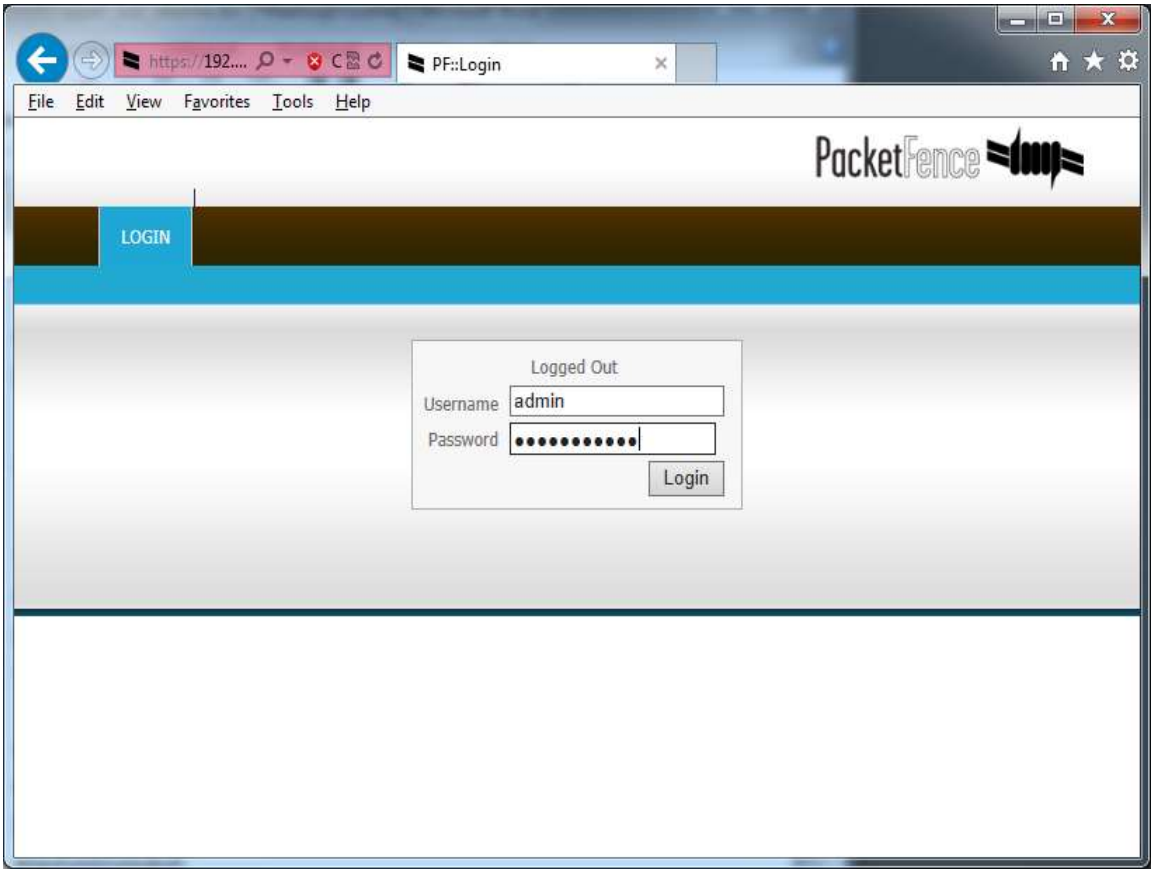
Näillä asetuksilla kytkimen pitäisi olla valmis testaamista varten. Kytkimen koko konfiguraatiotiedosto on esitetty liitteessä 3.

3.5 Toiminnan testaus

Toiminnan testaaminen voidaan aloittaa yksinkertaisella VLAN verkkojen välisen eristyksen testaamisella. Tämä testi kertoo lähinnä että kytkimen VLAN eivät vuoda

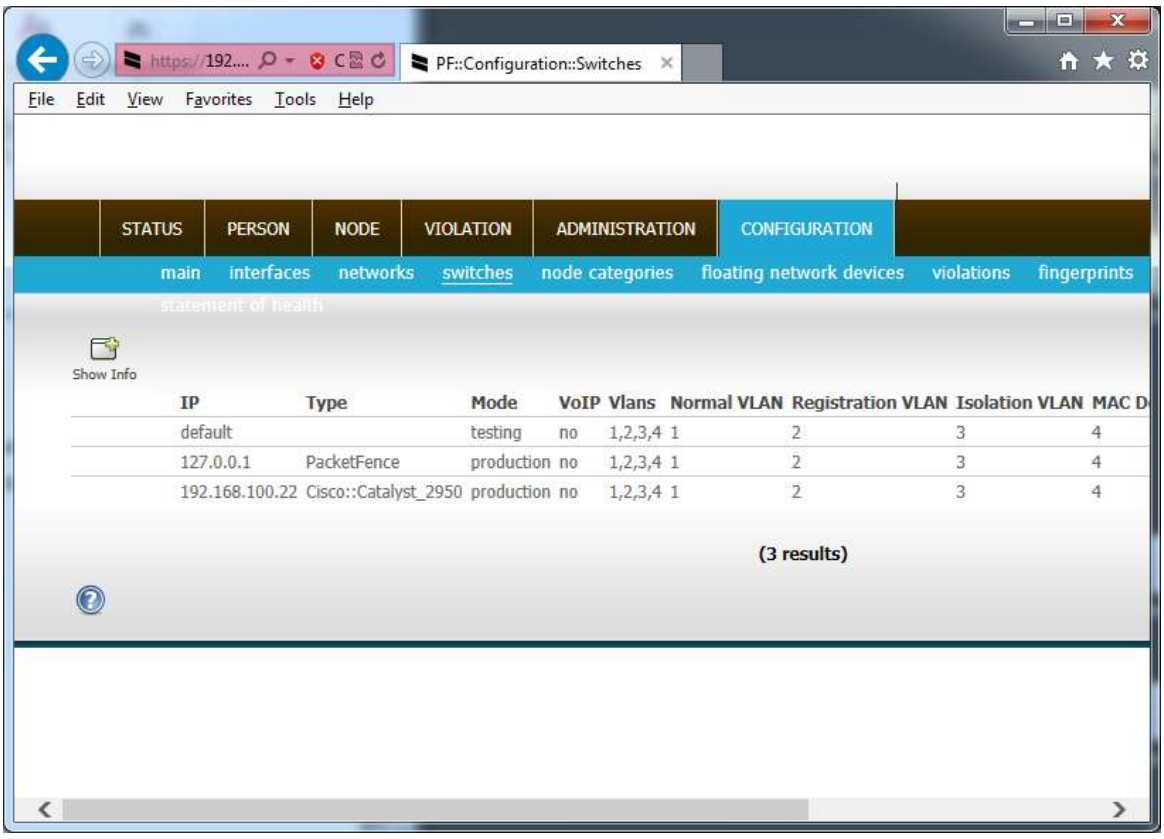
ja konfiguraatio on lähtökohtaisesti oikein. Testin kulku on kuvattu PacketFence ZEN asennusoppaan sivulla 11 (PacketFence ZEN asennusopas 2012).

Seuraavaksi siirrytään selainpohjaiseen hallintaan ja tarkastetaan että äsken lisätty kytkin näkyy hallittavien laitteiden listalla. Mene selaimella ositteeseen https://192.168.100.16:1443 ja anna avautuvalle sivulle aiemmin mainitut kirjautumistunnukset. Jos selain varottaa sertifikaatista voit jatkaa ottamalla harkitun riskin. Kuviossa 17 on esitetty kirjautumisikkuna.



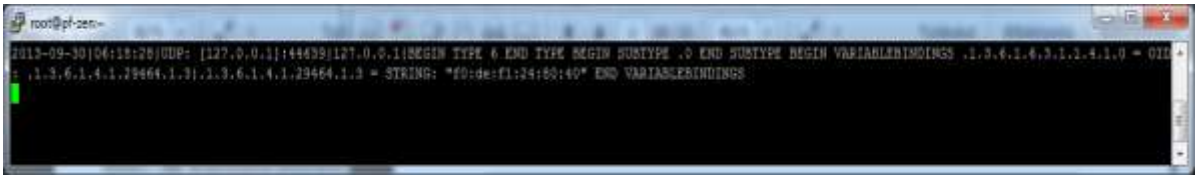
Kuvio 17. WWW-hallintaan kirjautuminen.

Kun olet onnistuneesti päässyt kirjautumaan sisään hallintasivuille, navigoi CONFIGURATION > switches välilehdelle. Tarkasta että äsken lisäämäsi kytkin näkyy listalla kuten alla olevassa kuviossa 18.

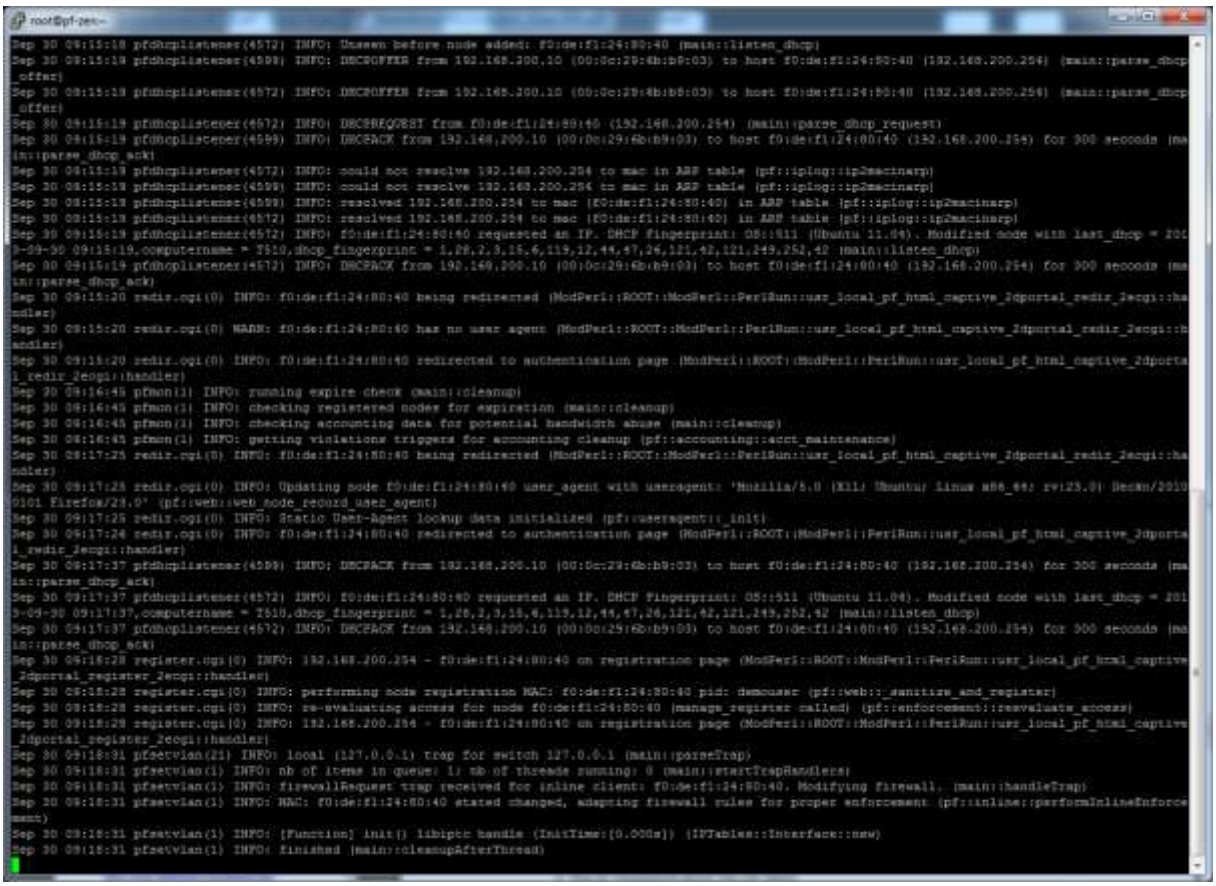


Kuvio 18. Lista hallittavista verkkolaitteista.

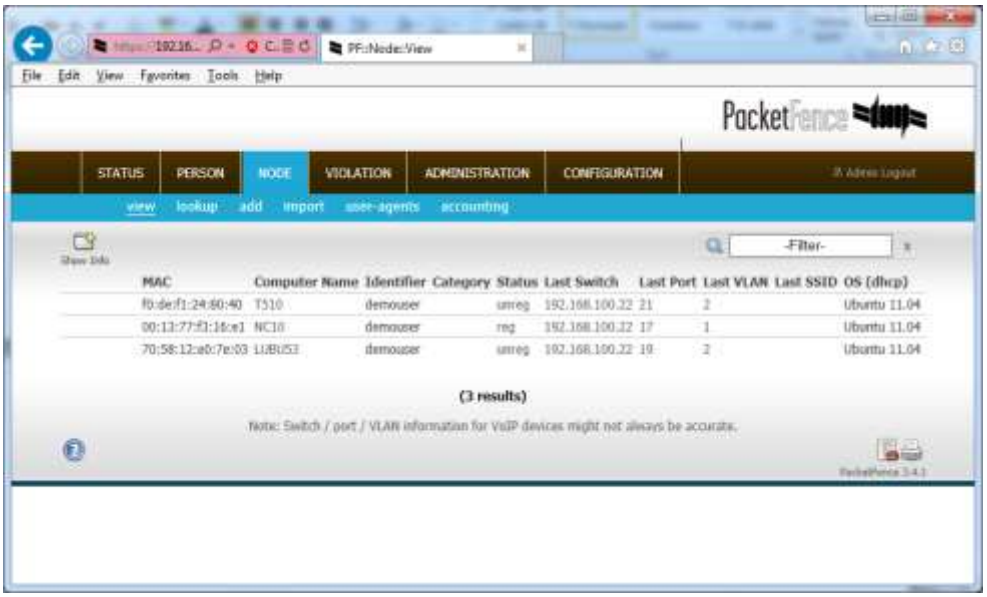
Seuraavaksi testataan päätelaitteen liittäminen Inline enforcement tilaan määritettyyn porttiin. Komennolla *tail -f /usr/local/pf/logs/packetfence.log* voidaan seurata palvelimen toimintaa rekisteröitymisen edetessä (ks. Kuvio 19). Komento *tail -f /usr/local/pf/logs/snmptrapd.log* taas kertoo PacketFencen vastaanottamat SNMP sanomat (ks. Kuvio 20). Nämä ovat hyödyllisiä tietoja etenkin vikatilanteita selvitettäessä. Verkkokaapeli kiinni portin Fa0/1 ja koneen T510 eth0 välille ja katsotaan mitä tapahtuu (ks. Kuvio 21).



Kuvio 19. Inline porttiin liitetyn laitteen aiheuttama SNMP liikenne.

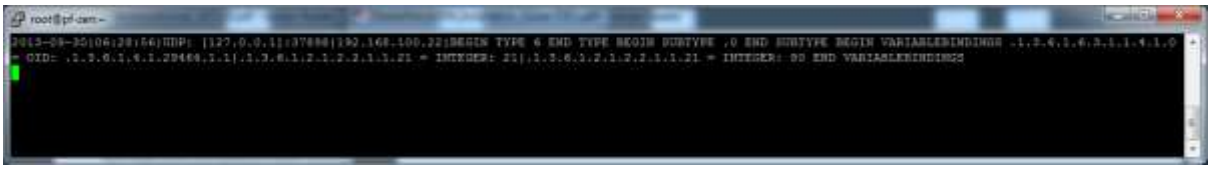


Kuvio 20. PacketFencen loki Inline porttiin rekisteröidyttäessä.

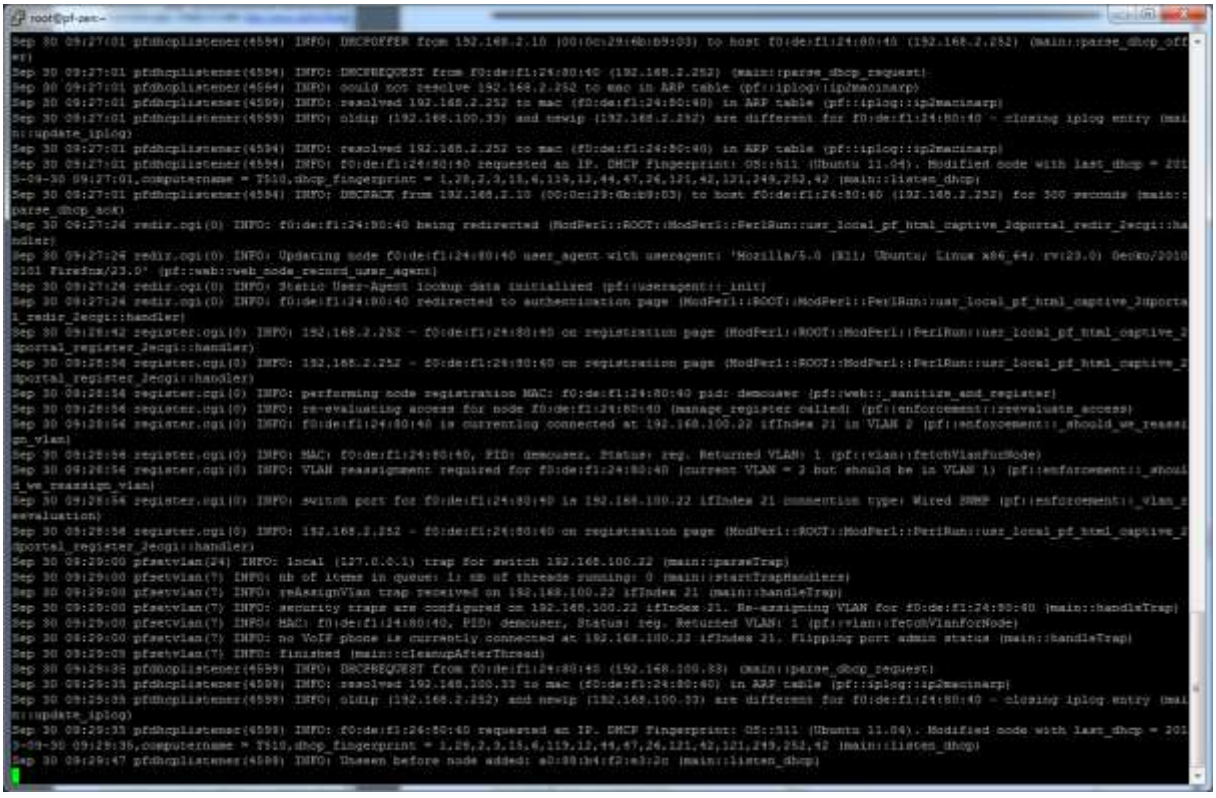


Kuvio 21. Tietokone T510 verkossa ennen rekisteröitymistä.

Seuraavaksi testataan samalla tavalla laitteen liittäminen VLAN enforcement tyypin porttiin, lokti esitetty kuvioissa 22 ja 23. Muista välillä käydä WWW-hallinnasta NODE > view välilehdeltä vaihtamassa päätelaitteen tila ”unreg”. Muuten laite pääsee suoraan verkkoon edellisen kirjautumisen perusteella.



Kuvio 22. SNMP loki VLAN enforcement tilanteessa.



Kuvio 23. PacketFencen loki VLAN enforcement laitteella.

Molemmilla tavoilla voitiin todeta toiminta oikeaksi ja kohdeverkon palvelut saavutettiin. Myös laitteen tilan vaihtaminen unregiksi sai yhteyden katkeamaan ja laite eristettiin kohdeverkosta.

Näin ollen käyttöönotto voitiin todeta onnistuneeksi ja järjestelmä toimintakykyiseksi.

4 POHDINTAA

4.1 Lähtökohdat

Työn tarkoituksena oli tutustua vapailla ohjelmistoilla toteutettuun tietoverkon pääsynhallintaan, NAC:iin. Toimeksiantajalla oli valmis ehdokas, PacketFence, jota lähdettiin tutkimaan. Pian osoittautuikin että kyseinen tuote on vapaiden ohjelmistojen monipuolisimmasta ja laadukkaimmasta päästä. Kehitystyö jatkuu edelleen voimakkaana, ja toteutus löytyy myös monen kaupallisen tuotteen taustalta.

Ominaisuuksiltaan varsin monipuolinen PacketFence soveltuu moneen käyttöön, eikä se laajuudestaan huolimatta ole kovinkaan monimutkainen käytettävä, varsinkaan käyttöönoton jälkeen. Hallinta tapahtuu joko komentokehotteesta käsin muokkaamalla muutamaa konfiguraatiotiedostoa, tai sitten informatiivisen selainpohjaisen käyttöliittymän kautta. Aivan kaikkea ei voida WWW-hallinan kautta toteuttaa, mutta peruskäyttö, kuten käyttäjien ja verkkolaitteiden lisääminen onnistuu.

Dokumentaatio on varsin laaja ja helppolukuinen; eri tilanteita varten on omat opuksensa, joten tarvittava tieto löytyy helposti kahlaamatta järkälemäistä opusta kannesta kanteen. Myös yhteisön tarjoaman tuki postituslistojen muodossa tarjoaa tukea ja vastauksia ongelmatilanteissa.

PacketFencen virtuaaliversion käyttö opetusympäristössä onnistuisi mielestäni erittäin hyvin. Etukäteen valmistellut virtuaalikoneet, ja erilaiset verkkolaite- ja konfiguraatiovaihtoehdot toisivat monipuolisen opetusympäristön useille tekniikoille. Vianhakua ja debuggausta olisi helppo käyttää opetuksen apuna.

Opinnäytetyötä tehdessä ideat PacketFencen monipuolisuudesta johtuen alkoivat kumpuamaan toinen toistaan käyttökelpoisempia toteutuksia. Sivutuotteena syntyi esimerkiksi mökkikylän vierailijaverkon käyttäjien hallintaan käypä sovellus. Erilaisten käyttäjätikettien tulostaminen ja liikenteen suodattaminen onnistuu yksinkertaisesti WWW-hallinan kautta valmiita sääntöjä käyttäen.

4.2 Jatkotoimenpiteet

Kehitysideoita tuli runsaasti mieleen työn edetessä. Jatkotoimenpiteinä voisi ottaa käyttöön laitteiden hallinnan ja rekisteröimisen lisäksi roolipohjaisia tunnistamisia erityyppisten laitteiden automaattista rekisteröintiä varten.

Inline toteutuksessa voisi tutkia jo oletuksena käytössä olevan Snortin mahdollisuuksia. Kuormittavat P2P-ohjelmat saataisiin kuriin verkosta jne.

Myös DHCP-sormenjälkiin perustuva laitteiden valikoiva suodatus on mielenkiintoinen ominaisuus, esimerkiksi erilaisten pelikonsoleiden eristäminen verkosta olisi helppo toteuttaa sen avulla.

PacketFence tarjoaa niin monipuolisen mahdollisuuden ominaisuuksiensa ja mukautettavuuden johdosta, että sen käytölle tuntuu löytyvän jatkuvasti uusia mahdollisuuksia. Etenkin vastikään julkaistu USB-muistilta ajettava live-versio kutsuu kokeilemaan PacketFenceä mitä moninaisimpiin tarkoituksiin.

LÄHTEET

Ajan asettaminen. 2010. CentOS käyttöjärjestelmän kellonajan ja päiväyksen asettaminen. Viitattu 24.9.2013. http://www.fir3net.com/Redhat-/-Fedora/how-to-set-the-time-date-and-timezone-in-centos.html

Autentikointiprotokollat. 2008. Cisco. Viitattu 22.9.2013 http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.shtml

Commercial support. 2013. Tuotteen kaupallinen tuki. Viitattu 18.9.2013. http://www.inverse.ca/english/support.html

Cram Session. n.d. Open source players show a knack for NAC. Viitattu 25.9.2013. http://www.networkworld.com/dimension/symantec/newsOpensource.html

EAP, protokollan toiminta. 2004. ftp://ftp.rfc-editor.org/in-notes/rfc3748.txt

Fingerbank. 2013. http://www.fingerbank.org/more_info.html

MAC Authentication Bypass. 2007. Viitattu 22.9.2013 http://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a008087ad6f.pdf

New Leadership! 2008. Uuden pääkehittäjän mukaantulo. Viitattu 18.9.2013 http://www.packetfence.org/news/2008/article/new-leadership-1.html

PacketFencen ominaisuudet, 2013. http://www.packetfence.org/about/advanced_features.html

PacketFence käyttöopas, versio 3.4.1. 2012. Viitattu 19.9.2013.
http://inverse.ca/downloads/PacketFence/doc/PacketFence_Administration_Guide-3.4.1.pdf

PacketFence overview. 2013. Yleiskatsaus järjestelmään. Viitattu 18.9.2013.
http://www.packetfence.org/about/overview.html

PacketFence releases. 2013. Julkaisuvaihtoehdot. Viitattu 18.9.2013.
http://www.packetfence.org/download/releases.html

PacketFence ZEN asennusopas. 2012. Viitattu 25.9.2013
http://inverse.ca/downloads/PacketFence/doc/PacketFenceZEN_Installation_Guide-3.4.1.pdf

PacketFenfen tekninen esittely. 2013. Viitattu 22.9.2013.
http://www.packetfence.org/about/technical_introduction.html

Port-security violation. N.d. Viitattu 26.9.2013.
http://www.cisco.com/web/techdoc/dc/reference/cli/nxos/commands/l2/switchport_port-security_violation.html

RFC 2616, HTTP 1.1, 2013. http://tools.ietf.org/html/rfc2616#section-14.43

Snort, 2013. Viitattu 28.11.2013 http://www.snort.org/snort

Spanning tree portfast. 2013. Viitattu 26.9.2013.
http://www.informit.com/library/content.aspx?b=CCNP_Studies_Switching&seqNum=36

Zero effort NAC. 2013. ZEN-version ajantasaiset jakelut. Viitattu 18.9.2013.
http://www.packetfence.org/download/zen.html

LIITTEET

Liite 1. PacketFencen yleiset asetukset, pf.conf

```
[general]
#
# general.domain
#
# Domain name of PacketFence system.
domain=elisa
#
# general.hostname
#
# Hostname of PacketFence system.  This is concatenated with the domain in Apache
rewriting rules and therefore must be resolvable by clients.
hostname=pf-zen
#
# general.logo
#
# Logo displayed on web pages.
logo=/common/packetfence-cp.png
#
# general.dnsservers
#
# Comma-delimited list of DNS servers.  Passthroughs are created to allow queries to
these servers from even "trapped" nodes.
dnsservers=4.2.2.2,192.168.100.1
#
# general.dhcpservers
#
# Comma-delimited list of DHCP servers.  Passthroughs are created to allow DHCP
transactions from even "trapped" nodes.
dhcpservers=192.168.100.1,192.168.2.10,192.168.3.10,192.168.200.10
#
# general.locale
#
# Locale used for message translation
# more than 1 can be specified
locale=en_US
#
# general.timezone
#
# System's timezone in string format. Supported list:
# http://www.php.net/manual/en/timezones.php
timezone=Europe/Helsinki
```

```
#
# general.maintenance_interval
#
# Interval at which Packetfence runs its maintenance tasks.
#maintenance_interval=60s
[trapping]
# trapping.range
#
# Comma-delimited list of address ranges/CIDR blocks that PacketFence will
monitor/detect/trap on.  Gateway, network, and
# broadcast addresses are ignored.
range=192.168.2.0/24,192.168.3.0/24,192.168.200.0/24
#
# trapping.registration
#
# If enabled, nodes will be required to register on first network access.  Further
registration options are configured in the
# registration section.
registration=enabled
#
# trapping.dectection
#
# If enabled, nodes will be trapped if triggering a SNORT rules.
detection=enabled

#
[database]
#
# database.pass
#
# Password for the mysql database used by PacketFence.
pass=pfz3n

[interface eth0]
ip=192.168.100.16
mask=255.255.255.0
type=management
gateway=192.168.100.1

[interface eth0.200]
ip=192.168.200.10
mask=255.255.255.0
type=internal,monitor
enforcement=inline
gateway=192.168.200.10

# REMOVE COMMENT TO ENABLE VLAN MODE
[interface eth0.2]
ip=192.168.2.10
```

```
mask=255.255.255.0
type=internal
enforcement=vlan
gateway=192.168.2.10

[interface eth0.3]
ip=192.168.3.10
mask=255.255.255.0
type=internal
enforcement=vlan
gateway=192.168.3.1

[guests_self_registration]
modes=email,sms,sponsor

[registration]
guests_self_registration=disabled
#[interface eth0.5]
#ip=192.168.5.10
#mask=255.255.255.0
#type=internal
#enforcement=vlan
#gateway=192.168.5.1
#[interface eth0.10]
#ip=192.168.1.10
#mask=255.255.255.0
#type=internal
#gateway=192.168.1.1
#authorizedips=
```

Liite 2. PacketFencen verkkolaitteiden määrittelyt, switshes.conf

```
# Copyright 2006-2008 Inverse inc.
#
# See the enclosed file COPYING for license information (GPL).
# If you did not receive this file, see
# http://www.fsf.org/licensing/licenses/gpl.html

[default]
vlans = 1,2,3,4
normalVlan = 1
registrationVlan = 2
isolationVlan = 3
macDetectionVlan = 4
#guestVlan = 5
#customVlan1 =
#customVlan2 =
#customVlan3 =
```

```
#customVlan4 =
#customVlan5 =
VoIPEnabled = no
voiceVlan =

mode = testing
macSearchesMaxNb = 30
macSearchesSleepInterval = 2
uplink = dynamic

#
# Command Line Interface
#
# cliTransport could be: Telnet, SSH or Serial
cliTransport = Telnet
cliUser =
cliPwd =
cliEnablePwd =

#
# SNMP section
#

# PacketFence -> Switch
SNMPVersion = 2c
SNMPCommunityRead=pfence
SNMPCommunityWrite=pfence

# Switch -> PacketFence
SNMPVersionTrap = 2c
SNMPCommunityTrap=pfence

#
# Web Services Interface
#
# wsTransport could be: http or https
wsTransport = http
wsUser =
wsPwd =
#
# RADIUS NAS Client config
#
# RADIUS shared secret with switch
radiusSecret=

[127.0.0.1]
type = PacketFence
mode = production
uplink = dynamic
```

```
[192.168.100.22]
type = Cisco::Catalyst_2950
mode = production
uplink = 50
#radiusSecret = s3cr3t
SNMPVersion = 3
SNMPEngineID = 8000000903000015638D02C1
SNMPUserNameRead = readUser
SNMPAuthProtocolRead = MD5
SNMPAuthPasswordRead = authpwdread
SNMPPrivProtocolRead = DES
SNMPPrivPasswordRead = privpwdread
SNMPUserNameWrite = writeUser
SNMPAuthProtocolWrite = MD5
SNMPAuthPasswordWrite = authpwdwrite
SNMPPrivProtocolWrite = DES
SNMPPrivPasswordWrite = privpwdwrite
SNMPVersionTrap = 3
SNMPUserNameTrap = readUser
SNMPAuthProtocolTrap = MD5
SNMPAuthPasswordTrap = authpwdread
SNMPPrivProtocolTrap = DES
SNMPPrivPasswordTrap = privpwdread
```

Liite 3. Cisco 2950-kytkimen konfoguraatio

```
Current configuration : 7806 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname PF
!
!
username cisco privilege 15 password 0 cisco
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
```

```
interface FastEthernet0/1
 description INLINE ENFORCEMENT
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/2
 description INLINE ENFORCEMENT
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/3
 description INLINE ENFORCEMENT
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/4
 description INLINE ENFORCEMENT
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/5
 description INLINE ENFORCEMENT
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/6
 description INLINE ENFORCEMENT
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/7
 description INLINE ENFORCEMENT
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/8
 description INLINE ENFORCEMENT
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/9
```

```
 description INLINE ENFORCEMENT
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/10
 description INLINE ENFORCEMENT
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/11
 description INLINE ENFORCEMENT
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/12
 description INLINE ENFORCEMENT
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/13
 description INLINE ENFORCEMENT
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/14
 description INLINE ENFORCEMENT
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/15
 description INLINE ENFORCEMENT
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/16
 description INLINE ENFORCEMENT
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/17
 description VLAN ENFORCEMENT PORT SECURITY
```

```
 switchport access vlan 4
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address 0200.0000.0017
!
interface FastEthernet0/18
 description VLAN ENFORCEMENT PORT SECURITY
 switchport access vlan 4
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address 0200.0000.0018
!
interface FastEthernet0/19
 description VLAN ENFORCEMENT PORT SECURITY
 switchport access vlan 4
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address 0200.0000.0019
!
interface FastEthernet0/20
 description VLAN ENFORCEMENT PORT SECURITY
 switchport access vlan 4
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address 0200.0000.0020
!
interface FastEthernet0/21
 description VLAN ENFORCEMENT PORT SECURITY
 switchport access vlan 4
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address 0200.0000.0021
!
interface FastEthernet0/22
 description VLAN ENFORCEMENT PORT SECURITY
 switchport access vlan 4
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address 0200.0000.0022
!
interface FastEthernet0/23
 description VLAN ENFORCEMENT PORT SECURITY
 switchport access vlan 4
```

```
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address 0200.0000.0023
!
interface FastEthernet0/24
 description VLAN ENFORCEMENT PORT SECURITY
 switchport access vlan 4
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address 0200.0000.0024
!
interface FastEthernet0/25
 description VLAN ENFORCEMENT PORT SECURITY
 switchport access vlan 4
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address 0200.0000.0025
!
interface FastEthernet0/26
 description VLAN ENFORCEMENT PORT SECURITY
 switchport access vlan 4
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address 0200.0000.0026
!
interface FastEthernet0/27
 description VLAN ENFORCEMENT PORT SECURITY
 switchport access vlan 4
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address 0200.0000.0027
!
interface FastEthernet0/28
 description VLAN ENFORCEMENT PORT SECURITY
 switchport access vlan 4
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address 0200.0000.0028
!
interface FastEthernet0/29
 description VLAN ENFORCEMENT PORT SECURITY
 switchport access vlan 4
 switchport mode access
```

```
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address 0200.0000.0029
!
interface FastEthernet0/30
 description VLAN ENFORCEMENT PORT SECURITY
 switchport access vlan 4
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address 0200.0000.0030
!
interface FastEthernet0/31
 description VLAN ENFORCEMENT PORT SECURITY
 switchport access vlan 4
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address 0200.0000.0031
!
interface FastEthernet0/32
 description VLAN ENFORCEMENT PORT SECURITY
 switchport access vlan 4
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address 0200.0000.0032
!
interface FastEthernet0/33
!
interface FastEthernet0/34
!
interface FastEthernet0/35
!
interface FastEthernet0/36
!
interface FastEthernet0/37
!
interface FastEthernet0/38
!
interface FastEthernet0/39
!
interface FastEthernet0/40
!
interface FastEthernet0/41
!
interface FastEthernet0/42
!
interface FastEthernet0/43
```

```
!
interface FastEthernet0/44
!
interface FastEthernet0/45
!
interface FastEthernet0/46
!
interface FastEthernet0/47
!
interface FastEthernet0/48
!
interface GigabitEthernet0/1
 description PF TRUNK
 switchport mode trunk
!
interface GigabitEthernet0/2
 description UPLINK to prod network VLAN 1
 switchport mode access
!
interface Vlan1
 ip address 192.168.100.22 255.255.255.0
 no ip route-cache
define interface-range inline FastEthernet0/1 - 16
define interface-range ps FastEthernet0/17 - 32
define interface-range 8021x FastEthernet0/33 - 48
!
no ip http server
snmp-server group readGroup v3 priv notify *tv.00000000.80000000.00000000
snmp-server group writeGroup v3 priv write v1default
snmp-server enable traps port-security
snmp-server enable traps port-security trap-rate 1
snmp-server host 192.168.100.16 version 3 priv readUser  port-security
!
line con 0
 privilege level 15
line vty 0 4
 exec-timeout 30 0
 login local
line vty 5 15
 exec-timeout 30 0
 login local
!
!
end
```