UNIVERSITAT POLITÈCNICA DE VALÈNCIA

ESCOLA POLITÈCNICA SUPERIOR DE GANDIA

Grau en Enginyeria de Sistemes de Telecomunicacions, So i Imatge

---

"Configuració de seguretat perimetral en una xarxa domèstica utilitzant projectes open source"

TREBALL FINAL DE GRAU

Autor:
Rafael Bono Aguilar

Tutor:
Jaime Lloret Mauri

Per als meus pares, raó principal de que haja pogut cursar aquesta carrera i vertaders herois en aquest treball que culmina quatre anys d'esforç per part meva, i tota una vida d'esforç per part seva. A ells, Rafa i Fani, és a qui dedique aquesta última i més important entrega. Gràcies, pares.

Al meu germà Joan, el que espere que prompte entregue un projecte i siga l'enginyer que ha demostrat ser a la seva feina, i amb l'impagable ajuda que m'ha proporcionat amb el desenvolupament d'aquesta infraestructura. Tu has sigut el motiu principal del meu interès en la seguretat informàtica, així que gràcies per haver-me descobert aquest món i gràcies, sobretot, per estar sempre al meu costat.

Com no, també vull dedicar aquest treball als meus companys i amics de SGS, font inesgotable d'aprenentatge des que vaig començar a treballar amb ells, i la raó principal per la que m'haja quedat al món de la seguretat informàtica. A vosaltres també, moltes gràcies.

Als meus amics de la universitat, que se que per molt que les circumstàncies de la vida ens allunyen, ni la mort evitarà que sempre us guarde amb el millor record que una persona pot desitjar. A tots vosaltres, mil gràcies per haver fet de la meva vida universitària una vertadera aventura, i haver-me fet sentir un vertader amic i germà.

Per últim, i no menys important, agrair a la meva companya, la meva amiga, el meu suport durant tot aquest trajecte. Gràcies per estar al meu costat els dies d'estrès, de nervis abans dels exàmens, de mals i bons moments, tant a la universitat, com al treball, com al meu dia a dia. Sense tu, tot s'hagués fet una mica més difícil. Moltíssimes gràcies, Roser.

Índex

Llistat d'images

1. Introducció

1.1 – Introducció

A l'actualitat, la seguretat informàtica està creixent a un ritme molt ràpid degut a que cada vegada podem trobar noves amenaces front a vulnerabilitats als sistemes informàtics. Aquestes amenaces poden tindre diversos tipus de finalitats, que poden anar des de interessos únicament econòmics, com pot ser el fet de demanar un rescat per a que l'usuari afectat puga recuperar les dades encriptades per un *ransomware*; fins a la recol·lecció d'informació personal d'un usuari o altres dades més crítiques que es poden allotjar a una base de dades, com poden ser comptes bancaris o correus electrònics amb contingut informatiu altament classificat; passant per un *Command & Control* dels equips infectats, per realitzar altre tipus de accions de forma remota.

La majoria de països compten amb agències d'intel·ligència, dedicades a la protecció i l'anàlisi de possibles vulnerabilitats a les infraestructures d'informació estatal o de persones que necessiten un nivell de protecció elevat en quan a la seva informació diària, com seria un cap d'estat o un alt càrrec governamental.

Cada vegada és més comú que als exèrcits dels diferents països del món s'estiguen creant divisions de *hackers*, dedicats a intentar recaptar aquesta informació classificada, així com a intentar penetrar a diversos sistemes per espiar usuaris i poder fer un seguiment de les seves activitats, aprofitant vulnerabilitats no conegudes (*Zero-Days*) per infiltrar-se als seus equips electrònics.

Per fer front a aquests atacs, es van desenvolupar antivirus o escàners d'arxius, que es basaven en una sèrie de patrons que buscaven per saber si podia ser perillós o no, però pronte els *hackers* van poder trobar la forma de fer front a aquests escàners, degut a que podien modificar els patrons que buscaven aquestes eines per a que no detectés els virus com a tal. Els antivirus per altra banda, no feien front a intrusions als sistemes, pel que no hi havia cap forma de detectar connexions il·legítimes a un sistema, ja que aquestes podien tindre lloc sense la necessitat de que s'infectés un ordinador amb un virus per poder accedir a ella. És per aquests motius que va sorgir la necessitat d'implementar un nou tipus de seguretat a les capes externes d'una xarxa connectada a Internet. Per fer front a aquestes amenaces, es va implementar la seguretat perimetral de xarxa, ubicada entre aquesta i l'accés a Internet de tots els dispositius que la componen, per a la que s'han desenvolupat una sèrie de dispositius electrònics molt especialitzats en realitzar deteccions i prevencions d'intrusions de forma molt específica i amb un alt potencial de rendiment per a l'anàlisi de tràfic dins d'aquesta xarxa securitzada, que trobarem cada vegada més segmentada per poder separar els distints elements que la formen segons el seu nivell de criticitat en quan al al tipus d'informació que es pot trobar en ells.

És per això que en aquest treball ens disposarem a crear una xarxa domèstica a la que introduirem elements de seguretat perimetral Open Source. Tots aquests elements, que anirem explicant, ofereixen solucions de seguretat a grans xarxes amb informació i tràfic crític i molt delicat, però a canvi d'un cost econòmic molt elevat. A un entorn domèstic, com que el volum de tràfic i la quantitat d'informació confidencial que pot haver no és tan elevada com, per exemple, a un banc, amb elements software de distribució lliure virtualitzats podrem protegir el nostre entorn, degut a que mai seria rentable assumir un cost per hardware dedicat a la seguretat per salvaguardar una xarxa domèstica.

1.2 – Objectius

Amb aquest treball, s'intentarà donar una visibilitat de la senzillesa amb la que qualsevol usuari amb coneixements de xarxa pot configurar la seva pròpia xarxa securitzada al seu propi entorn domèstic, així com realitzar instal·lacions a més gran escala, depenent de les necessitats a les que s'haja de fer front, considerant necessària la securització de totes les xarxes, independentment de la seva magnitud.

Per tant, podem concretar que els objectius específics serien els següents:

- Donar a conèixer els distints elements que es poden trobar a una xarxa perimetral.
- Oferir solucions de seguretat de caràcter Open Source.
- Explicar com desenvolupar una xarxa de seguretat perimetral.
- Explicar com configurar els elements que composen una xarxa perimetral.
- Comprovar la seguretat interna d'una xarxa.

1.3 – Precedents del projecte

Fins a dia d'avui, a l'Escola Politècnica Superior de Gandia no s'ha realitzat cap projecte relacionat amb la seguretat perimetral de xarxa o la seguretat informàtica degut a que és un àmbit de les telecomunicacions en el que no es focalitza al llarg de les dues branques de telecomunicacions que s'imparteixen.

L'interès per la Seguretat Informàtica és un un tema que es tracta cada vegada més als sectors de les telecomunicacions i a les grans empreses que ofereixen serveis en línia, com poden ser tendes, bancs, serveis sanitaris o de telecomunicacions. Altre factor influent és el creixement que està experimentant aquest sector, junt a tots els problemes relacionats amb la seguretat informàtica o atacs informàtics que sorgeixen cada dia als mitjans de comunicació, fet que està generant un increment de l'expectació i la demanda per aquells àmbits empresarials dedicats a les Tecnologies de la Informació.

1.4 – Estructura del projecte

En primer lloc, introduirem al lector en la seguretat informàtica i especificarem què és la seguretat perimetral de xarxa i en què consisteix, on es llistaran i es farà un anàlisi dels elements més comuns que podem trobar a una infraestructura de seguretat perimetral, quines són les seves funcions dins d'aquesta xarxa o es citaran alguns exemples de dispositius que solen ser els més utilitzats, bé siguen Open Source o de pagament. També es farà referència a la normativa actual en relació a la seguretat informàtica.

A continuació, estudiarem quines són les nostres necessitats per poder dissenyar la infraestructura de la nostra xarxa, i haurem d'identificar, una vegada conegudes les necessitats i els requeriments, quins elements de seguretat anem a implementar, per així poder dissenyar l'esquema de xarxa de la nostra infraestructura.

La següent part, la dedicarem completament a la implementació de tota la xarxa i a la configuració i la parametrització de tots els elements de seguretat que la conformaran. Inicialment, configurarem la xarxa a nivell d'enrutament, assignant, en cas de ser necessari, IP estàtiques als equips que ho requerisquen. Una vegada les IP dels equips estiguen

repartides, procedirem a crear les regles de protecció per als equips que gestionarem segons la política de seguretat que necessitem aplicar en cada segment de la xarxa. Per finalitzar la part d'implementació, dotarem la nostra xarxa d'un sistema de monitorització d'alertes de seguretat, el qual podrem utilitzar per veure tots els atacs o qualsevol comportament anòmal que pogueren afectar a la nostra infraestructura domèstica.

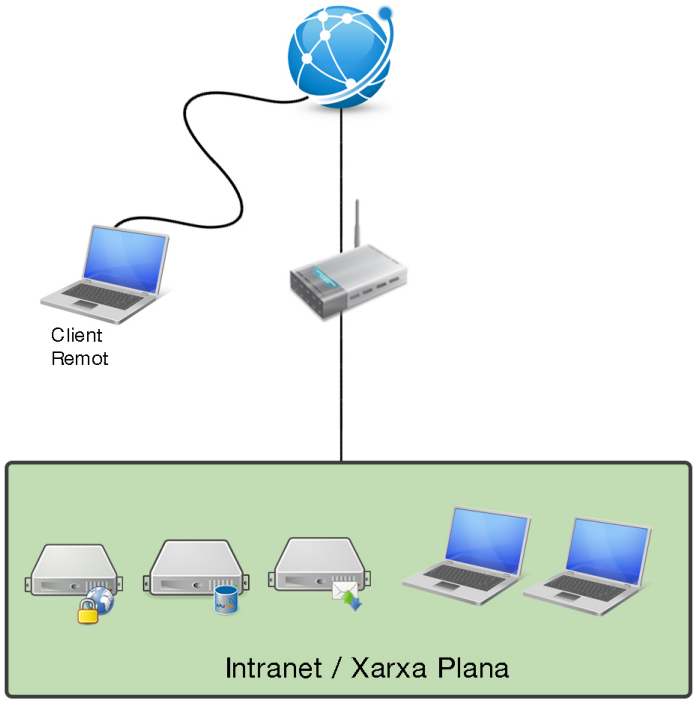
Per concloure el projecte, analitzarem els resultats finals i comprovarem el correcte funcionament de tots els elements ajudant-nos amb un escàner de vulnerabilitats.

2. La seguretat perimetral de xarxa

2.1 – Què és la seguretat perimetral i quina és la finalitat?

La seguretat perimetral de xarxa és el conjunt d'elements d'una infraestructura de xarxa interna a la que disposen de seguretat front a altra xarxa externa, anomenada Internet.

Generalment, les arquitectures sense seguretat perimetral es caracteritzen per ser xarxes planes i sense segmentar, on no es filtra tràfic ni a l'entrada ni a l'eixida a Internet i on els clients remots poden accedir directament als serveis de la xarxa, bé siguen basses de dades o clients de correu electrònic sense la necessitat de passar a través de cap tipus d'autenticació ni certificació per accedir a les dades que hi ha al seu interior. A la *Imatge 1* podem observar la topologia d'una xarxa interna que no compta amb una securització perimetral:

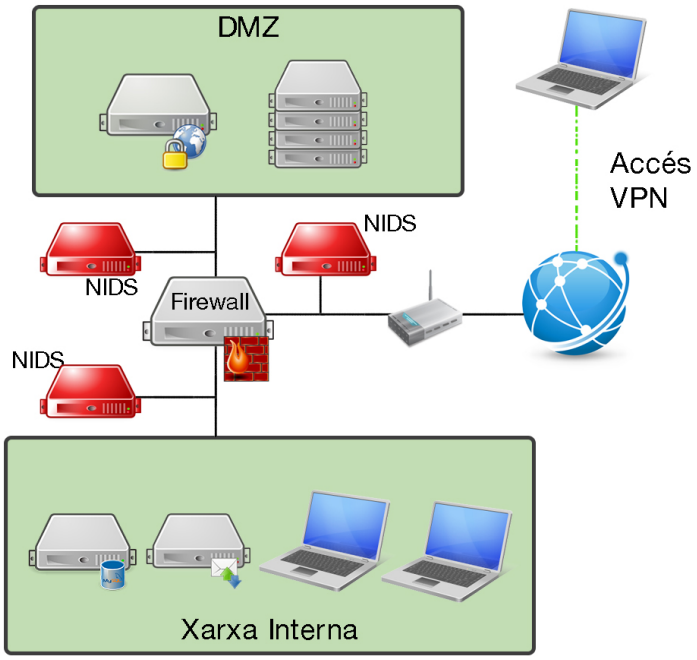


Imatge 1. Topologia d'una xarxa sense seguretat perimetral

Les xarxes amb seguretat perimetral no sempre tenen la mateixa disposició ni segueixen un patró [1]. Tot depèn de les necessitats de cada client i de la magnitud que puga tindre la infraestructura. A una arquitectura que disposa de seguretat perimetral, podem trobar dos segmentacions clarament diferenciades, anomenades DMZ (Demilitarized Zone) i Xarxa Interna. A la DMZ solen trobar-se els servidors de correu electrònic, els servidors Web i els servidors DNS (*Domain Name System*), pel que pot oferir servei a l'exterior sense comprometre la xarxa interna en cas d'intrussió, encara que els serveis que oferix son una espècie de pont entre Internet i la Xarxa Interna. La DMZ està dividida de la Xarxa Interna i d'Internet mitjançant Firewalls i, en certes ocasions, per altres

equips de seguretat. El tràfic d'aquesta infraestructura es filtra i es monitoritza constantment. A més, els usuaris que vulguin accedir a la xarxa interna, ho hauran de fer mitjançant un túnel VPN (*Virtual Private Network*) utilitzant autenticació, que pot ser una contrasenya emmagatzemada en local, un certificat d'usuari instal·lat a la màquina que es connecta o bé un toquen que es genera cada vegada i és enviat, per exemple, mitjançant un SMS a un mòbil donat d'alta per a l'usuari que pretén accedir a la VPN.

Tal i com es mostra a la *Imatge 2*, la topologia d'una xarxa amb seguretat perimetral compta amb una sèrie d'elements que segmenten la infraestructura en subxarxes més menudes i perfectament aïllades entre sí, gràcies a aquests dispositius dedicats a la detecció, prevenció i bloqueig d'intrusions, com els Firewalls o els NIDS (*Network Intrussion Detection Systems*), que analitzarien cadascun d'aquests segments en busca de possibles amenaces o intrusions no legítimes:



Imatge 2. Topologia d'una xarxa amb seguretat perimetral

2.2 – Elements habituals a una xarxa de seguretat perimetral

Com ja hem comentat anteriorment, no a totes les xarxes amb seguretat perimetral podem trobar tots els elements que anem a citar a continuació, ja que pot variar segons la necessitat de la infraestructura de xarxa i el nivell de seguretat que es vulga implementar a aquesta. Generalment, els elements més comuns a una infraestructura amb seguretat perimetral compta amb els següents elements:

- *SIEM* (*Security Information and Event Management*): És un sistema de monitorització d'events informació d'alertes de seguretat. Els distints dispositius de seguretat d'una infraestructura poden configurar-se per a que envien *logs* al SIEM per a poder monitoritzar tots els events, que bé poden ser de seguretat o d'estat del dispositiu. Depenent de la necessitat de la xarxa, també es poden enviar *logs* (arxius de registre que contenen tota la informació del dispositiu que necessitem extraure, depenent de la configuració que s'aplique) des d'altres equips que formen part d'aquesta, sense necessitat de que aquests siguen equips destinats a la seguretat, com és el cas d'alguns switchs que tenen la capacitat d'enviar informació al SIEM per a poder traçar rutes de fluxe d'informació dins la xarxa o servidors de bases de dades que poden enviar registres on s'audita quin usuari ha accedit a un fitxer determinat i quines accions ha realitzat sobre aquest, per exemple. La característica més important d'un SIEM és que pot correlar events buscant atributs comuns a tots els registres que rep i agrupant-los per poder convertir les dades dels *logs* en informació. Tota aquesta informació és guardada pel SIEM per a que després d'un temps determinat, es puga accedir a aquesta informació mitjançant cerques i per a que es puga utilitzar per a anàlisis forense de seguretat. Un exemple de SIEM podrien ser QRadar (IBM [Propietari]), ArcSight (HP [Propietari]), OSSIM (AlienVault [Open Source]) o SIEMonster (Kustodian [Open Source]).

- *Firewall*: Element de la xarxa en el que es defineix la política d'accés, tant d'entrada com d'eixida, permetent o denegant el tràfic, segons estiguen definides les seves regles o polítiques, que poden ser restrictives (també anomenades llistes blanques, en les que es denega tot excepte el que s'accepta explícitament) o permissives (també anomenades llistes negres, en les que es permet tot excepte allò que es denega expressament). Utilitza tres regles bàsiques, que poden ser *deny* (bloqueig d'una connexió), *allow* (autorització d'una connexió) o *drop* (redirecció d'una petició de connexió sense donar un avís previ a l'emissor d'aquesta). Els Firewalls poden filtrar per aplicació, per port, per protocol o per IP d'origen o destí, així com controlar el nombre de connexions que es produeixen des d'un mateix punt, evitant possibles atacs de denegació de servei, més coneguts com *DoS* o *DDoS*. S'utilitzen per evitar intrusions des d'internet cap a l'interior d'una xarxa privada, així com per evitar connexions no permeses des d'una xarxa privada cap a Internet. Són un element essencial en la infraestructura de les xarxes DMZ (Demilitarized), ja que són el primer element de protecció de la informació d'aquesta xarxa. Molts routers contenen el seu propi Firewall, evitant així escanejos de ports en el sistema, una font de vulnerabilitat per als usuaris en cas que es descobrisquen ports oberts als seus equips. Alguns d'aquests routers que integren Firewall, també poden utilitzar-se com a Firewalls NAT (Routers Firewall que utilitzen el protocol NAT (Network Adress Translation))

per utilitzar una sola IP pública per a tota una xarxa privada. Actualment estàn fent-se un lloc molt important els *Next-Generation Firewalls* (NGFW), que són Firewalls hardware que compten amb funcionalitats de seguretat més enllà de les polítiques de Firewall, com pot ser l'inspecció de tràfic SSL (*Secure Sockets Layer*), antivirus, autenticació centralitzada o funcionalitats d'IPS (*Intrussion Prevention System*). Un exemple de Firewall podrien ser els SRX Series (NGFW de Juniper [Propietari]), el PA-7050 (NGFW de Palo Alto Networks [Propietari]) el Fortigate 7000 (NGFW de Fortinet [Propietari]) o el pfSense (FreeBSD [Open Source]).

- *IDS/IPS*: Intrussion Detection/Prevention System. Sistema dedicat a la detecció i/o prevenció d'intrusions a la xarxa. Els IPS naixen per suplir certes cadències del Firewalls, degut a que certes polítiques dels Firewalls podien resultar massa permissives. La diferència entre un IDS i un IPS és que l'IDS sols detecta les intrusions, és a dir, que ens informa de que ha hagut una intrusió però no realitza cap acció al respecte, mentre que els IPS reaccionen de manera activa front a una intrusió, bloquejant el tràfic que considera il·legítim. Aquests dispositius analitzen el tràfic de la infraestructura en temps real detectant i bloquejant tràfic segons les polítiques que li han sigut establertes a la seva configuració. Aquest anàlisi el realitza comparant el tràfic amb firmes d'atacs coneguts, que contenen guardats a les seves bases de dades, o comportaments sospitosos de ser un atac, com bé pot ser un escanejos de ports. Junt als Firewalls, és un element indispensable a una xarxa amb seguretat perimetral, degut a que aporta la part "proactiva" que el Firewall no té, degut a que els IPS són una mica més autònoms gràcies a totes les firmes de que disposen a les seues bases de dades i a la quantitat tan elevada de tràfic que poden inspeccionar. Actualment, s'han implementat els *Next-Generation IPS* (NGIPS), amb una capacitat de processament molt major, així com l'habilitat d'autoaprenentatge i automatització de seguretat intel·ligent per bloquejar atacs o possibles amenaces instantàniament, així com l'enriquiment de la seva pròpia base de dades amb events ocorreguts dins la infraestructura de la que forma part per previndre futures intrusions o comportaments sospitosos per part d'usuaris determinats, actuant al mateix temps com a antivirus, inspeccionant fins i tot, aplicacions. Els FirePOWER 8000 (NGIPS de Cisco [Propietari]), els Intrushield NS9300 (McAfee [Propietari]), els GX7800 (IBM [Propietari]) o Suricata (OISF [Open Source]) són un exemple d'IPS.

- Proxy: Un servidor Proxy es bàsicament un element que es troba entre el client o peticionari i el servidor al que es realitza una petició. Aquests elements també poden ser software o hardware, intern o de xarxa, també conegut com a extern, i és un element de seguretat molt important quan s'empra en mode extern, ja que es pot fer un control molt específic de la navegació de xarxa, com analitzar el tràfic, bloquejar continguts, balancejar la càrrega, filtrar informació... El Proxy actua com a peticionari front al servidor al que es fa la petició, mantenint així l'anonimat del client que ha realitzat la petició al mateix Proxy, però no front a l'administrador d'aquest element de xarxa. Un Proxy necessita realitzar moltes peticions, ja que ha d'actuar íntegrament com si fos el client front al servidor web al que el vertader peticionari vol accedir. Com a exemples de Proxy, podem trobar una gran quantitat dels anomenats *web Proxies*, que són webs amb les que la navegació ocorre de forma totalment

anònima i sense deixar rastre, degut a que la web actua com a Proxy entre el client que navega i Internet, preservant així la nostra pròpia privacitat dintre d'aquest. Exemples molt coneguts de Proxy són els SG300 (Blue Coat [Propietari]), Burp Proxy (Portswigger [Propietari]) o Zorp GPL (Balabit [Open Source]).

- WAF (*Web Application Firewall*): Es tracta d'un Firewall a nivell d'aplicació Web, com el seu propi nom indica. La diferència amb que conta un WAF respecte d'un Firewall és que aquest aplica les regles per a tràfic web. Un WAF també es considera un Proxy invers, degut a que pot realitzar la funció contraria a la d'un Proxy, ja que aquest últim està destinat a protegir al client, mentre que el WAF està destinat, depenent de la configuració que li apliquem, a protegir en essència un servidor web d'atacs com els famosos *DoS* (Denegació de Servei), *SQL Injection* (introducció de codi SQL que vulnere la base de dades del servidor web) o *XSS (Cross-site scripting.* Introducció de codi maliciós al client que realitza una consulta a un servidor web). Existeixen dos tipus de WAF depenent de la seva situació a la xarxa, ja que els podem trobar a un servidor dedicat, fent que aquest WAF siga un element més de la xarxa; o el podem trobar allotjat en el mateix servidor d'aplicació al que intenten protegir. Els WAF més destacats podrien ser SecureSphere (Imperva [Propietari]), FortiWeb (Fortinet [Propietari]) o Shadow Daemon (Zecure [Open Source]).

2.3 – Legislació actual sobre la seguretat informàtica

Totes aquestes mesures de seguretat segueixen una reglamentació, definida a diverses legislacions d'àmbit Nacional o Europeu.

En el cas Europeu, existeix la Directiva 2016/1148 [2] en la que s'estableixen unes mesures destinades a garantir un nivell de seguretat de xarxa i als sistemes de la informació comuns a tots els organismes de la Unió Europea, pel que tots els països que pertanyen a la UE han de tindre unes mesures de seguretat mínimes als seus sistemes d'Informació, tant els organismes públics de cada estat com aquelles empreses que es dediquen a la distribució de serveis digitals, com poden ser tele operadores o bancs.

Cal destacar els articles 14 [3] i 16 [4] d'aquesta Directiva, en els que es responsabilitza a cada estat membre de vetllar per la seguretat de la informació que cadascuna de les operadores de serveis, essencials i digitals, respectivament, han de plantejar i proporcionar per a totes la seves instal·lacions, tant a nivell de xarxa com de protecció de totes aquelles dades que custodien. Cadascuna d'aquestes entitats haurà de complir uns requisits mínims, depenent de la criticitat de la informació que manegen, independentment de que aquestes entitats siguin públiques o privades.

Al mateix temps, cada membre de la UE ha de comptar amb mesures de mitigació, reducció i previsió front a possibles incidents que puguen posar en perill la seguretat de la informació, notificant en tot cas i sense cap tipus de retràs al CSIRT (*Computer Security Incident Response Team*) corresponent tots aquells incidents que puguen tindre afectació en aquells serveis essencials per a que es prenguin les mesures adients.

Altre reglament a nivell Europeu és el de la protecció de dades [5], en el que es recullen una sèrie de requisits a tenir en compte en quan a la transmissió de dades de forma internacional, com el cas del *Privacy Shield* [6].

En el cas de l'estat Espanyol, trobem el Codi de Dret de la Ciberseguretat [7], en el que podem destacar les normatives següents:

- Normativa de seguretat nacional:
  - Llei 36/2015, del 28 de setembre, de Seguretat Nacional, que regula els organismes clau així com les funcions que han de desenvolupar en la defensa de la Seguretat Nacional.
  - Ordre TIN/3016/2011, del 28 d'Octubre, amb la que es crea el Comitè de Seguretat de les Tecnologies de la Informació i les Comunicacions del Ministeri de Treball i Immigració.

- Normatives de seguretat:
  - Llei Orgànica 4/2015, del 30 de març, de protecció de la seguretat ciutadana.
  - Llei 5/2014, del 4 de abril, de Seguretat Privada.

- Normes relacionades amb les telecomunicacions:
  - Real Decret 381/2015, del 14 de maig, pel que s'estableixen mesures contra el tràfic no permès o irregular amb finalitat fraudulenta en les comunicacions electròniques.
  - Llei 50/2003, del 19 de desembre, de signatura electrònica.
  - Llei 25/2007, del 18 d'octubre, de conservació de dades relacionades amb les comunicacions electròniques i a les xarxes públiques de comunicaciones.

- Normes relacionades amb la ciberdelinqüència:
  - Llei Orgànica 5/2000, del 12 de gener, reguladora de la responsabilitat penal dels menors; o al Real Decret d'aprovació de la Llei d'Enjudiciament Criminal.

- Normativa de protecció de dades:
  - Llei Orgánica 15/1999, del 13 de desembre i el seu Reglament, aprovat pel Real Decret 1720/2007, el 21 de desembre, que tracta la protecció de dades de caràcter personal.

Com calia esperar, totes aquestes lleis venen regides per la Directiva Europea, que regula totes les normes que entren en vigor a l'Estat Espanyol en quan a protecció de dades i actuacions front a Cibercrim.

En el cas d'Espanya, compta amb l'INCIBE (*Instituto Nacional de Ciberseguridad*), dedicat al desenvolupament de projectes i investigació en els camps de la Ciberseguretat; i el CNI (*Centro Nacional de Inteligencia*), dedicat a la protecció de l'estat també en camps de seguretat de xarxa i de protecció de dades confidencials i molt crítiques en quan a la seguretat del país o dels seus dirigents.

3. Disseny de l'entorn

3.1 – Requeriments/Necessitats de la nostra infraestructura

Al tractar-se d'una infraestructura domèstica relativament menuda, no serà necessari realitzar un desplegament molt gran que implique despeses econòmiques elevades.

Com a necessitats, necessitarem que els elements de seguretat siguen completament Open Source i que, una vegada configurats, pogam obtindre reports de l'estat de la seguretat de la xarxa, com els atacs que s'han produït, d'on provenen, de quin tipus són, etc. Aquest report es requerirà tant a nivell extern com intern de la xarxa, degut a que pot donar-se el cas d'infecció amb un *malware* que vulga connectar a servidors extern que, malgrat no poder perquè el Firewall ho blocarà, s'ha d'informar al propietari de la màquina infectada per a que procedisca a eliminar l'infecció.

Al mateix temps, els equips de seguretat i pertanyents a la xarxa d'ús no personal, on exclourem els ordinadors de cada propietari, enviaran logs de sistema amb el registre d'activitat, bé siga auditoria de la base de dades interna o estat de descàrregues del client P2P configurat junt a aquesta.

En aquest punt, considerem de vital importància que sigui l'IPS/IDS qui ens proporcione la informació necessària per a realitzar els reports d'atacs o comportaments malintencionats dintre la xarxa, ja que se li aplicaran unes normes més restrictives per a que aquest estudi puga ser el més precís possible.

Finalment, serà necessari l'ús d'un analitzador de vulnerabilitats a nivell d'entrada a la xarxa interna, per polir les regles que s'han d'implementar al Firewall i realitzar altres tipus de modificacions de seguretat en cas de ser requerides una vegada finalitzat l'anàlisi.

3.2 – Elements que utilitzarem

Primerament, serà necessari adquirir un equip que allotjarà el sistema operatiu del Firewall, que serà el primer element de seguretat que hi haurà entre Internet i la xarxa domèstica. Els requeriments necessaris que tindrem en compte per a l'elecció d'aquest dispositiu seran la capacitat de processat (nuclis i memòria RAM). Per a aquest desplegament, tenint en compte les necessitats domèstiques i el nivell de seguretat que va a requerir la xarxa, buscarem un dispositiu amb processador amb dos *cores* i un mínim de quatre gigues de memòria RAM.

El sistema operatiu per a aquest dispositiu serà *pfSense*, un sistema basat en *FreeBSD* que ens permetrà configurar el Firewall, l'IPS i una VPN al mateix equip. Essencialment, el sistema operatiu *pfSense* és un Firewall, però ens permet utilitzar altres eines Open Source per configurar altres capes de seguretat perimetral, com serà Suricata (IPS/IDS) i OpenVPN (servei VPN), degut a que existeixen una gran varietat d'extensions que se li poden afegir com a paquets desenvolupats també per col·laboradors de distints projectes Open Source.

Aprofitant que a la infraestructura domèstica es compta amb màquines virtualitzades

allotjades a un servidor hardware mitjançant la plataforma de virtualització de l'empresa VMWare anomenada *vSphere*, així com per a l'execució d'arxius potencialment sospitosos de contindre algun tipus de *malware*, ja que estaran connectades a Internet directament, sense passar pel Firewall, exceptuant la seva interfície de *management*, que sí que formarà part de la xarxa interna, així es podran executar completament i es podrà procedir a l'anàlisi del comportament amb totes les característiques possibles amb les que aquest arxiu maliciós ha estat creat.

Per altra part, comptarem a un servidor NAS (*Network Attached Storage*), amb un sistema operatiu Open Source anomenat *FreeNAS,* també bassat en *FreeBSD*, on s'allotgen els arxius dels integrants de la xarxa, que ha d'estar completament aïllat d'internet, degut a que les connexions a aquest es realitzaran íntegrament per una Raspberry Pi amb un client de descàrregues que allotjarà automàticament a un dels discs del NAS, que no formarà part del RAID configurat per als discs d'emmagatzematge d'arxius personals dels usuaris. L'accés a aquest NAS haurà de ser verificat sempre pel Firewall de l'entrada de la xarxa, al que se li configurarà una llista blanca amb les IP dels dispositius autoritzats a accedir a la partició del servidor d'arxius dedicada a emmagatzemar informació i arxius personals de cada usuari, mentre que la partició destinada a les descàrregues multimèdia, serà accessible per al gestor de descàrregues i la resta d'usuaris de la xarxa, també filtrats per IP pel Firewall. Aquest gestor de descàrregues instal·lat a la Raspberry Pi correrà mitjançant el sistema operatiu *Raspbian*, que és una distribució de Debian Linux adaptada per al hardware de la Raspberry Pi. El client de descàrregues serà bàsicament un client P2P basat en torrent.

Per finalitzar, requerirem una eina gratuïta anomenada Nessus, que és un escàner de vulnerabilitats de xarxa, per a comprovar la fiabilitat i l'eficàcia de les solucions de seguretat perimetral implementades a l'entrada de la xarxa domèstica interna.

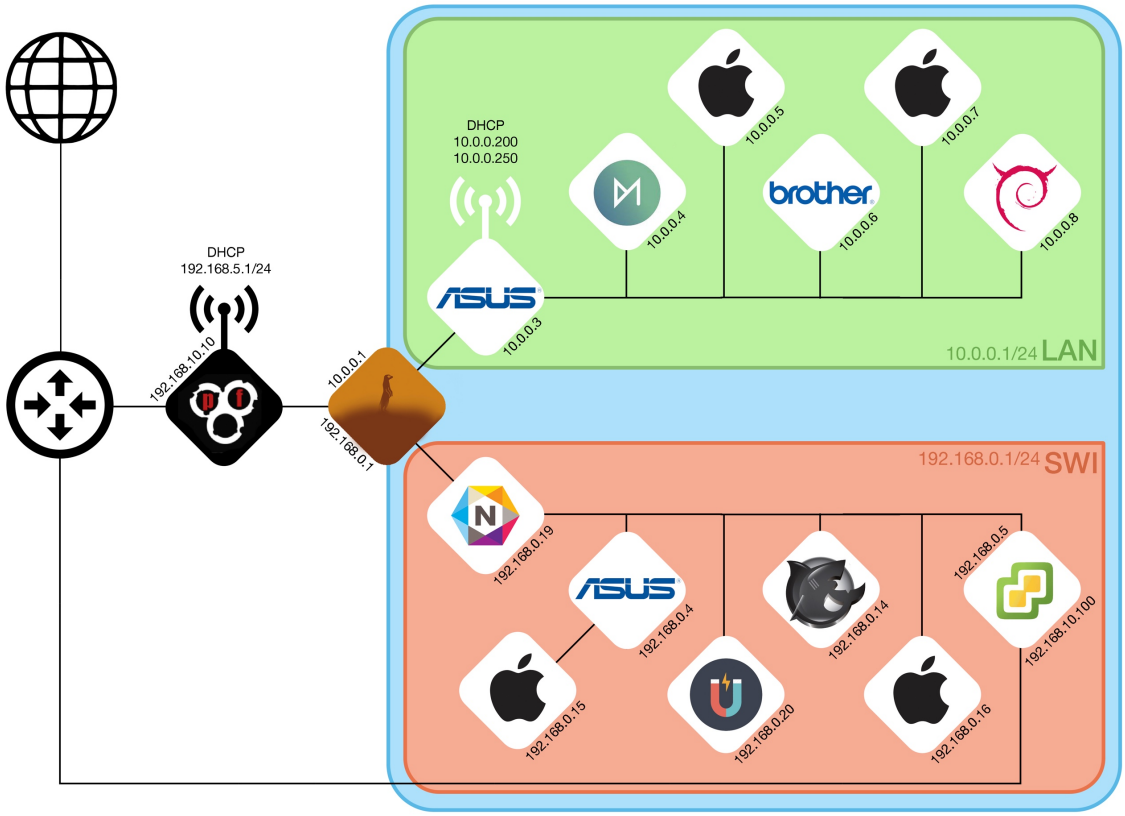
3.3 – Esquema de la infraestructura

Tenint en compte totes les necessitats exposades anteriorment, s'ha dissenyat un esquema de xarxa i s'ha fet l'assignació d'IP estàtiques per a tots els equips que la formaran. És important que utilitzem IP estàtiques per a tots els equips, que assignarem en funció de l'adreça MAC de cadascun, degut a que les regles que s'han d'aplicar al Firewall potser van customitzades per IP o per a un rang d'IP concret, pel que ens interessa implementar aquesta configuració als equips per a que la securització siga més eficient i ens ocasione el menor nombre de bloquejos de tràfic legítim en cas d'aplicar polítiques de seguretat més restrictives al Firewall d'entrada i sortida a Internet.

Com es pot observar a l'esquema de la *Imatge 3*, el router que dona accés a internet anirà connectat a el dispositiu que comptarà amb el pfSense instal·lat com a Firewall, i aquesta primera barrera anirà seguida d'un IPS Suricata, allotjat a la mateixa màquina, i ja es donarà pas a la xarxa domèstica interna, que es segmentarà en dos subxarxes per necessitats de l'habitacle, LAN i SWI.

La xarxa LAN compta amb un router utilitzat com a punt d'accés en el que es configura un DHCP, i que al mateix temps dona connexió cablejada a una Raspberry Pi amb un OSMC instal·lat, que serà utilitzada com a centre multimèdia; una impressora i tres ordinadors personals.

Per altra banda, trobem la xarxa SWI, que va precedida per un switch al que es connecta altre router configurat com a punt d'accés al que hi haurà connectat un ordinador personal; una Raspberry Pi configurada com a client de descàrrega, un servidor NAS, altre ordinador personal i el servidor amb el client vSphere (Sistema de virtualització d'escriptoris remots) connectat a la subxarxa mitjançant l'IP de *management* i amb sortida a internet directa mitjançant altra interfície d'aquest servidor, que està connectada directament el router extern.



Imatge 3. Topologia de la xarxa amb seguretat perimetral a implementar

4. Implementació

4.1 – Instal·lació del sistema operatiu pfSense

Una vegada seleccionat el dispositiu hardware que farem servir com a Firewall, procedirem a instal·lar el sistema operatiu Open Source pfSense [8], basat en *FreeBSD*, que és una eina molt potent i valorada dintre de la seguretat informàtica a xicotets entorns, com petites o mitjanes empreses, degut a la seva eficàcia, versatilitat i el seu preu gratuït.

El dispositiu que hem triat, mostrat a la *Imatge 4*, és un PcEngines APU1D4 amb un processador AMD G-T40E a 1'2 GHz amb dos cores, quatre gigues de memòria RAM i un disc dur d'estat sòlid de 128 gigues.

Imatge 4. PcEngines APU1D4. Dispositiu que allotjarà el pfSense.

La instal·lació del sistema operatiu no dista molt de qualsevol altre FreeBSD, aportant una gran facilitat i comoditat per realitzar el procés. Una de les característiques d'aquest sistema operatiu és que una vegada està muntat i configurat dintre la xarxa, la seva gestió es pot fer completament mitjançant GUI (*Graphic User Interface*) al nostre navegador web.

Per accedir a l'equip necessitarem un cable *serial* RS-232 a USB, per connectar-nos des del nostre ordinador. Una vegada connectats, introduirem una memòria USB, on prèviament haurem *bootejat* el sistema operatiu que volem instal·lar, que en aquest cas és el *pfSense*, a un dels dos ports dels que disposa el dispositiu. Una vegada està tot connectat, engegarem el que serà el nostre Firewall i automàticament aquest arrancarà des de la memòria USB. Obrirem una terminal al nostre ordinador i accedirem mitjançant *Minicom*, un programa de comunicació per port sèrie basat en menús per a dispositius Unix, que emularà una terminal amb la que podrem configurar tots els paràmetres del *pfSense* [15]. Per a que aquest procés comence, haurem d'introduir la següent comanda a la terminal del nostre ordinador:

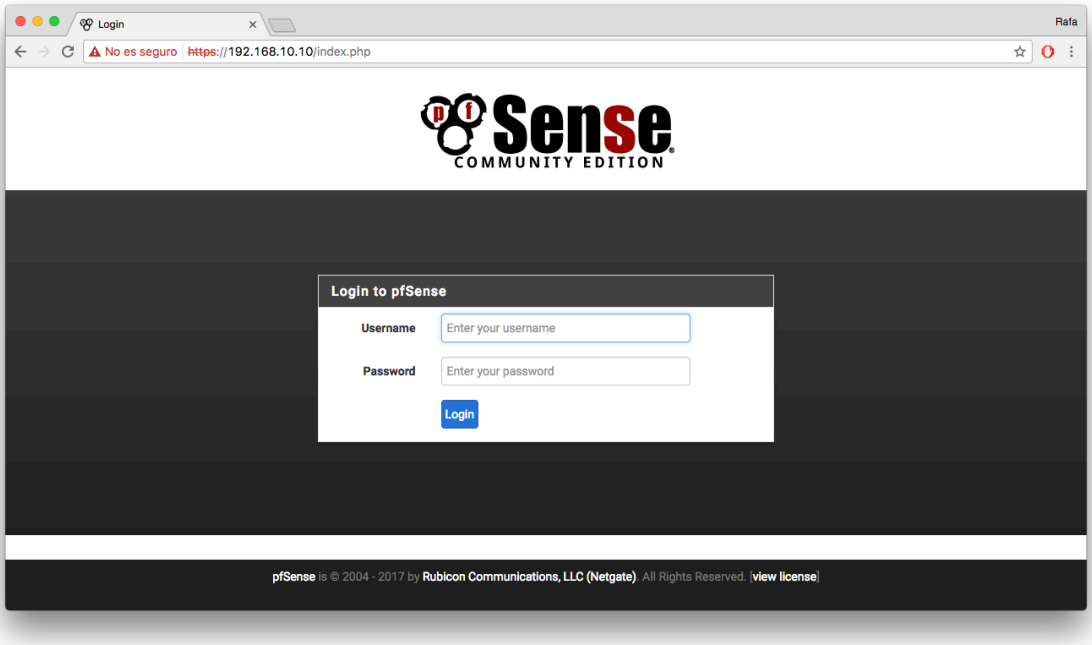
```
minicom -D /dev/cu.usbmodem600A -b 115200 -8 -C Conf_pfSense.txt
```

Amb aquesta comanda, estarem utilitzant el dispositiu conversor de RS232 a USB connectat al port `/dev/cu.usbmodem600A` al que li indicarem la relació de bauds a la

que ha de treballar el dispositiu i, com a mesura preventiva, exportarem els logs del procés per si aquest fallés o ens donés qualsevol tipus d'error, estudiar on s'ha donat per si hem de modificar manualment algun paràmetre o realitzar algun tipus de canvi.

Durant el procés d'instal·lació ens requerirà que assignem una IP estàtica a l'equip, així com la seva màscara i la porta d'accés. També ens donarà l'opció de crear dues subxarxes a l'eixida de les dues interfícies de les que disposa aquest dispositiu. Com aquesta possibilitat ja l'havíem plantejada en el moment de dissenyar l'esquema de xarxa, procedirem a assignar-li la IP estàtica planificada, així com a crear les dues subxarxes, que anomenarem LAN i SWI, a les que també assignarem les seves IP estàtiques i la màscara de subxarxa. Per altra banda, haurem de configurar un usuari administrador, amb nom i contrasenya, per poder accedir a l'eina de gestió de la que disposa utilitzant el nostre navegador. Una vegada finalitzada la configuració mitjançant consola, haurem de reiniciar l'equip per a que s'apliquen aquests canvis.

Una vegada finalitzat el reinici, haurem d'accedir a l'IP que li haguem assignat al dispositiu durant el procés d'instal·lació per poder entrar al portal web on podrem configurar tots els paràmetres que necessitem d'una manera molt més senzilla que mitjançant la consola de FreeBSD. En quan es carregue aquest portal, ens demanarà l'usuari i la contrasenya que li hem assignat a l'administrador del sistema per poder accedir, tal com podem observar a la *Imatge 5*:



Imatge 5. Pàgina d'accés al Firewall pfSense

Ara que ja hem finalitzat la instal·lació del Firewall, haurem de procedir a la seva customització de regles i polítiques per al bloqueig d'accessos.

4.2 – Creació de les regles de FW

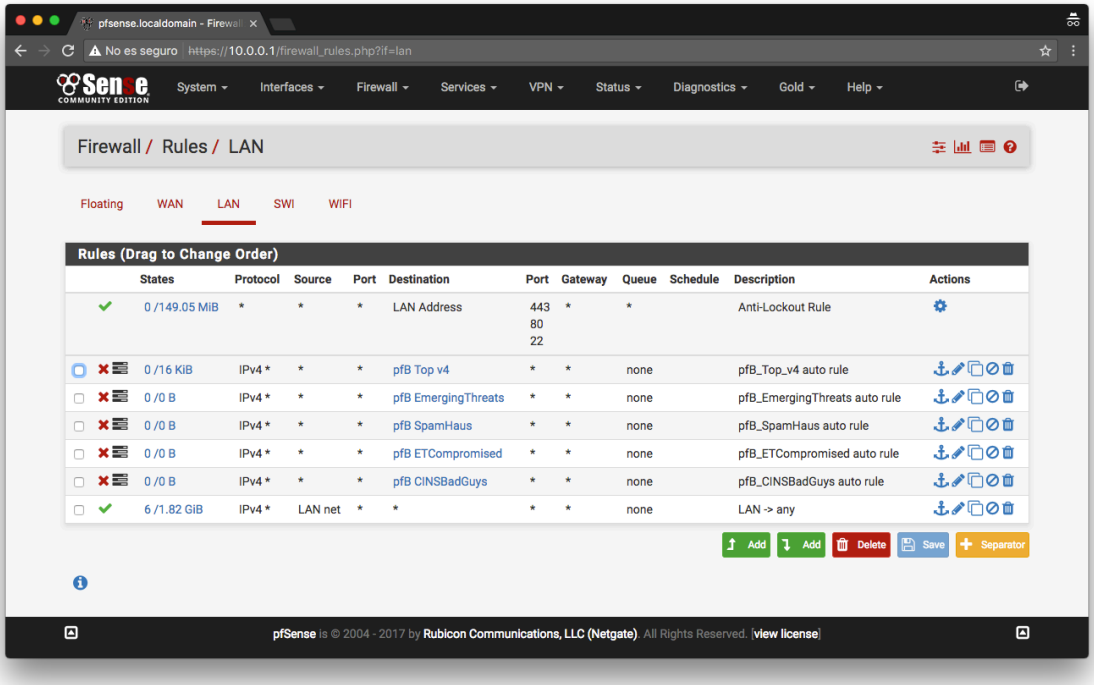
Les regles de Firewall són xicotetes sentències que defineixen la política d'accés o de pas a través dels dos segments de xarxa que separa. El format d'una regla de Firewall és el següent:

```
Source IP – Source Port – Destination IP – Destination Port – Application – Action
```

Coneixent el format d'una regla de Firewall [10], ja podem especificar quina serà la IP origen/destí, el port d'origen/destí, l'aplicació a la que volem afectar (tràfic web, accés SSH, tràfic UDP, tràfic TCP, protocol ICMP, etc) i quina acció realitzarem sobre aquesta, bé siga bloqueig (*deny*) o permissió (*allow*).

Durant la creació de regles de Firewall, hem de tindre en compte que potser no ens interessa començar a aplicar regles fins tindre una llista negra molt perfilada. En determinats casos, les llistes negres poden no ser útils degut al nivell tan elevat de customització que poden requerir per bloquejar distints rangs d'IP o no permetre cap tipus de comunicació excepte uns quants molt específics. És aquí on ens hem de plantejar que també podem crear llistes blanques on aplicaríem polítiques de permissió, fent així que el Firewall no contemple cap tipus de connexió fora de les establertes a la llista blanca, creant així un llistat no tan extens per a un entorn domèstic, degut a que coneguem les IP i els protocols que s'utilitzaran dintre d'aquest entorn, podem permetre tot el tràfic d'aquests a una llista blanca, mentre que el tràfic que no considerem legítim, podem afegir-lo a una llista negra. D'aquesta manera, optimitzarem molt més les polítiques que hem d'aplicar al dispositiu i farem que aquest tinga una capacitat de processat molt més eficient.

A l'interfície web del nostre *pfSense*, mostrada a la *Imatge 6*, ens dirigirem a la pestanya Firewall i seleccionarem la subxarxa a la que volem aplicar les polítiques i, tenint en compte què volem blocar exactament per a no tallar tràfic legítim, crearem polítiques d'accés:



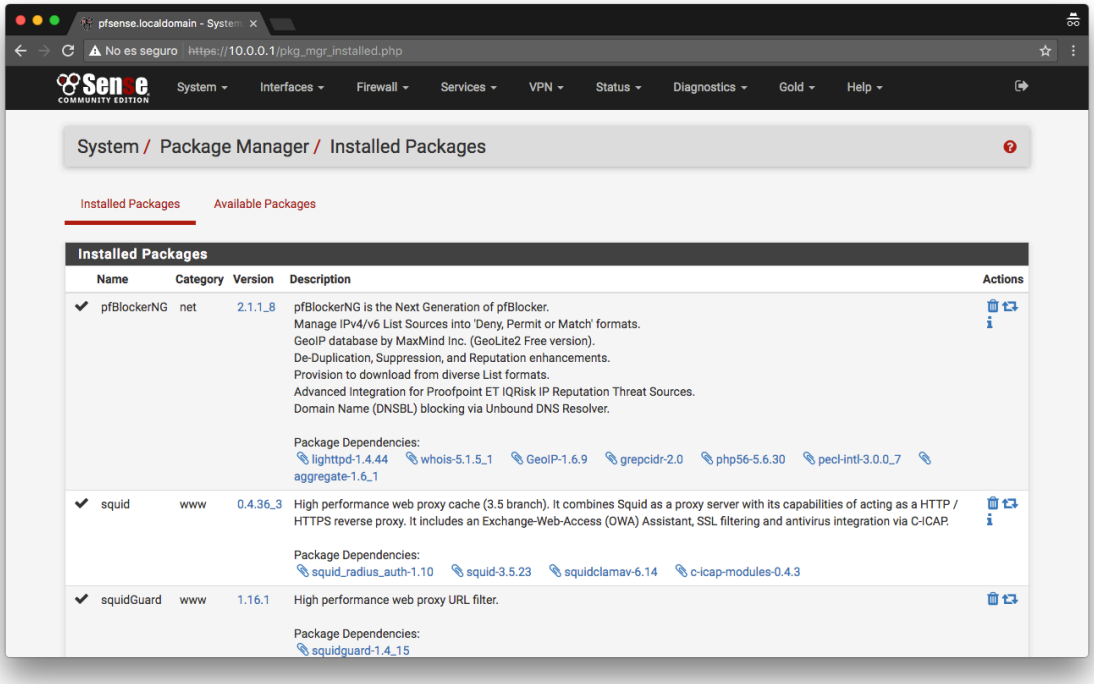
Imatge 6. Pàgina de customització de regles Firewall pfSense

Com es pot observar, existeixen regles en les que no s'ha realitzat cap *match* i d'altres en les que sí. A la interfície web podem afegir tantes regles com ens siguin necessàries, filtrant, com no, per protocol, IP o port tant a l'origen com al destí, així com especificar quina ha de ser l'acció que ha de realitzar el Firewall quan es cumplisca qualsevol regla aplicada. També és comú a les regles de Firewall l'ús dels denominats *Any*, que implementen la regla per a qualsevol paràmetre. En el nostre cas, el bloqueig al mateix Firewall per qualsevol accés que no provinent de la xarxa interna, serà bloquejat. Amb aquesta mesura podrem evitar que tant des d'internet com des del propi Router que ens dona accés a Internet ningú es puga connectar al Firewall si no forma part de la xarxa domèstica.

4.3 – Configuració del IPS

El sistema *pfSense* també ens dona l'oportunitat d'instal·lar *plugins* al Firewall, com pot ser un Proxy, un servidor DNS, un IPS/IDS, entre molts altres. En aquest cas, ens interessa afegir un IPS/IDS que inspeccione el tràfic tant del Firewall cap a la xarxa domèstica com en direcció contrària, podent així saber si hi ha algun dispositiu infectat amb qualsevol tipus de *malware* que vulga accedir a Internet. Amb aquestes funcionalitats allotjades al mateix equip, podrem dir que ens trobem front a un NGFW [11] (*Next-Generation Firewall*).

Per accedir a les llibreries de *plugins* de *pfSense* tansols hem d'anar a la pestanya *System* i accedir a l'opció de *Package Manager*. Aquí podrem llistar totes les extensions que hem instal·lat al nostre dispositiu així com totes aquelles que hi ha disponibles. A la *Imatge 7* es mostra una captura d'aquest apartat del sistema operatiu:



Imatge 7. Pàgina Installed Packages en Firewall pfSense

En aquest cas, com volem un IPS Open Source, no podem optar per altre que no siga Suricata [12], una solució d'OISF (*Open Information Security Fundation*) mundialment reconeguda com a una de les millors solucions en quan a seguretat informàtica, pel que fa a la velocitat de processat de paquets, front a l'altra gran solució, Snort, propietat de Cisco en l'actualitat, que també és Open Source. Suricata implementa les seves pròpies regles, que reben el mateix nom, i la seva sintaxi és una mica més complexa que la utilitzada amb els Firewalls. A continuació, un exemple de regla Suricata:

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Sqlmap SQL Injection Scan"; flow:to_server,established; content:"User-Agent|3a| sqlmap"; fast_pattern:only; http_header; detection_filter:track by_dst, count 4, seconds 20; reference:url,sqlmap.sourceforge.net;
reference:url,doc.emergingthreats.net/2008538; classtype:attempted-recon; sid:2008538; rev:8;)
```

Aquesta regla ens està mostrant una alerta amb protocol tcp d'un escaneig del tipus *sqlmap* fet a un servidor HTTP des de fora d'una xarxa utilitzant els ports HTTP. La regla ens mostraria l'alerta amb el missatge `ET SCAN Sqlmap SQL Injection Scan`. A més, si aquest comportament es produeix cap al servidor, amb una comprovació de la capçalera dels paquets amb per corroborar que s'estan fent escanejos *sqlmap* i es repeteix la connexió un màxim de quatre vegades en un interval de vint segons, Suricata bloquejaria aquesta comunicació i ja no la permetria. A més, ens aporta una font de referència indicant-nos la URL `sqlmap.sourceforge.net` on podem trobar informació en línia sobre aquest tipus d'atac i, a més, la documentació a la pàgina web especialitzada en events de seguretat informàtica *Emerging Threats* amb l'enllaç `doc.emergingthreats.net/2008538` per conèixer més sobre aquesta regla creada per previndre un atac *SQLi* (*SQL Injection*) i poder veure d'altres similars amb altres paràmetres de configuració, com un interval de temps diferent, o més

restrictives en quant al nombre d'intents de connexió cap al servidor intern, tot depenent de les nostres necessitats o del nivell de rigidesa amb el que volem dotar el nostre IPS.

Molts IPS poden estar sols en mode detecció (IDS), reportant alertes segons les regles aplicades. Sol ser molt comú que mai es configure un IPS en mode bloqueig de primeres, degut a que sol estar "dotat" de certa intel·ligència, a diferència dels Firewalls, i pot arribar a bloquejar tràfic legítim si no s'estudia bé el seu comportament abans configurant-lo solament en mode detecció. Pel que durant uns dies, deixarem el IPS en mode detecció per veure amb quines polítiques s'activa i en cas de ser necessari, afinar aquestes per a que siguen més concretes per a quan activem el mode de bloqueig.

4.4 – Correlació de logs

La correlació d'alertes a un entorn de seguretat es realitza mitjançant un SIEM [13], que és una eina específica per al tractament de logs, així com per al seu emmagatzematge per poder realitzar històrics de cerques aplicant filtres específics. A més, a un SIEM es poden crear alertes per quan es reben un determinat tipus d'events que es poden considerar perillosos.

Existeixen molts SIEMs Open Source, com és el cas d'OSSIM, una eina d'Alien Vault. A més, també podem trobar una gran quantitat de ferramentes per tractar logs que no han de ser específicament un SIEM. Aquestes ferramentes s'empren per realitzar un tractament massiu de dades, inclús es podria parlar de Big Data en molts casos, ja que tots aquests registres provinents de tots els sistemes pertanyents a una mateixa xarxa contenen la informació de tots els events que han succeït a la xarxa des que s'han començat a enregistrar events, fet que mostra tot el potencial que pot tindre un SIEM o un correlador de logs si s'implementa a un entorn de securització perimetral.

Per mancança de recursos, al nostre entorn domèstic no es pot implementar un SIEM, ja que seria necessari altre dispositiu físic dedicat amb una quantitat de recursos per a processar els logs que elevarien molt el cost del projecte, degut a que la correlació de tots els events que el SIEM ha de recollir suposa una gran quantitat de feina per al dispositiu, sense comptar amb la creació de regles i les alertes, que ja generarien una sobrecàrrega computacional que no és capaç d'assolir un equip de cost relativament baix amb un sol processador, independentment dels nuclis dels que aquest disposa, pel que afegir un SIEM a la nostra xarxa interna, no seria una opció viable, almenys econòmicament parlant.

4.5 – Generació de reports

S'ha de tindre clar que implementar una xarxa de seguretat en la que no es puga tindre visibilitat dels events que tenen lloc resulta una mica inútil, ja que és l'única manera de saber si tot està anant correctament i de poder saber quin nivell de seguretat s'ha assolit en veure la quantitat d'alertes al report que un SIEM generaria. Per aquest fet, s'ha de plantejar una solució que es puga implementar a les eines de les que podem fer ús per realitzar aquesta tasca.

Tinguent en compte aquestes limitacions, ens disposarem a programar el nostre propi correlador de logs per a que, basant-nos amb els events que l'IDS/IPS Suricata ens aporta, genere un report en PDF diari on se'ns mostren les estadístiques i el recompte dels

intents d'accés no legitimats cap a la nostra xarxa, així com les eixides no legítimes cap a internet. Aprofitant que disposem d'una Raspberry Pi amb una distribució Debian Linux adaptada, podrem fer ús de la terminal de Linux per crear aquest programa en *bash*, un llenguatge molt complet i que no generarà una sobrecàrrega de procés computacional massa elevada a la Raspberry Pi. Com aquest dispositiu es troba a la xarxa interna i té accés directe al Firewall i al IPS/IDS, pot extraure els logs sense cap tipus de problema i sense necessitat de crear cap regla específica per permetre aquest accés.

El report es deu generar en PDF i ha de ser el més exhaustiu possible, ja que quanta més informació es puga obtindré d'aquest, es podran implementar noves regles més precises o, fins i tot, afegir amb el temps noves eines de seguretat havent pogut realitzar un bon estudi acord amb les necessitats de la xarxa i les possibles vulnerabilitats que pot tindre en un moment donat.

A l'*script* en bash [14, 15] cridarem a una llibreria en *python* [16] encarregada de geolocalitzar la providència o la destinació de les comunicacions a un mapa geopolític, en el que es marcaran els distints països del Top 10 en el que ens anem a focalitzar, seguint un codi de colors acord amb el nombre d'alertes provinents de dit país. Aquesta llibreria està proporcionada per l'empresa americana *MaxMind*, especialitzada en la prevenció de la geolocalització IP i el frau en línia. Per altra banda, utilitzarem codi *html* per a generar la visualització de les diferents seccions del report, com els títols, les taules dels top 10 o les gràfiques amb els recomptes del nombre d'atacs, així com una llibreria *css* per donar-li el format necessari a aquest *html*, com el codi de color per a les taules, el text, els mapes i les gràfiques generades amb les dades provinents del IDS/IPS Suricata. En total es generaran cinc arxius en format *html*, que es correspondran a cadascuna de les pàgines de l'arxiu PDF que es crearà.

A continuació, es pot veure el codi del programa simplificat per a poder veure quines funcions s'han implementat i quina és la finalitat de cadascuna:

```
#!/bin/bash
# Title: Parser.sh

NOW=$(echo $(date +%Y-%m-%d))
NOWSHORT=$(echo $(date +%Y%m%d))

function ipfinder() {

#Busca a una base de dades proporcionada per MaxMind el país associat a la IP.

}

function prepareall() {

#Preparar el necessari per a crear el report (Fitxers CSS, Logs, etc).

}

function parser() {

        #TOP ALERT NAME: Llista el top 10 d'alertes generades
        #TOP SRC IP: Llista el top 10 d'adreces IP origen
        #TOP DST IP: Llista el top 10 d'adreces IP destí
        #TOP SRC COUNTRY: Llista el top 10 de països origen
        #TOP DST COUNTRY: Llista el top 10 de països destí
        #TOP PROTOCOL: Llista el top 10 de protocols utilitzats
        #TOP ALERT CLASSIFICATION: Llista el top 10 d'alertes per categoria
        #TOP RISK: Llista el top 10 d'alertes per severitat

}

function reporter() {

        #Llistat de països amb les IP extretes amb ipfinder per destí/origen

}

function htmlgen () {

        #Genera el report en format HTML per exportar-lo a PDF posteriorment

}

function redbutton() {

        #Esborra els arxius generats en local una vegada s'ha generat el report

}

function main() {

        prepareall
        parser
        reporter
        htmlgen
        redbutton
}


main
```

Una vegada creat el codi que realitzarà el report, configurarem un *cron* a la Raspberry Pi per a que l'execute cada dia a la una de la matinada. Un *cron* és una tasca automatitzada per terminal Linux. Per a realitzar aquesta tasca automatitzada, accedirem al *crontab* de la Raspberry Pi, que és l'arxiu de text on s'afegeix el llistat de *crons* a executar en un ordre determinat, i afegirem la següent línia de text:

```
01 00 * * * RasPi /bin/bash /home/raspberrypi/scripts/Parser.sh
```

Amb aquesta comanda, estem indicant a la Raspberry Pi que execute l'*script* `Parser.sh` que es troba a la ruta `/home/raspberrypi/scripts/` cada dia de la setmana a la 01:00 hores. Per assegurar-nos que aquest procés es complirà, hem de donar-li permisos d'execució a l'*script* per a que es llance sense cap problema. Per a dotar d'aquests permisos, escriurem la comanda següent:

```
chmod +x /home/raspberrypi/scripts/Parser.sh
```

A partir d'aquest punt, es generarà de forma totalment automatitzada un report diari amb el contingut de les alertes, el protocol utilitzat, el tipus d'alerta que s'ha produït, la magnitud de risc que aquestes suposen, la categorització d'aquestes, el percentatge d'alertes bloquejades per haver fet *match* amb alguna alerta, així com la seva procedència i la seva destinació, distribuïda per pais.

A continuació es pot veure el report complet que es genera amb l'script referenciat com a *Imatge 8*, sent aquesta la primera pàgina, i finalitzant en la *Imatge 12*, que ens mostrarà la cinquena i última pàgina:

Suricata Report: 2017-05-02

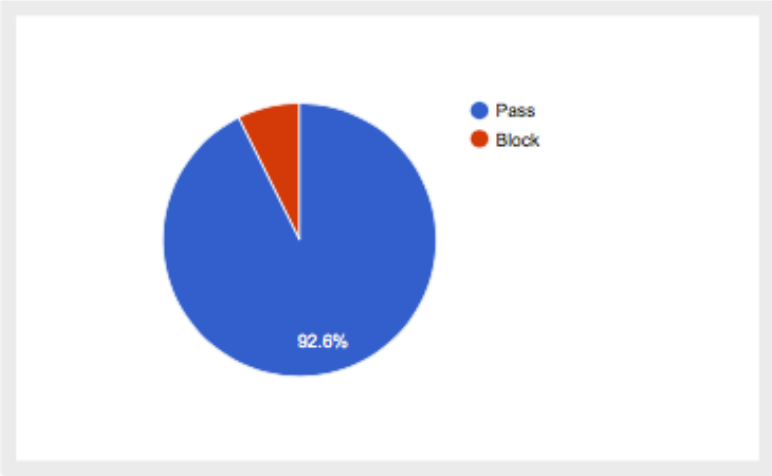
1. PROTOCOL ALERT USAGE

TCP	UDP	ICMP
301	79	

2. RISK ALERT COUNT

HIGH	MEDIUM	LOW
270	72	38

3. Alerts Blocked by policies



Imatge 8. Pàgina 1 del report generat amb l'script

4. TOP Attack Category

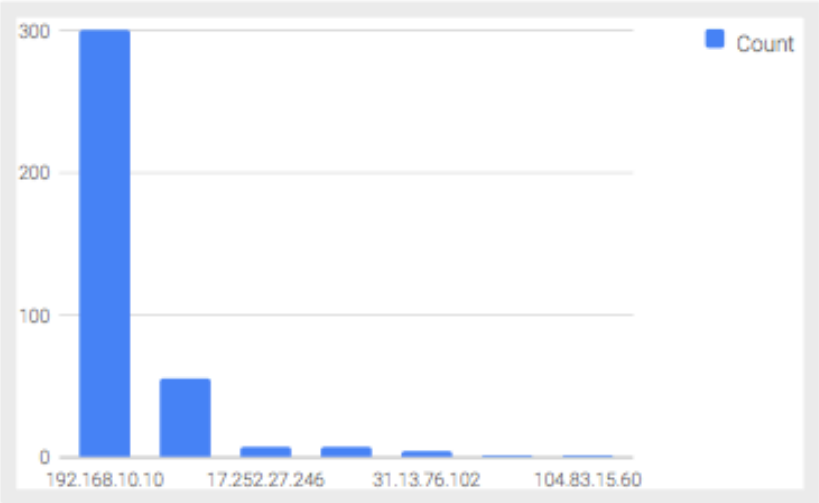
Count	Attack Category
228	Not Suspicious Traffic
42	Generic Protocol Command Decode
38	Potential Corporate Privacy Violation
28	Misc Attack
15	Potentially Bad Traffic
1	Attempted Information Leak

5. TOP 10 Attack Name

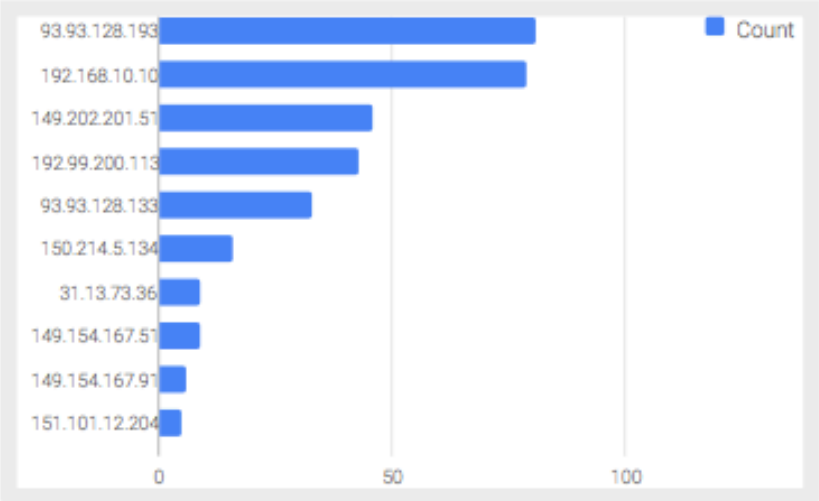
Count	Attack Name
228	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management
56	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 521
18	ET P2P BitTorrent DHT ping request
15	SURICATA STREAM Packet with invalid timestamp
14	ET POLICY HTTP traffic on port 443 (POST)
8	SURICATA STREAM 3way handshake excessive different SYN/ACKs
8	SURICATA STREAM 3way handshake SYNACK with wrong ack
7	ET P2P BitTorrent DHT nodes reply
6	ET POLICY Possible External IP Lookup ipinfo.io
5	SURICATA STREAM 3way handshake with ack in wrong dir

Imatge 9. Pàgina 2 del report generat amb l'script

6. TOP 10 Source IP



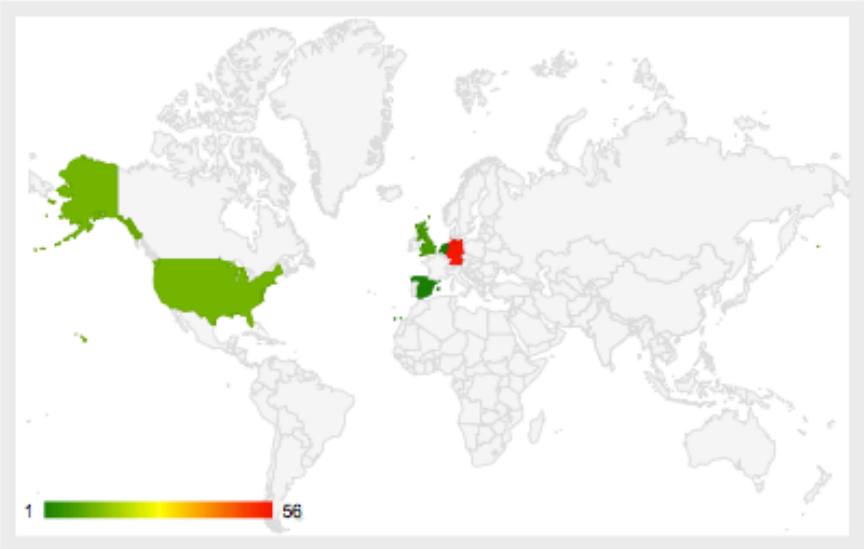
7. TOP 10 Destination IP



Imatge 10. Pàgina 3 del report generat amb l'script

8. TOP Source Country

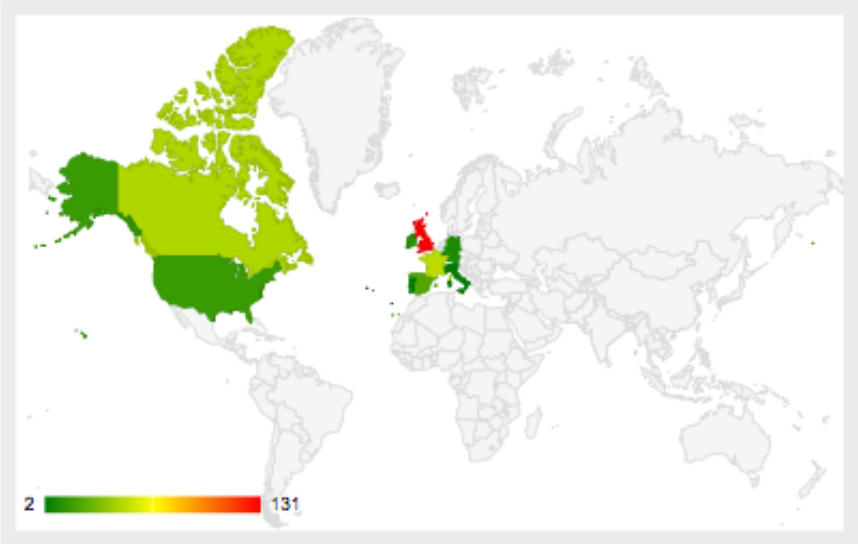
Count	Country
56	Germany
13	United States
8	United Kingdom
1	Netherlands
1	Spain



Imatge 11. Pàgina 4 del report generat amb l'script

9. TOP Destination Country

Count	Country
131	United Kingdom
50	France
46	Canada
23	Spain
17	United States
13	Ireland
9	Germany
3	Luxembourg
2	Portugal
2	Italy



Imatge 12. Pàgina 5 del report generat amb l'script

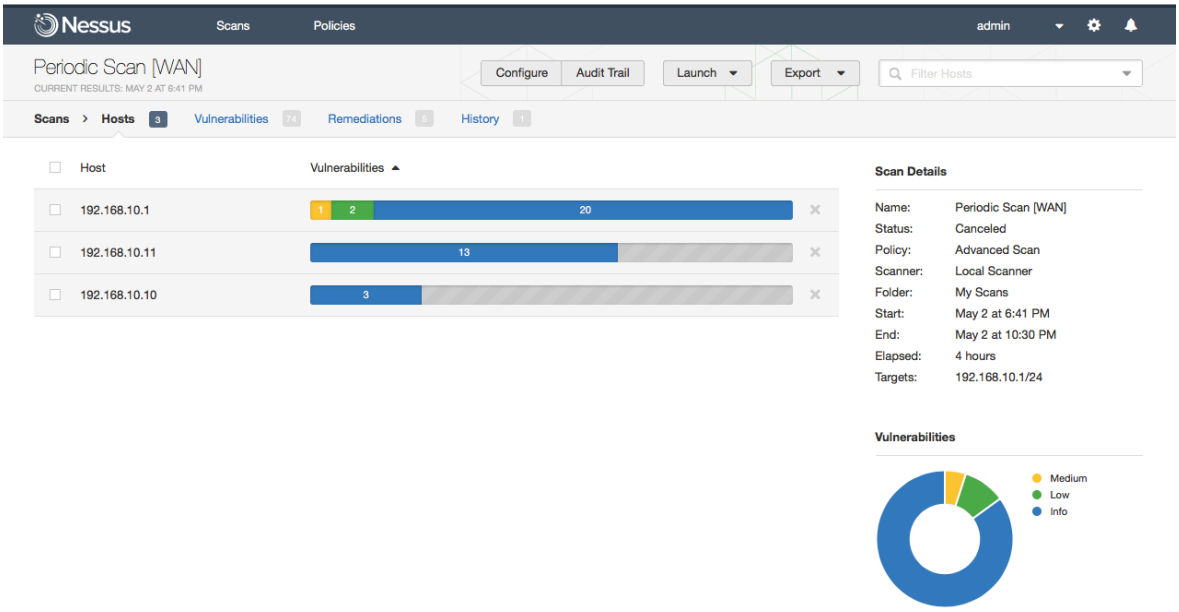
5 – Anàlisi de vulnerabilitats

Per a l'anàlisi de vulnerabilitats, farem ús d'un escàner de vulnerabilitats anomenat Nessus [17]. Aquesta eina és molt potent, ja que es bassa en vulnerabilitats publicades i, per tant, conegudes, per comprovar el nivell de seguretat d'un entorn [18], buscant possibles punts dèbils de la xarxa securitzada. Va ser creada per l'empresa americana *Tenable Network Security* i ofereix dos tipus de solucions, una de pagament, en la que es poden trobar moltes vulnerabilitats customitzades en temps real al *cloud* de l'empresa, i amb actualitzacions cada molt poc de temps, i altra gratuïta, que compta amb un llistat una mica més limitat de vulnerabilitats [19], però que així i tot, no deixa de ser exactament l'eina que necessitarem, ja que les vulnerabilitats més potents i amb menys temps de vida des del seu descobriment solen estar més dirigides a grans empreses, com multinacionals o bancs i, en cas que es dirigirà cap a un entorn domèstic, possiblement aquest no compta amb la tecnologia suficient com per a fer front a un atac de grans dimensions.

5.1 – Anàlisi de vulnerabilitats a nivell de Firewall

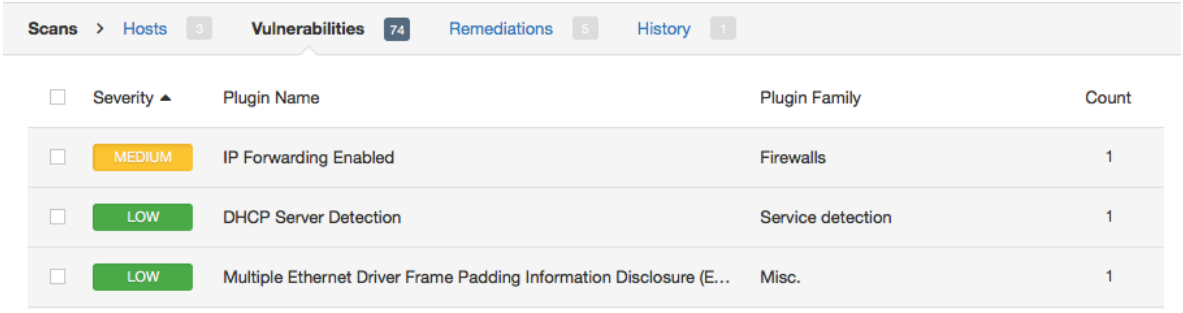
Primer, realitzarem un anàlisi situant-nos fora de la xarxa interna, justament entre el router que ens proporciona connexió a Internet i el Firewall que ens separa de la intranet. Per tant, ens connectarem mitjançant un cable al router i llençarem el Nessus des de la nostra màquina, on el deguem haver instal·lat prèviament registrant-nos a la web del fabricant. Hem de tindre en compte que aquest anàlisi triga molta estona en finalitzar, degut a que aquesta sonda de xarxa realitza moltes proves diverses. Configurarem l'escaneig per indicar tots els paràmetres que volem que tinga en compte l'analitzador, així com l'agressivitat amb la que l'escàner ha d'actuar front a totes les possibles vulnerabilitats a través del Firewall, en aquest cas.

Quan l'escaneig conclou, la interfície web de Nessus ens mostra unes estadístiques de l'anàlisi, i ens dona un petit report d'aquest, tal i com es veu a la *Imatge 13*:



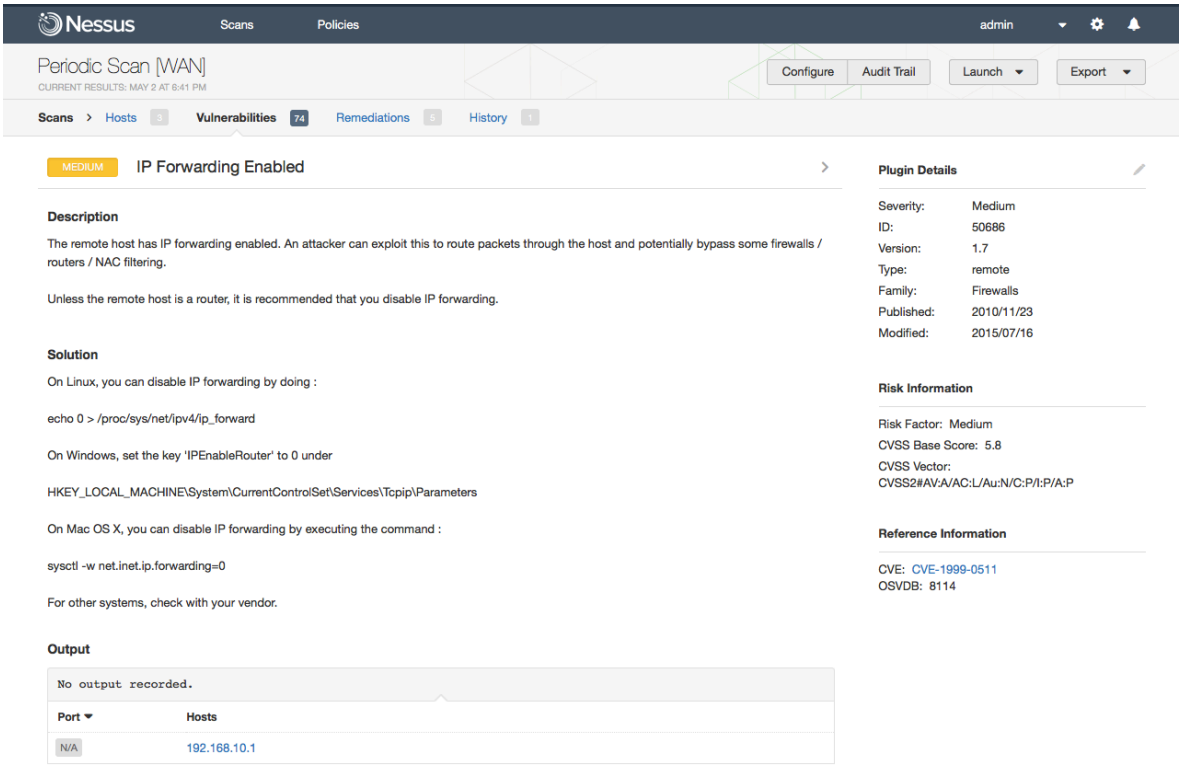
Imatge13. Resultat de l'escaneig de vulnerabilitats de la xarxa WAN.

Com podem observar ala *Imatge 14*, Nessus ens mostra una alerta de tipus *Medium* que fa referència a vulnerabilitats al Router, amb IP 192.168.10.1, anomenada *IP Forwarding Enabled*:



Imatge 14. Interfície de Nessus on ens mostra la gravetat de les vulnerabilitats trobades.

Si volem veure més informació sobre aquesta alerta, tan sols hem de clicar a sobre, i ens mostrarà la següent pantalla, com apareix a la *Imatge 15*:



Imatge 15. Interfície de Nessus on ens mostra el detall de la vulnerabilitat IP Forwarding Enabled.

Tal i com es pot veure, Nessus ens proporciona un detall sobre les conseqüències de seguretat adverses que pot ocasionar aquesta vulnerabilitat, seguit de les solucions que es poden dur a terme des de distints sistemes operatius en els quals l'alerta es done. En aquest cas, al tractar-se d'un router propietat de la companyia de telecomunicacions que

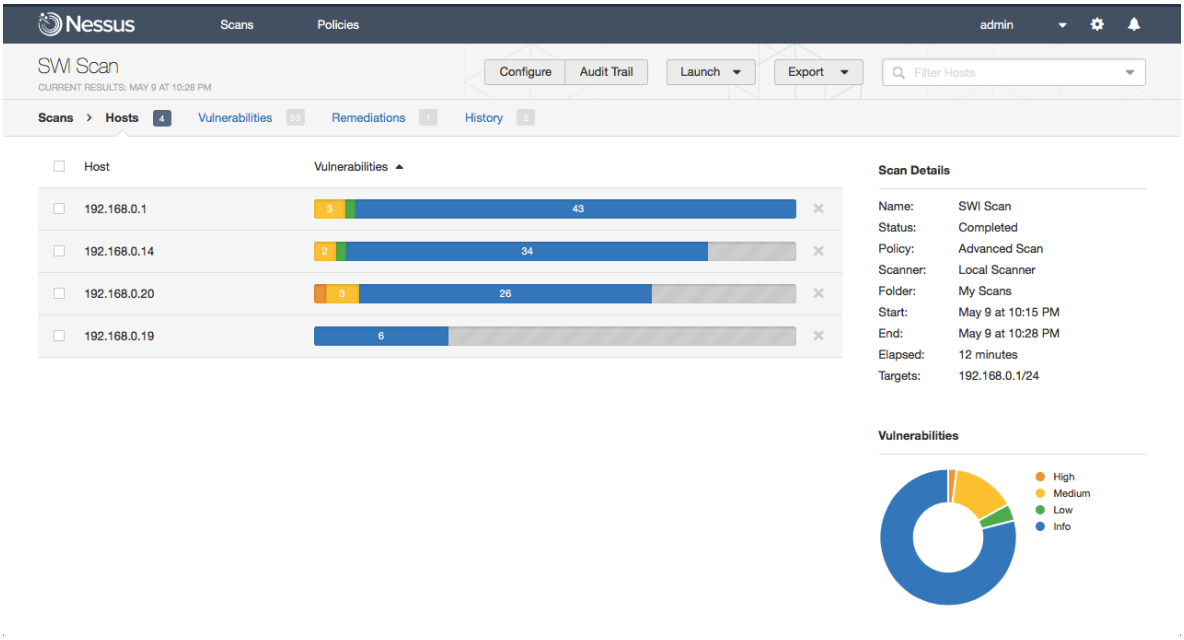
presta servei d'internet al domicili, corre sobre un sistema operatiu propi del fabricant amb el seu firmware customitzat, pel que no es pot fer cap cosa per mitigar aquesta alerta.

El que realment és rellevant en aquest cas, és que el nostre Firewall ha estat ben configurat, ja que no mostra cap possible bretxa de seguretat al sistema, pel que podem confirmar que des d'Internet cap a la nostra xarxa interna, gaudim d'un entorn segur.

5.2 – Anàlisi de vulnerabilitats a la xarxa interna SWI

A continuació realitzarem l'escaneig des de la xarxa interna, ja que tindre seguretat de foca cap a dins no significa que seguint el camí invers l'entorn siga també segur. El procediment serà el mateix que hem fet servir per a l'escaneig de la xarxa externa.

Com es pot visualitzar a la *Imatge* 16, una vegada finalitzat l'anàlisi, trobem els següents resultats, referents a l'escaneig de la subxarxa SWI:



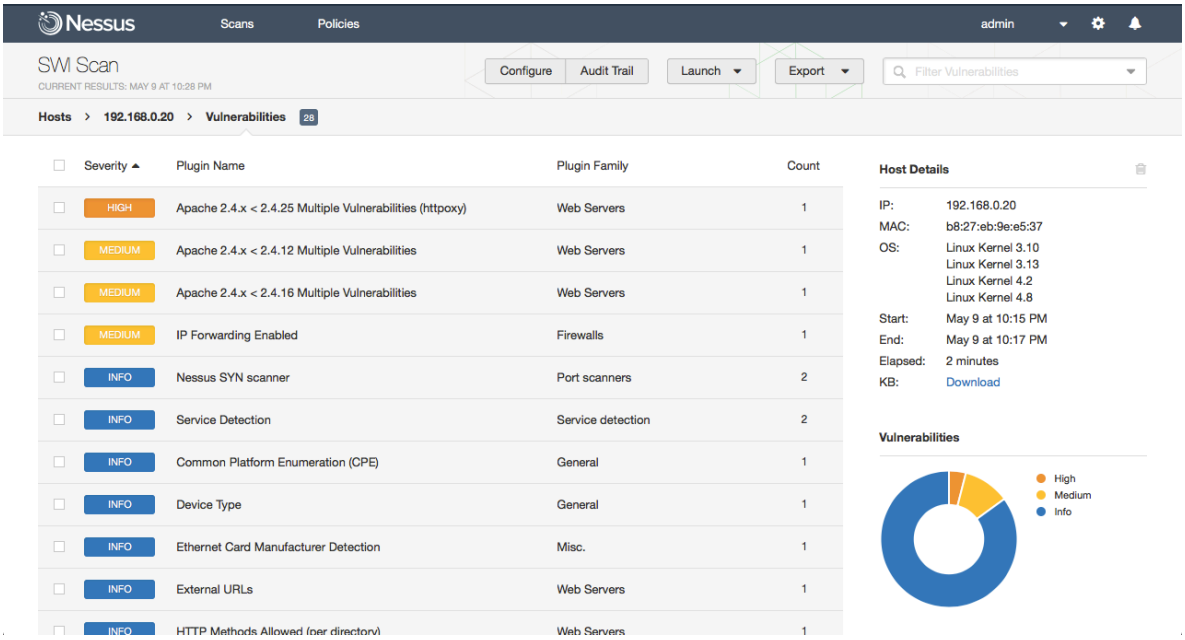
Imatge 16. Resultat de l'escaneig de vulnerabilitats de la xarxa SWI.

Finalitzat l'escaneig d'aquest segment de la xarxa, podem veure que existeixen hosts amb algunes vulnerabilitats de seguretat que són de menor importància en aquest cas, com versions de certificats SSL no fiables, degut a que no podem tindre accés a cap tipus de certificació de seguretat en la comunicació feta entre els nostres equips; o que ha trobat accessos que sols suporten claus SSH amb una encriptació que utilitza un algoritme que no és massa complex; o la detecció d'un servidor DHCP. Totes aquestes vulnerabilitats no ens han de preocupar a la xarxa interna, ja que són equips als que sols podran accedir màquines de confiança filtrades per IP al Firewall.

Per altra part, a la Raspberry Pi utilitzada com a client torrent connectada al FreeNAS, existeix una vulnerabilitat amb un risc potencial. Si volem saber quin és aquest,

ho podem saber fent click a la mateixa barra d'estat, on Nessus ens mostra el detall, tal i com es mostra a la *Imatge 17*.

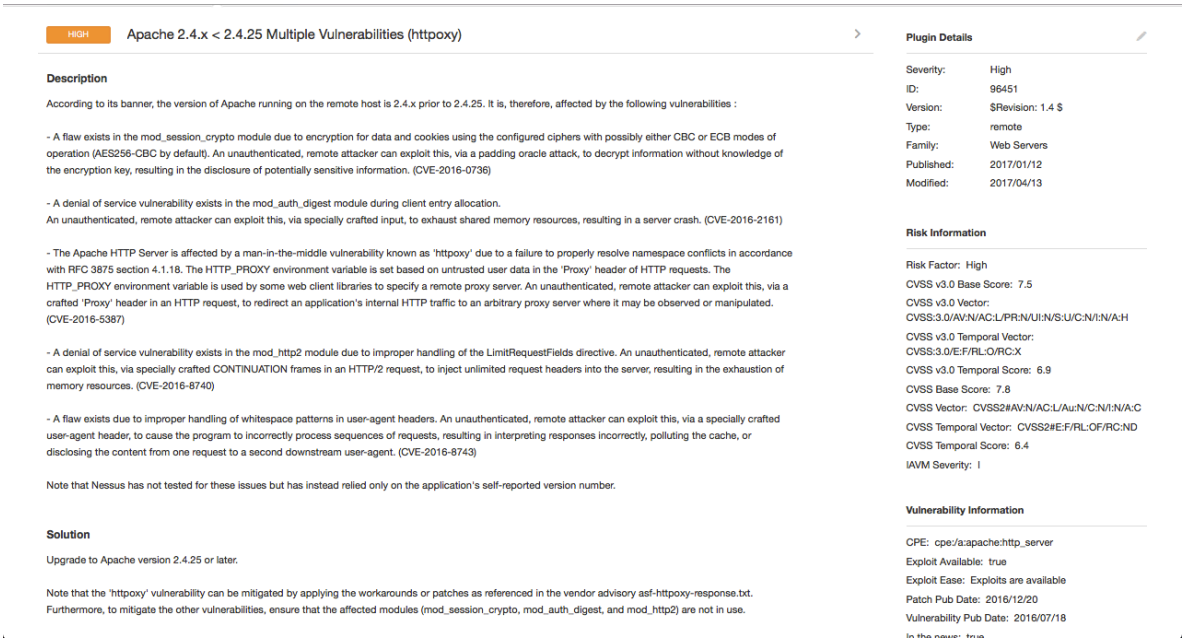
Aquest risc ve donat per una versió obsoleta del servidor Apache instal·lat a aquest Host. Aquesta versió d'Apache, concretament la 2.4.X, compta amb algunes vulnerabilitats menors i una més crítica, relacionada amb la versió del *httpproxy* amb la que compta.



Imatge 17. Interfície de Nessus on ens mostra el detall de vulnerabilitats trobades a un host concret.

Si volguérem conèixer més sobre aquesta amenaça, Nessus compta amb una gran base de dades on podem consultar el detall sobre aquesta vulnerabilitat crítica. Com mostra la *Imatge 18*, en entrar dins d'una amenaça en concret a la interfície web de Nessus, aquest ens dona informació de totes les vulnerabilitats que afecten aquesta versió d'Apache, així com els CVE (*Common Vulnerabilities and Exposures*) en el que s'han registrat aquestes totes aquestes vulnerabilitats.

Finalment, ens indica amb detall el procediment que s'ha de seguir i què hem de saber sobre com es pot solucionar o mitigar el risc al que ens exposem utilitzant aquesta versió obsoleta del conegut servidor de lliure distribució.



Imatge 18. Interfície de Nessus on ens mostra el detall de vulnerabilitats trobades al servidor Apache.

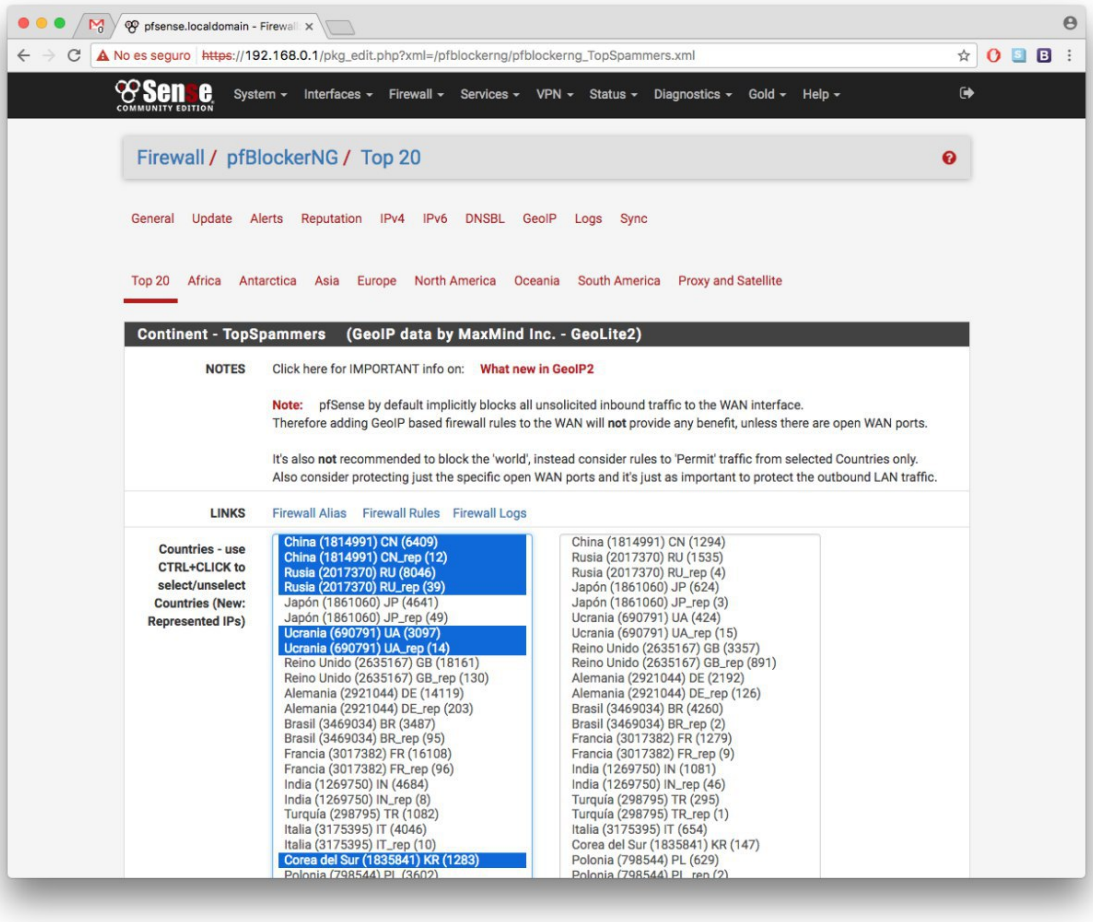
Com bé ens indica el Nessus, serà necessari procedir a actualitzar el servidor Apache instal·lat per a poder fer front a aquestes vulnerabilitats. Aquesta solució pot resultar òbvia en aquest cas, però ens podem trobar molts d'altres casos en que l'escàner de vulnerabilitats ens pot ajudar molt, be siga aportant-nos informació de mesures per mitigar vulnerabilitats que desconeguem o inclús ens pot aportar una solució de la que potser els nostres coneixements per atenuar aquesta casuística no resulten suficients, com bé pot ser l'existència d'una eina per eliminar algun tipus de *malware* concret, o un enllaç a una web on podem descarregar un *patch* que soluciona una vulnerabilitat concreta, dos exemples de solucions de les quals Nessus ens estalviaria moltes hores d'investigació i, probablement, ens puguen permetre actuar abans de que alguna amenaça puga afectar-nos.

5.3 – Testeig del Firewall

Altra prova que cal realitzar a banda de l'escaneig de vulnerabilitats és fer un anàlisi exhaustiu de les alertes que ens reporta el Firewall per crear regles més específiques i, per tant, més segures.

Per començar bloquejarem tot el tràfic dirigit cap a Rússia o Xina, evitant així connexions il·legítimes que puguen aconseguir executar una línia de comandes inversa (*Reverse Shell*). El motiu del bloqueig d'ambdós països no és altre que la gran quantitat de connexions que s'ha comprovat que intenten tindre lloc entre la xarxa interna i aquestes dues localitzacions i que el Firewall bloqueja per defecte. Els bloquejos del Firewall es donen tant per a les connexions entrants com per a les que surten, pel que probablement a l'interior de la xarxa es perden connexions dirigides a aquests països, siguen o no dolentes, pel que es decideix permetre el tràfic d'entrada però no el d'eixida, per a poder realitzar consultes utilitzant l'Internet, però no permetre cap tipus d'accés que no estiga controlat.

Als Firewalls de nova generació (NGFW) podem crear regles específiques per a geolocalització utilitzant la interfície gràfica, on podríem seleccionar els països que desitgem blocar per geolocalització, tal i com es pot observar a la *Imatge 19*:

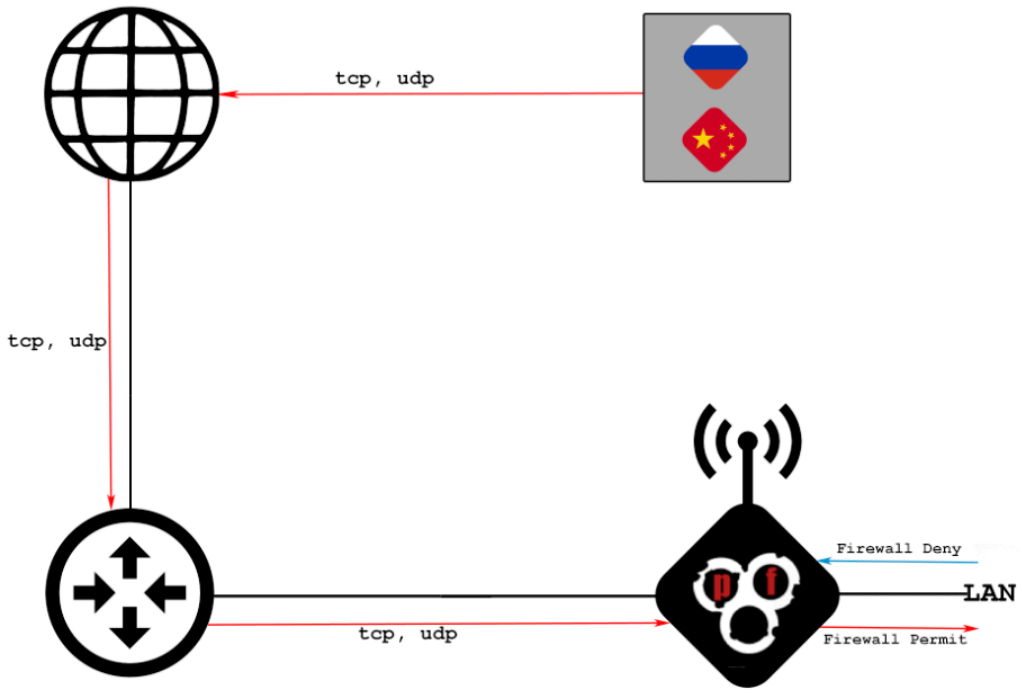


Imatge 19. Interfície de pfSense on ens mostra el llistat de països a bloquejar.

Aquesta pràctica, bloquejaria absolutament tot el tràfic provinent de servidors dels països que seleccionem al llistat, tant legítim com il·legítim. En el cas de no disposar d'un NGFW, sempre podrem aplicar les regles mitjançant *iptables* per terminal. En aquest cas, podríem passar un llistat de països que volem bloquejar per a que la cap dispositiu de la xarxa interna no tinga accés a servidors allotjats a aquests:

```
FROM $local_network
TO GeoIP_$denied_countries
PORT any
ACTION deny
```

Per tant, el tràfic que estaríem permetent quedaria esquematitzat tal i com es mostra a la *Imatge 20*, en la que es pot comprovar que el tràfic provinent dels països esmenats anteriorment queda permés per a que arribe a la xarxa interna, però no es permet la conectivitat de cap host en direcció contrària:



Imatge 20. Fluxe de les conexions permeses i denegades pel Firewall mitjançant geolocalització.

Aquest bloqueig pot semblar agressiu en un primer moment, degut a que estaríem denegant qualsevol accés a tots aquells dominis i/o IP que es troben a aquests països, però tenint en compte els serveis més utilitzats al dia a dia pels usuaris, les grans empreses de les que més es fa ús a la sortida cap a Internet tenen els seus servidors als Estats Units en gran part, pel que no tindríem cap indisponiblitat en quan a l'ús diari d'Internet ni percebríem aquest bloqueig si no accedim de costum a dominis *.ru* o *.cn*. En canvi, estariem protegint els equips interns de dues de les localitzacions mundials on més connexions procedents d'atacs de control invers es produeixen cada dia.

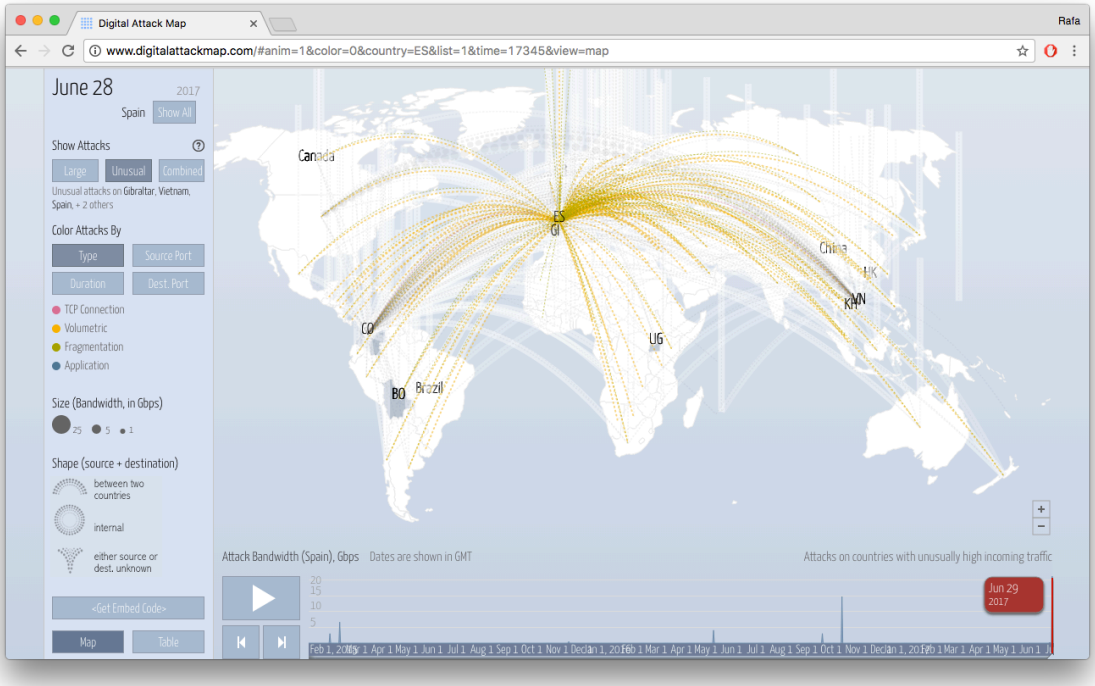
5.4 – Testeig del IPS

L'IPS analitzarà el tràfic i realitzarà reports segons les alertes que hajam predefinit. Aquestes alertes, sols són informatives, pel que no es realitzarà ningún bloqueig a priori, ja que el Firewall ha sigut configurat amb polítiques molt restrictives.

No obstant, existeixen una sèrie d'atacs els quals es volen bloquejar, ja que en aquests casos concrets, no es sofriria cap compromís a la connexió ni es tallaria cap tipus de tràfic legítim, ja que es van a crear alertes específiques per a atacs coneguts, com serà el cas d'un atac de denegació de servei distribuït (*DDoS*), que sol ser un dels més comuns i dels més fàcils de realitzar.

Per elaborar la regla que ha de fer front a l'atac *DDoS*, haurem de valorar quines casuístiques es poden donar per a que es considere un atac de denegació de servei, entenent en què consisteix aquest tipus d'atac. A la pàgina web *Digital Attack Map* [20]

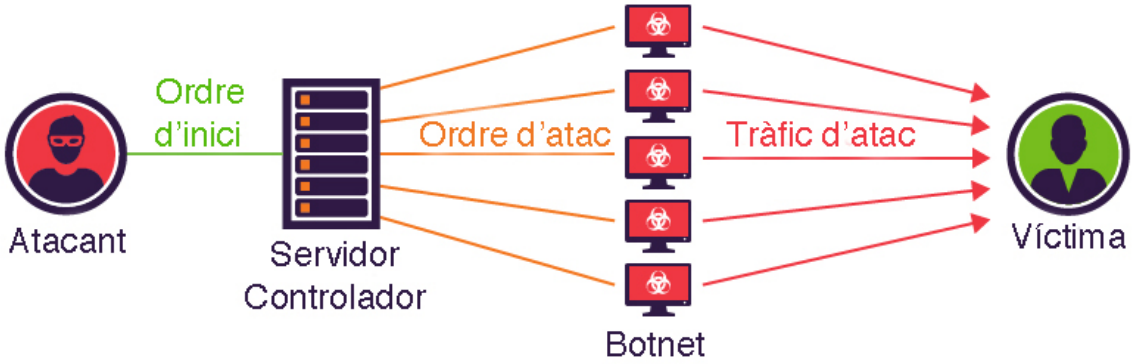
podem veure molts d'aquests atacs diàriament en temps real o filtrant per data a un mapamundi. A la *Imatge 21* es pot veure una captura de la web esmentada en la que es produeix un atac *DDoS* en el que l'estat espanyol és el destí:



Imatge 21. Pàgina web on es mostra un atac DDoS amb Espanya com a destí d'aquest.

Tal i com es pot observar, un atac *DDoS* és quelcom molt més usual del que sembla, i compta amb nivells de volum de tràfic molt elevats, amb procedència pràcticament d'arreu del món, pel que ens fa adonar-nos que crear una regla front un atac d'aquest tipus pot ser molt positiu per a la seguretat del nostre entorn.

A la *Imatge 22* podem veure una de les topologies més típiques d'una infraestructura preparada per a realitzar un tipus d'atac *DDoS* on, mitjançant una *botnet*, un usuari amb accés a moltes màquines, que perfectament poden ser virtualitzades, ordena realitzar moltes peticions massives cap a una direcció concreta:



Imatge 22. Infraestructura i procés d'un atac DDoS.

Un atac DDoS pot donar-se de moltes maneres. Aquest, pot estar compost per un conjunt de poques peticions amb un TTL molt elevat al paquet transmès; o per un volum de peticions molt elevat i de forma massiva, arribant a assolir fins un terabit per segon en aquestes connexions. Com que aquest últim és el més comú, centrarem la regla de l'IPS Suricata en mitigar aquest possible atac:

```
drop tcp any any -> $HOME_NET any (msg:"Possible TCP DDoS Attempt"; flow: stateless;
threshold: type both, count 40, seconds 10; sid:10001;rev:1;)

drop udp any any -> $HOME_NET any (msg:"Possible UDP DDoS Attempt"; flow: stateless;
threshold: type both, count 40, seconds 10; sid:10002;rev:1;)

drop icmp any any -> $HOME_NET any (msg:"Possible ICMP DDoS Attempt"; flow: stateless;
threshold: type both, count 40, seconds 10; sid:10003;rev:1;)
```

Amb aquestes regles, estarem bloquejant totes aquelles IP que es troben fora de la nostra xarxa interna i que intenten accedir a ella a través de qualsevol port, fixant un ombrall de bloqueig sempre i quan realitzen un total de 40 intents de connexió en un termini màxim de 10 segons.

Per tant, ara tindrem un nivell de protecció més elevat contra un tipus d'atac molt comú, i un dels que més problemes ocasiona a nivell mundial, degut a que es pot realitzar de diverses formes sense necessitat de tindre molts recursos. Hi ha molts equips de seguretat que poden fer front a una denegació de servei, però així i tot, tots són vulnerables si aquesta es realitza amb una quantitat de paquets per segon molt elevada, arribant a ficar en perill infraestructures molt crítiques.

6 - Conclusió

6.1 – Compliment de l'objectiu

El desenvolupament de la xarxa securitzada ha sigut exitós, així com la configuració de tots els elements que la componen. S'han assignat IP estàtiques a tots els equips per evitar problemes amb el Firewall i per a que el port de *management* dels elements que la formen siga accessible per als usuaris interns, possibilitant la seva configuració en cas de que la xarxa es tingués que escalar en un futur o s'implementaren nous equips a aquesta, bé elements de seguretat com altres dispositiu d'ús domèstic, com una *smart* TV o impressores Wifi.

Per altra banda, es corrobora que amb una inversió gens elevada, es pot adquirir un dispositiu per a configurar com a Firewall entre Internet i la xarxa interna, possibilitant així l'accés a tothom a poder muntar una infraestructura segura a un entorn domèstic o, fins i tot, a una petita o mitjana empresa, variant el preu del dispositiu depenent del tipus de segmentació que es desitja fer dintre la xarxa.

6.2 – Conclusions sobre el projecte

Com hem pogut observar al llarg del desplegament d'aquesta xarxa securitzada, podríem concloure en que deuria ser pràcticament obligatori que tothom comptés amb algun mètode de securització de xarxa al seu desplegament domèstic, independentment del tamany d'aquesta.

És clar que els antivirus protegeixen les nostres màquines de *malware* conegut, ja que aquests es basen en una sèrie de patrons que busquen a tots els arxius que escanejen; però disposar d'un antivirus no ens lliura de que les nostres comunicacions estiguen sent interceptades, o que qualsevol persona puga tindre accés remot a una màquina personal sense que nosaltres sigam conscients d'aquest fet, com bé podria ser un televisor o un servidor multimèdia, en els que no instal·lem cap tipus d'analitzador de *malware* per evitar que siguen infectats o vulnerables a qualsevol mètode *C&C* (*Command & Control*).

Per altra part, amb un simple antivirus mai podem saber quines connexions tenen lloc a la nostra xarxa, tant cap a l'interior d'aquesta com d'ixida a Internet, pel que en cap moment podem saber si tot el tràfic que està cursant-se a una mateixa xarxa interna, és o no legítim, ficant en perill total la nostra privacitat, tant de dades com altre tipus d'informació més delicada. Així que si no és suficient amb l'ús d'un antivirus, tampoc és suficient utilitzant una contrasenya molt complexa amb encriptació WPA2 al router que ens dona accés a internet, ja que aquest fet no ens està protegint més enllà dels usuaris que puguen tindre accés a la nostra xarxa Wifi, i de segur que no tothom és aliè als mètodes per vulnerar la seguretat d'una contrasenya Wifi, independentment de quin siga el tipus d'encriptació que utilitze aquesta.

Un dels problemes més evidents que presenta la societat avui en dia és el desconeixement front al perill que suposa Internet i la quantitat de dades que, bé poden estar proporcionant conscientment o bé inconscientment, així com la gran quantitat d'informació personal que pot estar sent robada sense que un usuari ho sàpiga o la falta d'informació de la que disposem front a vulnerabilitats a una xarxa domèstica. És molt comú

escoltar la frase "*Si em hackejen em te igual, perquè no tinc res que amagar*", i és un error molt gran tindre aquest pensament, ja que així, donem pas a que vulneren la nostra pròpia privacitat, i ja no a les xarxes socials, si no amb escoltes telefòniques o rastrejos d'activitat al nostre dia a dia, tant dins d'Internet com fora.

És per totes aquestes raons, que securitzar un entorn domèstic, encara que siga amb un Firewall entre la xarxa i Internet deuria ser necessari a tots els domicilis, ja que és l'única forma que podem tindre de controlar les connexions que tenen lloc al nostre propi entorn. Està clar que no tothom compta amb coneixements com per realitzar un desplegament d'un Firewall, però avui en dia, existeixen molts llocs a la web on podem trobar explicacions de com realitzar tots aquests processos, tant per a usuaris novells com per a d'altres amb més experiència. Pel que podem afirmar que un entorn securitzat a nivell d'usuari és pot considerar un benefici a curt termini que està a l'abast de tothom.

6.3 – Problemes sorgits i solucions

El major problema que s'ha trobat durant el desenvolupament de la xarxa ha sigut la configuració de les interfícies del Firewall. Per a un usuari que no està familiaritzat amb una distribució FreeBSD, potser és una mica complexe moure's a través dels menús, de vegades molt abstractes, que ens ofereixen certes distribucions d'aquest sistema operatiu. En aquest cas,

En el cas de *pfSense*, existeixen molts fòrums online on es solucionen els problemes que els usuaris exposen, així com al manual d'instal·lació, on s'especifiquen els passos a seguir. És amb aquest manual en el que es va trobar com solucionar un dels problemes més crítics que han hagut durant el desplegament, i és que en configurar el mateix Firewall, aquest et bloqueja l'accés al port de configuració pel que has fet la instal·lació, pel que s'ha de fer servir un cable USB-RS232 connectat directament al dispositiu, deixant les interfícies Ethernet únicament per a tràfic de xarxa.

6.4 – Aportacions personals

Aquest projecte m'ha ajudat a consolidar molts dels conceptes que he assolit durant l'any en el que m'he dedicat a la Seguretat Informàtica. Quan entres a treballar a un lloc on ja està tota la infraestructura muntada, realment coneixes com s'han d'administrar les eines o com explotar les seves funcionalitats, però tot el procés de configuració i el desplegament de tota la xarxa perimetral el desconeixes completament.

Gràcies a aquest treball, he pogut muntar la meva pròpia xarxa securitzada, i he aprés com desplegar eines de seguretat des de zero, un complement d'alt valor per a mi i el meu dia a dia laboral, ja que m'aporta un valor afegit tant personal com professional, i en un moment de creixement de la demanda d'experts en seguretat informàtica, són característiques que poden ser decisives per a que una empresa es decidisca per un treballador o altre.

6.5 – Futures línies de treball

Cada vegada aniran sorgint noves vulnerabilitats als sistemes que componen la xarxa, així com nous tipus d'atacs, cada vegada més complexos i més difícils d'aturar. En aquests casos, el tindre programat un escaneig de vulnerabilitats setmanalment és essencial, perquè s'han d'anar aplicant actualitzacions i customitzacions de regles, tant a nivell de Firewall com a nivell d'IPS, pel que es pot considerar que l'administració d'una xarxa securitzada mai acaba.

Per altra banda, no es descarta el fet d'afegir altres elements amb el temps, com la implementació de Firewalls a l'entrada de cada subxarxa o, fins i tot, sistemes de autenticació centralitzada per accedir als dispositius crítics que puga haver distribuïts per la xarxa.

7 – Bibliografia

[1] EC-Council Press, *Network Defense: Perimeter Defense, Course Technology*, Abril 2010.

[2] DIRECTIVA (UE) 2016/1148 DEL PARLAMENT EUROPEU Y DEL CONSELL del 6 de juliol de 2016. Disponible a: https://www.boe.es/doue/2016/194/L00001-00030.pdf

[3] Directiva 2016/1148 de la UE. Capítol IV: Seguretat de les xarxes i sistemes d'informació dels operadors de serveis essencials. Article 14: Requeriments en matèria de seguretat i notificació d'incidents. Disponible a: https://www.boe.es/doue/2016/194/L00001-00030.pdf

[4] Article 16: Directiva 2016/1148 de la UE. Capítol VI: Seguretat de les xarxes i sistemes d'informació dels operadors de serveis digitals. Article 16: Requeriments en matèria de seguretat i notificació d'incidents. Disponible a:
https://www.boe.es/doue/2016/194/L00001-00030.pdf

[5] Reglament (UE) 2016/679 del Parlament Europeu i del Consell. 27 d'abril de 2016. Disponible a:
http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES

[6] Escut de Privacitat per als fluxes de dates transatlàntics. European Comission Press Release Database. Disponible a: http://europa.eu/rapid/press-release_IP-16-2461_es.htm

[7] Codi de Dret de la Ciberseguretat. BOE-173. Disponible a:
https://www.boe.es/legislacion/codigos/codigo.php?id=173_Codigo_de_Derecho__de_la_Ciberseguridad

[8] *pfSense*. Pàgina web de pfSense. Disponible en https://www.pfsense.org

[9] Christopher M. Buechler, Jim Pingle, *pfSense: The Definitive Guide*, Reed Media Services, Novembre 2009.

[10] Brian Komar, Ronald Beekelaar,Joern Wettern, *Firewalls for dummies*, Wiley Publishing, Març 2003.

[11] Lawrence C. Miller, *Next-Generation Firewalls for dummies*, Wiley Publishing, Novembre 2011.

[12] Open Information Security Foundation, *Suricata User Guide*, Maig 2016. Disponible en https://media.readthedocs.org/pdf/suricata/latest/suricata.pdf

[13] David R. Miller, Shon Harris, Allen Harper, Stephen Vandyke, Chris Blask, *Security Information and Event Management (SIEM) Implementation*, McGrawHill Education, Novembre 2010.

[14] Dave Taylor, *Wicked Cool Shell Scripts: 101 Scripts for Linux, OS X, and UNIX Systems*, No Starch Press, Novembre 2016.

[15] William E. Shotts, *The Linux Command Line: A Complete Introduction*, No Starch Press, ISBN: 978-15-93273-89-7, PÀGINES 480, Gener 2012.

[16] Mark Lutz, *Programming Python: Powerful Object-Oriented Programming*, O'Reilly Media, Gener 2011.

[17] TENABLE: Nessus Product Overview.
http://www.tenable.com/products/nessus-vulnerability-scanner

[18] Russ Rogers, Mark Carey, Paul Criscuolo, Mike Petruzzi, *Nessus Network Auditing*, Syngress, Maig 2008.

[19] Rafay Baloch, *Ethical hacking and Penetration Testing Guide*, Auerbach Publications, ISBN: 978-14-82231-61-8, PÀGINES 498, Gener 2014.

[20] Digital Attack Map. Disponible a: http://www.digitalattackmap.com/

[21] Understandig DDoS Atack. Disponible a:
http://www.digitalattackmap.com/understanding-ddos/

Jon Erickson, *Hacking: The Art of Exploitation*, No Starch Press, Febrer 2008.

The Snort Project, *Snort User Manual*, Novembre 2016
https://www.snort.org/documents/snort-users-manual

Pàgina web de The Proxy Authority. Disponible en https://www.proxy.org

Pàgina web de The Snort Project. Disponible en https://www.snort.org

Pàgina web de Open Information Security Foundation. Disponible en https://oisf.net

Pàgina web de w3schools. Disponible en
https://www.w3schools.com/html/default.asp