1.1 Introdución

Esta actividade ten como finalidade entender qué é un tornalume ou firewall e cal é a súa finalidade como elemento de seguridade perimetral. Analizaranse os diferentes tipos de firewalls e o seu funcionamiento para poder escoller cal é o máis axeitado en base ós requerimentos da organización.

Empregarase a distribución pfSense para comprender qué son as regras de filtraxe, cómo crealas e organizalas para crear un *ruleset* ou xogo de regras. Esta distribución, baseada no sistema UNIX FreeBSD, permite implantar un sistema firewall extremadamente potente e fiable; á vez que sinxelo de xestionar, grazas a súa interface web.

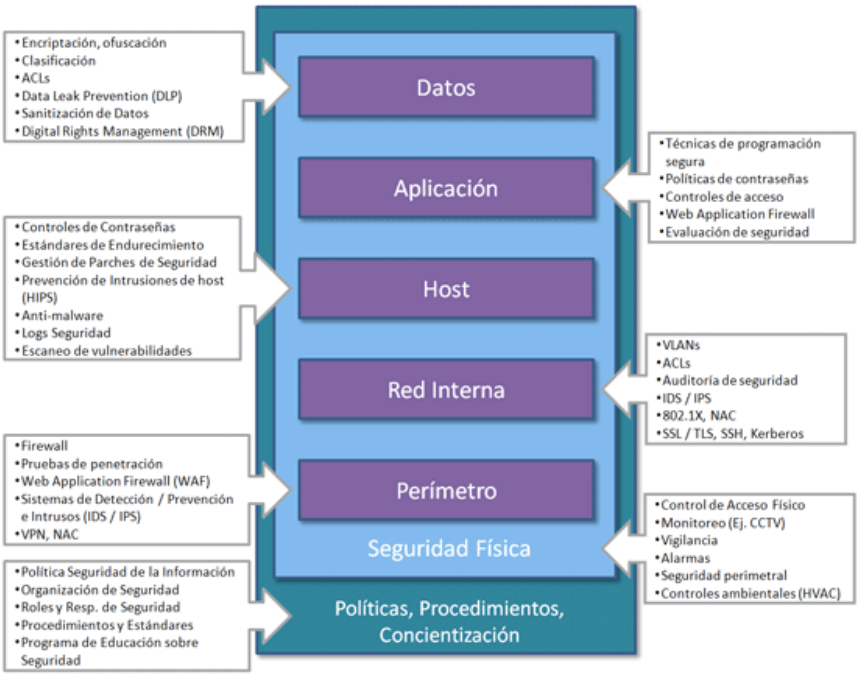
Ademais de crear regras de filtraxe axeitadas, deseñaranse probas para verificar que o firewalls funciona en base ós requerimentos estabrecidos no momento do deseño, sen bloquear nin permitir máis tráfico do desexado.

1.2 Actividade

1.2.1 A defensa en profundidade e o perímetro

O concepto de defensa en profundidade procede do ámbito militar e fai referencia a establecer múltiples liña de defensa, en vez dunha única liña moi forte. A idea deste sistema é a de atrasar o máximo posible o avance do inimigo.

Levando este concepto ao mundo da informática, crearanse capas de defensa para evitar ataques directos á información sensible dun ámbito. Este sistema proporciona un maior tempo para defenderse á vez de aumentar a probabilidade de detectar un ataque.



Asegurar o perímetro é unha das estratexias defensivas máis eficaces comunmente utilizadas dende antano no campo da seguridade. Abonde para iso recordar as fortificacións medievais nas que existía tan só un número restrinxido de puntos de entrada nos que se aplicaba un forte control de acceso. Reducir a superficie de exposición, crear puntos controlados de acceso e centrar as defensas neses puntos permite optimizar a capacidade defensiva. Para reforzar a eficacia da fortificación existían así mesmo, elementos engadidos de seguridade como gardas, fosos, barreiras naturais, portas falsas ou perímetros internos á propia fortificación. Tamén foron moitas as portas traseiras ou poternas construídas por comodidade, e que cando non foron debidamente mantidas en segredo supuxeron a caída de fortalezas.

O mundo das tecnoloxías da información e as comunicacións (TIC) adoptou estas ideas ao longo dos últimos anos, creando arquitecturas e dispositivos que permitisen realizar as mesmas tarefas con idéntica eficacia. No centro destas tecnoloxías encóntranse os tornalumes ou *firewalls*: puntos controlados de acceso.

1.2.2 Firewalls

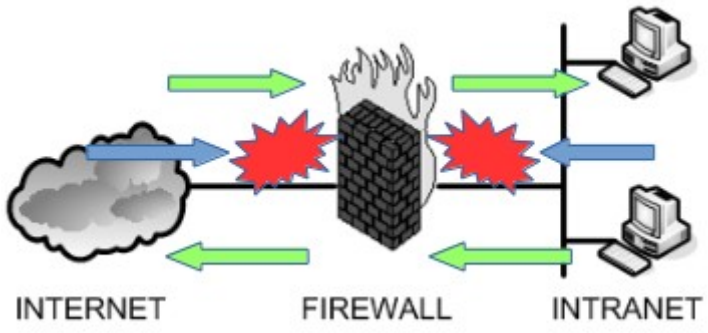
Un firewall consiste nun dispositivo formado por un ou varios equipos que se sitúan entre a rede da empresa e a rede exterior que analiza todos os paquetes que transitan entre ambas as dúas redes e filtran os que non deben ser reenviados, de acordo con algún criterio establecido de antemán.

Un firewall trata de resolver os problemas de acceso seguro cara a/dende o exterior, e para isto analiza os paquetes poñendo a atención en varios puntos:

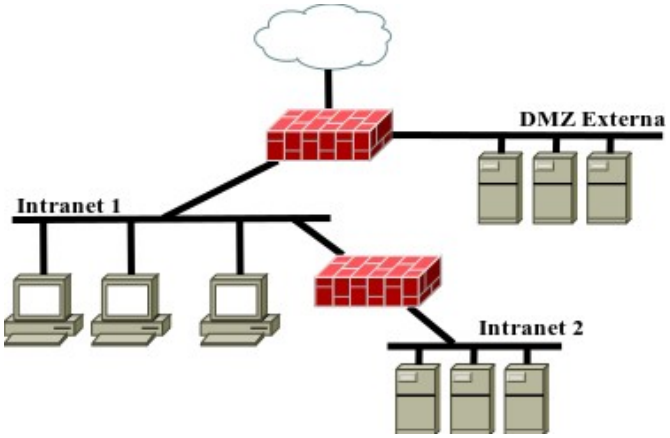
- Procedencia: equipo ou rede de procedencia do paquete, interface pola que se recibe, etc.
- Destino: equipo ou rede de destino, interface pola que sae, porto destino, etc.
- Protocolo empregado: IP, ICMP, TCP, UDP, etc.
- Contido: tamaño do paquete, contido dos datos de aplicación (url, palabras presentes na páxina), etc.

En resumo, un firewall permite:

- Protexer e illar as aplicacións, servizos e máquinas da rede interna de tráfico entrante non desexado procedente de redes externas (Internet).
- Limitar ou cortar o acceso de equipos da rede interna a servizos ofertados por redes externas á organización (Internet).



Os firewalls non só úsanse para separar Internet e a rede interna dunha organización, tamén se usan para separar ámbitos dentro da organización que requiran niveis de seguridade diferentes. A modo de exemplo, na seguinte imaxe pódese ver un primeiro firewall separando Internet dunha rede DMZ externa (onde estarían os servidores públicos da organización accesibles desde Internet) e o resto da rede interna da organización. Ademais, un segundo firewall separa a rede interna da organización en dúas zonas (Intranet 1 e Intranet 2).



A misión dun firewall é a de facer cumprir unha política de control de acceso entre redes; é dicir, permitirase ou denegará o acceso a recursos de rede a determinados clientes. Estes privilexios de acceso estarán recollidos nunha ou varias regras (*rules*), formando o que se coñece como xogo de regras ou *ruleset*. Cada regra identificará un determinado tipo de paquete e define que acción debe aplicarse.

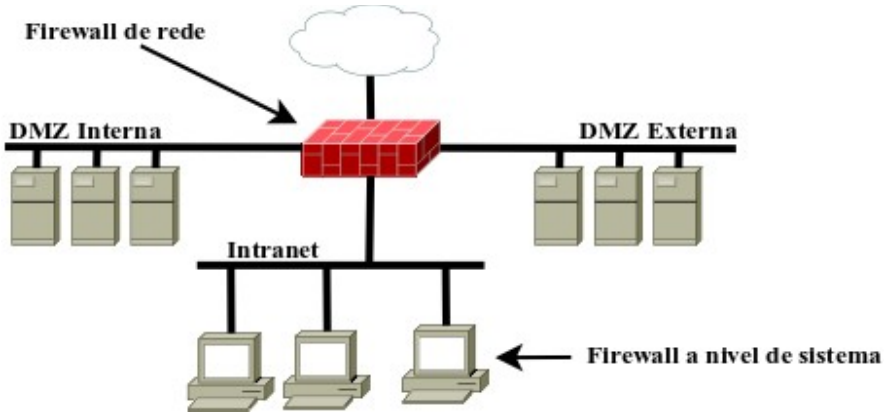
ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	*	*	*	192.168.0.255	*	*	none		no registrar broadcasts
	TCP	*	*	192.168.2.110	22 (SSH)	*	none		NAT ssh ubuntu server 10.04-2
	TCP	*	*	192.168.2.110	21 (FTP)	*	none		NAT ssh ubuntu server 10.04-2
	TCP	*	*	192.168.2.110	10000	*	none		NAT webmin ubuntu server 10.04-2

1.2.3 Tipos de firewalls

Existen múltiples clasificacións dos firewalls sobre a base de criterios como nivel da pila TCP/IP no que traballan, ámbito de aplicación, funcionalidades...

Sobre a base do ámbito de aplicación:

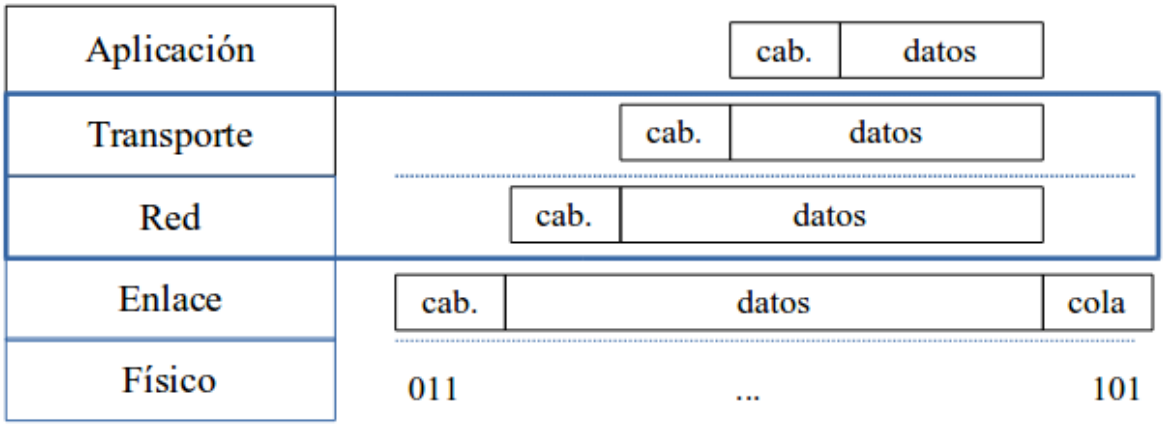
- Firewalls de rede: controla o tráfico da rede permitindo unha xestión centralizada da seguridade.
- Firewalls a nivel de sistema: instalado como aplicación local controlando o tráfico con orixe ou destino o equipo.



Sobre a base do nivel da pila TCP/IP na que traballan :

- Network Level Firewalls: serían similares a routers que traballan fundamentalmente nos niveis de rede e transporte, encargándose de analizar os valores contidos nas cabeceiras dos datagramas IP, segmentos TCP e datagramas UDP e sobre a base dunha serie de regras establecidas polo administrador deciden a acción a realizar co paquete de datos: aceptalo, descartalo ou reenvialo. Ademais do filtrado estes dispositivos adoitan facer NAT.

firewall nivel de pila



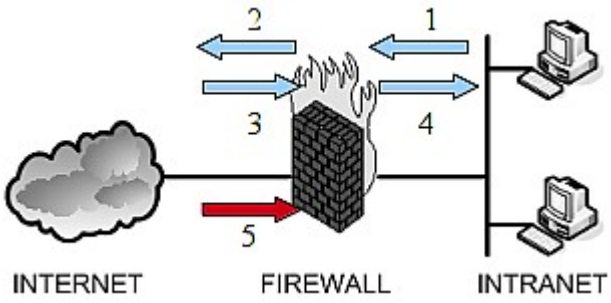
Os network level firewall clasifícanse en dous grandes subtipos:

- Static/Stateless Packet Filtering: cada paquete analízase de forma individual e independente en base a unha lista de control de acceso sobre a información de cabeceira das capas de rede e transporte (dir. IP orixe/destino, portos TCP/UDP, flags TCP...). Este tipo de firewall non memoriza o estado das conexións a nivel de transporte permitidas con anterioridade. Por exemplo, unha regra que permita conexións ó porto tcp 80, permitirá calquera paquete tcp con porto destino o 80, con independeza de que sexa o primeiro paquete dunha conexión tcp, o último, un paquete de datos ou un paquete sen ningún sentido pero que cumpre destino porto 80 tcp. Un exemplo deste tipo de firewalls é un router con funcións de filtrado básicas.
- Stateful/Dynamic Packet Filtering: mellora ao stateless packet filtering mantendo información de estado das conexións establecidas. A información de estado das comunicacións gárdase nunha *táboa de estado* que permite tratar aos paquetes non de forma individual, se non como paquetes participantes dunha conexión existente ou como paquetes iniciadores dunha nova comunicación.

  As regras son 'dinámicas' e cambian en función da situación. Por exemplo, este tipo de firewall recoñecerá todos os paquetes procedentes de equipos da rede da empresa e unicamente permitirá tráfico do exterior que sexa resposta a peticións internas. Para explicar con detalle este punto, na seguinte figura o firewall está configurado para permitir únicamente que os equipos da intranet poidan navegar por Internet; é dicir, pódese solicitar páxinas web e recibir as respostas dos servidores pero o resto do tráfico está prohibido:

  - Paquete 1: o equipo A da intranet lanza unha petición para ver unha páxina web nun servidor de Internet.
  - Paquete 2: o firewall déixao pasar en base ás regras e garda na súa táboa de estado toda a información relativa a esta conexión tcp.
  - Paquete 3: o firewall recibe unha resposta do servidor á solicitude enviada polo equipo A.
  - Paquete 4: grazas a información gardada na táboa de estado, o firewall recoñece este paquete coma un paquete lexítimo pertencente á conexión anteriormente autorizado e déixao pasar hacia ó interior da organización.
  - Paquete 5: o firewall recibe un paquete dende Internet para abrir unha conexión co equipo A da Intranet. Como non hai regra que o deixe entrar e non está asociado na

táboa de estado a algunha conexión coñecida e autorizada previamente, o firewall non o deixa pasar.



O firewall pode coñecer a historia dun paquete grazas á súa táboa de estado. As entradas da táboa de estado bórranse ao pecharse a conexión ou pasado un tempo de inactividade.

Proto	Source -> Router -> Destination	State
icmp	192.168.0.253:12383 -> 192.168.0.100	0:0
tcp	192.168.1.253:443 <- 192.168.1.1:37048	ESTABLISHED:ESTABLISHED
udp	192.168.1.253:53 <- 192.168.1.1:54137	SINGLE:MULTIPLE
udp	192.168.0.253:38080 -> 80.58.32.97:53	MULTIPLE:SINGLE
udp	192.168.0.253:38080 -> 80.58.0.33:53	MULTIPLE:SINGLE
udp	192.168.1.253:53 <- 192.168.1.1:44515	SINGLE:MULTIPLE
udp	192.168.0.253:44834 -> 80.58.32.97:53	MULTIPLE:SINGLE
udp	192.168.0.253:44834 -> 80.58.0.33:53	MULTIPLE:SINGLE
udp	192.168.1.253:53 <- 192.168.1.1:36206	SINGLE:MULTIPLE
udp	192.168.0.253:48118 -> 80.58.32.97:53	MULTIPLE:SINGLE
udp	192.168.0.253:48118 -> 80.58.0.33:53	MULTIPLE:SINGLE

Exemplos de stateful packet filtering son pfSense e netfilter (iptables).

- Application Level (proxys ou circuit level): Traballan no nivel de aplicación actuando de intermediarios entre unha rede segura e unha rede non segura, aceptando peticións dos clientes e actuando no seu nome ante os servidores.

  Entre os labores típicos deste tipo de firewall encóntranse:

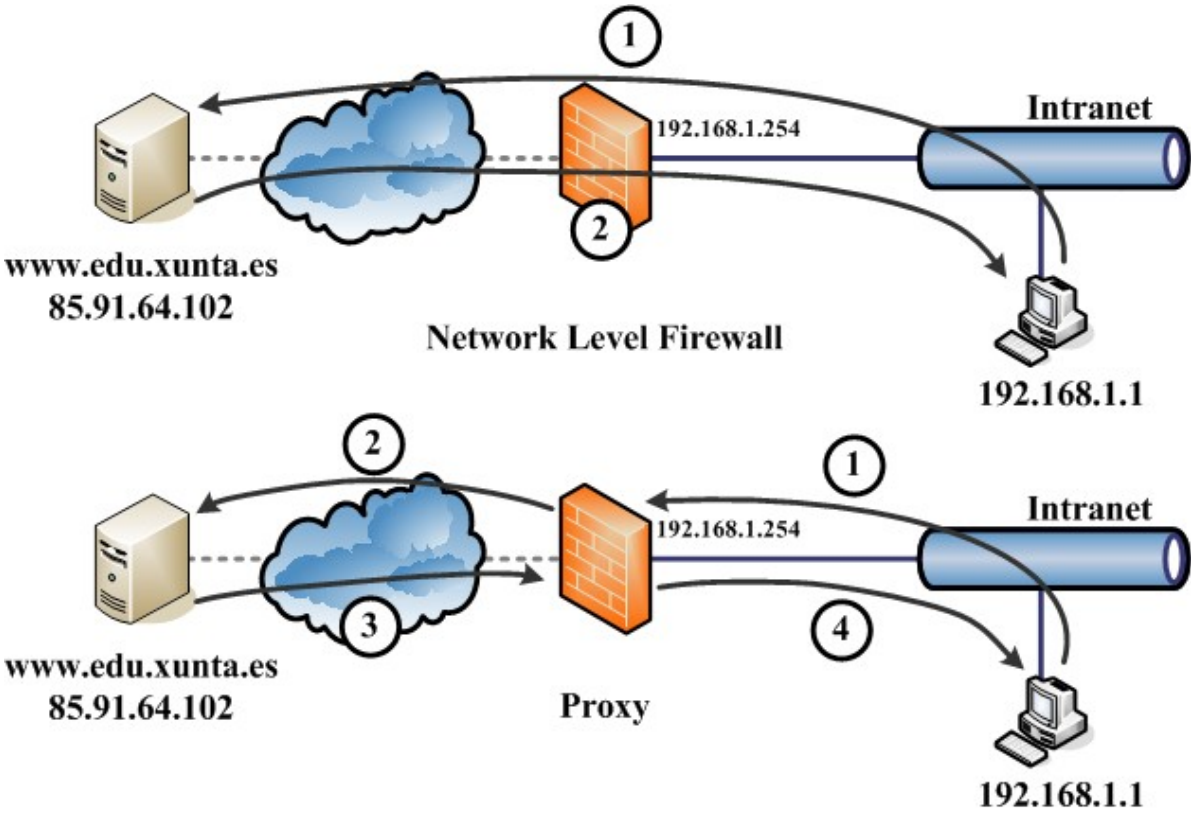
  - Permitir (ou non) as comunicacións en función de:
    - A súa orixe e/ou destino.
    - O protocolo de nivel de aplicación usado.
    - A aplicación utilizada para comunicarse co exterior (p.e. permitir firefox e I.E. e bloquear o resto de navegadores).
    - O contido dos datos de aplicación (p.e. impedir o acceso a páxinas deportivas, páxinas pornográficas, ...).
  - Autenticar ós usuarios contra bases de datos locales ou directorios (Active Directory, LDAP, Radius, etc.).
  - Propocionar un servizo de logs a nivel de aplicación, o que proporciona información para fins de auditorías.

Na seguinte imaxe pódese comparar o funcionamento dun network level firewall e un firewall de nivel de aplicación. Co network level firewall, o cliente contacta directamente co servidor, saíndo a Internet a través do firewall (que será visto como un router polo cliente). Sen embargo, co proxy o cliente non fala directamente co servidor onde está a información que lle interesa; o cliente contacta co seu proxy e indica a información na que está interesado, e é o proxy o que contacta co servidor.

- Paquete 1: o proxy recibe unha solicitude dun programa cliente (p. e., un cliente web como Firefox ou IE que solicita http://www.edu.xunta.es).
- Paquete 2: o proxy reempaqueta a solicitude coma se fose súa e envíaa ao servidor.
- Paquete 3: o servidor realiza o servizo solicitado e envía a información ao proxy.
- Paquete 4: unha vez obtida a resposta, o proxy envíalla ao cliente que a solicitara.

Debido ó seu modo de funcionamento son considerados como os máis seguros ao illar completamente os clientes e os máis intelixentes ao traballar na capa superior da pila de protocolos. Non obstante, estas características levan consigo unha maior necesidade de recursos.

Exemplos de proxys son Squid e HAProxy.



1.2.4 pfSense

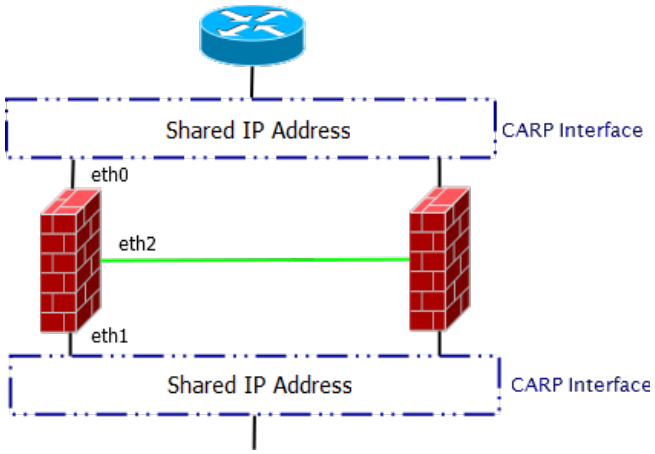
PfSense é unha distribución baseada en UNIX FreeBSD adaptada para funcionar como firewall de rede ou como router.

Na páxina web https://www.pfsense.org/about-pfsense/features.html pódese atopar

unha listaxe coas funcionalidades proporcionadas por pfSense.

Entre as funcionalidades máis salientables de pfSense están:

- Stateful firewall:
  - Baseado en PF (The OpenBSD Packet Filter).
  - Permite filtrar por IP orixe/destino, porto tcp/udp orixe/destino, sistema operativo que inicia a conexión...
  - Permite rexistrar (*log*) ou non o tráfico afectado polas regras.
  - Permite definir políticas de enrutamiento para ter balanceo de carga (load balancing), tolerancia a fallos (failover), varias saídas a Internet (multiple WAN)...
  - Permite usar *alias* para construír xogos de regras complexos pero lexibles.
  - Deshabilitando o filtrado convértese nun router puro.
- Táboa de Estado: Mantén a información das conexións abertas permitindo ademais:
  - Axustar o seu tamaño en función do hardware do equipo.
  - Elixir entre varias políticas de xestión para optimizar o seu funcionamento sobre a base das características dos enlaces (p. ex. para liñas de satélite con alta latencia as entradas asociadas a conexións inactivas consérvanse durante máis tempo do normal).
  - Poder controlar en cada regra o n.º de conexións simultáneas n.º de novas conexións por segundo...
- Redundancia: usando CARP dous ou máis firewalls pódense configurar para formar un *failover group*. Se unha interface falla no principal ou o principal cae totalmente, o secundario pasa a estar activo.

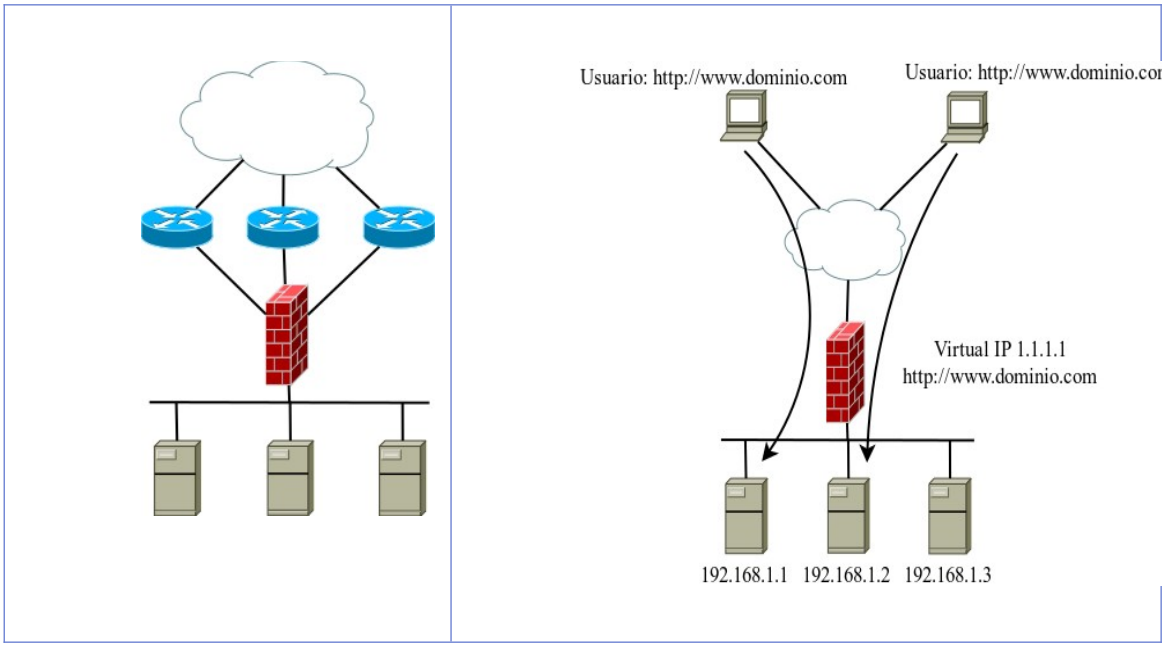


PfSense proporciona sincronización para que os cambios de configuración no principal se teñan en conta no secundario. Ademais sincronízase tamén a táboa de estado o que permite o mantemento das conexións establecidas en caso de fallo.

- Balanceo de carga (Load Balancing): pfSense permite balancear tanto as conexións saíntes coma entrantes:
  - Outbound Load Balancing: permite usar varias conexións WAN, mellorando o rendemento ademais de proporcionar failover. Por exemplo, se hai tres conexións a Internet, pfSense reparte o tráfico saínte da organización entre as tres saídas. No caso de que unha das saídas caia, automáticamente pfSense deixa de enviar paquetes por

ela, empregando unicamente as saídas que funcionan. Cando detecte que esa saída volve estar operativa, comezará a enviar paquetes novamente por ela.

- Inbound Load Balancing: permite distribuír a carga entre varios servidores. Por exemplo, pódese montar tres servidores web coa mesma información e cando pfSense reciba unha solicitude procederá a enviala o primeiro servidor, a seguinte ó segundo e así sucesivamente.



NAT: traducción de direcciones públicas-privadas para:

- Permitir a saída a Internet a equipos de organizacións que empregan direccionamento privado na intranet.
- Permitir o acceso dende Internet a servidores ubicados dentro da organización e que empregan direccionamento privado.

- Portal Cautivo (*captive portal*): para forzar a autenticación ou a aceptación de condicións antes de poder navegar, permitindo ademais:
  - Controlar o n.º máximo de conexións concorrentes por cliente.
  - Desconectar clientes ao cabo de certo tempo de uso ou de inactividade.
- DDNS (Dynamic DNS): permite a actualización en tempo real da información dns. Usado habitualmente para asignar un nome de dominio a un equipo cunha ip variable (asignada por dhcp).
- VPN (Virtual Private Network): as redes privadas virtuais permiten que equipos situados no exterior poidan traballar coma si estivesen dentro da intranet da organización dun xeito seguro, grazas ó estabrecemento de tuneis cifrados.
- Servizos básicos: servidor DHCP, axente de retransmisión dhcp, servidor DNS, etc.
- Sistema de paquetes: que permite ampliar as funcionalidades da instalación inicial permitindo a instalación e configuración vía web de paquetes como squid e squidguard para converter pfSense nun proxy caché con filtrado de contidos, HAVP para detección de virus en http, Snort para converter pfSense nun sensor IDS/IPS, PfBlocker, postfix forwarder, freeradius, etc.

pfSense pode considerarse un exemplo do concepto UTM (Unified Threat Management) ou Xestión Unificada de Ameazas que a día de hoxe a industria da seguridade informática está a impulsar. Trátase de dispositivos 'todo nun', que engloban múltiples funcionalidades: network level firewall, proxy http-smtp-pop-imap, filtro anti-spam, antivirus-antispyware, filtro de contidos, IDS/IPS, autenticación de usuarios, Virtual Private Networks (VPN), Hotspot, portal cativo (captive portal), alta dispoñibilidade, etc.

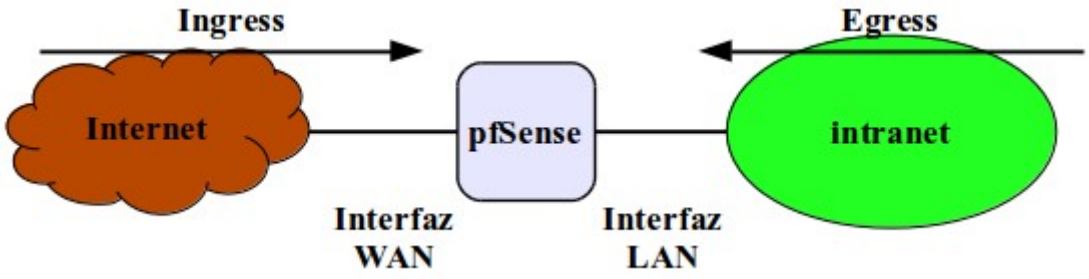
A continuación realizarase a tarefa 1, consistente nunha práctica guiada onde se instalará e configurará pfSense como network level firewall para cumprir cunha política de tráfico dunha organización.

1.2.5 Filtrado e regras

Os firewalls á hora de filtrar paquetes poden combinar distintas técnicas:

- Xogo de regras (*ruleset*): tamén chamado ACL (listas de control de acceso) en moitos dispositivos. Posteriormente falarase con mais detalle dos ruleset.
- Filtrado de camiño inverso (*Reverse Path Filtering* - RPF): permite verificar todo o tráfico de entrada dun interface, comprobando que as direccións de orixe son coñecidas mediante a táboa de enrutamiento (Routing Information Base- RIB). Verifícase cada paquete coa táboa de rutas e se a conexión procede dunha IP e interface onde se sabe que non reside a rede, o paquete descártase directamente (p.e. un paquete procedente da WAN con IP da nosa organización). É un filtrado baseado en direccións IP de orixe.
- Rutas de descarte (*null routes*): permite enviar o tráfico especificado a unha interface virtual de descarte. Impleméntase modificando a táboa de enrutamiento. É polo tanto un filtrado baseado na dirección IP de destino.

En moitos firewalls perimetrais adoita aplicarse un filtrado coñecido como de entrada/saída (*ingress*/*egress*) de maneira que sexan o primeiro punto de control do tráfico. Para un rendemento óptimo, o habitual é filtrar no interface máis próximo; é dicir, o tráfico de saída cara a Internet filtralo no interface interno e o tráfico de entrada de Internet filtralo no interface externo.



Á hora de decidir que facer cun paquete os firewalls adoitan adoptar algunha estas accións:

- PASS: o paquete é aceptado e continúa a súa marcha.
- BLOCK: o paquete é descartado silenciosamente.
- REJECT: o paquete é descartado pero infórmase o remitente:
  - Se é unha conexión tcp, envíase ao remitente unha mensaxe TCP RST (reset).

- Se é unha conexión udp, envíase ao remitente unha mensaxe ICMP Porto inaccesible.

Utilizar BLOCK en vez de REJECT, permitirá manter oculto o firewall dificultando a tarefa de descubrir a política de seguridade implantada. Coma contrapartida, descartar paquetes usando BLOCK provoca que o

1.2.6 Boas prácticas no deseño de firewalls

A continuación indícanse unha serie de boas prácticas á hora de crear regras para configurar un firewall:

- Denegar por defecto (*CleanUp Rule*): permítese unicamente o tráfico requirido polas necesidades da rede e rexeitase o resto. Todo tráfico non autorizado nas regras será eliminado; polo que, para permitilo habería que contactar co administrador do firewall e que éste procedese a autorizalo.

  Aínda que a opción de 'Permitir por defecto' é máis cómoda e vén activada por defecto en moitos routers e firewalls, non é a máis segura. Hai que crear regras para bloquear o tráfico non desexado. É moi cómodo, pero non é o máis seguro xa que pode haber tráfico non desexado atravesando o firewall (p.e. o administrador esqueceu crear a regra correspondente para bloquealo).

- Sinxeleza e claridade: á hora de crear o ruleset hai que pensar e planificar para que sexa o máis claro e sinxelo. Conxuntos de regras moi longos, desorganizados ou excesivamente complexos facilitan que os administradores cometan erros permitindo ou bloqueando tráfico que non corresponde. Hai que seguir o principio KISS (Keep It Simple).

  Sempre que o dispositivo o permita é recomendable empregar *alias* para facilitar a comprensión e o mantemento das regras. Por exemplo, usando un alias de nome IP_admin asociado á dirección IP do equipo do administrador, facilitase a interpretación das regras. Ademais, no caso de que o equipo do administrador cambiase de dirección, poderíamos actualizar o valor do alias á nova dirección, actualizándose todas as regras onde apareza, sen necesidade de reemplazar un a un o valor en todas as regras do firewall.

- Direccións marcianas (*martians*): denega a entrada e saída de direccións marcianas. As direccións marcianas son todas aquelas que pola súa asignación non poden xerar tráfico Internet válido (e, polo tanto, seguramente enmascaran tráfico ilícito). As direccións a bloquear serían:
  - Direccións reservadas pola IANA: 0.0.0.0/8, 10.0.0.0/8, 169.254.0.0/16, 172.16.0.0/12, 192.0.2.0/24, 192.88.99.0/24, 198.18.0.0/15, 192.168.0.0/16, 224.0.0.0/4, 240.0.0.0/4.
  - Direccións recollidas no RFC 3232: este documento e establece unha base de datos online e en continuo cambio como referencia obrigada para a asignación dos rangos de direccións IP por IANA.

  No caso de firewalls que están dentro de organizacións que usan direccionamento privado, habería que analizar cales destas redes están en uso para permitir o seu tráfico, bloqueando o resto.

- Direccións non asignadas (*unallocated*): denega a entrada e saída de tráfico orixinado en direccións válidas pero que non están en uso.

- Regras Antispoofing: denega a entrada de tráfico coas túas direccións e a saída de tráfico non orixinado coas túas direccións; é dicir, tráfico cuxa IP de orixe non se corresponde co segmento de rede do que procede. Non ten sentido que o firewall reciba dende a Intranet paquetes con IP orixe unha IP que non é da Intranet e do mesmo xeito, non ten sentido que o firewall reciba paquetes dende Internet con IP orixe unha IP da Intranet da organización.
- Permite explícitamente o tráfico de retorno cara ás túas direccións e de saída orixinado coas túas direccións.
- Xestión do firewall: prohibe o acceso non autorizado ós firewalls. Para facelo correctamente debería haber dous grupos de regras:
  - En primeiro lugar, garantir o acceso dende equipos autorizados (*anti Lockdown Rule*).
  - En segundo lugar, prohibir o acceso ó resto (*Lockdown Rule* ou *Stealth Rule*).
- Tráfico de xestión e monitorización: unicamente permite o tipo de tráfico de xestión e monitorización necesario e estrcitcamete ós equipos implicados.
- Permite o tráfico dos protocolos de enrutamiento e de rede necesarios.
- Servizos ofrecidos pola organización: este punto será explicado con maior detalle na seguinte actividade, pero como adianto recoméndase:
  - Permitir unicamente o acceso ós portos/servizos ofrecidos pola organización. Normalmente estes servizos correrán en servidores ubicados nunha rede especial chamada DMZ.
  - Denegar o tráfico de saída aos servidores da DMZ (*Sneaky Rule*): os servidores recibirán peticións e responderán ós clientes. É dicir, a conexión é iniciada por un cliente e autorizada polo firewall, polo que as respostas dos servidores estarán autorizadas para saír. O que se está a impedir con esta regra é que os servidores inicien conexións hacia fóra, que normalmente non son necesarias para desempeñar ás súas funcións.

Un aspecto moi importante nun sistema de seguridade é a monitorización e os rexistros. O administrador debe poder saber o estado do firewall e que tráfico é/foi autorizado ou bloqueado. É recomendable:

- Rexistrar o tráfico denegado *(Log Denied Rule*).
- Rexistar e alertar en caso de tráfico dende unha zona DMZ.
- Non rexistrar o tráfico ruidoso pero necesario como o broadcast (*No Logging Rule*).
- Centralización dos rexistros nunha máquina onde se faga unha análise automática de rexistros. Para isto existen ferramentas específicas coñecidas como SIM (Security Information Management) e SIEM (Security Information and Event Management).

Outro punto de especial importancia é documentar a configuración:

- Comentar as regras para facilitar a súa finalidade. Hai que pensar que pode pasar tempo dende que se crearon unhas regras ata o día en que hai que cambiar o ruleset do firewall ou que o firewall sexa revisado por outra persoa diferente á que creou as regras.
- En ámbitos grandes débese manter unha documentación detallada describindo a configuración. Debido ao sensible desta documentación, debe estar protexida.

A continuación realizarase a tarefa 2, consistente nunha práctica guiada onde se crearán regras de filtrado nun network level firewall para crear un ruleset que permita cumprir cunha política de tráfico dunha organización.

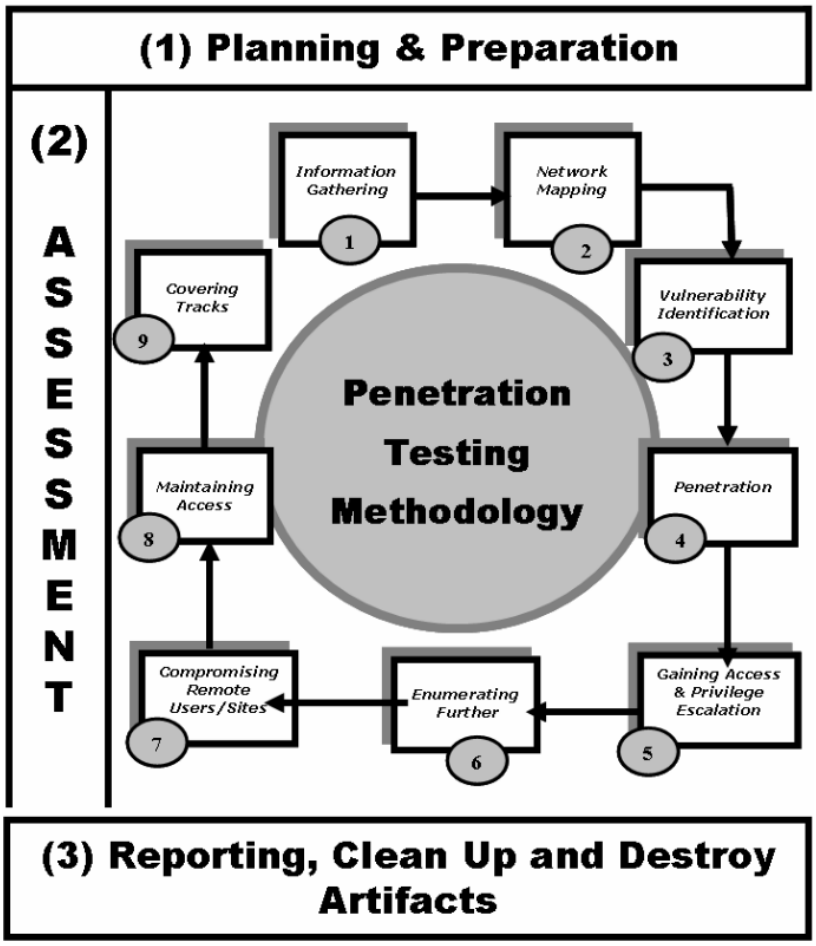
A continuación realizarase a tarefa 3, consistente nunha práctica onde se modificará o ruleset dun firewall dunha organización, creando, movendo e eliminando regras para satisfacer a política de tráfico dunha organización.

1.2.7 Verificación da política de tráfico e diagnóstico de problemas de conectividade

Como se explicou, a misión dun firewall é lograr o cumprimento dunha política de control de acceso entre redes; é dicir, permitir o paso de paquetes asociados a comunicacións autorizadas e bloquear o resto. Ademais de instalar o firewall e configurar as regras de filtrado, o administrador debe verificar que as regras configuradas funcionan correctamente. A verificación debe facerse dende cada unha das redes controladas polo firewall; por exemplo, no caso típico dun firewall de dúas patas (controlando as comunicación entre unha intranet e Internet), habería que comprobar o funcionamento tanto dende a intranet coma dende Internet.

Hai que sinalar que un dos primeiros pasos nun proceso de auditoría ou dun ataque é o *Network Mapping* no que trátase de determinar:

- Os equipos activos.
- Os portos abertos e as aplicacións executándose neles.
- O sistema operativo e versións de aplicacións executándose.
- A topoloxía da rede (perímetro, redes internas, ...).



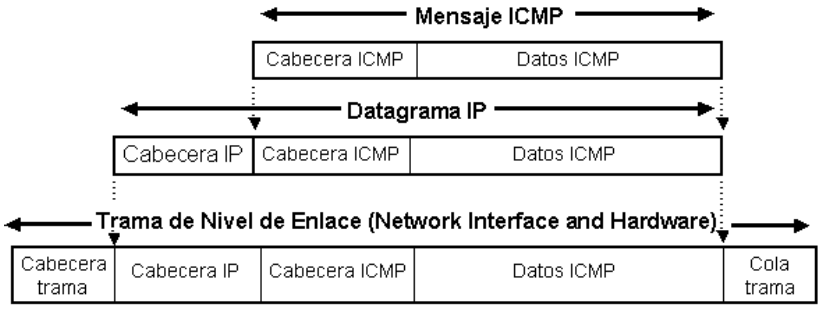
As regras definidas nos firewalls han de permitir as comunicacións desexadas sen desvelar mais información que a necesaria; por exemplo, non permitindo o acceso dende Internet a servizos que unicamente deben ser accesibles dende a Intranet. Os administradores de sistemas, analistas e atacantes dispoñen de diversas técnicas e ferramentas para abordar o mapeado da rede e verificar as regras do firewall.

ICMP (Internet Control Message Protocol)

No funcionamento normal dunha rede danse ás veces situacións extraordinarias que requiren enviar avisos especiais; por exemplo, se un datagrama co bit DF (Don't Fragment) posto a 1 non pode pasar por unha determinada rede, o router onde se produce o problema debe devolver unha mensaxe ó host emisor indicándolle o sucedido. O mecanismo para indicar todos estes incidentes en Internet é o protocolo coñecido como ICMP, que proporciona un descarte informado.

Entre as características mais importantes de ICMP están:

- As mensaxes ICMP viaxan pola rede viaxando sobre datagramas IP.
- As mensaxes ICMP están suxeitas nos routers ás mesmas regras que cualquira outro datagrama (enrutamiento, fragmentación, tempo de vida, etc.).
- As mensaxes ICMP son xeradas polo host ou router que detecta o problema ou situación extraordinaria, e van dirixidos ó host ou router que aparece no campo dirección orixe do datagrama que causou o problema.



As mensaxes ICMP posúen unha cabeceira e un campo de datos:

- Cabeceira ICMP:
  - Tipo: tipo de mensaxe ICMP (eco, resposta de eco, destino inalcanzable, etc.).
  - Código: especifica a mensaxe ICMP dentro dun tipo (destino inalcanzable por rede destino descoñecida, etc.).
  - Checksum: suma de comprobación de errores.
  - Datos específicos do tipo: datos opcionais para cada tipo de ICMP.
- Datos ICMP: no caso de mensaxes de erro e para facilitar a identificación do datagrama por parte do host emisor, inclúe a cabeceira e os primeiros oito bytes de datos do datagrama orixinal.

Pódese profundizar no estudio do protocolo e as mensaxes ICMP: http://es.wikipedia.org/wiki/Internet_Control_Message_Protocol

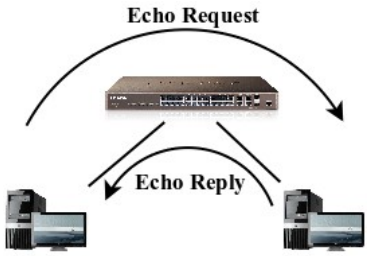
Na seguinte páxina web da IANA, http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml, pódese ver a listaxe completa das mensaxes ICMP.

Aínda que hai 42 tipos de mensaxes ICMP é importante coñecelos e valorar a necesidade de permitir ou bloquear estas mensaxes.. Os máis habituais para facer probas de conectividade son os que aparecen na seguinte táboa e serán os que se estude:

Tipo ICMP	Descrición
0	Resposta de Eco (Echo Reply)
3	Destino inalcanzable (Destination Unreachable)
8	Solicitude de Eco (Echo Request)
11	Tempo Excedido (Time Exceeded)

ICMP Echo Request e Echo Reply

Son usados polo comando ping para detectar se un destino determinado está operativo. Automatizar o proceso de facer ping a varios equipos coñécese como varrido ping ou *ping sweep*.




```
manuel@pcmanuel:~$ ping 192.168.0.100
PING 192.168.0.100 (192.168.0.100) 56(84) bytes of data.
64 bytes from 192.168.0.100: icmp_req=1 ttl=255 time=0.627 ms
64 bytes from 192.168.0.100: icmp_req=2 ttl=255 time=0.615 ms
^C
--- 192.168.0.100 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.615/0.621/0.627/0.006 ms
```

Se ó enviar un ICMP Echo Request recíbese como resposta un Echo Reply sábese que o equipo destino está operativo; non obstante, non recibir o Echo Reply non implica necesariamente que o equipo destino non estea operativo:

- Pode que o equipo non exista
- Pode que estea apagado nese momento.
- Pode que algún equipo intermedio prohiba o paso de mensaxes ICMP.
- Pode que o equipo estea configurado para non responder a este tipo de mensaxes.

No caso de non obter resposta, haberá que utilizar outras técnicas para descubrilo.

Destino Inalcanzable (Destination Unreachable)

Esta mensaxe prodúcese cando non se pode entregar o datagrama no seu destino por diversas situacións. A xeito de exemplo:

- Cando un router non encontra nas súas táboas ningunha ruta pola que poida chegar á dirección para a que vai dirixido un datagrama.
- Cando un router se encontra cun datagrama que ten posto a 1 o bit DF (Don't Fragment) e que non cabe na MTU da rede pola que ha de envialo.
- Cando un router non pode reenviar un datagrama debido a que existe un filtro de paquetes
- Cando o router final non recibe un ARP Reply por parte do equipo destino.
- Cando a comunicación co destino está prohibida.

```
▷ Ethernet II, Src: 08:00:09:72:74:e0 (08:00:09:72:74:e0), Dst: 00:00:b4:34:b7:fa (00:00:b4:34:b7:fa)
▷ Internet Protocol, Src: 168.156.1.33 (168.156.1.33), Dst: 134.39.89.236 (134.39.89.236)
▽ Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 1 (Host unreachable)
    Checksum: 0xa7a2 [correct]
  ▷ Internet Protocol, Src: 134.39.89.236 (134.39.89.236), Dst: 10.0.0.1 (10.0.0.1)
```

Tempo excedido (Time Exceeded):

Envíase ao emisor dunha mensaxe cando:

- Cando un router ao decrementar o TTL da cabeceira IP chega a 0. Isto pode ser síntoma de que se produciu algún bucle na rede ou que o valor do TTL utilizado é demasiado baixo para o diámetro da rede.
- Cando o temporizador de reensamblado dun datagrama IP fragmentado chega expira.

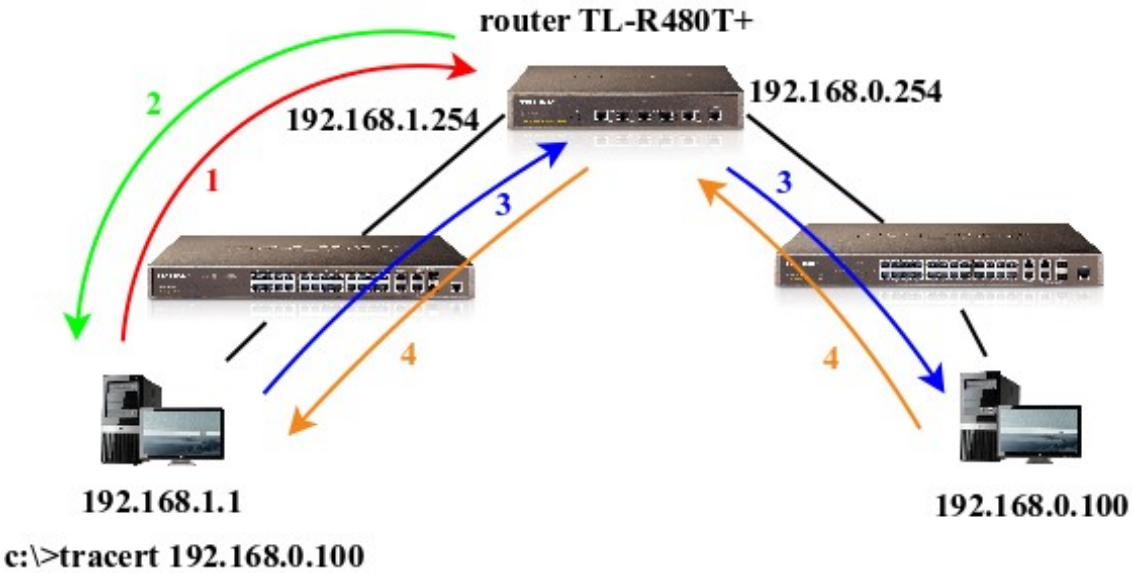
Tendo presente as características destas mensaxes ICMP e o funcionamento dos routers, o comando tracert (ou traceroute en sistemas Window) permite ós administradores verificar as conexións cun equipo ademais de coñecer a ruta seguida para chegar ó mesmo. No seguinte exemplo vese como funciona a traza de rutas:

```
C:\>tracert 192.168.0.100

Traza a la dirección router.iesxulianmagarinos.edu.xunta.es [192.168.0.100]
sobre un máximo de 30 saltos:

  1    10 ms    <10 ms    <10 ms  brazilfw.iesxulianmagarinos.edu.xunta.es [192.168.1.254]
  2    <10 ms   <10 ms    <10 ms  router.iesxulianmagarinos.edu.xunta.es [192.168.0.100]

Traza completa.
```



A secuencia de mensaxes é:

- Paquete#1: ICMP Echo Request con destino 192.168.0.100 e con ttl=1 .
- Paquete#2: ICMP Time Exceeded enviado pola interface mais próxima do router (192.168.1.254) .
- Paquete#3: ICMP Echo Request con destino 192.168.0.100 e con ttl=2 (atraviesa o router).
- Paquete#4: ICMP Echo Reply procedente de 192.168.0.100.

Ó remate do proceso, o administrador sabe que o equipo 192.168.0.100 está operativo e que as comunicacións entre o seu equipo e o 192.168.0.100 pasan a través do router 192.168.1.254.

Un aspecto interesante á ter en conta cando se fagan este tipo de probas é que a ferramenta tracert de Windows envía mensaxes ICMP Echo Request pero as ferramentas traceroute de Linux permiten enviar ICMP Echo Request, mensaxes TCP ou datagramas UDP. Todas estas mensaxes viaxarán sobre datagramas IP con tempos de vida (ttl) que se incrementan e irán morrendo nos sucesivos routers provocando a resposta estudada. É moi habitual bloquear as mensaxes ICMP nos firewalls para non facilitar a atacantes descubrir equipos da organización, polo que as trazas baseadas con ICMP seguramente non proporcionarán moita información. Sen embargo, os protocolos tcp/udp si están permitidos normalmente (a lo me-

nos para os portos máis empregados); deste xeito, usando traceroute e escollendo tcp/udp e algún porto habilitado poderíase obter máis información.

Exemplo de traza a www.nikef.nl usando mensaxes ICMP

```
$ sudo traceroute -I www.nikhef.nl
traceroute to www.nikhef.nl (192.16.199.166), 30 hops max, 60 byte packets
 1  192.168.0.100 (192.168.0.100)  0.945 ms  1.205 ms *
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  xe-8-1-0.ams10.ip4.tinet.net (89.149.186.241)  108.801 ms  117.806 ms
116.590 ms
 8  surfnet-gw.ip4.tinet.net (77.67.72.110)  116.794 ms  120.519 ms  129.637
ms
 9  AE2.500.JNR01.Asd002A.surf.net (145.145.80.66)  136.570 ms  141.634 ms
144.588 ms
10  nikhef-router.Customer.surf.net (145.145.19.126)  160.577 ms  159.670 ms
164.490 ms
11  ferro.nikhef.nl (192.16.199.166)  156.443 ms  162.536 ms  105.817 ms
```

Exemplo de traza a www.nikef.nl usando mensaxes UDP

```
sudo traceroute -p 53 www.nikhef.nl
traceroute to www.nikhef.nl (192.16.199.166), 30 hops max, 60 byte packets
 1  192.168.0.100 (192.168.0.100)  0.675 ms  0.921 ms  1.154 ms
 2  192.168.153.1 (192.168.153.1)  51.717 ms  54.496 ms  58.398 ms
 3  194.Red-80-58-114.staticIP.rima-tde.net (80.58.114.194)  98.573 ms
98.660 ms  98.745 ms
 4  So6-0-0-0-grtmadde2.red.telefonica.wholesale.net (84.16.8.117)  85.402
ms  89.297 ms  94.416 ms
 5  Xe1-0-6-0-grtparix3.red.telefonica-wholesale.net (84.16.14.250)  113.396
ms  123.224 ms  126.150 ms
 6  * * *
 7  xe-4-3-0.ams10.ip4.tinet.net (89.149.184.201)  118.119 ms  118.948 ms
xe-0-0-0.ams10.ip4.tinet.net (89.149.186.233)  125.882 ms
 8  surfnet-gw.ip4.tinet.net (77.67.72.110)  116.661 ms  121.812 ms  121.904
ms
 9  AE2.500.JNR01.Asd002A.surf.net (145.145.80.66)  127.681 ms  130.542 ms
128.656 ms
10  nikhef-router.Customer.surf.net (145.145.19.126)  135.452 ms  143.517 ms
142.524 ms
11  ferro.nikhef.nl (192.16.199.166)  109.798 ms * *
```

Exploración de portos (Port Scanning)

O método máis habitual de comprobar a configuración dun firewall consiste en utilizar un escáner de portos xunto cunha ferramenta de análise de tráfico, realizar un barrido de portos e verificar a correspondencia coa política de seguridade estipulada. Este proceso debe repetirse dende todos e cada un dos interfaces do firewall cara a todas e cada unha das redes que encóntranse detrás deste, poñendo especial énfase naqueles portos que se han deixado abertos segundo a política de seguridade e verificando que son só accesibles segundo o especificado por esta.

O obxectivo final das futuras inspeccións de seguridade é comparar o estado do sistema

en cada momento co seu estado nun momento no que o devandito sistema tiña unha configuración, comportamento, etc. coñecido e determinado. Polo tanto, é fundamental almacenar os resultados da inspección de seguridade inicial así como os resultados das inspeccións posteriores.

Un port scanning é o proceso de conexión a portos TCP e UDP do sistema obxectivo para determinar que servizos se están a executar. Identificar os portos que están á escoita permitirá:

- Descubrir equipos funcionando.
- Determinar que aplicacións se están a executar.
- Determinar o tipo de sistema operativo.
- Determinar que comunicacións están permitidas polo firewall: esquipos destino/orixe, portos destino/orixe, protocolos, …

Ao ser TCP/UDP os protocolos encargados de encapsular os datos de nivel de aplicación (datos de usuario) pódese superar as limitacións das técnicas anteriores: o máis que habitual bloqueo das mensaxes icmp nos routers-firewall.

Aínda que existen multitude de ferramentas para facer análise de portos, a máis coñecida pola súa potencia e funcionalidades é nmap. Nmap ademais de explorar portos é capaz de detectar que sistema operativo corre na máquina obxectivo (*fingerprinting*). Para iso analiza os paquetes procedentes da máquina obxectivo e compáraos con implementacións coñecidas dos fabricantes.

Nmap posúe diversos tipos de análise e moitas opcións (dende especificar o rango de portos a analizar ata falsificar a IP orixe do análise pasando por especificar a rapidez da análise). No seguinte exemplo vese o modo de uso e o tipo de resultado que da:

```
root@kaliLinux:~# nmap -sV -O -p 1-65535 192.168.56.92

Starting Nmap 6.25 ( http://nmap.org ) at 2013-06-25 23:28 CEST
Nmap scan report for 192.168.56.92
Host is up (0.0026s latency).
Not shown: 65529 closed ports
PORT     STATE SERVICE      VERSION
80/tcp   open  http         Apache httpd 1.3.17 ((Win32))
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows 2003 or 2008 microsoft-ds
1025/tcp open  msrpc        Microsoft Windows RPC
1026/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:1B:18:51 (Cadmus Computer Systems)
Device type: general purpose
Running: Microsoft Windows 2000|XP|2003
OS CPE: cpe:/o:microsoft:windows_2000::sp2 cpe:/o:microsoft:windows_2000::sp3 cpe:/o:microsoft:w
indows_2000::sp4 cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3 cpe:/o:micros
oft:windows_server_2003::- cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_se
rver_2003::sp2
OS details: Microsoft Windows 2000 SP2 - SP4, Windows XP SP2 - SP3, or Windows Server 2003 SP0 -
 SP2
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submi
t/ .
Nmap done: 1 IP address (1 host up) scanned in 109.60 seconds
```

Opcións:

- -sV: para detectar os servizos correndo nos portos abertos detectados.
- -O: para detectar o sistema opertativo da máquina a analizar (*fingerprinting)*.

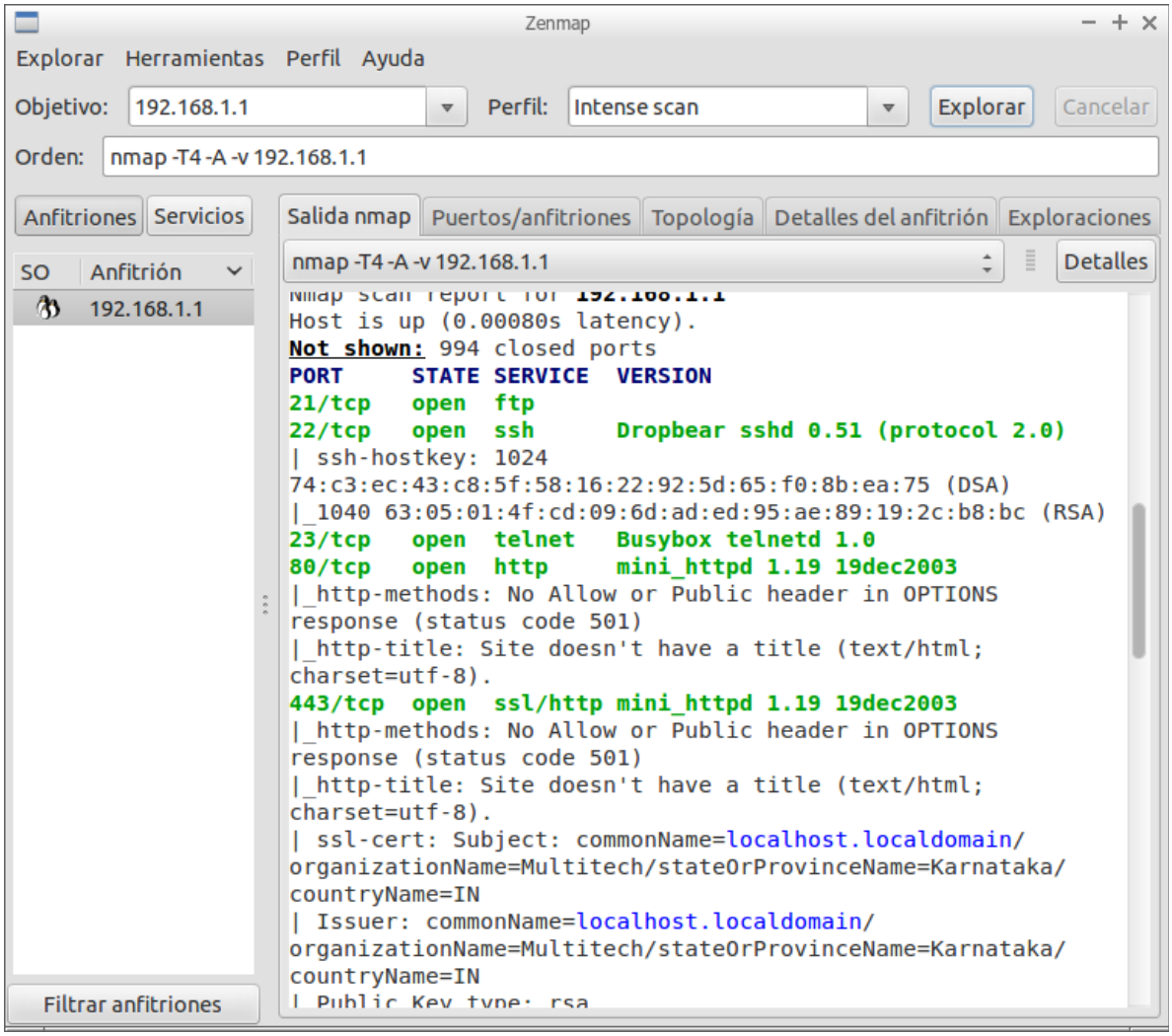
– -p 1-65535: para especificar o rango de portos a analizar.

No exemplo, nmap detectou unha máquina Microsoft Windows correndo diversos servizos (servidor web e compartición de arquivos e carpetas). No exemplo especificáronse todos os portos, o que implica que a análise xenerou moitos paquetes que inundaron a rede. Facer esto nun contorno de producción pode provocar caídas ou baixadas de rendemento nos servizos da organización; polo que, é recomendable limitar este tipos de análise a momentos de baixa demanda ou limitar o número de portos a analizar (ou deixar os portos que analiza nmap que son os de uso máis habitual nas redes actuais).

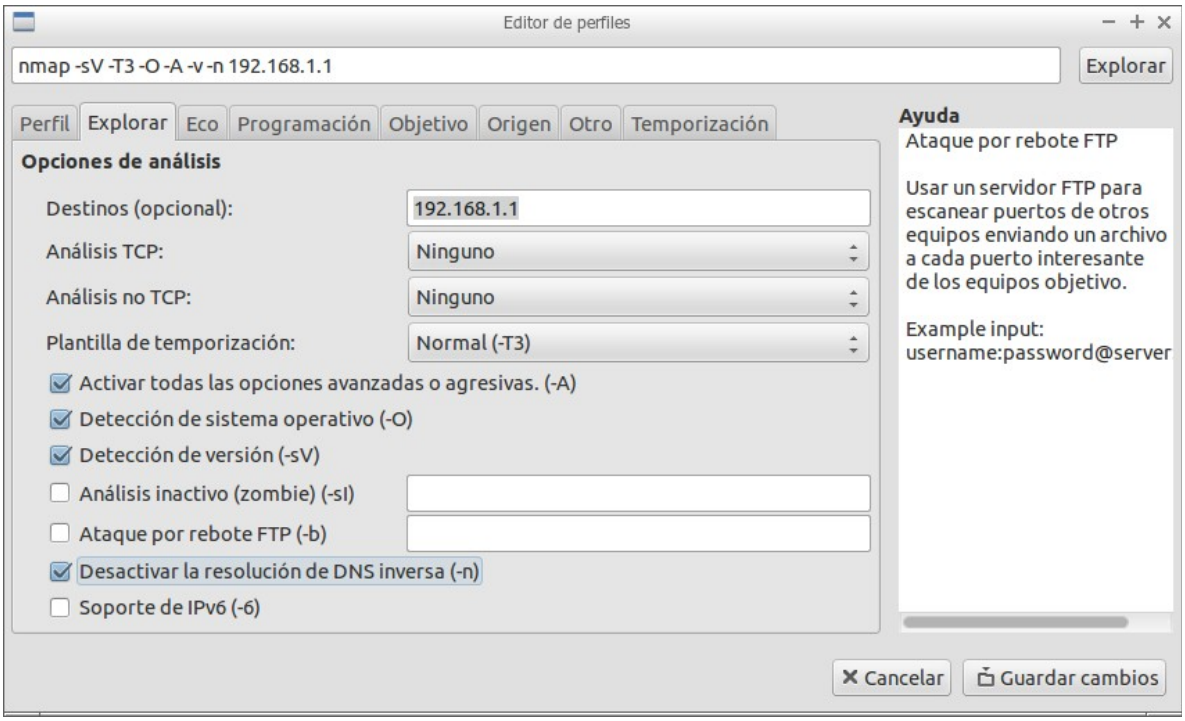
Pódese profundizar no estudio de nmap en https://nmap.org/ e https://nmap.org/man/es/

Nmap posúe unha interface gráfica que facilita enormemente a realización das análises personalizadas; xa que, a través de asistentes se poden escoller as opcións desexadas. A ferramenta é Zenmap e para instalala e exexcutala en Linux Ubuntu faise:

```
manuel@lubuntu:~$ sudo apt-get update
manuel@lubuntu:~$ sudo apt-get install zenmap
manuel@lubuntu:~$ sudo zenmap
```



Zenmap proporciona os mesmos resultados que daría nmap por liña de comando, no caso de executar nmap coas opcións indicadas no campo 'Orden' da interface de zenmap. A través do menú Perfil pódese acceder ó asistente de análises, podendo escoller as opcións desexadas (rango de portos, velocidade de análise, resolución dns inversa, facer algún tipo de 'ping' ou proba previa ó barrido de portos para ver se o equipo obxectivo está activo, etc.).



Os rexistros (logs)

Un aspecto fundamental da seguridade perimetral é a verificación das mensaxes rexistradas polos distintos compoñentes desta, en especial os firewalls. O principal papel dos firewalls é garantir que a política de seguridade duha organización cúmprese; polo tanto, as mensaxes emitidas por estes indican violacións na política de seguridade.

É fundamental revisar periodicamente os rexistros ou logs de todos os sistemas que conforman o sistema de seguridade perimetral. ~~A periodicidade dependerá das capacidades~~ da organización, pero é recomendable facelo polo menos diariamente; aínda que, en organizacións con altos requisitos de seguridade pódese ter un equipo dedicado a esta función en tempo real.

A información obtida debe vixiarse, prestando especial atención ás zonas particularmente sensibles ou expostas; xa que, a detección a tempo dun compromiso nun sistema pode evitar que o incidente chegue a ser crítico. Sen embargo, ás veces o ruído de fondo" existente (ataques indiscriminados, barridos de rede, etc.) e a cantidade de mensaxes xeradas dificultan enormemente á análise. Este problema complícase xa que na maioría das organizacións hai máis dun firewalls, ademais doutros sistemas de seguridade perimetral. Para resolver este problema pódese:

- Centralizar os rexistros de eventos: a maior parte dos sistemas e dispositivos permiten a redirección dos logs a un sistema remoto, ademais de gardar estes localmente. O estándar para este rexistro remoto é do mundo UNIX, syslog, e a maior parte dos dispositivos de

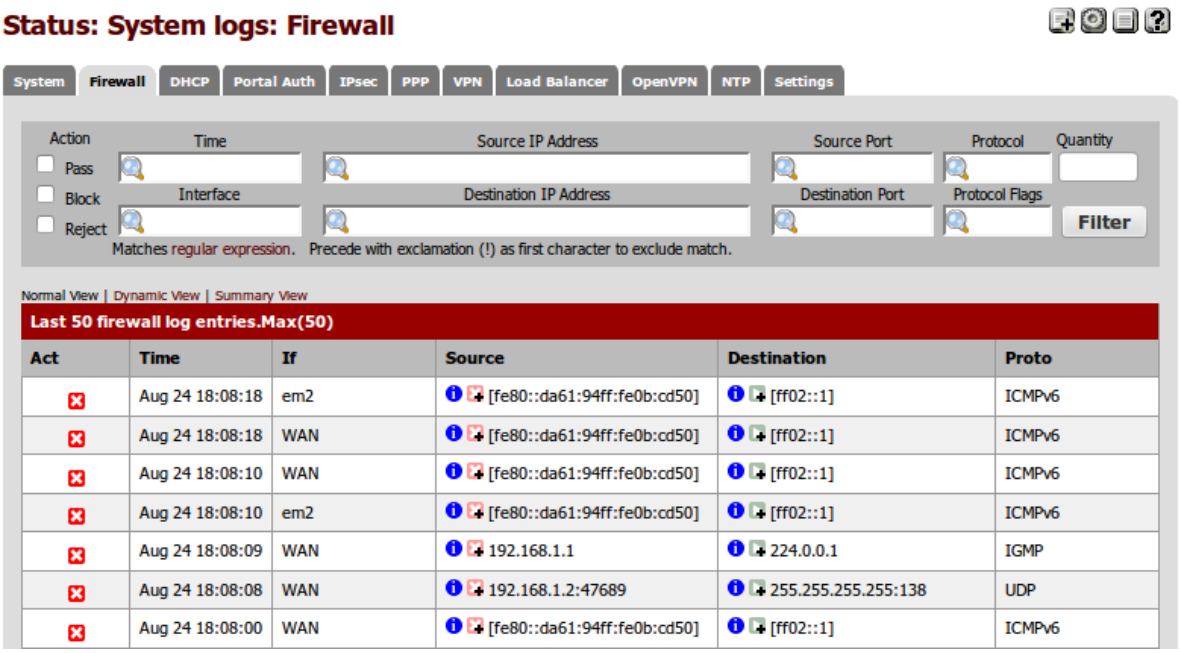
rede e sistemas operativos adoitan poder ser configurados dun modo ou outro para enviar as alertas remotamente utilizando este sistema.

- Análise automatizada dos rexistros: existen sistemas para a clasificación e o análise dos eventos dos logs. A destacar son os sistemas de xestión de eventos de seguridade (SEM - Security Event Managers ou SIEM - Security Information Event Management). Están deseñados para aceptar, xestionar e correlacionar un elevado volume de eventos de multitude de dispositivos distintos, polo que adoitan resultar moi útiles en Organizacións de gran tamaño.
- Xeración automática de alertas: para eventos que representen ser un claro indicio dun incidente de seguridade.

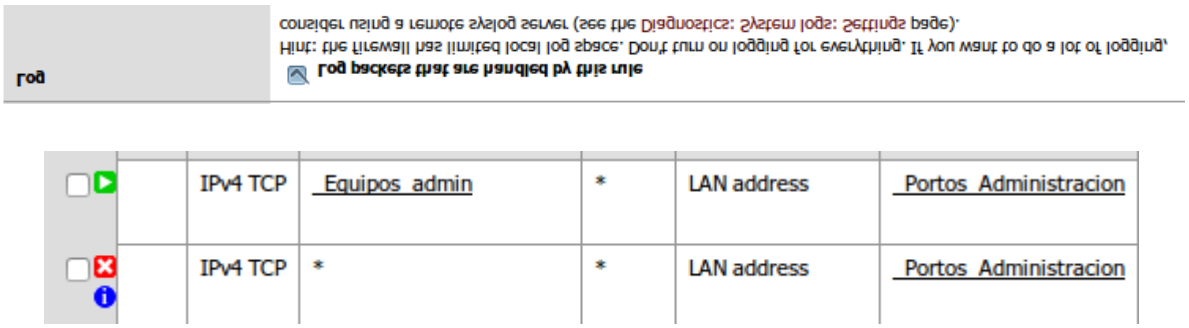
Como recomenda o Centro Criptolóxico Nacional, son boas prácticas en relación ós log:

- Almacenalos fóra do propio firewall: no caso de que o firewall fose comprometido, poden ser eliminadas as trazas que permitan identificar o incidente e reaccionar axeitadamente. No caso de centralizar os logs, este problema queda resolto.
- Uso de canle seguras (cifrado ou fóra de liña) para transmitir os logs: debido a que os logs conteñen información sensible (equipos orixe/destino, información sobre autenticación de usuarios, información sobre violacións na política de seguridade, etc.).
- Política de rotación, análise e arquivo dos logs: hai que aplicar ós logs as correspondentes medidas de seguridade física e copias de seguridade. Hai que lembrar que moitas organizacións están obrigadas por lei a gardar os seus logs durante un período variable de tempo e que dependendo da información rexistrada, os logs poden estar suxeitos ás obrigas recollidas na lei de protección de datos.

pfSense pode proporcionar moita información sobre o seu funcionamento a través dos menús Status e Diagnostics. Para ver os eventos de firewall rexistrados por pfSense hai que ir a Status → System Logs → Firewall.



O firewall rexistrará os paquetes que cumpran regras onde a opción de rexistro esté habilitada:



	IPv4 TCP	Equipos_admin	*	LAN address	Portos_Administracion
	IPv4 TCP	*	*	LAN address	Portos_Administracion

A través da pestana Settings é posible configurar entre outras:

- Forward/Reverse Display: permite ver as mensaxes máis recentes primeiro ou ó revés.
- Log File Size: permite indicar o tamaño dos rexistros antes de rotalos.
- Log Firewall Default Blocks: controla o rexistro dos paquetes descartados pola regra por defecto, regra de bloqueo das redes bogon e redes privadas.
- Enable Remote Logging: habilitar o envío dos logs a un servidor remoto.
- Remote Syslog Servers: especificar servidore syslog remotos.
- Remote Syslog Contents: especificar os logs a enviar ó servidor syslog remoto.

General Logging Options

Forward/Reverse Display	☐ **Show log entries in reverse order (newest entries on top)**
GUI Log Entries to Display	50 Hint: This is only the number of log entries displayed in the GUI. It does not affect how many entries are contained in the actual log files.
Log File Size (Bytes)	Logs are held in constant-size circular log files. This field controls how large each log file is, and thus how many entries may exist inside the log. By default this is approximately 500KB per log file, and there are nearly 20 such log files. NOTE: Log sizes are changed the next time a log file is cleared or deleted. To immediately increase the size of the log files, you must first save the options to set the size, then clear all logs using the "Reset Log Files" option farther down this page. Be aware that increasing this value increases every log file size, so disk usage will increase significantly. Disk space currently used by log files: 9.6M. Remaining disk space for log files: 4.9G.
Log Firewall Default Blocks	☑ **Log packets matched from the default block rules put in the ruleset** Hint: packets that are blocked by the implicit default block rule will not be logged if you uncheck this option. Per-rule logging options are still respected. ☐ **Log packets matched from the default pass rules put in the ruleset** Hint: packets that are allowed by the implicit default pass rule will be logged if you check this option. Per-rule logging options are still respected. ☑ **Log packets blocked by 'Block Bogon Networks' rules** ☑ **Log packets blocked by 'Block Private Networks' rules**
Web Server Log	☑ **Log errors from the web server process.** Hint: If this is checked, errors from the lighttpd web server process for the GUI or Captive Portal will appear in the main system log.
Raw Logs	☐ **Show raw filter logs** Hint: If this is checked, filter logs are shown as generated by the packet filter, without any formatting. This will reveal more detailed information, but it is more difficult to read.
Filter descriptions	Dont load descriptions **Show the applied rule description below or in the firewall log rows.** Displaying rule descriptions for all lines in the log might affect performance with large rule sets.
Local Logging	☐ **Disable writing log files to the local disk**
Reset Logs	Reset Log Files Note: Clears all local log files and reinitializes them as empty logs. This also restarts the DHCP daemon. Use the Save button first if you have made any setting changes.

Remote Logging Options

Source Address	DPTOS This option will allow the logging daemon to bind to a single IP address, rather than all IP addresses. If you pick a single IP, remote syslog severs must all be of that IP type. If you wish to mix IPv4 and IPv6 remote syslog servers, you must bind to all interfaces. NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.
IP Protocol	IPv4 This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; If an IP address of the selected type is not found on the chosen interface, the other type will be tried.
Enable Remote Logging	☑ **Send log messages to remote syslog server**
Remote Syslog Servers	Server 1 192.168.56.100 Server 2 Server 3 IP addresses of remote syslog servers, or an IP:port.
Remote Syslog Contents	☐ Everything ☐ System events ☑ Firewall events ☐ DHCP service events ☐ Portal Auth events ☐ VPN (PPTP, IPsec, OpenVPN) events ☐ Gateway Monitor events ☐ Server Load Balancer events ☐ Wireless events

A continuación realizarase a tarefa 4, consistente nunha práctica onde faranse probas para comprobar o ruleset do firewall e revisaranse os logs de pfSense.

1.3 Tarefas

As tarefas propostas son as seguintes.

- **Tarefa 1. Instalación de pfSense.** Práctica guiada de instalación e configuración dun net-work level firewal.
- **Tarefa 2. Creación dun ruleset en pfSense.** Práctica guiada de creación de regras de filtrado nun network level firewall para cumprir a política de tráfico dunha organización.
- **Tarefa 3. Modificación do ruleset dun network level firewall.** Práctica consistente na modificación das regras dun ruleset dun network level firewall para adecuarse á una nova política de tráfico da organización
- **Tarefa 4. Probas de tráfico e logs.** Realización de probas de conectividade para comprobar o ruleset do firewall e revisión dos logs de pfSense.

1.3.1 Tarefa 1. Instalación de pfSense

Realizar unha práctica guiada onde se instalará e configurará pfSense como network level firewall para cumprir cunha política de tráfico sinxela dunha organización.

1.3.2 Tarefa 2. Creación dun ruleset en pfSense

Realizar unha práctica guiada consistente na creación de regras de filtrado nun network level firewall para crear un ruleset que permita cumprir cunha política de tráfico dunha organización.

1.3.3 Tarefa 3. Modificación do ruleset dun network level firewall

Empregando como punto de partida a máquina pfSense configurada na tarefa 2, proceder a modificar o ruleset para cumprir coa seguinte política de tráfico:

- A maiores dos dous DNS autorizados na tarefa 3, engádese o servidor 8.8.4.4.
- Os equipos dos administradores poderán facer consultas dns a calquera servidor DNS. Ademais de consultas normais (usando udp) poderán facer transferencias de zona (usando tcp).
- Permítese o acceso ó servidor FTP ftp.rediris.es. No caso do Dpto. Comercial unicamente no horario de 08:00 a 14 de luns a venres.
- Permítese enviar correos electrónicos por smtp usando o servidor smtp.gmail.com que traballa no porto tcp 465. No caso do Dpto. Comercial unicamente no horario de 08:00 a 14 de luns a venres.

- Permítese leer os correos electrónicos por imaps usando o servidor imap.gmail.com que traballa no porto tcp 993. No caso do Dpto. Comercial unicamente no horario de 08:00 a 14 de luns a venres.
- Dende os equipos dos administradores poderán facerse probas tipo ping e traceroute (trazas de rutas).
- Rexistra o tráfico denegado (*Log Denied Rule*).
- Crear unha regra anterior á CleanUp Rule que descarte todo o tráfico de tipo broadcast e multicast pero sen rexistralo (*NoLogging Rule*).

Solución

En primeiro lugar crearanse os alias a usar nas regras. Na solución plantexada creáronse os seguinte alias:

Name	Values	Description
LAN_ruidoso	255.255.255.255/32, 192.168.56.255/32, 224.0.0.0/4	Direccións broadcast e multicast
_Equipos_Dpto_Comercial	192.168.56.50/31, 192.168.56.52/30, 192.168.56.56/29, 192.168.56.64/28, 192.168.56.80/29, 192.168.56.88/31, 192.168.56.90/32	Equipo Dpto. Comercial
_Equipos_admin	equipo_admin1, equipo_admin2	Equipos administradores
_Portos_Administracion	443, 22	Portos admin pfsense
_Servidores_DNS	dns_n1, dns_n2, dns_n3	Servidores DNS
_Servidores_FTP	ftp.rediris.es	Servidores FTP
_Servidores_IMAP	imap.gmail.com	Servidores email IMAP
_Servidores_SMTP	smtp.gmail.com	Servidor email SMTP
dns_n1	192.168.56.253	Servidor DNS 1
dns_n2	8.8.8.8	Servidor DNS 2
dns_n3	8.8.4.4	Servidor DNS 3
equipo_admin1	192.168.56.2	Equipo de Manuel (administrador)
equipo_admin2	192.168.56.21	Equipo do administrador 2
portos_imap	993	Portos email IMAP
portos_smtp	465	Portos email SMTP
portos_web	80, 443	Ports tráfico web

- Alias de Host para o servidor ftp.rediris.es, imap.gmail.com, smtp.gmail.com e engadiuse o terceiro servidor DNS ó alias de _Servidores_DNS.
- Alias de porto para o porto de traballo do servidor smtp e o porto do servidor imap. A modo de exemplo, para os portos DNS (53) e FTP (21) non se crearon alias e escolleuse directamente o porto dende a listaxe de portos ofertada polo pfSense no momento de crear as regras.
- Alias de Networks para as direccións especiais de difusión limitada (255.255.255.255), broadcast na rede LAN (192.168.56.255) e multicast (240.0.0.0/4).

En segundo lugar e co gallo de reducir o número de regras, creouse un schedule para controlar a activación dunha regra que bloqueará o tráfico do Dpto. Comercial fóra do

horario de traballo. Durante o horario de traballo a regra estará desactivada e regras posteriores permitirán o tráfico ós equipos do Dpto. Comercial.

Name	Time Range(s)		Description
BloquearDptoComercial	Mon - Fri Mon - Fri Sat - Sun	0:00-7:59 14:00-23:59 0:00-23:59	Horario de bloqueo Dpto Comercial

Por último, créanse as regras tendo en conta a ubicación das mesmas dentro do ruleset e activando o rexistro nas regras de bloqueo, agás na No Logging Rule.

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
		IPv4 TCP	_Equipos_admin	*	LAN address	_Portos_Administracion	*	none		Anti-lockdown rule
		IPv4 TCP	*	*	LAN address	_Portos_Administracion	*	none		Lockdown rule
		IPv4 UDP	LAN net	*	_Servidores_DNS	53 (DNS)	*	none		Consultas DNS
		IPv4 *	_Equipos_Dpto_Comercial	*	*	*	*	none	BloquearDptoComercial	Bloquear todo o tráfico Dpto. Comercial
		IPv4 TCP	LAN net	*	*	portos_web	*	none		Tráfico web
		IPv4 TCP	LAN net	*	_Servidores_SMTP	portos_smtp	*	none		Envío de emails
		IPv4 TCP	LAN net	*	_Servidores_IMAP	portos_imap	*	none		Lectura de emails
		IPv4 TCP	LAN net	*	_Servidores_FTP	21 (FTP)	*	none		Acceso a ftp.rediris.es
		IPv4 TCP/UDP	_Equipos_admin	*	*	53 (DNS)	*	none		Adminisitradores consultas DNS
		IPv4 ICMP echoreq	_Equipos_admin	*	*	*	*	none		Probas ping e traceroute
		IPv4 *	*	*	LAN_ruidoso	*	*	none		No Logging Rule
		IPv4 *	*	*	*	*	*	none		CleanUp Rule IPv4
		IPv6 *	*	*	*	*	*	none		CleanUp Rule IPv6

1.3.4 Tarefa 4. Probas de tráfico e logs

Empregando como punto de partida a máquina pfSense configurada na tarefa 3, realizar as seguintes accións:

- Configurar pfSense para amosar as 100 últimas entradas dos logs (as máis recentes na parte de arriba).
- Conectarse dende un equipo da Lan diferente ós dos admins para administrar pfSense vía ssh e localizar as entradas correspondente nos logs.
- Conectarse dende un equipo da Internet para administrar pfSense vía web e localizar as entradas correspondente nos logs.
- Facer ping dende un equipo da Lan diferente ós dos admins a un equipo da Internet e localizar as entradas correspondente nos logs.
- Facer un barrido de portos con nmap á Interface WAN de pfsense e analizar o resultado.

- Facer un barrido de portos con Zenmap de tipo Intense á Interface LAN de pfsense dende un equipo dos admins e analizar o resultado.

Solución

Configurar pfSense para amosar as 100 últimas entradas dos logs (as máis recentes na parte de arriba).

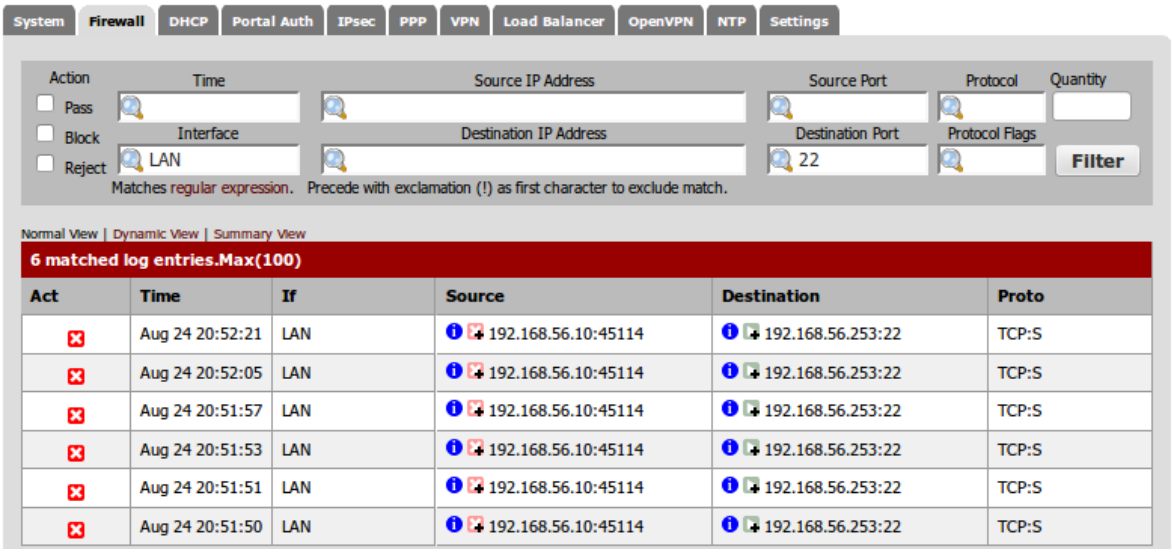
Ir a Status → System Logs → Settings e:

Conectarse dende un equipo da Lan diferente ós dos admins para administrar pfSense vía ssh e localizar as entradas correspondente nos logs

Para ver os eventos de firewall rexistrados por pfSense hai que ir a Status → System Logs → Firewall. Pódese filtrar en base a diversos criterios:

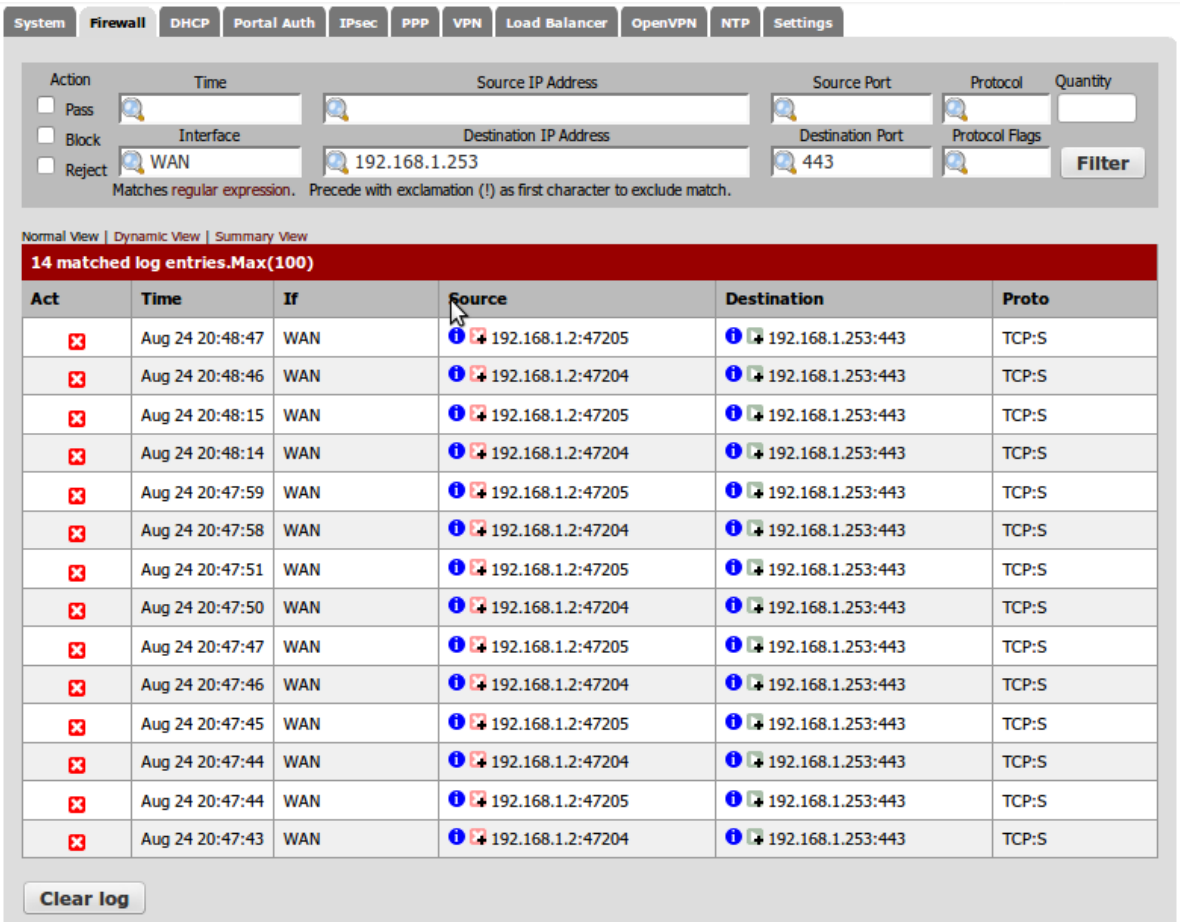
- Acción realizada sobre o paquete (pass, block, reject).
- Data.
- IP orixe /destino.
- Portos orixe/destino.
- Protocolo.
- Interface.

Escóllese a interface LAN e o porto 22 para escoller o tráfico ssh recibido pola interface LAN:

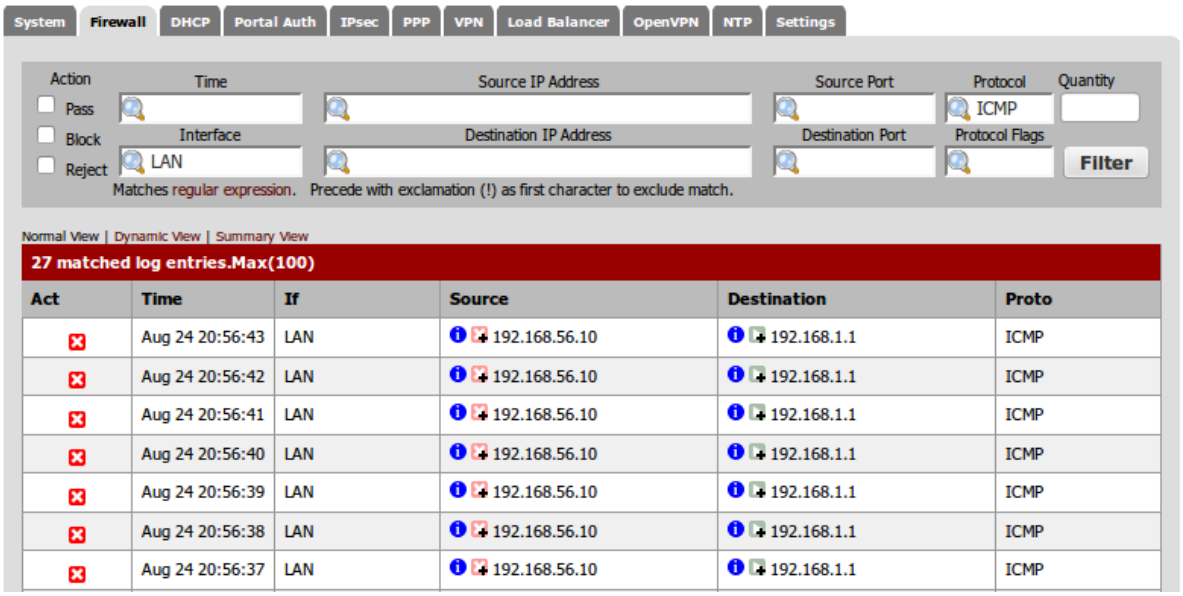


Conectarse dende un equipo da Internet para administrar pfSense vía web e localizar as entradas correspondente nos logs

A modo de exemplo, aplícase un filtro máis preciso para visualizar os paquetes procedentes de Internet (interface WAN) con destino á IP de pfsense (192.168.1.253) e ó servidor web de administración (tcp/443):



Facer ping dende un equipo da Lan diferente ós dos admins a un equipo da Internet e localizar as entradas correspondente nos logs.



Facer un barrido de portos con nmap á Interface WAN de pfsense e analizar o resultado.

Dende a liña de comando execútase:

```
manuel@lubuntu:~$ sudo nmap -sV -O -p 1-65535 192.168.1.253
[sudo] password for manuel:

Starting Nmap 6.40 ( http://nmap.org ) at 2015-08-24 17:02 CEST
Nmap scan report for 192.168.1.253
Host is up (0.00024s latency).
All 65535 scanned ports on 192.168.1.253 are filtered
MAC Address: 08:00:27:D2:8A:C4 (Cadmus Computer Systems)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1317.09 seconds
```

Vese que non hai ningún porto aberto; é dicir, non é accesible ningún servizo dende Internet (non se poden iniciar conexións dende Internet hacia pfSense). Neste exemplo especificáronse todos os portos, tardando 1317 segundo en rematar. Facendo a mesma análise pero limitándose ós portos por defecto que analiza nmap a análise é moito máis rápida (pero menos completa):

```
manuel@lubuntu:~$ sudo nmap -sV -O  192.168.1.253
[sudo] password for manuel:

Starting Nmap 6.40 ( http://nmap.org ) at 2015-08-24 21:09 CEST
Nmap scan report for 192.168.1.253
Host is up (0.00028s latency).
All 1000 scanned ports on 192.168.1.253 are filtered
MAC Address: 08:00:27:D2:8A:C4 (Cadmus Computer Systems)
```

```
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.38 seconds
```

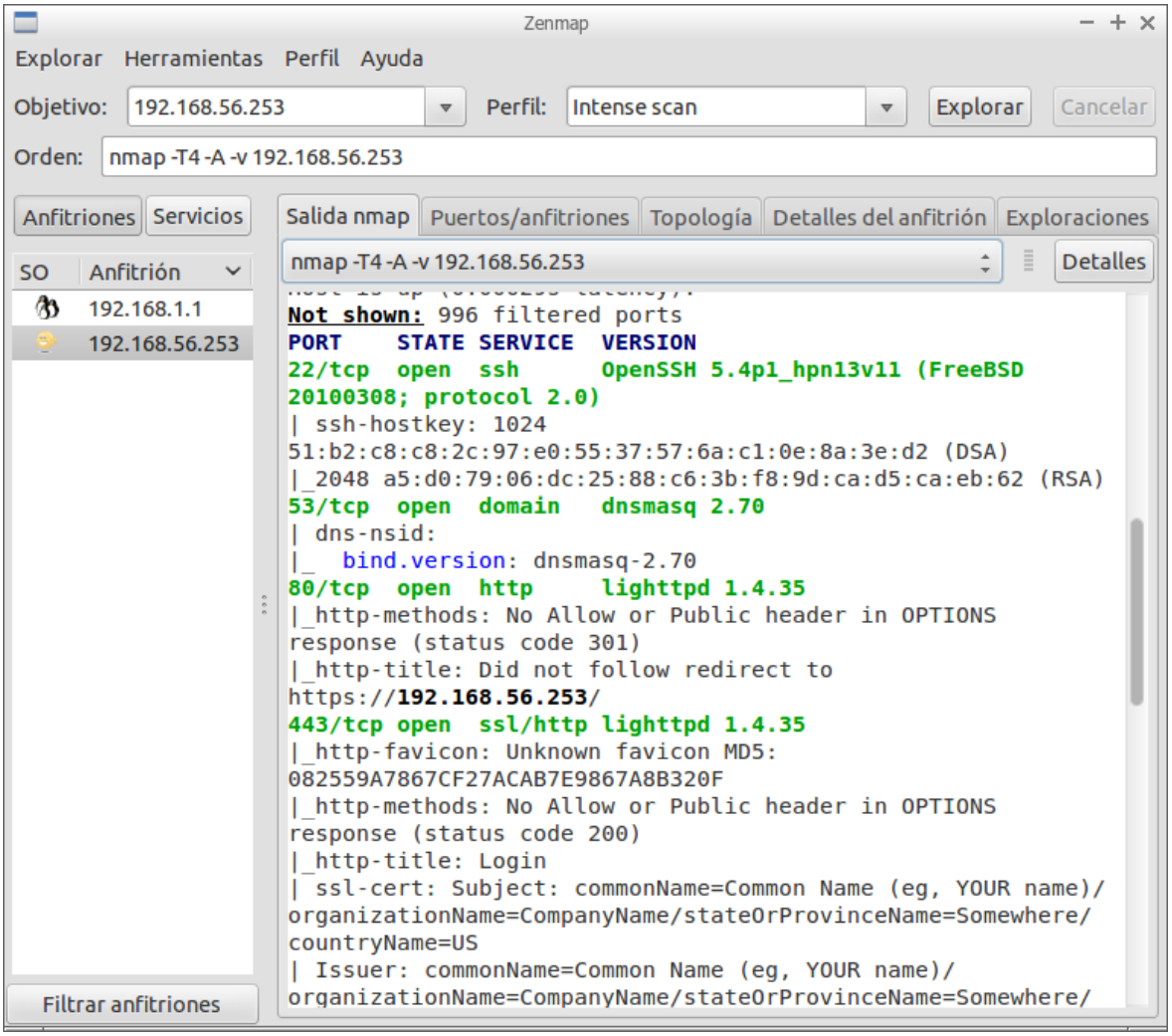
Facer un barrido de portos con Zenmap á Interface LAN de pfsense dende un equipo dos admins e analizar o resultado.

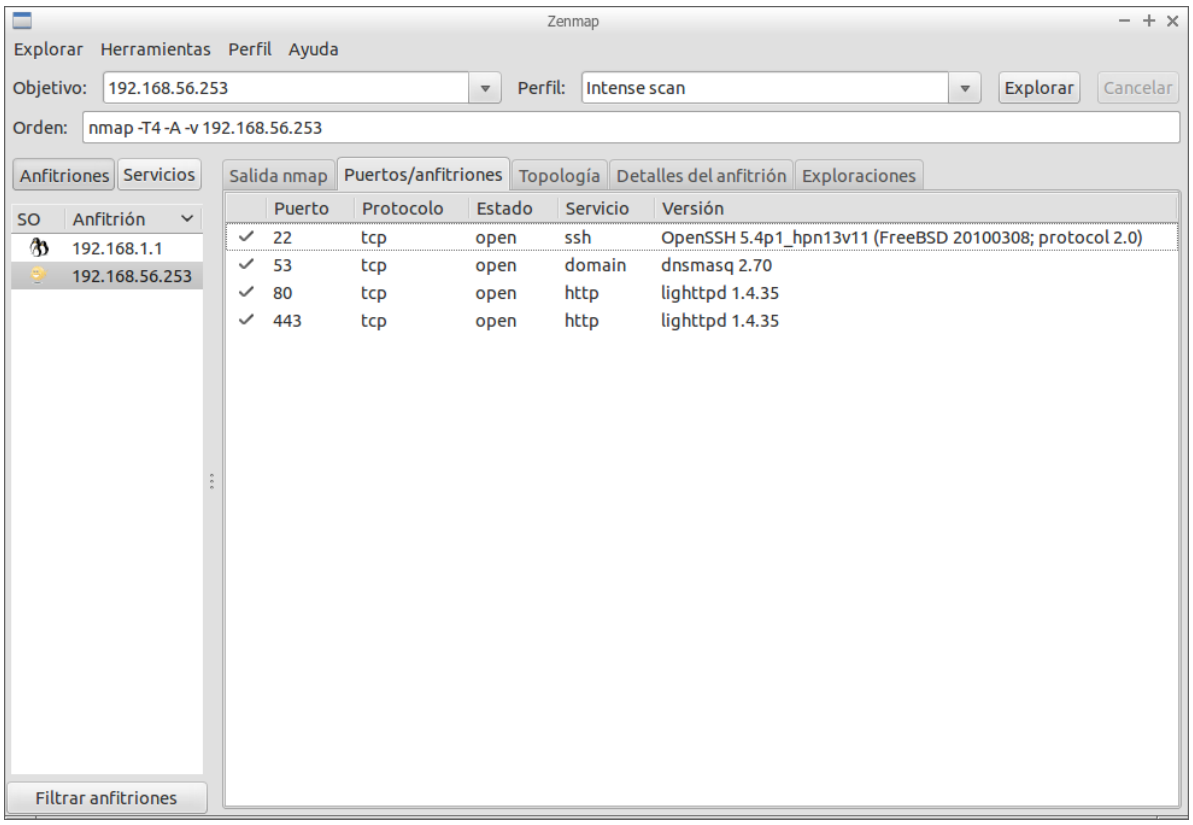
Aparecen os seguintes portos abertos (servizos):

- 22/tcp ssh, correndo OpenSSH.
- 53/tcp DNS, correndo dnsmasq.
- 80/tcp web, correndo lighttpd.
- 80/tcp web, correndo lighttpd.
- 443/tcp web, correndo lighttpd.

Os resultados corresponden co esperado:

- Servizo ssh no porto 22/tcp para administrar pfSense.
- Servizo DNS para permitir a resolución dns dos clientes LAN. Ollo, aquí detectouse que hai un servizo dns correndo no porto 53/tcp, habería que personalizar a análise para barrer os portos udp para confirmar que tamén escoita no 53/udp.
- Porto 80/tcp que escoita peticións para administrar pfSense vía web e redirixe a petición ó porto 443/tcp para traballar con https.
- Servizo web https no porto 443/tcp para administrar pfSense vía web.


Zenmap
Explorar Herramientas Perfil Ayuda
Objetivo: 192.168.56.253
Perfil: Intense scan
Explorar
Cancelar
Orden: nmap -T4 -A -v 192.168.56.253
Anfitriones
Servicios
SO
Anfitrión
192.168.1.1
192.168.56.253
Filtrar anfitriones
Salida nmap
Puertos/anfitriones
Topología
Detalles del anfitrión
Exploraciones
nmap -T4 -A -v 192.168.56.253
Detalles
Not shown: 996 filtered ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 5.4p1_hpn13v11 (FreeBSD 20100308; protocol 2.0)
| ssh-hostkey: 1024 51:b2:c8:c8:2c:97:e0:55:37:57:6a:c1:0e:8a:3e:d2 (DSA)
|_2048 a5:d0:79:06:dc:25:88:c6:3b:f8:9d:ca:d5:ca:eb:62 (RSA)
53/tcp open domain dnsmasq 2.70
| dns-nsid:
|_ bind.version: dnsmasq-2.70
80/tcp open http lighttpd 1.4.35
|_http-methods: No Allow or Public header in OPTIONS response (status code 301)
|_http-title: Did not follow redirect to https://192.168.56.253/
443/tcp open ssl/http lighttpd 1.4.35
|_http-favicon: Unknown favicon MD5: 082559A7867CF27ACAB7E9867A8B320F
|_http-methods: No Allow or Public header in OPTIONS response (status code 200)
|_http-title: Login
| ssl-cert: Subject: commonName=Common Name (eg, YOUR name)/organizationName=CompanyName/stateOrProvinceName=Somewhere/countryName=US
| Issuer: commonName=Common Name (eg, YOUR name)/organizationName=CompanyName/stateOrProvinceName=Somewhere/


Zenmap
Explorar Herramientas Perfil Ayuda
Objetivo: 192.168.56.253
Perfil: Intense scan
Explorar
Cancelar
Orden: nmap -T4 -A -v 192.168.56.253
Anfitriones
Servicios
SO
Anfitrión
192.168.1.1
192.168.56.253
Filtrar anfitriones
Salida nmap
Puertos/anfitriones
Topología
Detalles del anfitrión
Exploraciones
Puerto Protocolo Estado Servicio Versión
22 tcp open ssh OpenSSH 5.4p1_hpn13v11 (FreeBSD 20100308; protocol 2.0)
53 tcp open domain dnsmasq 2.70
80 tcp open http lighttpd 1.4.35
443 tcp open http lighttpd 1.4.35