

Práctica de Evaluación 12 Conceptos y Practicas con cortafuegos

<u>2ºASIR</u>

DIEGO ACOSTA CABRERA



Actividad 1 – 2p Describe las características, tipos y funciones de los cortafuegos

Un cortafuegos actuá principalmente de forma que trata de **prevenir** todo tipo de ataque que intentas entrar a nuestra red desde el exterior y **controlar** el traspaso de paquetes para mantener la seguridad de nuestra red o equipo personal.

Para poder llevar acabo dicho control estos deben realizar unas funciones especificas como:

- Establecer una protección basada en normas
- Filtrar el tráfico de entrada a través de sistemas más confiables.
- Establecer mecanismos de autenticación más fuertes.
- Ocultar información sobre la red que se quiere proteger.
- Crear registros LOG de información.

Estos tambien se puedes diferenciar según su área de influencia o su tecnología utilizada de forma que se clasifican de la siguiente manera:

Según su área de influencia pueden ser:

-**Personales**: estos suelen estar incluidos dentro del software de los sistemas operativos de los dispositivos y se centran principalmente en proteger el trafico que entra y sale de el equipo.

-**Corporativos**: se utilizan en pequeñas redes locales utilizando diferentes extensiones que añades mas funciones al cortafuegos como antivirus, filtrado IP, filtrado de contenidos web, o detección de intrusos.

-**De pequeña oficina**: se encargan de controlar las conexiones de la red de una organización, por lo que deben soportar miles de conexiones. Su potencia y capacidad de proceso deben ser mayores que las de las instalaciones personales o de pequeñas oficinas.

Según sus tecnologías utilizadas se clasifican según sus objetivos como:

-**Filtrado de paquetes**: su objetivo es comparar cada paquete recibido con un conjunto de criterios establecidos, como las direcciones IP, tipo de paquete, número de puerto, etc. Los paquetes marcados como sospechosos son desechados y por lo tanto dejan de existir.

-**Circuito a nivel de pasarela**: en este caso la seguridad solo se aplica en la conexión TCP o UDP establecida. Esto hace que nada mas establecida la conexión ya se pueda navegar libremente por la red sin ningún tipo de examen de seguridad lo que hace que solo se use normalmente si se tiene confianza en los usuarios internos

-Inspección de estado: este caso es muy parecido al filtrado de paquetes pero con la diferencia de que hace un seguimiento del paquete al completo hasta que se establezca una conexión TCP establecida. Esto también hace que se genere mayor consumo del rendimiento de la red.

-**Capa de aplicación**: también llamado firewall proxy, estos combina algunos de los atributos de los firewalls de filtrado de paquetes con los de las pasarelas de nivel de circuito y filtran los paquetes no solo de acuerdo con el servicio para el que están destinados sino también por otras características

Administración de Sistemas informáticos en Red Seguridad y Alta Disponibilidad

Actividad 2 – 2p Clasifica y describe los distintos niveles en los que se realiza el filtrado de tráfico a través de un cortafuegos

En términos generales se suelen clasificar en:

Firewall de Nivel de Red:

- Trabaja con direcciones IP de origen y destino extraídas de la cabecera de la trama IP.
- Identifica los puertos de origen y destino en la comunicación.
- Analiza la cabecera IP a nivel 3 para los protocolos TCP, UDP e ICMP.
- Reconoce si el paquete es el inicio de una solicitud de conexión.

Firewall de Nivel de Aplicación:

- Capaz de inspeccionar datos utilizados por protocolos como FTP, HTTP y SMTP, abordando transferencias de archivos, páginas web y correos electrónicos.
- Ejecuta software de servidor proxy para facilitar un control más profundo sobre las comunicaciones.

Actividad 3 – 6p

Instala pfsense con 3 tarjetas de red como bastión de tu arquitectura de red. A continuación se describe su configuración.

- Tarjeta 1: va a la red WAN
- Tarjeta 2: va a la LAN 192.168.10.0/24
- Tarjeta 3: va a la DMZ 192.168.20.0/24

· · · · · · · · · · · · · · · · · · ·	
FreeBSD/amd64 (pfSense.home.arpa) (ttı	(0vl
KVM Guest – Netgate Device ID: a8cee5o	17332657f0f395
*** Welcome to pfSense 2.7.2-RELEASE	(amd64) on pfSense ***
WAN (wan) -> em0 -> v4/I LAN (lan) -> em1 -> v4: OPT1 (opt1) -> em2 -> v4:	DHCP4: 192.168.52.189/24 192.168.10.1/24 192.168.20.1/24
 Ø) Logout (SSH only) 1) Assign Interfaces 2) Set interface(s) IP address 3) Reset webConfigurator password 4) Reset to factory defaults 5) Reboot system 6) Halt system 7) Ping host 8) Shell 	 9) pfTop 10) Filter Logs 11) Restart webConfigurator 12) PHP shell + pfSense tools 13) Update from console 14) Enable Secure Shell (sshd) 15) Restore recent configuration 16) Restart PHP-FPM
8) Snell	

Administración de Sistemas informáticos en Red Seguridad y Alta Disponibilidad

Realiza los siguientes puntos:

a) muestra la instalación del cortafuegos con la configuración que se dicta

Empezamos la instalación aceptando los términos de copyright y dándole a Instalar pfsense

pfSense Installer
Copyright and distribution notice
Copyright 2004–2016. Electric Sheep Fencing, LLC ("ESF"). All Rights Reserved.
Copyright 2014–2023. Rubicon Communications, LLC d/b/a Netgate ("Netgate"). All Rights Reserved.
All logos, text, and content of ESF and/or Netgate, including underlying HTML code, designs, and graphics used and/or depicted herein are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of ESF and/or Netgate.
"pfSense" is a registered trademark of ESF, exclusively licensed to Netgate, and may not be used without the prior express written permission of ESF and/or Netgate. All other trademarks shown herein are
[Accept]

pfSense Installer 	
Welcome to pfSense!	Helcome Install pfSense
Rescue Shell Recover config.xml	Launch a shell for rescue operations Recover config.xml from a previous install
<.	0 <mark>K ></mark> <cancel></cancel>

Seleccionamos la opcion de UFS para particionar nuestro disco entero.

pfSense Installer
Partitioning How would you like to partition your disk?
Auto (ZFS) Guided Root-on-ZFS Puto (UFS) Guided UFS Disk Setup Manual Manual Disk Setup (experts) Shell Open a shell and partition by hand
<pre>Cancel></pre>
Menu options help choose which disk to setup using UFS and standard partitions



Seleccionamos la versión GUI de la tabla de particiones para verla de forma grafica y le damos a finish.

FreeBSD Installer		
Hould (ada0 share Using curre	Partition Scheme Select a partition scheme for this volume: APM Apple Partition Map BSD BSD Labels PT BUID Partition Table MBR DOS Partitions	na k data
Rootable on most x86 su	stems and FFI aware ARM64	

FreeBSD Installer	
Prese review the disk setup. When complete, press the Finish button.	
ada0p2 9.5 GB freebsd-ufs / ada0p3 512 MB freebsd-swap none	
[Create] [Delete] [Modify] [Devert] [Auto] [Finish]	

Esperamos a que termine la instalación y ahora ya podremos ver la interfaz de pfsense con las tres tarjetas que hemos configurado, ademas de aplicar el comando **pfctl -d** que nos dejara abrir la interfaz grafica de pfsense desde nuestra maquina real para mas comodidad.

pfSense Installer 	
	Base.txz I Extracting distribution files Overall Progress 22%

FreeBSD/amd64 (pfSense.home.arpa) (tt	tyv0)
KVM Guest - Netgate Device ID: a8cee	5d7332657f0f395
*** Welcome to pfSense 2.7.2-RELEASE	(amd64) on pfSense ***
WAN (wan) -> em0 -> v4 LAN (lan) -> em1 -> v4 OPT1 (opt1) -> em2 -> v4	/DHCP4: 192.168.52.189/24 : 192.168.10.1/24 : 192.168.20.1/24
 Ø) Logout (SSH only) 1) Assign Interfaces 2) Set interface(s) IP address 3) Reset webConfigurator password 4) Reset to factory defaults 5) Reboot system 6) Halt system 7) Ping host 8) Shell 	9) pfTop 10) Filter Logs 11) Restart webConfigurator 12) PHP shell + pfSense tools 13) Update from console 14) Enable Secure Shell (sshd) 15) Restore recent configuration 16) Restart PHP-FPM

Enter an option: 8

[2.7.2-RELEASE][root@pfSense.home.arpa]/root: pfctl -d pf disabled [2.7.2-RELEASE][root@pfSense.home.arpa]/root:

Administración de Sistemas informáticos en Red Seguridad y Alta Disponibilidad

b) Realiza algunos filtros en el cortafuegos, los que tu quieras, por ejemplo, que los nodos de la red DMZ no puedan comunicarse con los nodos de la red LAN, o que los nodos de la LAN no puedan conectarse a internet y los de la DMZ si.
 Prohibir conexión de la DMZ a la LAN

En esta regla especifico que toda comunicación IPv4 que salga de la DMZ este permitida menos la entrada a la red 192.168.10.0 (LAN).

Firewall / Rules /	Edit				≑ ਘ 🖩 😧
Edit Firewall Rule					
Action	Pass		•		
	Choose what to do with p Hint: the difference betwe whereas with block the pa	ackets that match the criteria specified below. en block and reject is that with reject, a packe cket is dropped silently. In either case, the original sectors in the sector of the sec	t (TCP RST or ICMP ginal packet is disca	port unreachable for UDP) is re rded.	turned to the sender,
Disabled	Disable this rule				
	Set this option to disable	this rule without removing it from the list.			
Interface	OPT1	Ň	·		
	Choose the interface from	which packets must come to match this rule			
Address Family	IPv4		·		
	Select the Internet Protoc	ol version this rule applies to.			
Protocol	Any				
	Choose which IP protocol	this rule should match.			
Source					
Source	Invert match	Network	~	192.168.20.10	/ 24 ~
Destination					
Destination	Invert match	Network	v)	192.168.10.0	/ 24 ~
Eutra Ontinga					
Extra Options					
Log	 Log packets that are h Hint: the firewall has limit. 	andled by this rule ad local log space. Don't turn on logging for ex	enthing. If doing a l	ot of logging, consider using a	remote syslog server (see
	the Status: System Logs:	Settings page).	crything. It doing a t	or of logging, consider using a	cinote by slog bennen (acc
Description	Pasar todo menos DMZ	a LAN			
	A description may be ente log.	red here for administrative reference. A maxir	num of 52 character	s will be used in the ruleset and	I displayed in the firewall
Advanced Options	🕸 Display Advanced				

Aqui vemos que en nuestra DMZ tenemos todo tipo de conexión a internet o la interfaz WAN pero al tratar de conectar con la IP de la LAN no nos deja comunicar, en cambio como se ve en la izquierda de la LAN a la DMZ si hay comunicacion



Permitir acceso de la LAN a la interfaz, pero no a la maquina de la DMZ

Aqui implemente 2 reglas:

1º. Que la LAN tenga acceso a la interfaz de la DMZ

Firewall / Rules /	Edit				≢ ਘ 🖩 😧
Edit Firewall Rule					
Action	Pass Choose what to do with pa Hint: the difference betwee whereas with block the page	ckets that match the criteria specified below. n block and reject is that with reject, a packe ket is dropped silently. In either case, the ori	t (TCP RST or ICMP ginal packet is disca	port unreachable for UDP) is retur rded.	ned to the sender,
Disabled	Disable this rule Set this option to disable t	nis rule without removing it from the list.			
Interface	LAN Choose the interface from	which packets must come to match this rule			
Address Family	IPv4 Select the Internet Protoco	l version this rule applies to.			
Protocol	Any Choose which IP protocol	his rule should match.			
Source <u>Source</u>	Invert match	Network	v	192.168.10.0	/ 24 ~
Destination Destination	Invert match	OPT1 address	~	Destination Address	/ v
Extra Options Log	Log packets that are had Hint: the firewall has limite the Status: System Logs: S	ndled by this rule d local log space. Don't turn on logging for ev ettings page).	rerything. If doing a	lot of logging, consider using a ren	note syslog server (see
Description	Acceso a la interfaz de la A description may be enter log.	DMZ ed here for administrative reference. A maxir	num of 52 character	rs will be used in the ruleset and di	splayed in the firewall
Advanced Options	Display Advanced				

2º. Que la LAN tenga prohibido comunicarse con toda IP dentro de la red 192.168.20.0 (DMZ)

	Luit				₽ □ □
lit Firewall Rule					
Action	Defect				
Action	Choose what to do with	nackets that match the criteria specified b			
	Hint: the difference betw whereas with block the	ween block and reject is that with reject, a p packet is dropped silently. In either case, th	acket (TCP RST or ICMP te original packet is disc	port unreachable for UDP) is retur arded.	ned to the sender,
Disabled	Disable this rule				
	Set this option to disab	le this rule without removing it from the list			
Interface	LAN		~		
	Choose the interface fro	om which packets must come to match this	s rule.		
Address Family	IPv4		~		
	Select the Internet Prote	ocol version this rule applies to.			
Protocol	Any		~		
	Choose which IP protoc	ol this rule should match.			
ource					
Source	Invert match	Network	~	192.168.10.0	/ 24
estination					
	Invert match	OPT1 subnets	~	Destination Address	1
Destination	0				
Destination					
<u>Destination</u> tra Options					
Destination tra Options Log	Log packets that are	handled by this rule			
<u>Destination</u> tra Options Log	 Log packets that are Hint: the firewall has lin the Status: System Log 	: handled by this rule nited local log space. Don't turn on logging s: Settings page).	for everything. If doing a	lot of logging, consider using a ren	note syslog server (see
Destination ttra Options Log Description	Log packets that are Hint: the firewall has lin the Status: System Log Prohibir acceso de la I	: handled by this rule vited local log space. Don't turn on logging s: Settings page). AN Ia maquina de la DMZ	for everything. If doing a	lot of logging, consider using a rer	note syslog server (see
Destination tra Options Log Description	Log packets that are Hint: the firewall has lin the Status: System Log Prohibir acceso de la L A description may be er log.	: handled by this rule vited local log space. Don't turn on logging a: Settings page). AN la maquina de la DMZ tered here for administrative reference. A r	for everything. If doing a	lot of logging, consider using a ren	note syslog server (see splayed in the firewall

Y al poner por arriba la primera regla podemos ver que como esta tiene prioridad sobre la segunda y aunque la interfaz de la DMZ este dentro del rango de IPs bloqueadas podemos seguir comunicándonos con esta.

anr.										s ping 192,168,1.74
сомми		ISE Sy	stem -	Interfaces -	Fire	ewall - Sen	vices ·	- VPM	N v S	^{ta} PING 192.168.1.74 (192.168.1.74) 56(84) bytes of data. 64 bytes from 192.168.1.74: icmp sec=1 ttl=64 time=4.15 ms
W/	ARNII	NG: The 'adm	in' accoun	t password is set to	the d	efault value. Cha	inge th	ie passwor	rd in the Us	64 bytes from 192.168.1.74: icmp_seq=2 ttl=64 time=12.1 ms 64 bytes from 192.168.1.74: icmp_seq=3 ttl=64 time=3.34 ms 64 bytes from 192.168.1.74: icmp_seq=4 ttl=64 time=2.18 ms ^C
Fi	rev	vall / Rul	les / L	AN						— 192.168.1.74 ping statistics — 4 packets transmitted, 4 received, 0% packet loss, time 3122ms rtt min/avg/max/mdev = 2.178/5.446/12.113/3.912 ms
										(kali@kali)-[~]
									10000	PING 192.168.20.10 (192.168.20.10) 56(84) bytes of data.
The	e cha	anges have be	een applied	successfully. The	firewa	Il rules are now r	eloadi	ng in the b	ackground	^c
Mo	onitoi	the filter relo	ad progre	SS.						- 192.168.20.10 ping statistics -
										2 packets transmitted, 0 received, 100% packet toss, time 1005ms
Flo										[(kali⊛ kali)-[~]
Ru	iles	(Drag to C States	Change (Order) Source	Port	Destination	Port	Gateway	Queue S	<pre>(kali@ kali)-[~]</pre>
Ru	iles v	(Drag to C States 1/2.07 MiB	Change (Protocol	Order) Source	Port *	Destination LAN Address	Port 443	Gateway *	Queue S	<pre>(kali@ kali)=[~]</pre>
Fle Ru	iles 🗸	(Drag to C States 1/2.07 MiB	change (Protocol	Order) Source	Port *	Destination LAN Address	Port 443 80	Gateway *	Queue S	<pre>[kali@ kali)=[~]</pre>
Fli Ru	iles	(Drag to C States 1/2.07 MiB	Change (Protocol *	Order) Source *	Port *	Destination LAN Address	Port 443 80	Gateway *	Queue S *	<pre>(kali@ kali)=[~]</pre>
Fli Ru	iles ✓	(Drag to C States 1/2.07 MiB 0/2 KiB	Change (Protocol * IPv4*	Opril	Port *	Destination LAN Address OPT1 address	Port 443 80 *	Gateway * *	Queue S * none	<pre>(kali@ kali)-[~]</pre>
Fli Ru O	iles ✓	(Drag to C States 1/2.07 MiB 0/2 KiB 0/672 B	Protocol * IPv4* IPv4*	Opril Source * 192.168.10.0/24 192.168.10.0/24	Port * * *	Destination LAN Address OPT1 address OPT1 subnets	Port 443 80 *	Gateway * * *	Queue S * none none	<pre>(kali@ kali)-[~]</pre>
	v v	(Drag to C States 1/2.07 MiB 0/2 KiB 0/672 B 0/13 KiB	Change (Protocol * IPv4* IPv4* IPv4*	OPTI Source * 192.168.10.0/24 LAN subnets	Port * * *	Destination LAN Address OPT1 address OPT1 subnets *	Port 443 80 * *	Gateway * * * * * *	Queue S * none none none	<pre>(kali@ kali)-[~]</pre>
	iles	(Drag to C States 1/2.07 MiB 0/2 KiB 0/672 B 0/13 KiB 0/0 B	Protocol * IPv4* IPv4* IPv4* IPv4* IPv6*	Oprider) Source * 192.168.10.0/24 192.168.10.0/24 LAN subnets LAN subnets	Port * * * * * * *	Destination LAN Address OPT1 address OPT1 subnets * *	Port 443 80 * * * *	Cateway * * * * * * * * *	Queue S *	<pre>(kali@kali)-[~]</pre>

c) Verifica los registros de sucesos para comprobar que los filtros que aplicaste en la actividad están funcionan correctamente.

Los registros de Logs los encontraremos en el apartado **STATUS/SYSTEM** LOGS/FIREWALL/

	ISE System	- Interi	faces 🕶	Firewall 👻	Services 🗸	VPN 🗸	Status 👻	Diagnostics		÷		G
WARNII	NG: The 'admin' acco	ount passwo	ord is set to	the default va	lue. Change the	password in th	e User Manag	er.				
Statu	is / System I	Logs / F	Firewall	/ Norma	al View							₹⊁₿
System	Firewall	DHCP	Authentic	ation IP	sec PPP	PPPoE/L2	TP Server	OpenVPN	NTP	Packages	Settings	
Norma	View Dynam	ic View	Summary	y View								
Last 5	00 Firewall Loc	a Entries.	(Maximu	ım 500)								
Action	Time	Interface	Rule	,				Source		Destination		Protocol
×	Jan 19 02:01:11	WAN	Default	t deny rule IPv	4 (1000000103)			i = 202.12	27.33:53	i 🕀 192.1	68.1.74:57128	TCP:SA
×	Jan 19 02:01:27	WAN	Block p	private networ	ks from WAN blo	ck 192.168/16	(12004)	192.16	8.1.140:4949	95 192.1	68.1.74:80	TCP:S
×	Jan 19 02:01:27	WAN	Block p	orivate network	ks from WAN blo	ick 192.168/16	(12004)	i 🗖 192.16	8.1.140:4949	96 192.1	68.1.74:80	TCP:S
×	Jan 19 02:01:28	WAN	Block p	orivate networl	ks from WAN blo	ck 192.168/16	(12004)	192.16	8.1.140:4949	97 🚹 192.1	68.1.74:80	TCP:S
×	Jan 19 02:01:28	WAN	Block p	private network	ks from WAN blo	ick 192.168/16	(12004)	192.16	8.1.1	1 224.0	.0.1	IGMP
×	Jan 19 02:02:05	WAN	Block p	orivate network	ks from WAN blo	ck 192.168/16	(12004)	192.16	8.1.140:494	95 🚹 192.1	68.1.74:80	TCP:S
×	Jan 19 02:02:09	WAN	Block p	orivate network	ks from WAN blo	ck 192.168/16	(12004)	192.16	8.1.140:4949	96 192.1	68.1.74:80	TCP:S
×	Jan 19 02:02:09	WAN	Block p	private networl	ks from WAN blo	ck 192.168/16	(12004)	192.16	8.1.140:4949	97 192.1	68.1.74:80	TCP:S
×	Jan 19 02:02:55	WAN	Block p	private network	ks from WAN blo	ick 192.168/16	(12004)	192.16	8.1.140:495	10 192.1	68.1.74:80	TCP:S
×	Jan 19 02:02:55	WAN	Block p	orivate networl	ks from WAN blo	ick 192.168/16	(12004)	192.16	8.1.140:495	11 192.1	68.1.74:80	TCP:S
×	Jan 19 02:02:55	WAN	Block p	orivate networl	ks from WAN blo	ick 192.168/16	(12004)	i 🗖 192.16	8.1.140:495	12 192.1	68.1.74:80	TCP:S
~	lan 19 02:02:55	WAN	Block	rivate network	ks from WAN blo	ck 192 168/16	(12004)	192 16	8 1 140:495	10 1 192 1	68.1.74:80	TCP:S

Donde podemos observar como se ven los paquetes que se bloquearon al aplicar la primera regla que hicimos para que la DMZ no conectara con la LAN.

×	Jan 19 05:19:38	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
×	Jan 19 05:19:40	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
×	Jan 19 05:19:41	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
×	Jan 19 05:19:42	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
×	Jan 19 05:19:43	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
×	Jan 19 05:19:52	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
×	Jan 19 05:20:06	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
×	Jan 19 05:20:11	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
×	Jan 19 05:20:21	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
×	Jan 19 05:20:26	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
×	Jan 19 05:20:31	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
×	Jan 19 05:20:37	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
×	Jan 19 05:20:38	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
×	Jan 19 05:20:39	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
×	Jan 19 05:20:44	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
×	Jan 19 05:20:49	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
×	Jan 19 05:20:54	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
×	Jan 19 05:21:09	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP
×	Jan 19 05:21:15	OPT1	Default deny rule IPv4 (1000000103)	192.168.20.10	192.168.10.10	ICMP

×	Jan 19 03:55:02	WAN	192.168.1.1:138	192.168.1.255:138	UDP
×	Jan 19 03:59:06	WAN	192.168.1.1	224.0.0.1	IGMP
×	Jan 19 03:59:45	LAN	0.0.0:68	255.255.255.255:67	UDP
×	Jan 19 03:59:55	LAN	0.0.0.0:68	255.255.255.255:67	UDP
×	Jan 19 03:59:58	LAN	0.0.0:68	255.255.255.255:67	UDP
×	Jan 19 04:00:07	LAN	0.0.0:68	255.255.255.255:67	UDP
×	Jan 19 04:00:33	OPT1	0.0.0.0:68	255.255.255.255:67	UDP
×	Jan 19 04:00:44	OPT1	0.0.0.0:68	255.255.255.255:67	UDP
×	Jan 19 04:00:59	OPT1	0.0.0:68	255.255.255.255:67	UDP
×	Jan 19 04:01:28	LAN	0.0.0:68	255.255.255.255:67	UDP
×	Jan 19 04:02:04	OPT1	0.0.0:68	255.255.255.255:67	UDP
×	Jan 19 04:02:14	OPT1	0.0.0:68	255.255.255.255:67	UDP
×	Jan 19 04:02:51	WAN	192.168.1.1	224.0.0.1	IGMP
×	Jan 19 04:07:57	WAN	192.168.1.1	224.0.0.1	IGMP
×	Jan 19 04:12:03	WAN	192.168.1.1	224.0.0.1	IGMP
×	Jan 19 04:15:05	WAN	192.168.1.1	224.0.0.1	IGMP
×	Jan 19 04:19:46	WAN	192.168.1.1	224.0.0.1	IGMP
×	Jan 19 04:24:26	WAN	192.168.1.1	224.0.0.1	IGMP
×	Jan 19 04:28:23	WAN	192.168.1.1	224.0.0.1	IGMP
×	Jan 19 04:29:06	OPT1	192.168.20.10	192.168.10.10	ICMP
×	Jan 19 04:29:11	OPT1	192.168.20.10	192.168.10.10	ICMP
×	Jan 19 04:29:16	OPT1	192.168.20.10	192.168.10.10	ICMP
×	Jan 19 04:29:17	OPT1	192.168.20.10	192.168.10.10	ICMP
~	Ion 10 01.20.22	ODT1	102 168 20 10	102 168 10 10	ICMD