

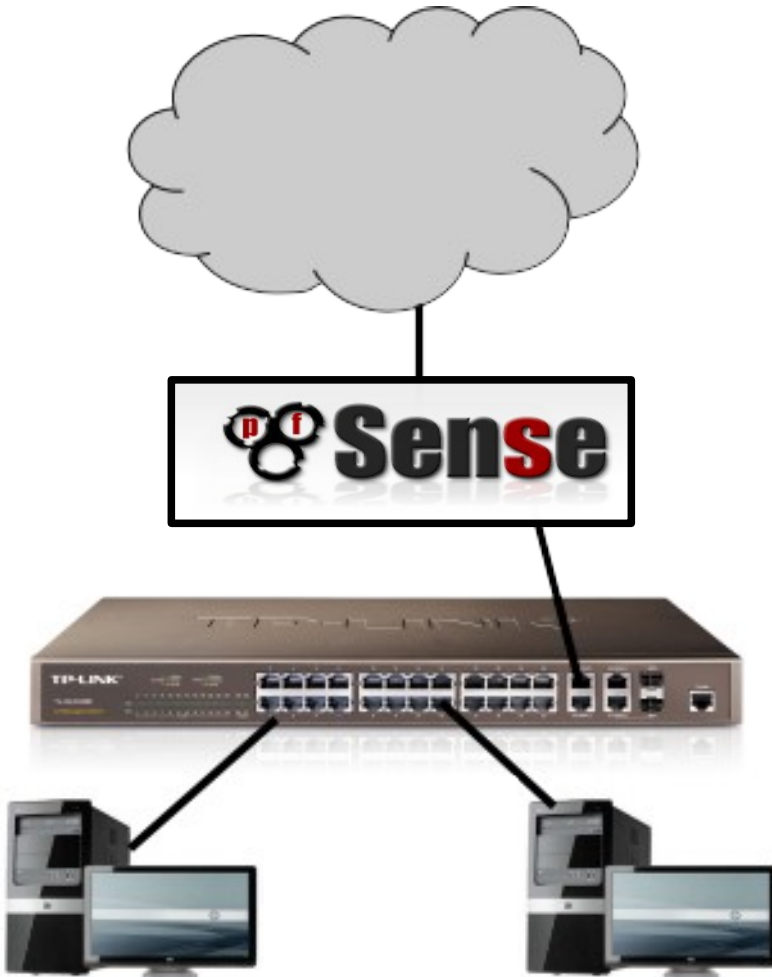
Actividade A01: Os firewalls e as regras de filtraxe

Tarefa 3: Práctica guiada consistente na creación de regras de filtrado nun network level firewall para cumprir cunha política de tráfico dunha organización.

Autor: Manuel González Regal

Obra baixo unha licenza Creative Commons Recoñecemento-Non Comercial-Compartir Igual 4.0 Internacional. Para ver unha copia desta licenza ir a <http://creativecommons.org/licenses/by-nc-sa/4.0/>

Proxecto: creación de regras de filtrado (*ruleset*)



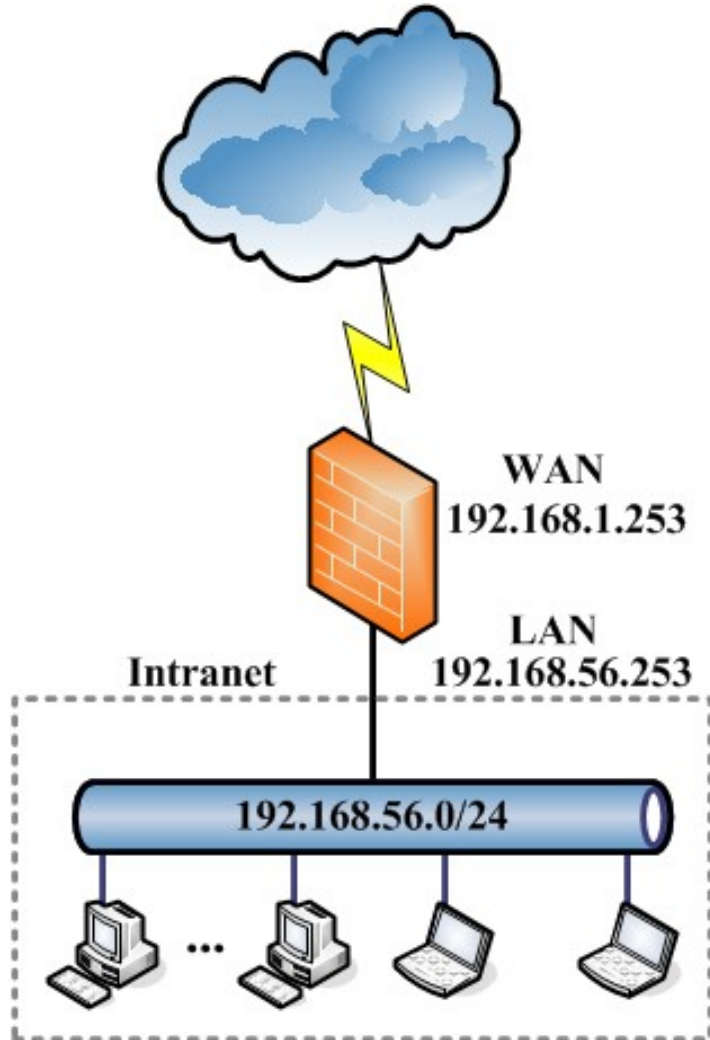
Obxectivo

Control do tráfico dende/hacia Internet cun firewall de rede

Procedemento

Configurar regras en pfsense para satisfacer unha política de tráfico definida

Proxecto: creación de regras de filtrado (*ruleset*)



admin1 → .2

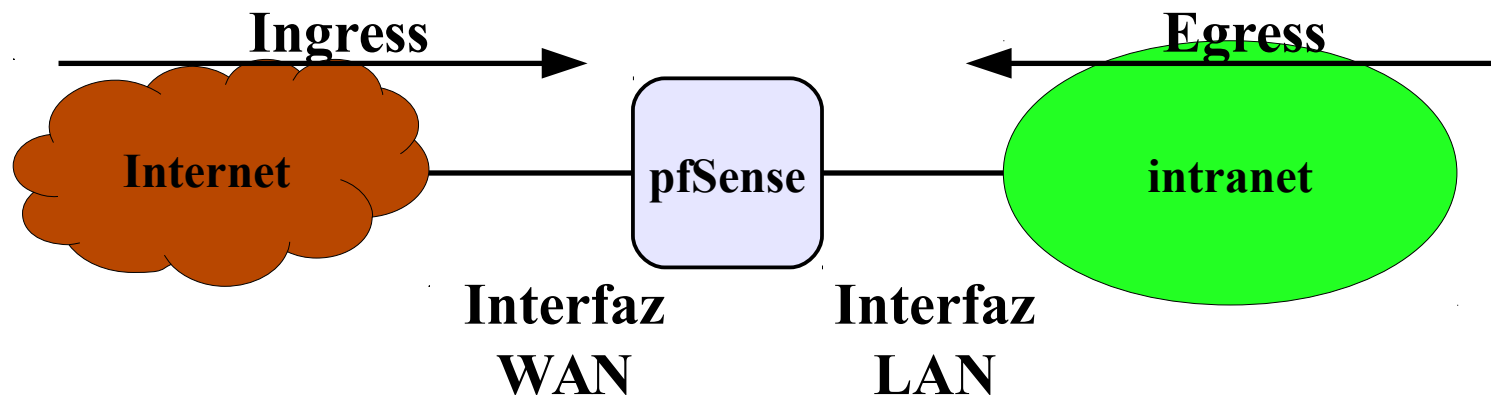
admin2 → .21

Dpto. comercial → de .50 a .90

- Os equipos dende onde se configurará pfSense:
 - Equipo admin1 → 192.168.56.2
 - Equipo admin2 → 192.168.56.21
 - Acceso por ssh y https
- Servidores DNS autorizados:
 - DNS principal: el propio pfSense
 - DNS secundario: 8.8.8.8
- Únicamente estará permitido ós usuarios da Intranet (só IPv4):
 - Tráfico DNS, únicamente ós DNS autorizados.
 - Visitar páxinas web por http/https.
 - Os equipos do departamento comercial (de 192.168.56.50 a 192.168.56.90), únicamente poderán visitar as webs en horario de 8:00 am a 14:00 de luns a venres.

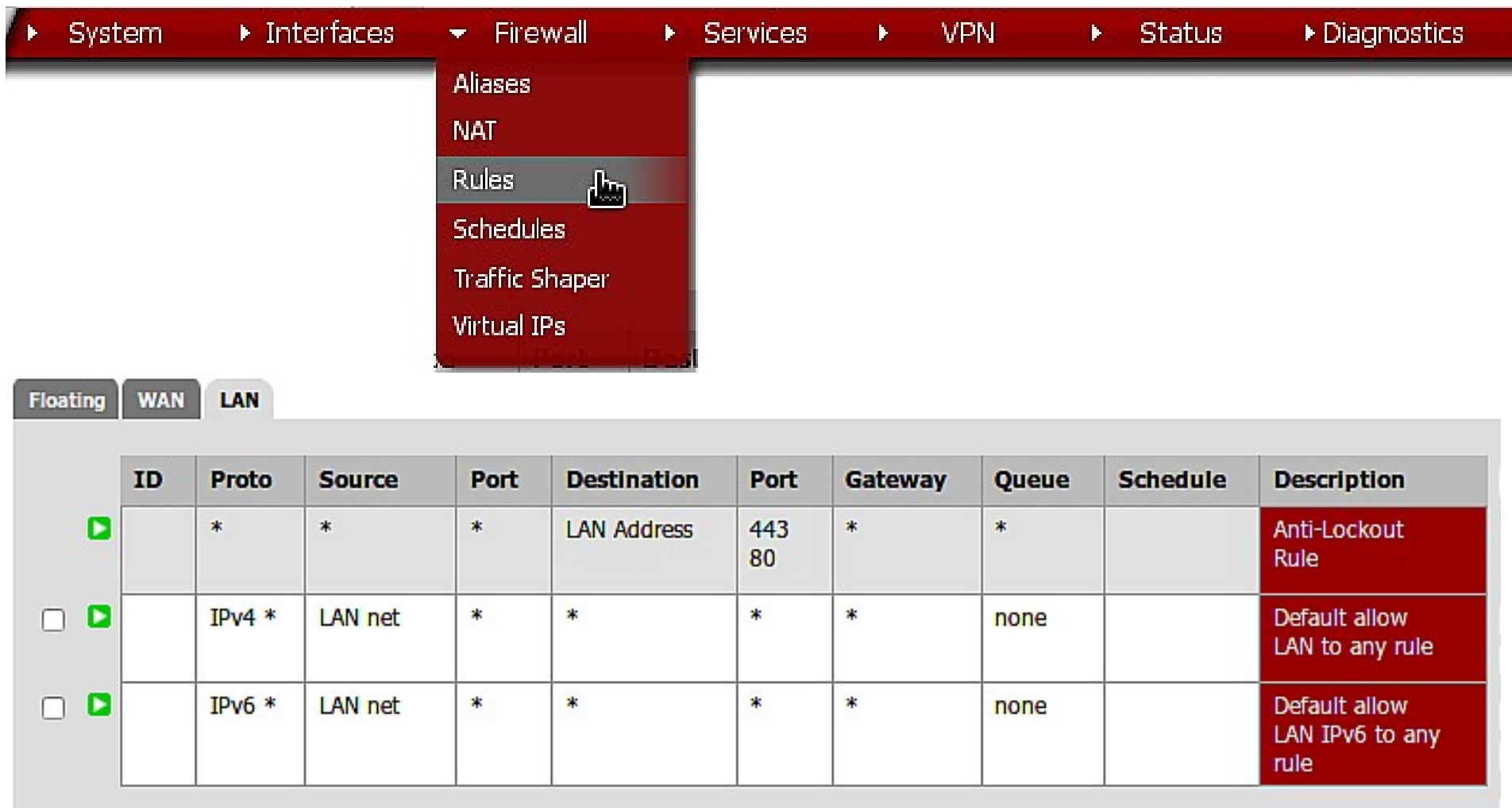
Para traballar correctamente con pfSense hai que ter en conta o seguinte:

- Stateful Packet Filtering.
- Filtrado en base a conxuntos de regras por interface (ruleset).
- Accións:
 - PASS → paquete aceptado → continúa a súa marcha
 - BLOCK → descarte silencioso
 - REJECT → descarte informado
 - Conexión tcp → TCP RST
 - Conexión udp → ICMP porto inaccesible
- Filtrado Ingress/Egress.



Hai que definir as regras na interface por onde chega o paquete

BOAS PRÁCTICAS: CleanUp Rule



The screenshot shows the pfSense web interface. The top navigation bar includes System, Interfaces, Firewall, Services, VPN, Status, and Diagnostics. The Firewall menu is expanded, showing Aliases, NAT, Rules (highlighted with a mouse cursor), Schedules, Traffic Shaper, and Virtual IPs. Below the navigation bar, the 'LAN' tab is selected under the 'Floating' section. A table displays the firewall rules for the LAN interface.

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input checked="" type="checkbox"/>		*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule
<input type="checkbox"/>		IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule
<input type="checkbox"/>		IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule

Por defecto está permitida a saída de todo o tráfico IPv4 e IPv6 orixinado na Intranet e que chega ó pfSense a través da interface LAN

BOAS PRÁCTICAS: CleanUp Rule

Firewall: Rules



Floating

WAN

LAN

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
1	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule
2	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule
2	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule

1. **Anti-Lockout Rule** → permitir acceso admin a pfsense

2. **Permitir todo:**

- **É o máis cómodo.**
- Ven activada por defecto en moitos routers/firewalls.
- **Non é o máis seguro.**

BOAS PRÁCTICAS: CleanUp Rule

Firewall: Rules



Floating

WAN

LAN

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
1	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule
2	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule
2	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule

1. **Anti-Lockout Rule** → permitir acceso admin a pfsense

2. **Permitir todo:**

3. **CleanUp Rule** → denegar por defecto

- Cando un paquete 'atravesar' todas as regras sen verse afectado chega a esta última e descártase.
- En pfSense a CleanUp Rule non é visible, pero é a última regra a aplicar a un paquete no caso de atravesar todas.

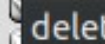
BOAS PRÁCTICAS: CleanUp Rule

Firewall: Rules

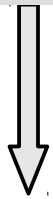


Floating WAN LAN

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input checked="" type="checkbox"/>	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule
<input type="checkbox"/>	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule
<input type="checkbox"/>	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule



delete rule



Bórranse as regras que permiten todo o tráfico saínte para IPv4 e IPv6. Para que os cambios sexan efectivos hai que confirmalos no botón *Apply Changes* que aparecerá

Floating WAN LAN

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input checked="" type="checkbox"/>	*	*	*	LAN Address	80 443	*	*		Anti-Lockout Rule



No rules are currently defined for this interface
All incoming connections on this interface will be blocked until you add pass rules.

Click the  button to add a new rule.

BOAS PRÁCTICAS: CleanUp Rule



Firewall: Rules

Floating **WAN** LAN

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	*	*	*	LAN Address	80 443	*	*		Anti-Lockout Rule

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until you add pass rules.
Click the  button to add a new rule.

 pass
 pass (disabled)

 block
 block (disabled)

 reject
 reject (disabled)

 log
 log (disabled)

Hint:
Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you

add new rule

pfSense is © 2004 - 2011 by BSD Perimeter LLC. All Rights Reserved. [view license]

Aínda que non é necesario, engadirase unha CleanUp Rule ó final do conxunto de regras para tela explicitamente e así ver como se crean regras co asistente web en pfSense.

Action	<div>Block</div> <div>Pass</div> <div>Block</div> <div>Reject</div>
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	<div>LAN</div> <div>Choose on which in</div>
TCP/IP Version	<div>IPv4+IPv6</div> Select the Internet Protocol version this rule applies to
Protocol	<div>TCP</div> <div>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</div>
Source	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <div>any</div> Address: <div></div> / <div>127</div> <div>Advanced</div> - Show source port range
Destination	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <div>any</div> Address: <div></div> / <div>127</div>
Destination port range	from: <div>(other)</div> <div></div> to: <div>(other)</div> <div></div> Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the 'to' field empty if you only want to filter a single port.
Log	<input type="checkbox"/> Log pack Hint: the firewa using a remote
Description	<div></div> <div>You may enter a description here for your reference.</div>

Acción a realizar sobre o paquete

Interface por onde chega o paquete


Características do paquete:

- Protocolo (tcp,udp,icmp, ...)
- IP orixen
- IP destino
- Portos

Activar rexistro dos paquetes que cumpren a regra

Comentario/descrición da regra

Facendo a CleanUp Rule visible

Edit Firewall rule	
Action	<div>Block</div> <p>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</p>
Disabled	<div><input type="checkbox"/> Disable this rule</div> <p>Set this option to disable this rule without removing it from the list.</p>
Interface	<div>LAN</div> <p>Choose on which interface packets must come in to match this rule.</p>
TCP/IP Version	<div>IPv4</div> Select the Internet Protocol version this rule applies to
Protocol	<div>any</div> <p>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</p>
Source	<div><input type="checkbox"/> not</div> <p>Use this option to invert the sense of the match.</p> <p>Type: <div>any</div></p> <p>Address: <div></div> / <div>127</div></p>
Destination	<div><input type="checkbox"/> not</div> <p>Use this option to invert the sense of the match.</p> <p>Type: <div>any</div></p> <p>Address: <div></div> / <div>127</div></p>
Log	<div><input type="checkbox"/> Log packets that are handled by this rule</div> <p>Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).</p>
Description	<div> CleanUp Rule</div> <p>You may enter a description here for your reference.</p>

Firewall: Rules

Firewall: Rules


Firewall: Rules

Firewall: Rules


BOAS PRÁCTICAS: CleanUp Rule

Firewall: Rules

Floating WAN LAN

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until you add pass rules.

Click the  button to add a new rule.

Nesta imaxe vese que na interface WAN non se permite a entrada de ningún paquete dende o exterior. Están bloqueadas explicitamente as redes bogon e por última hai unha CleanUp Rule que bloquea todo.

OLLO: pfSense é un stateful firewall; esto tradúcese en que unha conexión iniciada dende a Intranet, se é autorizada pasa á táboa de estado e polo tanto todos os paquetes de resposta procedentes de Internet ó chegar a WAN serán autorizados a entrar, aínda que non haxa ningunha regra que na listaxe de regras WAN:


Alias: permiten agrupar portas, hosts ou redes e facer referencia a eles polo nome. Calquera modificación nos Alias aplícase a todas as regras do firewall nas que se use o alias, facilitando a interpretación das regras e o seu mantemento.



Firewall: Aliases: Edit


Alias Edit

Name

 equipo_admin1

The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description

 Equipo de Manuel (administrador)


You may enter a description here for your reference (not parsed).


Type

Host(s)

Host(s)

Enter as many hosts as you would like. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used.

IP		Description
192.168.56.2	32	



Save

Cancel

A partir deste momento, poderase usar o alias `equipo_admin1` para facer referencia á IP 192.168.56.2 nas regras do firewall. PfSense reemplazará o alias polo seu valor real.

Firewall: Aliases

IP

Ports

URLs

All

Name	Values	Description
equipo_admin1	192.168.56.2	Equipo de Manuel (administrador)

Floating

WAN

LAN

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input checked="" type="checkbox"/>		*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 TCP	<u>equipo_admin1</u>	*	*	80 (HTTP)	*	none		admin1 pode visitar páxinas web
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 *	*					none		CleanUp Rule IPv4

Equipo de Manuel (administrador) - 1 item edit

192.168.56.2

Se máis adiante a IP do `equipo_admin1` cambia, únicamente hai que modificar o alias e actualizaranse todas as regras ó novo valor.

Alias: Host

Firewall: Aliases: Edit



Alias Edit													
Name	<div> _Servidores_DNS</div> <p>The name of the alias may only consist of the characters "a-z, A-Z and 0-9".</p>												
Description	<div> Serv. DNS</div> <p>You may enter a description here for your reference (not parsed).</p>												
Type	Host(s)												
Host(s)	<div>Enter as many hosts as you would like. Hosts must be specified by their IP address.</div> <table><thead><tr><th>IP</th><th></th><th>Description</th><th></th></tr></thead><tbody><tr><td>dns_n1</td><td>32 </td><td></td><td></td></tr><tr><td>dns_n2</td><td>32 </td><td></td><td></td></tr></tbody></table> <div></div>	IP		Description		dns_n1	32			dns_n2	32		
IP		Description											
dns_n1	32												
dns_n2	32												

é possible face alias de alias

Alias: Port

Firewall: Aliases: Edit



Alias Edit

Name

_Puertos_Administracion
The name of the alias may only consist of the characters "a-z, A-Z and 0-9".

Description

Puertos admin pfSense
You may enter a description here for your reference (not parsed).

Type

Port(s)

Port(s)

Enter as many ports as you wish. Port ranges can be expressed by separating with a colon.

Port

22 32

Description

por ssh

443 32

por https



Rango de portos: 20000:20100

Alias: Network

Firewall: Aliases: Edit



Alias Edit								
Name	<input type="text" value="_Equipos_Dpto_Comercial"/> <small>The name of the alias may only consist of the characters "a-z, A-Z and 0-9".</small>							
Description	<input type="text" value="Equipos del Dpto. Comercial"/> <small>You may enter a description here for your reference (not saved)</small>							
Type	<input type="text" value="Network(s)"/>							
Network(s)	<div><p>Networks are specified in CIDR format. Select the CIDR mask that pertains to each entry. /32 specifies a single host, /24 specifies 255.255.255.0, etc. Hostnames (FQDNs) may also be specified, using a /32 mask. You may also enter an IP range such as 192.168.1.1-192.168.1.254 and a list of CIDR networks will be derived to fill the range.</p><table><thead><tr><th>Network</th><th>CIDR</th><th>Description</th></tr></thead><tbody><tr><td>192.168.1.50-192.168.1.90</td><td><input type="text" value="32"/></td><td><input type="text"/></td></tr></tbody></table><div></div></div>		Network	CIDR	Description	192.168.1.50-192.168.1.90	<input type="text" value="32"/>	<input type="text"/>
Network	CIDR	Description						
192.168.1.50-192.168.1.90	<input type="text" value="32"/>	<input type="text"/>						

Permite crear alias indicando dirección IP/máscara, nombres de dominio completos (FQN) e rangos de IPs

Os rangos de equipos traducéanse en diferentes bloques CIDR que cubren todas as Ips desexadas

_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
-------------------------	--	------------------------

Alias

Firewall: Aliases

IP Ports URLs All

Name	Values	Description
_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
_Portos_Administracion	443, 22	Portos admin pfsense
_Servidores_DNS	dns_n1, dns_n2	Servidores DNS
dns_n1	192.168.56.253	Servidor DNS 1
dns_n2	8.8.8.8	Servidor DNS 2
equipo_admin1	192.168.56.2	Equipo de Manuel (administrador)
equipo_admin2	192.168.56.21	Equipo do administrador 2

A creación de alias é un proceso que inicialmente pode parecer tedioso e costoso en tempo, pero que máis tarde permite traballar dun xeito máis eficaz.

Unha vez creados e aplicados os cambios, poden ser empregados na creación das regras.

Control do tráfico DNS

Edit Firewall rule	
Action	<div>Pass</div> <p>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</p>
Disabled	<div><input type="checkbox"/> Disable this rule</div> <p>Set this option to disable this rule without removing it from the list.</p>
Interface	<div>LAN</div> <p>Choose on which interface packets must come in to match this rule.</p>
TCP/IP Version	<div>IPv4</div> Select the Internet Protocol version this rule applies to
Protocol	<div>UDP</div> <p>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</p>
Source	<div><input type="checkbox"/> not</div> <p>Use this option to invert the sense of the match.</p> <p>Type: <div>LAN net</div></p> <p>Address: <div></div> / <div>127</div></p> <div>Advanced</div> - Show source port range
Destination	<div><input type="checkbox"/> not</div> <p>Use this option to invert the sense of the match.</p> <p>Type: <div>Single host or alias</div></p> <p>Address: <div>Servidores_DNS</div> / <div>127</div></p>
Destination port range	<p>from: <div>DNS</div></p> <p>to: <div>DNS</div></p> <p>Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the 'to' field empty if you only want to filter a single port</p>

Permítense paquetes que entran pola interface LAN do pfSense de tipo IPv4 UDP con IP orixen algunha da LAN e con destino algún dos servidores DNS autorizados e porto destino UDP 53

Control do tráfico DNS

Firewall: Rules

<div>Floating WAN LAN</div>										
	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
		*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule
<input type="checkbox"/>		IPv4 UDP	LAN net	*	<u>Servidores DNS</u>	53 (DNS)	*	none		Consultas DNS
<input type="checkbox"/>		IPv4 *	*	*	*	*	*	none		CleanUp Rule IPv4
<input type="checkbox"/>		IPv6 *	*	*	*	*	*	none		CleanUp Rule IPv6

Permítese que os equipos da LAN fagan consultas DNS ós servidores DNS indicados. Non hai que crear regras na WAN, xa que pfSense é un stateful firewall.

Fixarse que:

- Empréase o alias _Servidores_DNS e LAN net (creado polo pfSense e que inclúe todos os equipos da LAN 192.168.56.0/24)
- **É de vital importancia a colocación da regra** xa que éstas son precesadas por orde, e a primeira que coincida co paquete execútase e non se analizan máis.

Control do tráfico web

Edit Firewall rule	
Action	<div>Pass</div> <p>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</p>
Disabled	<div><input type="checkbox"/> Disable this rule</div> <p>Set this option to disable this rule without removing it from the list.</p>
Interface	<div>LAN</div> <p>Choose on which interface packets must come in to match this rule.</p>
TCP/IP Version	<div>IPv4</div> Select the Internet Protocol version this rule applies to
Protocol	<div>TCP</div> <p>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</p>
Source	<div><input type="checkbox"/> not</div> <p>Use this option to invert the sense of the match.</p> <p>Type: <div>LAN net</div></p> <p>Address: <div></div> / <div>127</div></p> <div>Advanced</div> - Show source port range
Destination	<div><input type="checkbox"/> not</div> <p>Use this option to invert the sense of the match.</p> <p>Type: <div>any</div></p> <p>Address: <div></div> / <div>32</div></p>
Destination port range	<div>from: (other)</div> <div>tos_web</div> <div>to: (other)</div> <div></div>

Permítense paquetes que entran pola interface LAN do pfSense de tipo IPv4 TCP con IP orixen algunha da LAN e calquera IP destino con porto destino 80 ou 443

Any → calquera destino

O alias incluíndo os portos 80 e 443 permite controlar tráfico web cunha única regra

Control do tráfico web

Firewall: Rules

Floating WAN LAN										
	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input checked="" type="checkbox"/>		*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 UDP	LAN net	*	<u>Servidores DNS</u>	53 (DNS)	*	none		Consultas DNS
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 TCP	LAN net	*	*	<u>portos web</u>	*	none		Tráfico web
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 *	*	*	*	*	*	none		CleanUp Rule IPv4
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv6 *	*	*	*	*	*	none		CleanUp Rule IPv6

Igual que no caso da regra anterior, a colocación da regra é importante e non é necesario crear unha regra para permitir o tráfico de volta pola WAN.

Control dos equipos do Dpto. Comercial

Os equipos do departamento comercial (de 192.168.56.50 a 192.168.56.90), únicamente poderán visitar as webs en horario de 8:00 am a 14:00 de luns a venres.

Floating WAN LAN										
	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input checked="" type="checkbox"/>		*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule
<input type="checkbox"/>		IPv4 UDP	LAN net	*	<u>Servidores DNS</u>	53 (DNS)	*	none		Consultas DNS
<input type="checkbox"/>		IPv4 TCP	LAN net	*	*	<u>portos web</u>	*	none		Tráfico web
<input type="checkbox"/>		IPv4 *	*	*	*	*	*	none		CleanUp Rule IPv4
<input type="checkbox"/>		IPv6 *	*	*	*	*	*	none		CleanUp Rule IPv6

Con estas regras dase saída ás páxinas web a todas a rede LAN, incluíndo o rango de IPs dos equipos do Dpto. Comercial. Haberá que crear regras para prohibir o acceso a eses equipos e que esas regras se activen no horario indicado.

Schedules: regras baseadas en tempo



Firewall: Schedules: Edit



Schedule information

Schedule Name



The name of the alias may only consist of the characters a-z, A-Z and 0-9

Description



You may enter a description here for your reference (not parsed).

Month

June 12

June 2012						
Mon	Tue	Wed	Thu	Fri	Sat	Sun
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

Click individual date to select that date only. Click the appropriate weekday Header to select all occurrences of that weekday.

Time

Start Time

Stop Time

0 | Hr 00 | Min 23 | Hr 59 | Min

Select the time ranges for the day(s) selected on the Month(s) above. A full day is 0:00-23:59


Schedule information

Schedule Name

 Comercial

The name of the alias may only consist of the characters a-z, A-Z and 0-9

Description

 Horario Dpto. Comercial

You may enter a description here for your reference (not parsed).

Month

June 12 

June 2012						
Mon	Tue	Wed	Thu	Fri	Sat	Sun
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

Click individual date to select that date only. Click the appropriate weekday Header to select all occurrences of that weekday.

Time

Start Time

8  Hr 00  Min

Stop Time

14  Hr 00  Min

Select the time range for the day(s) selected on the Month(s) above. A full day is 0:00-23:59.

Time Range Description

 mañana

You may enter a description here for your reference (not parsed).

Add Time

Clear Selection

Schedule repeat

Configured Ranges

Day(s)	Start Time	Stop Time	Description
--------	------------	-----------	-------------

Save

Cancel

Schedule information

Schedule Name



Comercial

The name of the alias may only consist of the characters a-z, A-Z and 0-9

Description



Horario Dpto. Comercial

You may enter a description here for your reference (not parsed).

Month

June 12

June 2012						
Mon	Tue	Wed	Thu	Fri	Sat	Sun
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

Click individual date to select that date only. Click the appropriate weekday.

Time

Start Time		Stop Time	
0	Hr	00	Min
23	Hr	59	Min

Select the time range for the day(s) selected on the Month(s) above. A full day is 0:00-23:59.

Time Range Description



You may enter a description here for your reference (not parsed).

Add Time

Clear Selection

É posible definir varios rangos temporais no mesmo schedule

Schedule repeat

Configured Ranges

Day(s)	Start Time	Stop Time	Description
Mon - Fri	8:00	14:00	mañana



Save

Cancel

Firewall: Schedules

Name	Time Range(s)	Description
Comercial	Mon - Fri 8:00-14:00	Horario Dpto. Comercial

Ó crear a regra pódese escoller o schedule en propiedades avanzadas

Advanced features	
Source OS	<input type="button" value="Advanced"/> - Show advanced option
Diffserv Code Point	<input type="button" value="Advanced"/> - Show advanced option
Advanced Options	<input type="button" value="Advanced"/> - Show advanced option
TCP flags	<input type="button" value="Advanced"/> - Show advanced option
State Type	<input type="button" value="Advanced"/> - Show advanced option
No XMLRPC Sync	<input type="button" value="Advanced"/> - Show advanced option
Schedule	<div><div>none</div><div>none</div><div>Comercial</div></div>
Gateway	<input type="button" value="Advanced"/>
In/Out	<input type="button" value="Advanced"/>
Ackqueue/Queue	<input type="button" value="Advanced"/>
Layer7	<input type="button" value="Advanced"/>

Esto significa que a regra únicamente será tida en conta durante o horario definido no schedule. O resto do tempo non se procesará.

OLLO: non confundir 'non procesar' (non se avalía) con que o paquete ó chegar a ela denégase.

Control dos equipos do Dpto. Comercial

Floating WAN LAN

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input checked="" type="checkbox"/>		*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 UDP	LAN net	*	<u>Servidores DNS</u>	53 (DNS)	*	none		Consultas DNS
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 TCP	<u>Equipos Dpto. Comercial</u>	*	*	<u>portos web</u>	*	none	<input checked="" type="checkbox"/> <u>Comercial</u>	Tráfico web Dpto. Comercial
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 *	<u>Equipos Dpto. Comercial</u>	*	*	*	*	none		Bloquear todo o tráfico Dpto. Comercial
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 TCP	LAN net	*	*	<u>portos web</u>	*	none		Tráfico web
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 *	*	*	*	*	*	none		CleanUp Rule IPv4
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv6 *	*	*	*	*	*	none		CleanUp Rule IPv6

En primeiro lugar e durante o horario axeitado, permítese a navegación web ós equipos do Dpto. Comercial.

A continuación, hai que poñer unha regra para bloquear o tráfico dos equipos do Dpto. Comercial; xa que de non poñela, a regra de navegación web para toda a LAN os permitiría saír.

Control dos equipos do Dpto. Comercial → Solución#2

Fóra do horario de traballo a regra de bloqueo actívase e bloquea ó dpto. Comercial e dentro do horario a regra está desactivada (non ten efecto) e unha regra posterior autoriza a saída dos equipos do dpto. comercial

<input type="checkbox"/>		UDP	LAN net	*	<u>Servidores DNS</u>	<u>Puertos DNS</u>	*	none		Consultas DNS
<input type="checkbox"/>		TCP	<u>Equipos Dpto Comercial</u>	*	*	*	*	none	<u>BloqueoComercial</u>	Bloquear Tráfico Web Dpto. Comercial
<input type="checkbox"/>		TCP	LAN net	*	*	<u>Puertos Web</u>	*	none		Tráfico Web

Firewall: Schedules

Name	Time Range(s)			Description
BloqueoComercial	Mon - Fri	0:00-7:59	madrugada	Horario bloqueo Dpto. Comercial
	Mon - Fri	14:00-23:59	tarde-noche	
	Sat - Sun	0:00-23:59	fin de semana	

Aquí vese outra posible solución igualmente válida para o problema plantexado. Esto permite ver que para cumprir cunha política de tráfico pode haber varias solucións diferentes e correctas.

Control do acceso ó pfSense

Floating WAN LAN										
	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input checked="" type="checkbox"/>		*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule
<input type="checkbox"/>		IPv4 UDP	LAN net	*	<u>Servidores DNS</u>	53 (DNS)	*	none		Consultas DNS
<input type="checkbox"/>		IPv4 TCP	<u>Equipos Dpto Comercial</u>	*	*	<u>portos web</u>	*	none	<input checked="" type="checkbox"/> <u>Comercial</u>	Tráfico web Dpto. Comercial
<input type="checkbox"/>		IPv4 *	<u>Equipos Dpto Comercial</u>	*	*	*	*	none		Bloquear todo o tráfico Dpto. Comercial
<input type="checkbox"/>		IPv4 TCP	LAN net	*	*	<u>portos web</u>	*	none		Tráfico web
<input type="checkbox"/>		IPv4 *	*	*	*	*	*	none		CleanUp Rule IPv4
<input type="checkbox"/>		IPv6 *	*	*	*	*	*	none		CleanUp Rule IPv6

Por defecto, permítese a calquera equipo acceder á pantalla de administración web vía a interface LAN do pfSense.

Boas prácticas: Lockdown Rule – Stealth Rule

Floating

WAN

LAN

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule
<input type="checkbox"/>	IPv4 TCP	<u>Equipos admin</u>	*	LAN address	<u>Portos Administracion</u>	*	none		Anti-lockdown rule
<input type="checkbox"/>	IPv4 TCP	*	*	LAN address	<u>Portos Administracion</u>	*	none		Lockdown rule
<input type="checkbox"/>	IPv4 UDP	LAN net	*	<u>Servidores DNS</u>	53 (DNS)	*	none		Consultas DNS
<input type="checkbox"/>	IPv4	<u>Equipos Dpto Comercial</u>	*	*	portos web	*	none		Tráfico web

1.Antilockdown Rule → permitir acceso para administrar pfSense a equipos autorizados.

2.Lockdown Rule – Stealth Rule → bloquear acceso para administrar pfSense ó resto.

Recomendación: seguir esta orde

1º- Crear as regras que garanten o acceso para administrar pfSense dende os equipos autorizados.

2º- Eliminar a antilockdown rule por defecto.

- Admin Access
- Firewall / NAT
- Networking
- Miscellaneous
- System Tunables
- Notifications

Note: The options on this page are intended for use by advanced users only.

webConfigurator

Protocol

☐ HTTP ☒ HTTPS

SSL Certificate

webConfigurator default

TCP port

Enter a custom port number for the webConfigurator above if you want to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.

Max Processes

2

Enter the number of webConfigurator processes you want to run. This defaults to 2. Increasing this will allow more users/browsers to access the GUI concurrently.

WebGUI redirect

☐ **Disable webConfigurator redirect rule**

When this is unchecked, access to the webConfigurator is always permitted even on port 80, regardless of the listening port configured. Check this box to disable this automatically added redirect rule.

WebGUI Login Autocomplete

☐ **Disable webConfigurator login autocomplete**

When this is unchecked, login credentials for the webConfigurator may be saved by the browser. While convenient, some security standards require this to be disabled. Check this box to disable autocomplete on the login form so that browsers will not prompt to save credentials (NOTE: Some browsers do not respect this option).

WebGUI login messages

☐ **Disable logging of webConfigurator successful logins**

When this is checked, successful logins to the webConfigurator will not be logged.

Anti-lockout

☒ **Disable webConfigurator anti-lockout rule**

When this is unchecked, access to the webConfigurator on the LAN interface is always permitted, regardless of the user-defined firewall rule set. Check this box to disable this automatically added rule, so access to the webConfigurator is controlled by the user-defined firewall rules (ensure you have a firewall rule in place that allows you in, or you will lock yourself out!) *Hint: the "Set interface(s) IP address" option in the console menu resets this setting as well.*

Boas prácticas: Lockdown Rule – Stealth Rule

Floating WAN LAN										
	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>		IPv4 TCP	<u>Equipos admin</u>	*	LAN address	<u>Portos Administracion</u>	*	none		Anti-lockdown rule
<input type="checkbox"/>		IPv4 TCP	*	*	LAN address	<u>Portos Administracion</u>	*	none		Lockdown rule
<input type="checkbox"/>		IPv4 UDP	LAN net	*	<u>Servidores DNS</u>	53 (DNS)	*	none		Consultas DNS
<input type="checkbox"/>		IPv4 TCP	<u>Equipos Dpto Comercial</u>	*	*	<u>portos web</u>	*	none	<u>Comercial</u>	Tráfico web Dpto. Comercial
<input type="checkbox"/>		IPv4 *	<u>Equipos Dpto Comercial</u>	*	*	*	*	none		Bloquear todo o tráfico Dpto. Comercial
<input type="checkbox"/>		IPv4 TCP	LAN net	*	*	<u>portos web</u>	*	none		Tráfico web
<input type="checkbox"/>		IPv4 *	*	*	*	*	*	none		CleanUp Rule IPv4
<input type="checkbox"/>		IPv6 *	*	*	*	*	*	none		CleanUp Rule IPv6

Aínda que por cuestións formativas as regras de control de acceso foron creadas despois doutras, é recomendable que sexan as primeiras en facerse. É moi importante non equivocarse e bloquear o acceso a nos mesmos, xa que pode non ser sinxelo recuperalo.

E se estou bloqueado?

```
WAN (wan)      -> em0      -> v4: 192.168.1.253/24
LAN (lan)      -> em1      -> v4: 192.168.56.253/24

0) Logout (SSH only)          8) Shell
1) Assign Interfaces          9) pfTop
2) Set interface(s) IP address 10) Filter Logs
3) Reset webConfigurator password 11) Restart webConfigurator
4) Reset to factory defaults    12) pfSense Developer Shell
5) Reboot system               13) Upgrade from console
6) Halt system                 14) Enable Secure Shell (sshd)
7) Ping host                   15) Restore recent configuration

Enter an option: 2

Available interfaces:

1 - WAN (em0 - static, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.56.253
```

En pfSense é moi sinxelo, sempre e cando se teña acceso físico á máquina: asígnase unha IP á interface dende a consola e automaticamente créase a regra antibloqueo.

Cómo accedo por ssh? Cómo bloqueo a consola?

No sitio web de <https://doc.pfsense.org> recóllese a documentación do firewall pfSense. Na sección How-to pódese atopar información sobre a activación do acceso por ssh: System → Advanced → Admin Access

Secure Shell	
Secure Shell Server	<input checked="" type="checkbox"/> Enable Secure Shell
Authentication Method	<input type="checkbox"/> Disable password login for Secure Shell (RSA key only) When enabled, authorized keys need to be configured for each user that has been granted secure shell access.
SSH port	<input type="text"/> Note: Leave this blank for the default of 22.
Serial Communications	
Serial Terminal	<input type="checkbox"/> This will enable the first serial port with 9600/8/N/1 Note: This will redirect the console output and messages to the serial port. You can still access the console menu from the internal video card/keyboard. A null modem serial cable or adapter is required to use the serial console.
Console Options	
Console menu	<input checked="" type="checkbox"/> Password protect the console menu Changes to this option will take effect after a reboot.

Tamén é posible protexer con contrasinal o acceso ás opcións da Consola

Cómo accedo por ssh? Cómo bloqueo a consola?

```
Setting up polling defaults...done.
Setting up interfaces microcode...done.
Configuring LAGG interfaces...done.
Configuring VLAN interfaces...done.
Configuring QinQ interfaces...done.
Configuring WAN interface...done.
Configuring LAN interface...done.
Syncing OpenVPN settings...done.
Starting syslog...done.
Configuring firewall.....done.
Starting PFLOG...done.
Setting up gateway monitors...done.
Synchronizing user settings...done.
Starting webConfigurator...done.
Configuring CRON...done.
Starting DNS forwarder...done.
Configuring firewall...done.
Starting OpenNTP time client...done.
Generating RRD graphs...done.
Starting CRON... done.
Bootup complete

FreeBSD/i386 (pfSense.lc
login: 
```

```
manuel@ubuntu:~$ ssh admin@192.168.56.253
The authenticity of host '192.168.56.253 (192.168.56.253)' can't be established.
RSA key fingerprint is a5:d0:79:06:dc:25:88:c6:3b:f8:9d:ca:d5:ca:eb:62.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.56.253' (RSA) to the list of known hosts.
Password:
*** Welcome to pfSense 2.1.5-RELEASE-pfSense (i386) on pfSense ***

WAN (wan)          -> em0          -> v4: 192.168.1.253/24
LAN (lan)          -> em1          -> v4: 192.168.56.253/24
```

- | | |
|-----------------------------------|----------------------------------|
| 0) Logout (SSH only) | 8) Shell |
| 1) Assign Interfaces | 9) pfTop |
| 2) Set interface(s) IP address | 10) Filter Logs |
| 3) Reset webConfigurator password | 11) Restart webConfigurator |
| 4) Reset to factory defaults | 12) pfSense Developer Shell |
| 5) Reboot system | 13) Upgrade from console |
| 6) Halt system | 14) Disable Secure Shell (sshd) |
| 7) Ping host | 15) Restore recent configuration |

Enter an option: █