

# REGRAS DE FIREWALL – pfSENSE

## 1-Regras e Conjuntos de Regras de Firewall (**Rules, Ruleset**).

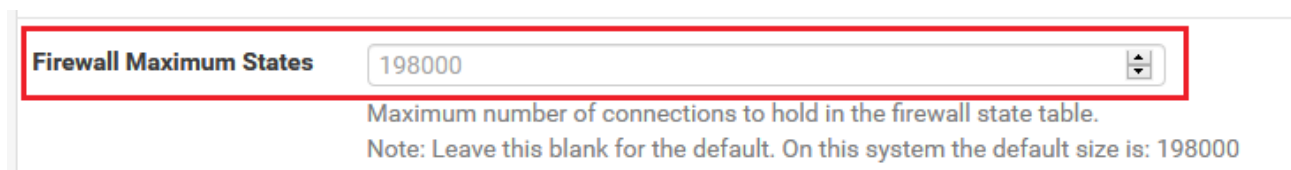
- **Rules:** regra é uma instrução para o Firewall através de uma simples entrada que define como deve se tratar determinada correspondência de tráfego de rede.
- **Ruleset:** é um conjunto de regras que compõem toda a configuração de Firewall adicionada em uma determinada interface de rede.

## 2-Firewall de Inspeção de Estados de Conexão (**Stateful Firewall**).

O pfSense é um Firewall de inspeção de estados de conexões, que mantém uma tabela com informações sobre as conexões que passam através do Firewall contendo interface, protocolos, endereço e porta de origem, endereço e porta de destino, estados e pacotes. Deste modo o tráfego que é iniciado por um host interno que corresponde com uma regra de permissão, o Firewall cria uma entrada na tabela de estados e libera automaticamente o tráfego externo de resposta para o host.

A tabela de estados do Firewall pfSense possui um tamanho máximo para evitar o consumo excessivo de memória RAM que é calculado usando 10% da memória instalada no sistema, cada estado mantém aproximadamente 1 KB de memória RAM. Por exemplo em 1 GB de RAM podem ser armazenados aproximadamente 100,000 entradas.

- Para aumentar o tamanho da tabela de estados do Firewall pfSense, se houver necessidade acesse “**System/Advanced/Firewall & NAT**”.



**Firewall Maximum States** 198000

Maximum number of connections to hold in the firewall state table.  
Note: Leave this blank for the default. On this system the default size is: 198000

- Para visualizar em tempo real as informações armazenadas na tabela de estados do Firewall pfSense, acesse “**Status/Dashboard/System Information/Show states**”.

States					
Interface	Protocol	Source (Original Source) -> Destination (Original Destination)	State	Packets	Bytes
LAN	tcp	192.168.30.10:17966 -> 157.240.12.38:443	TIME_WAIT:TIME_WAIT	10 / 12	1 KiB / 4 KiB
LAN	tcp	192.168.30.10:17967 -> 157.240.12.38:443	ESTABLISHED:ESTABLISHED	351 / 449	134 KiB / 389 KiB

### 3-Ações Aplicadas no Tráfego de Rede no Firewall pfSense (**Pass, Block, Reject**).

O firewall pfSense executa a filtragem de pacotes de rede inspecionando as regras que são preestabelecidas pelo administrador de rede, se algum pacote não corresponder as regras configuradas no Firewall o pacote será bloqueado.

O tráfego que passa através do Firewall pfSense podem ser tratado de três maneiras possíveis:

- **PASS:** permite que os pacotes passem através do Firewall pfSense normalmente.
- **BLOCK:** bloqueia os pacotes sem avisos, o cliente não recebe nem um tipo de resposta até receber uma mensagem **“time out”** da aplicação utilizada na conexão, este é o comportamento padrão do Firewall pfSense.
- **REJECT:** descarta os pacotes e envia uma mensagem de resposta **“TCP RST”** para conexões rejeitadas **“TCP”** e uma mensagem **“ICMP”** de destino inalcançável para conexões **“UDP”**. Na maioria das situações em uma rede **“LAN”** é recomendado rejeitar as conexões não permitidas.

### 4-Filtrando Entrada e Saída de Tráfego de Rede (**Ingress/Egress**).

Em sua instalação padrão o Firewall pfSense filtra o tráfego de entrada bloqueando todas as conexões externas originadas da Internet recebidas na interface **“WAN” (Ingress)** e filtra o tráfego de saída permitindo todas as conexões internas originadas da rede local na interface **“LAN” (Egress)**, deste modo o Firewall pfSense protege a rede interna contra possíveis tentativas de invasão originadas da rede externa e libera todo o trafego originado dentro da rede interna. Respostas para o tráfego iniciado na rede local que correspondem a uma entrada legítima na tabela de estados são automaticamente permitidos para retornar através do Firewall pfSense.

As melhores praticas para configurar o filtro de saída de um Firewall é permitir somente o mínimo necessário para o funcionamento de uma rede local controlando todo o tráfego originado nas estações de trabalho. Para aplicar regras de saída personalizadas desative as regras padrão na interface **“LAN”** do pfSense. Algumas razões importantes para filtragem do tráfego de saída são:

- Limitar o impacto de estações de trabalho com sistemas comprometidos por “malwares”, por exemplo alguns **“bots”** utilizam a porta **“TCP-6667 IRC”**, alguns ataques de **“DDoS”** utilizam a porta **“UDP-80”** para realizar negação de serviço distribuída, “spam zombies” **“TCP-25 SMTP”** transformam estações de trabalho em servidores de envio de spam.
- Prevenir exploração de falhas **“Exploits”** que necessitam de acesso em algumas portas externas localizadas remotamente para comprometer um sistema.

- Limitar o uso de aplicações não permitidas como **“Torrent”** e certos tipos de **“VPNs”** que são utilizadas por usuários para burlar políticas de restrição de acesso.
- Prevenir falsificação de endereço IP **“IP Spoofing”**.
- Prevenir vazamento de informações internas sobre a rede local **“Microsoft RPC TCP 135”**, **“NetBIOS TCP/UDP 137-139”**, **“SMB/CIFS TCP/UDP 445”**.

## 5-Abordagem básica para implementar regras de filtragem de saída do Firewall pfSense.

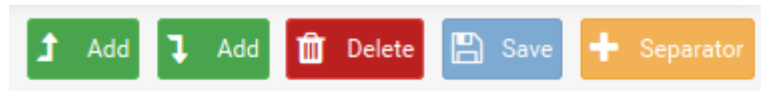
Um modo de implementar regras de filtragem de saída do Firewall é identificar o tráfego de rede através de monitoramento dos **“logs”** para definir uma tabela com os protocolos, endereços IP e portas **“TCP/UDP”** que são necessários para o funcionamento correto de um determinado ambiente de produção em uma rede de computadores.

Em alguns casos será necessário criar regras específicas para liberar um serviço de rede que se encontra localizado na rede interna para acesso através da **“Internet”** ou bloquear algum tipo de serviço na **“Internet”** para evitar acessos indevidos por usuários da rede interna. As regras do pfSense são aplicadas na ordem de cima para baixo, ou seja, as regras que estão na parte superior serão aplicadas primeiro, se uma determinada regra de permissão a um serviço for antecedida por uma regra de negação o serviço será bloqueado e a regra de permissão não terá efeito.

- Tabela básica de implementação de regras para filtragem de saída do Firewall pfSense.

Ação	Interface	Proto_IP	Protocolo	Origem	Destino	Porta	Descrição
Pass	LAN	IPv4	ICMP	LAN	ANY	*	PING
Pass	LAN	IPv4	TCP	LAN	ANY	21	FTP
Pass	LAN	IPv4/6	UDP	LAN	ANY	53	DNS
Pass	LAN	IPv4/6	TCP	LAN	ANY	80	HTTP
Pass	LAN	IPv4/6	UDP	LAN	ANY	123	NTP
Pass	LAN	IPv4/6	TCP	LAN	ANY	443	HTTPS
Pass	LAN	IPv4	TCP	LAN	ANY	110	POP3
Pass	LAN	IPv4	TCP	LAN	ANY	143	IMAP4
Pass	LAN	IPv4	TCP	LAN	ANY	465	SMTP/SSL
Pass	LAN	IPv4	TCP	LAN	ANY	587	SMTP/TLS
Pass	LAN	IPv4	TCP	LAN	ANY	993	IMAP4/SSL
Pass	LAN	IPv4	TCP	LAN	ANY	995	POP3/SSL
Pass	LAN	IPv4	UDP	LAN	ANY	1194	OPEN VPN
Pass	LAN	IPv4	TCP	LAN	ANY	3306	MySQL
Pass	LAN	IPv4	UDP	LAN	ANY	3478-3481	SKYPE
Pass	LAN	IPv4	TCP/UDP	LAN	ANY	5938	TEAMVIEWER

6-Para criar regras de saída “Egress” no Firewall para rede local acesse “Firewall/Rules/LAN”, para adicionar uma regra no topo da lista utilize o botão “Add” de seta para cima ou “Add” de seta para baixo para o fim da lista, utilize o botão “Delete” para remover uma regra da lista, o botão “Save” para salvar alterações e “Separator” para organizar opcionalmente.



- Defina o tipo de ação, família de endereços IP e o protocolo a serem aplicados na regra.

Firewall / Rules / Edit

### Edit Firewall Rule

**Action** Pass  
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.

**Disabled** ☐ Disable this rule  
Set this option to disable this rule without removing it from the list.

**Interface** LAN  
Choose the interface from which packets must come to match this rule.

**Address Family** IPv4+IPv6  
Select the Internet Protocol version this rule applies to.

**Protocol** TCP  
Choose which IP protocol this rule should match.

- Defina a origem para rede local “LAN net”, destino para qualquer “any” endereço na “Internet” e a porta de destino do serviço a ser liberado, neste exemplo porta “HTTPS 443”.

**Source**

**Source** ☐ Invert match. LAN net Source Address /

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

**Destination**

**Destination** ☐ Invert match. any Destination Address /

**Destination Port Range** HTTPS (443) Custom To HTTPS (443) Custom  
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

- Defina se quer gerar “logs” da regra e uma descrição para referência administrativa.

**Extra Options**

**Log** ☐ Log packets that are handled by this rule  
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

**Description** HTTPS Websites  
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

**Advanced Options** [Display Advanced](#)

7-Para criar regras de entrada **“Ingress”** no Firewall para rede externa **“Internet”** acesse **“Firewall/Rules/WAN”**, para adicionar uma regra no topo da lista utilize o botão **“Add”** de seta para cima ou **“Add”** de seta para baixo para o fim da lista, utilize o botão **“Delete”** para remover uma regra da lista, o botão **“Save”** para salvar alterações e **“Separator”** para organizar opcionalmente.

- Defina o tipo de ação, família de endereços IP e o protocolo a serem aplicados na regra.

**Edit Firewall Rule**

**Action** Pass  
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.

**Disabled** ☐ Disable this rule  
Set this option to disable this rule without removing it from the list.

**Associated filter rule** This is associated with a NAT rule.  
Editing the interface, protocol, source, or destination of associated filter rules is not permitted.  
[View the NAT rule](#)

**Interface** WAN  
Choose the interface from which packets must come to match this rule.

**Address Family** IPv4  
Select the Internet Protocol version this rule applies to.

**Protocol** TCP  
Choose which IP protocol this rule should match.

- Defina a origem para qualquer **“any”** endereço na **“Internet”**, destino para **“Single host or alias”** e digite o IP e a porta de destino do serviço localizado na rede local a ser liberado, neste exemplo **“IPv4 192.168.1.10”** e uma faixa de portas **“9101-9103”**.

**Source**

**Source** ☐ Invert match. any Source Address /

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

**Destination**

**Destination** ☐ Invert match. Single host or alias 192.168.1.10 /

**Destination Port Range** (other) 9101 (other) 9103  
From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

- Defina se quer gerar **“logs”** da regra e uma descrição para referência administrativa.

**Extra Options**

**Log** ☒ Log packets that are handled by this rule  
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

**Description** NAT Bareos Client  
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

**Advanced Options** [Display Advanced](#)

8-Encaminhamento de portas **“Inbound NAT”** permite redirecionar o tráfego originado da rede externa **“Internet”** via um endereço IP público para uma porta específica localizada em algum host interno da rede local **“LAN”** através de um endereço IP privado.

- Após criar uma regra para acesso externo na interface **“WAN”** é necessário configurar o encaminhamento de portas através do **“Firewall/NAT/Port Forward” Add**.

**Interface** WAN Choose which interface this rule applies to. In most cases "WAN" is specified.

**Protocol** TCP Choose which protocol this rule should match. In most cases "TCP" is specified.

- Defina o destino para **“WAN Address”**, uma faixa de portas de destino **“Custom” (9101-9103)**, o IP e a porta do host localizado na rede local para receber o redirecionamento e uma descrição para referência administrativa.

**Destination** ☐ Invert match. WAN address Type Address/mask

**Destination port range** Other 9101 Other 9103 From port Custom To port Custom

Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

**Redirect target IP** 192.168.1.10 Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12

**Redirect target port** Other 9101 Port Custom

Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). This is usually identical to the "From port" above.

**Description** Bareos Client A description may be entered here for administrative reference (not parsed).

- Defina a regra de filtragem para associação com a regra **“NAT”**.

**NAT reflection** Use system default

**Filter rule association** Rule NAT Bareos Client [View the filter rule](#)

- Detalhes da regra de **“NAT”** de encaminhamento de portas para o IP na rede local.

Rules												
			Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/>		WAN	TCP	*	*	WAN address	9101 - 9103	192.168.1.10	9101 - 9103	Bareos Client	

## 9-Criar “Aliases” com endereços de redes IP “Firewall/Aliases/IP Import”.

Aliases de redes contém grupos de endereços de redes IP que podem ser importados de um arquivo de texto utilizando notação “CIDR”, podem serem utilizados em diversas configurações do Firewall como regras de entrada e saída, encaminhamento de portas, bypass do Proxy Squid etc.

- **Alias Name:** Serpro
- **Description:** Serpro\_NET
- **Aliases to Import:** 161.148.0.0/16  
189.9.0.0/16  
200.198.192.0/18

Firewall / Aliases / Bulk import

### IP Alias Details



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

**Description**   
A description may be entered here for administrative reference (not parsed).

**Aliases to import**

Paste in the aliases to import separated by a carriage return. Common examples are lists of IPs, networks, blacklists, etc. The list may contain IP addresses, with or without CIDR prefix, IP ranges, blank lines (ignored) and an optional description after each IP. e.g.:

- 172.16.1.2
- 172.16.0.0/24
- 10.11.12.100-10.11.12.200
- 192.168.1.254 Home router
- 10.20.0.0/16 Office network
- 10.40.1.10-10.40.1.19 Managed switches

IP Ports URLs All			
Firewall Aliases IP			
Name	Values	Description	Actions
SERPRO	161.148.0.0/16, 189.9.0.0/16, 200.198.192.0/18	Serpro_NET	 

- Aliases podem ser criados utilizando “FQDN”, neste modo os endereços IP são resolvidos e atualizados via DNS a cada 5 minutos.

### Host(s)

**Hint** Enter as many hosts as desired. 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. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

**IP or FQDN**  Entry added Wed, 28 Mar 2018 09:56:46 -0300

## 10-Criar “Aliases” com portas “Firewall/Aliases/Ports Add”.

Aliases de portas contém grupos de portas “TCP/UDP”, logo abaixo temos um exemplo de um aliases de portas que tem a finalidade de simplificar uma regra para serviços de correio eletrônico que necessitam de acesso a várias portas para enviar e receber e-mails.

- **Name:** EMAIL
- **Description:** Email\_Ports
- **Type:** Port(s)
- **Port:** 110, 143, 465, 587, 993, 995

**Properties**

**Name** EMAIL

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

**Description** E-mail Clients


A description may be entered here for administrative reference (not parsed).

**Type** Port(s)













**Port(s)**

**Hint** Enter ports as desired, with a single port or port range per entry. Port ranges can be expressed by separating with a colon.

Port			
110	POP3		Delete
143	IMAP4		Delete
465	SMTP/SSL		Delete
587	SMTP/TLS		Delete
993	IMAP4/SSL		Delete
995	POP3/SSL		Delete

IP	Ports	URLs	All
Firewall Aliases Ports			
Name	Values	Description	Actions
EMAIL	110, 143, 465, 587, 993, 995	E-mail Clients	 

- Detalhes da regra utilizando o aliases criado para agrupar portas de serviços de E-mail.

<input type="checkbox"/>	✓	0 / 0 B	IPv4+6 TCP	LAN net	*	*	80 (HTTP)	*	none	HTTP Websites	  
<input type="checkbox"/>	✓	0 / 8.07 MiB	IPv4+6 TCP	LAN net	*	*	443 (H			HTTPS Websites	  
<input type="checkbox"/>	✓	0 / 0 B	IPv4 TCP	LAN net	*	*	EMAIL			E-mail Clients	  
Acesso Remoto VPN											
<input type="checkbox"/>	✓	0 / 1.35 MiB	IPv4 UDP	LAN net	*	*	1194 (OpenVPN)			VPN	  

Alias details

Value	Description
110	POP3
143	IMAP4
465	SMTP/SSL
587	SMTP/TLS
993	IMAP4/SSL
995	POP3/SSL



## 11-Criar “Aliases” com “URLs” “Firewall/Alises/URLs Add”.

Aliases de URL (IPs) podem ser criadas digitando quantas URLs desejar. Depois de salva, as URLs serão baixados e os itens importados para o alias. Use apenas com pequenos conjuntos de endereços IP (menos de 3000). Proteja a infraestrutura de rede com as informações coletadas sobre ameaças existentes através de uma lista negra de endereços IP disponibilizada pela Cisco Talos que pode ser configurada em um alias utilizando a URL: <https://www.talosintelligence.com/documents/ip-blacklist>.

Firewall / Aliases / Edit

**Properties**

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

**Description** Blacklist IPs Cisco Talos  
A description may be entered here for administrative reference (not parsed).

**Type** URL (IPs)



**URL (IPs)**

**Hint** Enter as many URLs as desired. After saving, the URLs will be downloaded and the items imported into the alias. Use only with small sets of IP addresses (less than 3000).








**URL (IPs)** <https://www.talosintelligence.com/documents/ip-blacklist> Blacklist Cisco Talos

IP Ports URLs All

**Firewall Aliases URLs**

Name	Values	Description	Actions
BLACKLISTS	<a href="https://www.talosintelligence.com/documents/ip-blacklist">https://www.talosintelligence.com/documents/ip-blacklist</a> 149.202.170.60, 46.98.196.45, 37.187.129.166, 91.146.121.3, 217.115.10.131, 64.113.32.29, 46.233.0.70, 204.17.56.42, 89.31.57.5, 46.235.227.70...	Blacklist IPs Cisco Talos	 

- Detalhes da regra de rejeição utilizando alias de URLs com lista negra da Cisco Talos.

Rules (Drag to Change Order)						Alias details			
States	Protocol	Source	Port	Destination		Value	Description	Description	Actions
✓ 1 / 287 KiB	*	*	*	LAN Address		149.202.170.60 46.98.196.45 37.187.129.166 91.146.121.3 217.115.10.131 64.113.32.29 46.233.0.70 204.17.56.42 89.31.57.5	Blacklist Cisco Talos	Anti-Lockout Rule	
Lista Negra de IPs Cisco Talos									
<input type="checkbox"/> 	0 / 0 B	IPv4 TCP	LAN net	* BLACKLISTS				Blacklist IPs Cisco Talos	   

**Obs:** Aliases é um recurso útil para simplificar a criação de regras de Firewall, facilitar o gerenciamento dos conjuntos de regras e também uma boa forma de documentação.

## 12-Melhores Práticas para Gerenciamento de Firewall e suas Regras.

- **Negar todo o tráfego por padrão:** o administrador do Firewall pode ter um controle maior do tráfego de rede de um determinado ambiente de produção permitindo somente os acessos necessários para o funcionamento de serviços legítimos.
- **Regras de Firewall simplificadas:** manter um conjunto de regras simples e funcionais que permitam gerenciamento facilitado utilizando “**Aliases**” o quanto for possível, eliminar regras redundantes ou conflitantes para otimizar sua performance.
- **Sempre revisar as regras de Firewall:** verificar periodicamente as configurações de regras de Firewall para reforçar a segurança e manter o ambiente de rede em pleno funcionamento em caso de necessidade de novas permissões ou remoção de regras obsoletas.
- **Documentação:** todas as configurações pertinentes ao Firewall devem ser bem documentadas para casos de substituição ou reconfiguração do hardware por motivos diversos, as informações desde os endereços IP de suas interfaces, as regras de filtragem de entrada e saída, regras de “**NAT**” e “**Aliases**” utilizados devem ser atualizadas sempre que necessário e salvas em lugar seguro.
- **Monitorar Logs:** verificar os “logs” do Firewall regularmente para garantir que as regras de filtragem que foram aplicadas em determinado ambiente de rede estão funcionando corretamente.
- **Atualizar o Firmware do Firewall:** aplicar atualizações recomendadas pelo fabricante do Firewall assim que estiverem liberadas para download.

**Obs:** Os “logs” de Firewall do pfSense podem ser visualizados acessando “**Status/System Logs/Firewall/**” e possuem três formas de visualização de relatórios: “**Normal View, Dynamic View e Summary View**”.

## 14-Reduzindo o “Log Noise”.

- Entradas de “log” do Firewall pfSense produzindo muito “**Log Noise**”.

Last 50 Firewall Log Entries. (Maximum 50) Pause ▢					
Action	Time	Interface	Source	Destination	Protocol
✗	Sep 21 07:31:00	LAN	[fe80::a9f1:69c:f708:db46]:51419	[[ff02::c]:1900	UDP
✗	Sep 21 07:31:03	LAN	[fe80::a9f1:69c:f708:db46]:51419	[[ff02::c]:1900	UDP
✗	Sep 21 07:31:03	LAN	10.0.0.247:5353	224.0.0.251:5353	UDP
✗	Sep 21 07:31:03	LAN	[fe80::1c1e:95d0:8820:60b2]:5353	[[ff02::fb]:5353	UDP
✗	Sep 21 07:31:04	LAN	10.0.0.247	224.0.0.2	IGMP
✗	Sep 21 07:31:04	LAN	10.0.0.247	224.0.0.251	IGMP

Por padrão o Firewall pfSense gera **“logs”** de todos os pacotes bloqueados, este comportamento cria um efeito que pode atrapalhar muito no momento de analisar os **“logs”** do Firewall para observar o que está sendo realmente bloqueado ou até mesmo verificar algum bloqueio não desejado no caso de instalação de um recurso novo no ambiente de rede. Para evitar este tipo de problema em redes locais utilizando diversos protocolos que geram um tráfego intenso de pacotes como por exemplo **“IGMP, NetBIOS, SSDP, mDNS etc”**, podemos criar no topo do conjunto de regras de uma determinada interface de rede **“LAN”** ou **“WAN”** uma regra de bloqueio que não registre os **“logs”** sobre o tráfego destes mesmos protocolos, esta nova regra terá preferência sobre a regra padrão e estes protocolos não mais irão ser registrados nas entradas de **“logs”** de Firewall do pfSense.

Tabela de protocolos que podem ser bloqueados na interface de rede local **“LAN”** com destino a rede externa **“WAN-Internet”**:

Ação	Interface	Proto_IP	Protocolo	Origem	Destino	Porta	Descrição	Log
Block	LAN	IPv4+6	IGMP	ANY	ANY	*	IGMP	Não
Block	LAN	IPv4+6	UDP	ANY	ANY	135	RPC	Não
Block	LAN	IPv4+6	UDP	ANY	ANY	137	NetBIOS-NS	Não
Block	LAN	IPv4+6	UDP	ANY	ANY	138	NetBIOS-Data	Não
Block	LAN	IPv4+6	UDP	ANY	ANY	139	NetBIOS-Session	Não
Block	LAN	IPv4+6	UDP	ANY	ANY	445	SMB	Não
Block	LAN	IPv4+6	UDP	ANY	ANY	1900	SSDP-UPnP	Não
Block	LAN	IPv4+6	UDP	ANY	ANY	3702	WDS	Não
Block	LAN	IPv4+6	UDP	ANY	ANY	5353	mDNS	Não
Block	LAN	IPv4+6	UDP	ANY	ANY	5355	LLMNR	Não

- Exemplo de regras com **“Aliases”** de portas para suprimir o **“Log Noise”**.

Floating
WAN
LAN
OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description																				
✓ 0 / 0 B	*	*	*	LAN Address	443 80 22																								
<div> Alias details </div> <div> <table> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>135</td> <td>RPC-Remote Procedure Call</td> </tr> <tr> <td>137</td> <td>NetBIOS-Name Service</td> </tr> <tr> <td>138</td> <td>NetBIOS-Datagram Service</td> </tr> <tr> <td>139</td> <td>NetBIOS-Session Service</td> </tr> <tr> <td>445</td> <td>SMB-Server Message Block</td> </tr> <tr> <td>1900</td> <td>SSDP/UPnP</td> </tr> <tr> <td>3702</td> <td>WSD-Web Services Discovery</td> </tr> <tr> <td>5353</td> <td>mDNS-Multicast DNS</td> </tr> <tr> <td>5355</td> <td>LLMNR-Link Local Multicast Name Resolution</td> </tr> </tbody> </table> </div>										Value	Description	135	RPC-Remote Procedure Call	137	NetBIOS-Name Service	138	NetBIOS-Datagram Service	139	NetBIOS-Session Service	445	SMB-Server Message Block	1900	SSDP/UPnP	3702	WSD-Web Services Discovery	5353	mDNS-Multicast DNS	5355	LLMNR-Link Local Multicast Name Resolution
Value	Description																												
135	RPC-Remote Procedure Call																												
137	NetBIOS-Name Service																												
138	NetBIOS-Datagram Service																												
139	NetBIOS-Session Service																												
445	SMB-Server Message Block																												
1900	SSDP/UPnP																												
3702	WSD-Web Services Discovery																												
5353	mDNS-Multicast DNS																												
5355	LLMNR-Link Local Multicast Name Resolution																												

## 15-Interpretando estados da tabela de conexão “TCP/UDP” no Firewall pfSense.

Tabela de estados de conexões TCP/UDP e descrições de suas operações:

Estados	Descrição
SYN_SENT	Indica o envio de um <b>TCP_SYN</b> tentando iniciar uma conexão <b>TCP</b> via handshake.
CLOSED	Indica conexão <b>TCP</b> foi fechada ou nenhum tráfego foi recebido.
ESTABLISHED	Indica que uma conexão <b>TCP</b> esta estabelecida.
TIME_WAIT/FIN_WAIT	Indica que uma conexão <b>TCP</b> está em processo de fechamento ou finalizando.
NO_TRAFFIC	Nenhum pacote foi recebido correspondente a este tráfego.
SINGLE	Um único pacote é observado neste estado.
MULTIPLE	Múltiplos pacotes são observados neste estado
ESTABLISHED:ESTABLISHED	Indica que a conexão <b>TCP</b> esta estabelecida no dois lados.
SYN_SENT:CLOSED	Indica que foi enviado um <b>TCP_SYN</b> mas não obteve resposta do outro lado, pode não ter alcançado o destino ou foi bloqueado no caminho.
SINGLE:NO_TRAFFIC	Nenhuma resposta <b>UDP</b> foi recebida vinda do outro lado, pode não ter alcançado o destino ou foi bloqueada no caminho.
SINGLE:MULTIPLE	Normalmente ocorre quando um cliente faz uma consulta via <b>DNS</b> enviando um pacote <b>UDP</b> e recebendo múltiplos pacotes em resposta.
MULTIPLE:MULTIPLE	Normalmente quando uma conexão <b>UDP</b> esta transmitindo múltiplos pacotes em ambas as direções.

**Obs:** A tabela de estados do Firewall pfSense pode se visualizada acessando dois caminhos na interface web:

- “Diagnostics/States”.

States					
Interface	Protocol	Source (Original Source) -> Destination (Original Destination)	State	Packets	Bytes
WAN	icmp	192.168.10.254:20464 -> 192.168.10.1:20464	0:0	36.506 K / 36.506 K	998 KiB / 998 KiB
LAN	tcp	192.168.30.10:13133 -> 52.173.26.181:443	ESTABLISHED:ESTABLISHED	287 / 162	24 KiB / 30 KiB

- “Diagnostics/pfTop”.

Output							
pfTop: Up State 1-100/102, View: default, Order: none							
PR	DIR	SRC	DEST	STATE	AGE	EXP	PKTS
icmp	Out	192.168.10.254:20464	192.168.10.1:20464	0:0	05:07:53	00:00:09	73480
tcp	In	192.168.30.10:13133	52.173.26.181:443	ESTABLISHED:ESTABLISHED	05:07:34	23:58:26	452
tcp	Out	192.168.10.254:53393	52.173.26.181:443	ESTABLISHED:ESTABLISHED	05:07:34	23:58:26	452

**16-**Comandos básicos para operar o Firewall pfSense em modo texto via acesso no terminal “SSH” ou via interface web na opção “**Diagnostics/Command Prompt/Execute Shell Command**”.

**#pfctl -sr** = visualizar regras de Firewall.

**#pfctl -sn** = visualizar regras de NAT.

**#pfctl -sa** = visualizar todas as regras.

**#pfctl -vvsr** = modo verbose.

**#pfctl -d** = desativa as regras de Firewall.

**#pfctl -e** = ativa as regras de Firewall.