

TREINAMENTO PFSense

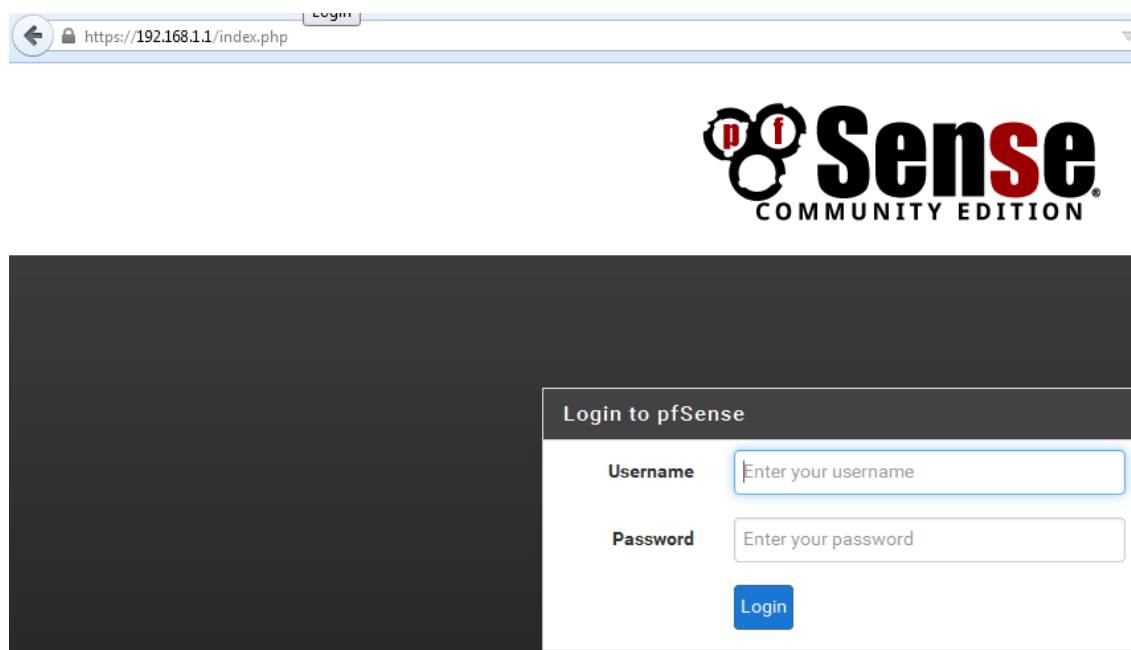
Aula 1 – Preparação do ambiente

Foram inseridas 2 máquinas virtuais, uma com Windows e outra com o PFSense. A máquina PF recebeu 2 interfaces, um em modo bridge e outra como rede interna. A Windows apenas como rede interna.

Em um momento inicial a rede interna não acessou a internet e qdo se verificou o PFSense não havia recebido IP. Utilizou-se a instrução `kill all dhclient` e depois a instrução `dhclient em0` – em0 é a interface wan neste caso. Para renovar um ip no Linux, `dhclient eth0 -v`

Para acessar utilizamos o ip 192.168.1.1, com o login admin e senha pfsense. O PFSense já habilita por padrão na interface lan, um servidor DHCP.

Aula 2 – Configurações Iniciais



The screenshot shows a web browser window with the address bar displaying 'https://192.168.1.1/index.php'. The page content includes the pfSense logo, which reads 'Sense COMMUNITY EDITION'. Below the logo is a dark grey rectangular area. On the right side of this area is a white box titled 'Login to pfSense'. Inside this box, there are two input fields: 'Username' with the placeholder text 'Enter your username' and 'Password' with the placeholder text 'Enter your password'. Below these fields is a blue 'Login' button.

System → General Setup – Onde informamos o hostname, o domínio e os servidores DNS, o time zone, o theme do PFSense. Se marcar Allow DNS Server list to be overriddden by DHCP/PPP on Wan, utilizará o DNS do provedor, mas não propagará para os clients VPN e DHCP.

No menu Interfaces podemos fazer a configuração das interfaces, inserindo IP, máscara, habilitando ou desabilitando IPV6. Para desabilitar o IPV6, antes vá no menu Services → DHCP v6 Server & RA e desabilite o servidor senão o DHCP irá fornecer um endereço IPv6 para os clientes.

O pfSense na versão mais recente possui um Wizard que inicia as configurações passo a passo para Timezone, interface Wan, NTP Client, interface Wan, senha do administrador.

Menu Status → Interfaces mostra como estão as interfaces. Isto tb é mostrado no dashboard. Tome cuidado com a interface WAN que, por padrão vem marcado Block private networks and loopback addresses e block bogon networks. Desmarque-as se for utilizar como servidor de VPN.

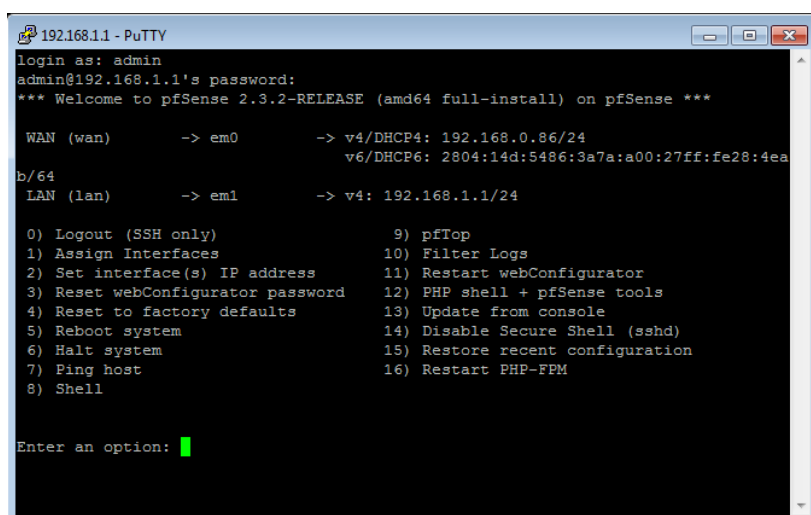
Reserved Networks

Block private networks and loopback addresses ☒ Blocks traffic from IP addresses that are reserved for unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses. This option is only turned on, unless this network interface resides in a virtual machine.

Block bogon networks ☒ Blocks traffic from reserved IP addresses (but not from private addresses). Bogon addresses never appear in the Internet routing table, and so should not be routed to the Internet. Note: The update frequency can be changed under System > Advanced > Bogon Update Frequency.

Habilitou o SSH em System → Advanced, desce até o item Secure Shell e marca a opção Secure Shell Server. Para entrar apenas com uma chave RSA/DAS, marque a opção Disable password login for Secure Shell (RSA/DAS key only).

Para autorizar uma chave, acesse System → User Manager, edite o usuário e lá embaixo no Grupo Keys, insira a chave que foi criada pelo software Putty Gen. Depois utiliza o Putty com a chave.



```
192.168.1.1 - PuTTY
login as: admin
admin@192.168.1.1's password:
*** Welcome to pfSense 2.3.2-RELEASE (amd64 full-install) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.0.86/24
                                     v6/DHCP6: 2804:14d:5486:3a7a:a00:27ff:fe28:4ea
b/64
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Disable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM

Enter an option: █
```

Aula 3 – Serviços Essenciais

Services → DHCP Server – habilitado apenas nas interfaces com ip estático.

Enable	<input checked="" type="checkbox"/> Enable DHCP server on LAN interface
Deny unknown clients	<input type="checkbox"/> Only the clients defined below will get DHCP leases from this server.
Ignore denied clients	<input type="checkbox"/> Denied clients will be ignored rather than rejected. This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is defined.
Subnet	192.168.1.0
Subnet mask	255.255.255.0
Available range	192.168.1.1 - 192.168.1.254
Range	<div>192.168.1.10</div> <div>From To</div>

Status → DHCP Leases – verifica os endereçamentos fornecidos pelo servidor

Para inserir um endereçamento ip estático, vc pode fazer por 2 formas: 1 pelo Services → DHCP Server, indo lá embaixo no grupo Static DHCP Mapping ou pela maneira mais fácil Status → DHCP Leases, clica no primeiro botão com o símbolo + , que ele já vai mostrar o mac address preenchido.

Status / DHCP Leases								
Leases								
IP address	MAC address	Hostname	Description	Start	End	Online	Lease Type	Actions
192.168.1.100	08:00:27:5b:13:6f	Cliente2		2016/09/17 21:15:41	2016/09/17 23:15:41	online	active	
Leases in Use								
Interface	Pool Start	Pool End	# of leases in use					
LAN	192.168.1.10	192.168.1.245	1					

Para fazer um servidor DHCP Relay é só ir no mesmo menu Services, mas vc deve parar o serviço Server DHCP.

DHCP Relay Configuration

Enable
☒ Enable DHCP relay on interface

Interface(s)

WAN
 LAN

Interfaces without an IP address will not be shown.

☐ Append circuit ID and agent ID to requests
If this is checked, the DHCP relay will append the circuit ID (pfSense interface number) to requests.

Destination server

Delete
 Add

This is the IP address of the server to which DHCP requests are relayed.

Save

Por padrão ele vai inserir como servidor DNS o próprio IP da interface lan. Para alterar tem que definir no serviço DHCP Server.

Services → DNS Forwarder para registrar um DNS interno onde pode-se ter o registro dos hosts que acessam a rede. Para habilitar, marque as opções Enable DNS forward, Register DHCP leases in DNS forwarder e Register DHCP static mappings in DNS forwarder, e tiver endereçamento estático. Ex: Na aula ele não conseguia pingar o hostname.

General DNS Forwarder Options	
Enable	<input checked="" type="checkbox"/> Enable DNS forwarder
DHCP Registration	<input checked="" type="checkbox"/> Register DHCP leases in DNS forwarder If this option is set, then machines that specify their hostname when requesting a DHCP lease can be resolved. The domain in System: General Setup should also be set to the proper value.
Static DHCP	<input checked="" type="checkbox"/> Register DHCP static mappings in DNS forwarder If this option is set, then DHCP static mappings will be registered in the DNS forwarder, so that General Setup should also be set to the proper value.

Não se esqueça de clicar no botão Apply Changes. Pode-se inserir quantas entradas DNS para vários hosts no grupo Host Overrides do menu Services → DNS Forward.

Services → Dynamic DNS – para registrar servidores DNS dinâmicos. Ele tem uma lista, onde está o dyndns, no-ip.com. Se utilizar outro servidor que não esteja na listagem, clica em RFC 2136 Clients e adiciona.

Dynamic DNS Client	
Disable	<input type="checkbox"/> Disable this client
Service Type	City Network
Interface to monitor	WAN
Hostname	Hostname Enter the complete fully qualified domain name. Example: myhost.dyndns.org he.net tunnelbroker: Enter the tunnel ID. GleSYS: Enter the record ID. DNSimple: Enter only the domain name. Namecheap: Enter the hostname and the domain separately, with the domain l
MX	Note: With DynDNS service only a hostname can be used, not an IP address. See this.
Wildcards	<input type="checkbox"/> Enable Wildcard
Verbose logging	<input type="checkbox"/> Enable verbose logging
Username	

Aula 4 – Configuração Geral e Regras de Firewall

Alias – É um apelido que pode ser vinculado a um ou vários Network, Host, Port, URL Table. Exemplo, para bloquear o Facebook pode-se criar um Alias. Pode-se importar dados em lote, clicando no botão IMPORT ou URLs. Para mais de 30.000 registros utilize URL Table (ip) ao invés URL (ip) – este último com até 3.000 registros. Para acessar Firewakk → Aliases.

Por exemplo existem várias listas na internet que contém as listas.

Properties

Name

IPS Diretorias

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

Description

IP dos computadores da Diretoria

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

Type

Host(s)

Host(s)

Hint

Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-1 as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

IP or FQDN

192.168.100.12

Diretoria adm

192.168.100.13

Diretoria finan

Save

Add Host

Firewall → Rules

Aqui podemos observar a regra que aparece na segunda linha (IPv4*) que permite com que possa se acessar a internet. Podemos por exemplo desabilitar e inserir passo a passo as regras de acesso.

Firewall / Rules / LAN

The settings have been applied. The firewall rules are now reloading in the background. Monitor the reload progress.

Floating

WAN

LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0/7.79 MiB	*	*	*	LAN Address	443 80 22	*	*		Anti-Lockout Rule	⚙️
☐ ✓	1/21.41 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	📌 ⚙️ 🗑️
☐ ✓	0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	📌 ⚙️ 🗑️

Lembrando que podemos utilizar os aliases criados anteriormente para as portas, por exemplo. É importante lembrar que a ordem das regras do Firewall é importante para q possa ser implantada. Exemplo: Para criar uma regra para bloqueio de facebook, é importante ao, inserir, colocar no início das regras pois se houver uma regra antes habilitando o acesso, a regra q vc criou não irá funcionar.

Firewall → Schedules

Para criar horários onde por exemplo vc vai liberar o acesso. Ex: criar uma schedule para o horário de almoço onde o facebook é liberado. Podem ser adicionados vários horários a um mesmo shcedule. Lá no Firewall Rules, edite a regra e depois na linha Schedule, selecione o que vc criou.

Schedule Information

Schedule Name

Horario_Almoço_Jantar

Description

Horário de almoço das 12:00 às 13:00 em q o Facebook é liberado

Month

September_16

Date

September_2016

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

0

00

23

59

Firewall → NAT – Exemplo de acesso ao Terminal Services de uma estação Windows

Neste exemplo iremo habilitar DNAT para rede interna, para um Servidor de TS, com endereço ip 192.168.1.254

Vá em Firewall | NAT | Port Forward

Clique em + para adicionar um nova Regra

Interface será Wan

Protocol será TCP

Destination Port Range, utilizar MS RDP

Redirect Target IP, coloque 192.168.1.254

Redirect Target Port, escolha MS RDP

Em Filter rule association, escolha Add associate filter rule.

E salve.

O Add associate filter rule vai criar uma regra no firewall permitindo a comunicação com este endereço.

Para indicar um horário, acesse a regra de firewall que foi criada, edite e atribua um Schedule para a regra.

AULA 5 – VPN

Qdo se cria uma VPN as redes precisam ser diferentes por questões de definição de rota. Exemplo não podemos ter uma rede 192.168.0.0/24 na matriz e uma 192.168.0.0/24 na filial. Aconselha-se criar pela Open VPN que é mais segura, ao invés do L2TP VPN e PPTP VPN.

O modelo Server-2-Server é utilizado para interligar 2 redes.

Neste exemplo utilizaremos 2 redes, uma com um gateway 200.0.0.4 que tem uma rede 192.168.1.0/24 e outro q tem como gateway 200.0.0.5 que tem uma rede 192.168.2.0/24.

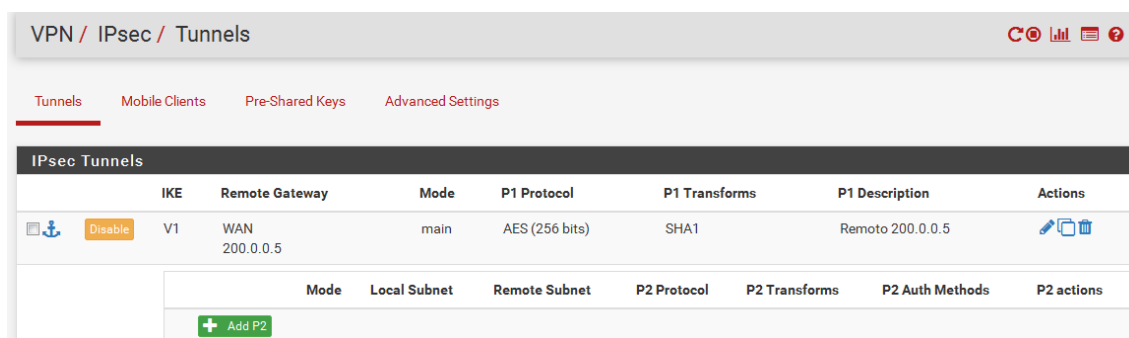
Para criar uma VPN IPsec

Usaremos o modelo Server-2-Server, para interligar Filial e Matriz.
 As redes internas devem ser distintas.
 Para configurar vamos em VPN | Ipsec , e clicamos no botão adicionar "+".
 Especifique o Remote Gateway
 Adicione uma Descrição em Description
 Em Pre-Shared Key digite sua senha
 Marque Enable Ipsec
 E por fim Salve.

Neste exemplo, no pfsense do 200.0.0.4 o remote gateway será 200.0.0.5

Para a chave Pre-Shared Key, utilize o site www.grc.com/passwords.htm que gera uma chave. A chave gerada no www.grc.com deve ser a mesma nos dois gateways.

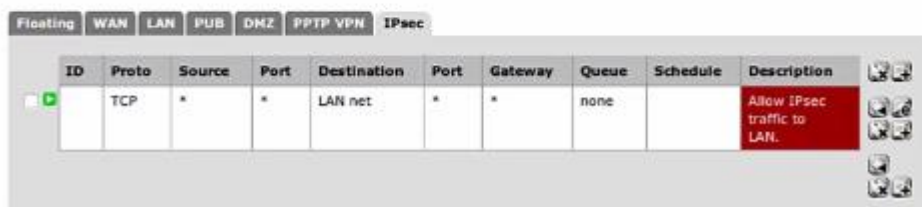
Uma vez criada, vc tem que Show Phase 2 Entries Phase 2 onde se especifica a rede de destino, em Remote Network neste caso 192.168.2.0/24. Selecione em PFS key group uma chave de criptografia, q pode ser 1024 bits.



Depois em

VPN → IPsec é só dá um play.

Agora devemos ir em Firewall | Rules, selecione a aba Ipsec, clique no botão "+".
 Em Destination selecione Lan Subnet
 Em Destination port selecione any
 Em Description coloque uma descrição
 E salve



Diagnostics → Ping utilizado para saber se está pingando um host.

OPENVPN

VPN → OpenVPN – configurado no 200.0.0.4

Server Mode – Peer to Peer (shared key)
Description – VPN para a Rede 200.0.0.5
IPv4 Tunnel Network – 10.0.0.0/24

Depois vai no 200.0.0.5, VPN → OpenVPN, agora na guia Client e adiciona

Sever Mode – Peer to Peer (shared key)
Server host or address – 200.0.0.4
Description – VPN Client para 200.0.0.4
Shared Key – desmarca Automatically generate a shared key e informa a key gerada na configuração do 200.0.0.4
IPv4 Tunnel Network – 10.0.0.0/24
IPv4 Remote Network – 192.168.1.0/24

Configurando Túnel

Em **Tunnel Network**, deverá ser digitado o endereço no formato CIDR, para os endereços que serão entregues para os clientes, diferente dos endereços da sua rede interna, por exemplo 10.0.0.0/24.

Em **Local Network**, a rede que será acessada pelos clientes, em nosso caso 192.168.1.0/24.

É possível especificar em **Cuncurrent Conections** a quantidade máxima de conexões e em **Redirect Gateways** forçar os clientes a usarem o túnel como gateway padrão.

Tunnel Settings	
Tunnel Network:	<input type="text" value="10.0.0.0/24"/> <small>This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.0.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses can optionally be assigned to connecting clients. (see Address Pool)</small>
Redirect Gateway:	<input type="checkbox"/> Force all client generated traffic through the tunnel.
Local Network:	<input type="text" value="192.168.1.0/24"/> <small>This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. You may leave this blank if you don't want to add a route to the local network through this tunnel on the remote machine. This is generally set to your LAN network.</small>
Concurrent Connections:	<input type="text"/> <small>Specify the maximum number of clients allowed to concurrently connect to this server.</small>

Vai em Status → OpenVPN vai mostrar se está open.

Não esquecer de ir em Firewall → Rules – guia Open VPN e criar a regra habilitando

O PFSense já gera os clientes (discadores) para conexão à VPN.

Foi mostrado no vídeo a criação de uma VPN PPTP, onde se instancia o servidor e se criam os usuários.

STATUS → System Logns, escolha a guia OPenVPN para verificar as conexões por rede, com o ip atribuído.

AULA 6 – VIRTUAL IP

FIREWALL → Virtual IPs

TIPOS:

1 - IP Other – Define IPs adicionais para uso qdo respostas ARP para o endereço IP não são necessários. Não pode ser usado para serviço (ex: serv web), pode estar em subnet diferente que a interface real e não responde a ping. Usado por exemplo para acessar a interface WEB do modem PPPOE.

Deve-se depois configurar um NAT Outbound

2 - IP Alias – adicionai mais um IP à interface. Pode ser utilizada para serviços e encaminhamentos. Normalmente usado para NAT 1:1 e responde a ping. Exemplo usado de IP público para IP privado.

Vai em Firewall → Nat, seleciona 1:1

Interface – wan

External subnet IP – insira o IP público

Internal IP – digite o IP interno do servidor web por exemplo

Description – insere a descrição da regra

Depois vai em Firewall → Rules e adiciona

Action – Pass

Interface – wan

Destination – mude para single host or Alias e altere o endereço IP para o servidor web (ip privado)

Description – insira uma descrição e clique em SAVE

3 - IP Proxy ARP – pode ser usado pelo firewall para encaminhar serviços gerando tráfego layer 2 da VIP. Pode estar em subnet diferentes da interface real e não responde à ping. Normalmente utilizado para encaminhar tráfego de clientes para DMZ.

Neste cenário temos um servidor WEB Interno, que pode ser por exemplo 192.168.1.100. O servidor WEB é acessado pelos clientes internos através deste endereço IP.

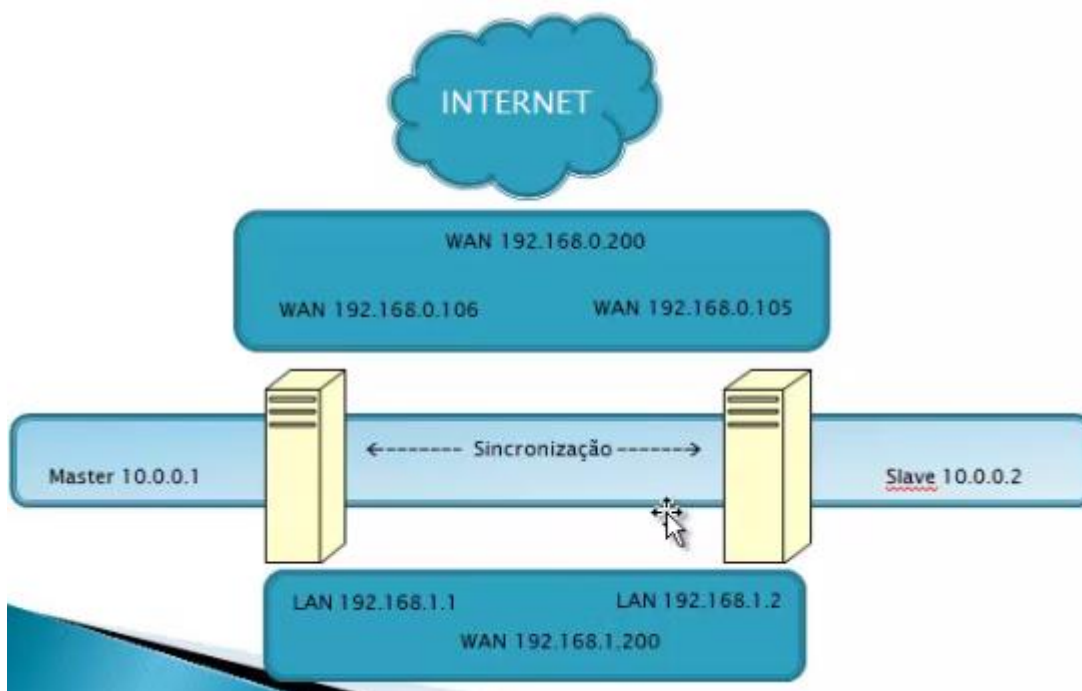
Mas precisamos permitir acesso ao público da Internet, é deixa-lo na rede interna é inseguro, de forma que devemos move-lo para DMZ.

Imagine que os clientes internos usem o servidor WEB através de um código fechado, onde não podemos configurar outro endereço IP.

Para resolver esse problema criamos um IP Proxy, simulando a presença dele, dentro da rede interna.

4 - CARP – responde a ping de configurado no firewall, utilizado para Cluster (failover)

Neste cenário teremos dois servidores com PFSense. Nestes servidores teremos 3 interfaces de Rede, onde serão utilizado uma para Rede Pública, Rede Privada e sincronismo com o Carp. A ideia é montar um cluster, de forma que o secundário assuma as responsabilidades como firewall do primário, e quando este retornar a ficar online, o secundário devolva as atribuições do primário.



Os 2 pfenses devem ter o mesmo ip carp para as interfaces lan e wan.

Vai no menu Status → Carp para habilitar o serviço CARP. Ele vai indicar quem é o MASTER e quem é o Backup.

AULA 7 – ROTEAMENTO A

System → Routing – mostra as rotas, incluindo a default. Para inserir mais um gateway repete o procedimento, não esquecendo de, ao configurar a interface WAN2 – Interfaces → Wan2, selecionar o ip da interface que é o seu gateway.

Depois tem que ir no Firewall → Rules e apontar o Alias (que pode ser um grupo de ips) e na parte advanced escolha o Gateway, apontando para o ip criado. Em source escolhe Single Host or alias e digita o nome do alias. O action da rule é PASS. Coloque sempre ca regra de firewall no início para sobrescrever as demais. Ao posicionar o mouse sobre o alias, ele vai mostrar o IP associado.

Redirecionando tráfego por pacotes

Neste segundo exemplo queremos configurar para que determinados pacotes saiam por um determinado Link. Em nosso exemplo usaremos pop, smtp e imap.

O mesmo procedimento será usado, ou seja criaremos um Firewall Aliases e depois uma regra na Wan.

Vamos até **Firewall | Alias**, clique em adicionar "+"

Em nome dê um nome como **Protocolos_Link1**

Em descrição coloque uma descrição

Em **Type** selecione **Port(s)**

E clique em mais para adicionar as portas

Cuidado ao configurar o DNS pois ambas as interfaces a utilizam.

Para criar a regra, vá em **Firewall | Rules**, selecione a aba **Lan** e clique em adicionar "+"

Vá em **Destination port range**, em **from** e **to**, digite o nome do Firewall Aliases criado anteriormente, no caso

Protocolos_Link1

Em **Advanced Features**, selecione Gateway e adicione o gateway desejado.

Em Destination port range, ao selecionar a opção other, basta digitar o nome do alias que ele já preenche.

Rotas Estáticas

System → Routing - Guia routes

TRAFFIC SHAPER

Firewall → Traffic Shapper

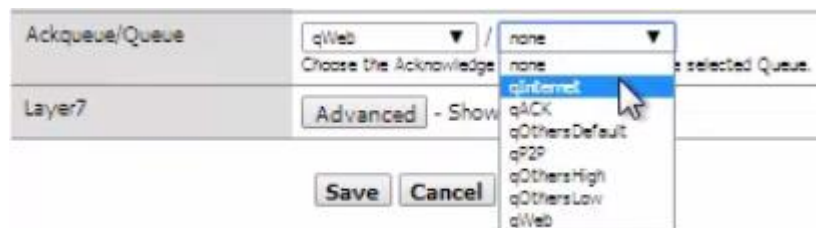
O Traffic Shaping, também conhecido como QoS, é a priorização e otimização de pacotes de rede. Priorizando os pacotes de rede de certos tipos de tráfego em relação a outros. Limita o pacote de rede fixando certos limites de velocidade de certos tipos de tráfego para certos momentos. Um administrador pode querer priorizar os pacotes de VoIP sobre todos os outros para garantir que chamadas telefônicas não vão ser descartadas ou interrompidas devido ao alto tráfego de rede. Além disso, podemos também limitar o rendimento do VoIP para 100kbps. Esse é um exemplo tipo de ambiente que roda VoIP.

Utiliza-se CBQ tanto para as regras nas interfaces LAN quanto na WAN.

No menu Status → Traffic Shapper vai mostrar em tempo real as queues definidas e sua utilização.

As regras dos queues são criadas na guia Floating do menu Firewall → Rules

Você pode criar regras específicas (QUEUES) e depois criar uma Firewall → Rules e setar o Ackqueue/Queue, nas opções avançadas da regra. Cuidado que as métricas vem com Kbp/s que são kbits por segundo e não kbytes por segundo KBp/s. Para converter, multiplique por 8. 56 Kbp/s = 8 KBp/s



Deve-se utilizar os wizards que já fazem a definição tanto das queues qto das regras que vão aparecer no Firewall → Rules guia Floating. No curso ele utilizou o Wizard Function → Dedicated Links.

Foi criado na Guia Limiter, uma configuração de limite (não esqueça de marcar a opção Enable Limiter) – crie 2 Limiters, uma para In e outra para Out.

Limiter | Layer7 | Wizards

☒ Enable limiter and its children

Name: LWeb2

Bandwidth: 128 Kbit/s | Burst: 30 Kbit/s | Bit type: Kbit/s | Schedule: none

Mask: 255.255.255.255/24 | IPv4 mask bits (1-32)

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

Queue Actions: Save | Add new queue | Delete this queue

Depois em Firewall → Rules inserida a regra. Na guia Lan, insere uma Rule e nas configurações avançadas dela, linha IN/OUT, seleciona o Limiter criado.

No XMLRPC Sync: Advanced - Show advanced option

802.1p: Advanced - Show advanced option

Schedule: Advanced - Show advanced option

Gateway: Advanced - Show advanced option

In/Out: LWeb2 / none

Choose the out queue/Virtual interface only if you have also selected In. The Out selection is applied to traffic leaving the interface where the rule is created, In is applied to traffic coming into the chosen interface. If you are creating a floating rule, if the direction is In then the same rules apply, if the direction is out the selections are reverted Out is for incoming and In is for outgoing.

Lembre-se de posicionar a regra em cima das outras regras do firewall.

BRIDGES – Vai no menu Interfaces e depois na guia Bridges e adiciona selecionando com o CTRL as interfaces. Informa a descrição e clica em Save.

VLAN – Menu Interfaces vai na guia VLAN.

AULA 8 – BALANCEAMENTO E FAILOVER

Primeiro temos que ter 2 ou mais WANs.

System → Routing e selecione a guia Gateway Groups

Group Name – Coloque qualquer nome Ex: Balance

Gateway Priority – Selecione Tier2 em ambos os Gateways

Trigger Level – Packet Loss or High latency

Description – Descreva o balanceamento – Ex: Balanceamento WAN

System / Routing / Gateway Groups / Edit

Edit Gateway Group Entry

Group Name

BALANCE

Gateway Priority

WAN_DHCP

Tier 2

Interface Address

WAN2_DHCP

Tier 2

Interface Address

Gateway

Tier

Virtual IP

Link Priority

The priority selected here defines in what order failover and balancing of links will be done. Monitor IP until all links in the priority will be exhausted. If all links in a priority level are exhausted then the

Virtual IP

The virtual IP field selects which (virtual) IP should be used when this group applies to a local

Trigger Level

Packet Loss or High latency

When to trigger exclusion of a member

Description

Balanceamento WAN

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

Depois vai em System → Routing e edita os 2 gateways.


Em Monitor IP – informa 8.8.8.8

Clica no botão Display Advanced – Weight escolhe 1

Em Loss Interval informe 3000 que são 3 segundos

No segundo Gateway repita o procedimento mas alterando o Monitor IP para 8.8.4.4 pois o PFSense não aceita monitoramento de 2 IP's iguais para 2 gateways.

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



Advanced

Weight
Weight for this gateway when used in a Gateway Group.

Data Payload
Define data payload to send on ICMP packets to gateway monitor IP.

Latency thresholds
Low and high thresholds for latency in milliseconds. Default is 200/500.

Packet Loss thresholds
Low and high thresholds for packet loss in %. Default is 10/20.

Probe Interval
How often an ICMP probe will be sent in milliseconds. Default is 500.






Loss Interval

Depois vai em Firewall → Rules e altera as configurações da LAN

Altera a regra que aparece geralmente na segunda linha qdo libera todo o tráfego IPV4* na interface LAN.
Nele vai em Advanced e escolhe como gateway o Balance que vc criou.

Floating WAN LAN WAN2 IPsec

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0/5.67 MiB	*	*	*	LAN Address	443 80 22	*	*		Anti-Lockout Rule	
✓ 3/6.74 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	   

Observe na figura acima a regra 2

Schedule
Leave as 'none' to leave the rule enabled all the time.

Gateway

 WAN_DHCP - 192.168.0.1 - Interface WAN_DHCP Gateway
 WAN2_DHCP - 192.168.0.1 - Interface WAN2_DHCP Gateway
 BALANCE - Balanceamento WAN

In / Out pipe

FAILOVER

System → Routing, guia Gateway Groups e adiciona.

Group Name – FailOver

Group Priority para a Wan1 selecione Tier1 e para a Wan2 selecione Tier2
Description – Failover para as Wans

System / Routing / Gateway Groups / Edit

Edit Gateway Group Entry

Group Name

Gateway Priority

<input type="text" value="WAN_DHCP"/>	Tier 1	<input type="text" value="Interface Address"/>
<input type="text" value="WAN2_DHCP"/>	Tier 2	<input type="text" value="Interface Address"/>

	Gateway	Tier	Virtual IP
Link Priority	The priority selected here defines in what order failover and balancing of links will balance connections until all links in the priority will be exhausted. If all links are exhausted, connections will be balanced to the next priority level.		
Virtual IP	The virtual IP field selects which (virtual) IP should be used when this group is the OpenVPN endpoint.		
Trigger Level	<input type="text" value="Packet Loss or High latency"/> When to trigger exclusion of a member		
Description	<input type="text" value="Failover das Wans"/>		

LOAD BALANCE - ver na internet pois o Professor do curso confundiu tudo
Vai em Services → Load Balancer, guia Monitors e clica em ADD

Figura 1

Figura 2

Depois vai na guia Pools e adiciona

Name – PoolWb

Mode – Load Balance

Description – Monitora os serviços WEB

Port – 80

Status → Load Balance : Pool vai mostrar os dados de redirecionamento dos servidores.

O Pool realiza também Failover de servidores.

AULA 09 – CAPTIVE PORTAL

Para conceder acesso pode-se utilizar um captive portal. Vá em Services → Captive Portal e crie um.

Services / Captive Portal / Add Zone


Add Captive Portal Zone

Zone name

Zone name. Can only contain letters, digits, and underscores (_) and may not start with a digit.

Zone description

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

 Save & Continue

Clique em Enable Captive Portal, selecione a interface onde será habilitado o portal. Maximum concurrent connections é o número máximo de conexões que um mesmo ip pode ter simultaneamente. Configure o tempo de inatividade e por quanto tempo é valido o login até ser exibido novamente a tela de login. Outra opção que pode ser utilizada é a Redirect URL que redireciona depois do login.

Captive Portal Configuration

Enable

☒ Enable Captive Portal

Interfaces

WAN
LAN
WAN2

Select the interface(s) to enable for captive portal.

Maximum concurrent connections

1

Limits the number of concurrent connections to the captive portal HTTP(S) portal, but rather how many connections a single IP can establish to the portal.

Idle timeout (Minutes)

10

Clients will be disconnected after this amount of inactivity. They may log in again.

Hard timeout (Minutes)

60

Clients will be disconnected after this amount of time, regardless of activity. hard timeout (not recommended unless an idle timeout is set).

Pode-se ainda restringir a banda por usuário logado.

Per-user bandwidth restriction

☒ Enable per-user bandwidth restriction

Default download (Kbit/s)

Default upload (Kbit/s)

If this option is set, the captive portal will restrict each user who logs in to the network.

Em Authentication podemos escolher se vamos autenticar localmente ou com um servidor RADIUS. Ainda podemos personalizar a tela de login, onde abaixo aparecem as orientações para colocar o código html FORM

Authentication

Authentication method

☐ No Authentication

☒ Local User Manager / Vouchers

☐ RADIUS Authentication

☒ Allow only users/groups with "Captive portal login" privilege set

HTTPS Options

Login

☐ Enable HTTPS login

When enabled, the username and password will be transmitted over an HTTPS connection to protect against eavesdropping. A valid SSL certificate must also be specified below.

HTML Page Contents

Portal page contents

Selecionar arquivo...

Nenhum arquivo selecionado.

Upload an HTML/PHP file for the portal page here (leave blank to keep the current one). Make sure to include a form with a submit button (name="accept") and a hidden field with name="redirurl" and value="\$PORTAL_REDIRURL\$. In addition, include "auth_pass" and/or "auth_voucher" input fields if authentication is enabled, otherwise it will always fail.

Example code for the form:

```
<form method="post" action="$PORTAL_ACTION$">
  <input name="auth_user" type="text">
  <input name="auth_pass" type="password">
  <input name="auth_voucher" type="text">
  <input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$" />
  <input name="zone" type="hidden" value="$PORTAL_ZONE$" />
</form>
```

Podemos ainda personalizar as páginas de logout e login errado. Não esqueça de ir em System → User Manager para cadastrar usuário com permissão de uso do Captive Portal. Depois de criar o usuário vai em editar e adiciona Effective Privileges – User Services Captive Portal Login

System / User Manager / Users / Edit / Add Privileges

Users

Groups

Settings

Authentication Servers

User Privileges

Assigned privileges

User - Config: Deny Config Write
User - Services: Captive Portal login
User - System: Copy files (scp)
User - System: Shell account access
User - System: SSH tunneling
User - VPN: IPsec xauth Dialin
User - VPN: L2TP Dialin

STATUS → Captive Portal é possível visualizar a utilização do portal.

AULA 10 – OUTROS SERVIÇOS

SERVICES → PPPOe Server – Servidor PPPOe. Nesta tela se cadastram os usuários.

Não se esqueça de ir em Firewall → Rules e na guia PPPOe Server criar uma regra que permita a conexão na interface.

Enable

☒ Enable PPPoE Server

Interface

LAN

Total User Count

10

The number of PPPoE users allowed to connect to this server simultaneously

User Max Logins

1

The number of times a single user may be logged in at the same time.

Server Address

10.0.0.200

Enter the IP address the PPPoE server should give to clients for use as their
Typically this is set to an unused IP just outside of the client range.
NOTE: This should NOT be set to any IP address currently in use on this fire

Remote Address Range

10.0.0.0

Specify the starting address for the client IP address subnet.

Subnet mask

24

Hint: 24 is 255.255.255.0

Description

DNS Servers

8.8.8.8

User table

andrejar

••••••••••

10.0.0.201

UsernamePasswordIP Address

+ Add user

FloatingWANLANWAN2PPPoE ServerIPsec

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 *	*	*	*	*	none			

~

Para implementações RIP, deve-se criar regra no firewall para permitir conexão na porta 520.

HABILITANDO O SNMP

Services → SNMP

HABILITANDO NTP SERVER

Services → NTP. Informa qual a interface conectará com o servidor NTP externo e quais servidores NTP ele irá pegar a hora. Uma vez estabelecido o NTP server, verifique se está funcionando em Status → NTP, verificando se o Status está Active Peer.

Status / NTP				
Network Time Protocol Status				
Status	Server	Ref ID	Stratum	Type
Active Peer	200.160.0.8	200.160.7.186	2	u

HABILITANDO WAKE ON LAN

Services → Wake On Lan

This service can be used to wake up (power on) computers by sending special "Magic Packets".
The NIC in the computer that is to be woken up must support Wake-on-LAN and must be properly configured (WOL).

Wake-on-LAN

Interface

LAN

Choose which interface the host to be woken up is connected to.

MAC address

Enter a MAC address in the following format: xxxxxxxxxx

Send

Wake-on-LAN Devices

Click the MAC address to wake up an individual device.

Interface	MAC address	Description
<div><div>+ Add</div><div>Wake All Devices</div></div>		

REGISTRANDO OS LOGS

Status → System Logs, guia Settings. Aqui é possível registrar quais logs serão armazenados e podemos ter um servidor específico para receber estas informações.

Enable Remote Logging

☒ Send log messages to remote syslog server

Source Address

Default (any) ▼

This option will allow the logging daemon to bind to a single IP address, rather than all be of that IP type. To mix IPv4 and IPv6 remote syslog servers, bind to all interfaces.

NOTE: If an IP address cannot be located on the chosen interface, the daemon will not log.

IP Protocol

IPv4 ▼

This option is only used when a non-default address is chosen as the source address. If the selected type is not found on the chosen interface, the other type will be tried.

Remote log servers

IP[:port]

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

DIAGNOSTICS → PING

Diagnostics / Ping

Ping

Hostname

8.8.8.8

IP Protocol

IPv4 ▼

Source address


WAN ▼

Select source address for the ping.

Maximum number of pings

3 ▼

Select the maximum number of pings.

 Ping

Results

PING 8.8.8.8 (8.8.8.8) from 192.168.1.1: 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=56 time=54.106 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=56 time=54.675 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=56 time=54.304 ms

DIAGNOSTICS → TRACEROUTE

FAZENDO O BACKUP E RESTORE DO PFSENSE

DIAGNOSTICS → Backup & Restore

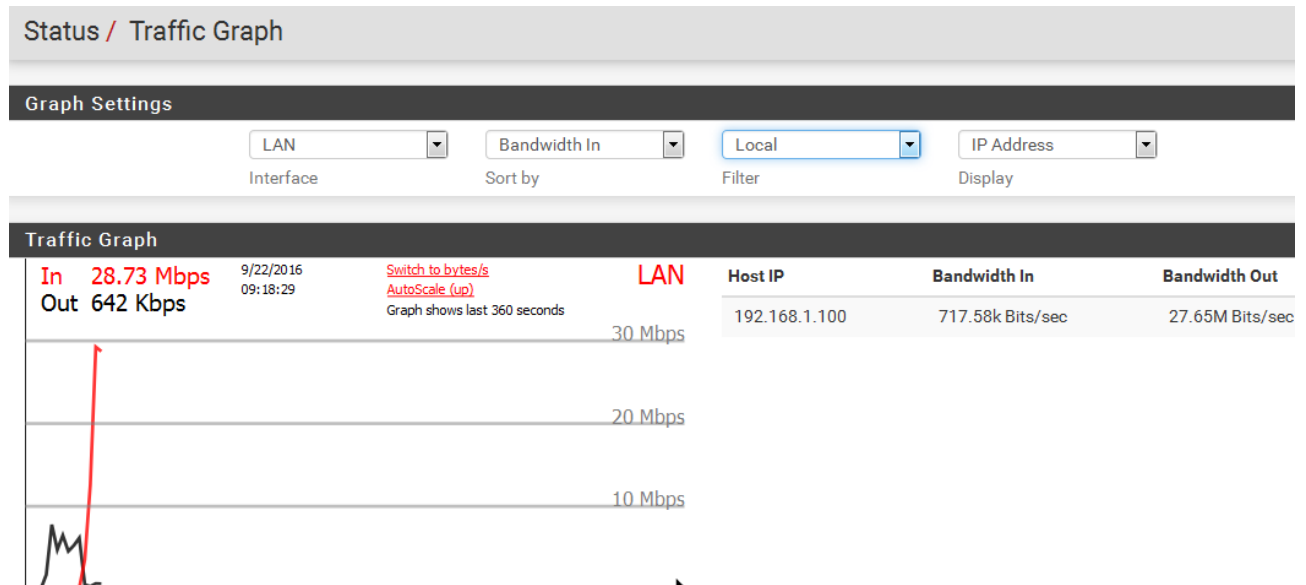
Para utilizar backup automático tem que instalar o pacote AutoBackup

ATUALIZAÇÃO DO PFSENSE

SYSTEM → Update

AULA 11 – MONITORAMENTO, LOGS E DASHBOARD

STATUS → TRAFFIC GRAPH – gráfico mostrando o uso da internet



Configurando SMTP para envio de notificações

System → Advanced notifications. Na linha Email se faz as configurações.

E-Mail server	<input type="text"/>	
	This is the FQDN or IP address of the SMTP E-Mail server to which notifications will be sent.	
SMTP Port of E-Mail server	<input type="text"/>	
	This is the port of the SMTP E-Mail server, typically 25, 587 (submission) or 465 (smtps).	
Secure SMTP Connection	<input type="checkbox"/> Enable SMTP over SSL/TLS	<input type="checkbox"/> Enable STARTTLS
From e-mail address	<input type="text"/>	
	This is the e-mail address that will appear in the from field.	
Notification E-Mail address	<input type="text"/>	
	Enter the e-mail address to send email notifications to.	
Notification E-Mail auth username (optional)	<input type="text"/>	
	Enter the e-mail address username for SMTP authentication.	
Notification E-Mail auth password	<input type="password"/>	<input type="password"/>
	Enter the e-mail account password for SMTP authentication.	Confirm
Notification E-Mail auth mechanism	<input type="text" value="PLAIN"/>	
	Select the authentication mechanism used by the SMTP server. Most work with PLAIN, some servers li	
Test SMTP Settings	Test SMTP Settings	

Visualizando os LOGS do sistema

System → System Logs – são vários os logs que podem ser consultados

Status / System Logs / System / General			
System	Firewall	DHCP	Captive Portal Auth
			IPsec
			PPP
			VPN
			Load Balancer
			OpenVPN
General	Gateways	Routing	DNS Resolver
			Wireless
Last 50 General Log Entries. (Maximum 50)			
Time	Process	PID	Message
Sep 22 09:04:18	php-cgi		rc.bootup: Creating rrd update script
Sep 22 09:04:18	kernel		done.
Sep 22 09:04:19	syslogd		exiting on signal 15
Sep 22 09:04:19	syslogd		kernel boot file is /boot/kernel/kernel
Sep 22 09:04:19	kernel		done.
Sep 22 09:04:19	php-fpm	300	/rc.start_packages: Restarting/Starting all packages.
Sep 22 09:04:21	login		login on ttyv0 as root
Sep 22 09:04:21	sshlockout	87011	sshlockout/webConfigurator v3.0 starting up

Dependendo da guia escolhida vão aparecer as guias Normal View, Dynamic View e Summary View

System

Firewall

DHCP

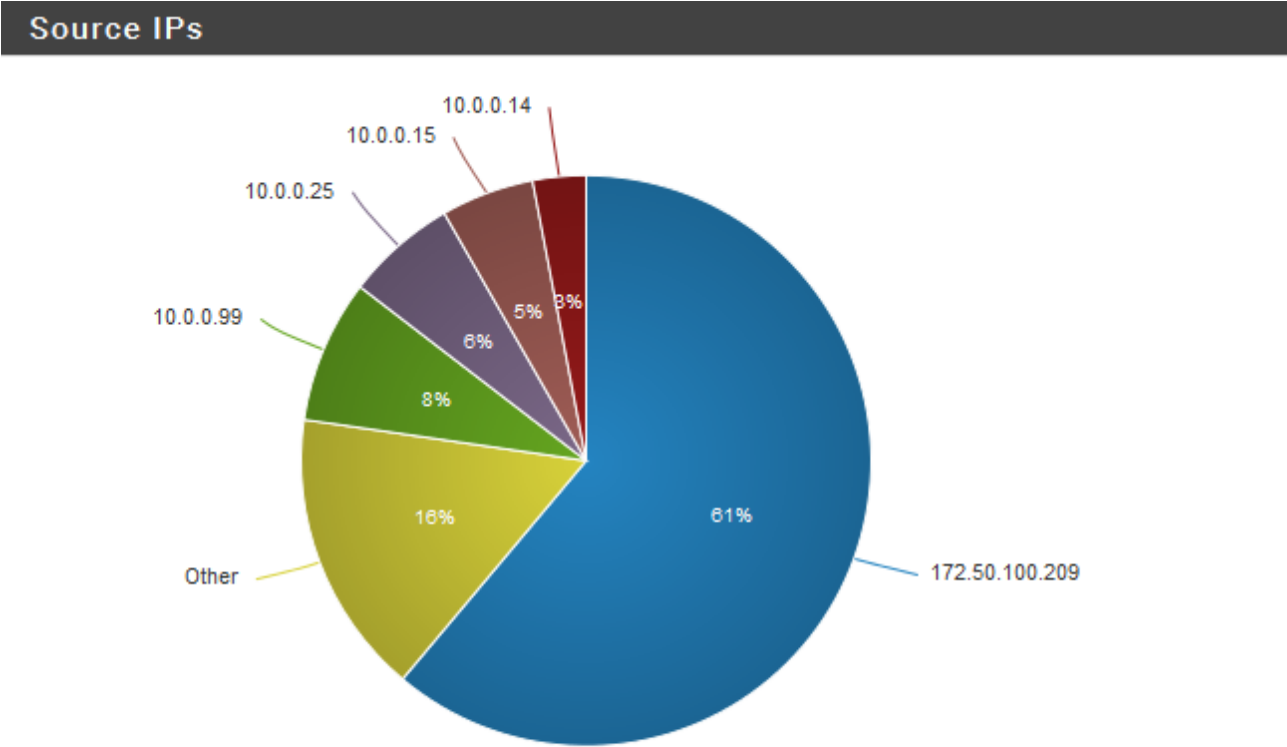
Captive Portal Auth

Normal View

Dynamic View

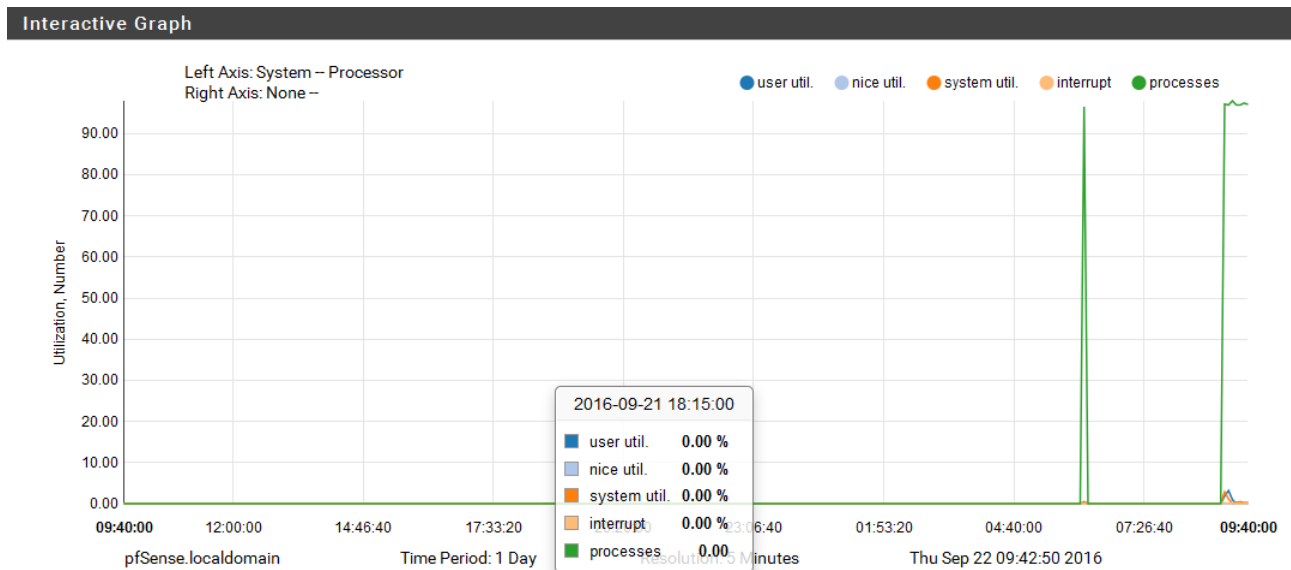
Summary View

O Dynamic View vai mostrando os dados em tempo real, no momento em que ocorrem. Mostrou quando utilizamos a guia Firewall. O Summary View mostra vários gráficos com as informações registradas no firewall, conforme podemos observar na figura abaixo:




Source IPs	Data points
172.50.100.209	730
10.0.0.99	97

Gráficos RRD – Na versão nova Status → Monitoring – veremos as informações de uso do sistema



Data Summary

	Minimum	Average	Maximum	Last
user util.	0.00 %	0.79 %	3.19 %	0.00 %
nice util.	0.00 %	0.00 %	0.00 %	0.00 %
system util.	0.05 %	0.75 %	2.84 %	0.39 %
interrupt	0.00 %	0.08 %	0.21 %	0.20 %
processes	96.58	97.18	98.02	97.14

Para alterar o tipo de gráfico e o parâmetro de monitoramento, clique no botão Settings  localizado no canto superior direito da tela. Por exemplo na figura abaixo, alteramos para verifica o uso de memória.

Settings

Left Axis: System (Category) Memory (Graph)

Right Axis: None (Category) (Graph)

Options: 1 Day (Time Period) 5 Minutes (Resolution) Line (Type (Disabled)) On (Inverse)

Settings: [Display Advanced](#) [Update Graphs](#)

Podemos ainda ter os gráficos de Traffic, Packets, Quality conforme verificamos abaixo:

Settings

Left Axis: System (Category) Memory (Graph)

Right Axis: System (Category) (Graph)

Options: 1 Day (Time Period) 5 Minutes (Resolution) Line (Type (Disabled)) On (Inverse)

Settings: [Display Advanced](#) [Update Graphs](#)

DIAGNOSTICS → pfInfo – mostra informações compiladas de pacotes trafegados nas interfaces.

DIAGNOSTIS → pfTOP – mostra as informações de uso do sistema

Diagnostics / pfTop

pfTop Configuration

View default

Sort by Bytes

Maximum # of States 100

Output

pfTop: Up State 1-28/28, View: default, Order: bytes

PR	D	SRC	DEST	STATE	AGE	EXP	PKTS	BYTES
tcp	I	192.168.1.100:50123	189.39.113.136:80	4:4	1688	86390	8806	8604K
tcp	O	10.0.0.254:19690	189.39.113.136:80	4:4	1688	86390	8798	8603K
tcp	I	192.168.1.100:50124	216.115.104.247:443	4:4	1651	86358	503	299K
tcp	O	10.0.0.254:47028	216.115.104.247:443	4:4	1651	86358	503	299K
tcp	I	192.168.1.100:50615	192.168.1.1:443	9:9	275	57	502	267K
icmp	O	10.0.0.254:12741	10.0.0.1:12741	0:0	794	10	3162	88536
tcp	I	192.168.1.100:50196	72.30.196.161:443	4:4	1481	86393	227	43684
tcp	O	10.0.0.254:54980	72.30.196.161:443	4:4	1481	86393	227	43684

DIAGNOSTICS → System Activity – Mostra dados do uso do Sistema como processador e memória ram, Uptime, memória SWAP.

Diagnostics / System Activity

CPU Activity

last pid: 33182; load averages: 0.04, 0.03, 0.00 up 0+01:20:51 10:35:34
101 processes: 2 running, 84 sleeping, 15 waiting

Mem: 46M Active, 45M Inact, 80M Wired, 1004K Cache, 53M Buf, 790M Free
Swap: 1024M Total, 1024M Free

PID	USERNAME	PRI	NICE	SIZE	RES	STATE	TIME	WCPU	COMMAND
11	root	155	ki31	0K	16K	RUN	79:13	100.00%	[idle]
6814	root	23	0	262M	35000K	pipe	0:01	0.98%	php-fpm: pool nginx (php-fpm)
0	root	-16	-	0K	176K	swapi	0:29	0.00%	[kernel{swapper}]
0	root	-92	-	0K	176K	-	0:15	0.00%	[kernel{em0 taskq}]
0	root	-92	-	0K	176K	-	0:12	0.00%	[kernel{em1 taskq}]
12	root	-60	-	0K	240K	WAIT	0:11	0.00%	[intr{swi4: clock}]
12	root	-92	-	0K	240K	WAIT	0:05	0.00%	[intr{irq19: em0 ehci0}]
15	root	-16	-	0K	16K	-	0:03	0.00%	[rand_harvestq]
5	root	-16	-	0K	16K	pftm	0:02	0.00%	[pf purge]
7561	root	20	0	39136K	7104K	kqread	0:01	0.00%	nginx: worker process (nginx)
10027	root	20	0	16676K	2228K	bpf	0:01	0.00%	/usr/local/sbin/filterlog -i

DIAGNOSTICS → Command Prompt – para executar comandos Linux.

DIAGNOSTICS → DNS Lookup – fazer consultas DNS.

DIAGNOSTICS → Factory Defaults – para resetar o PFSense.

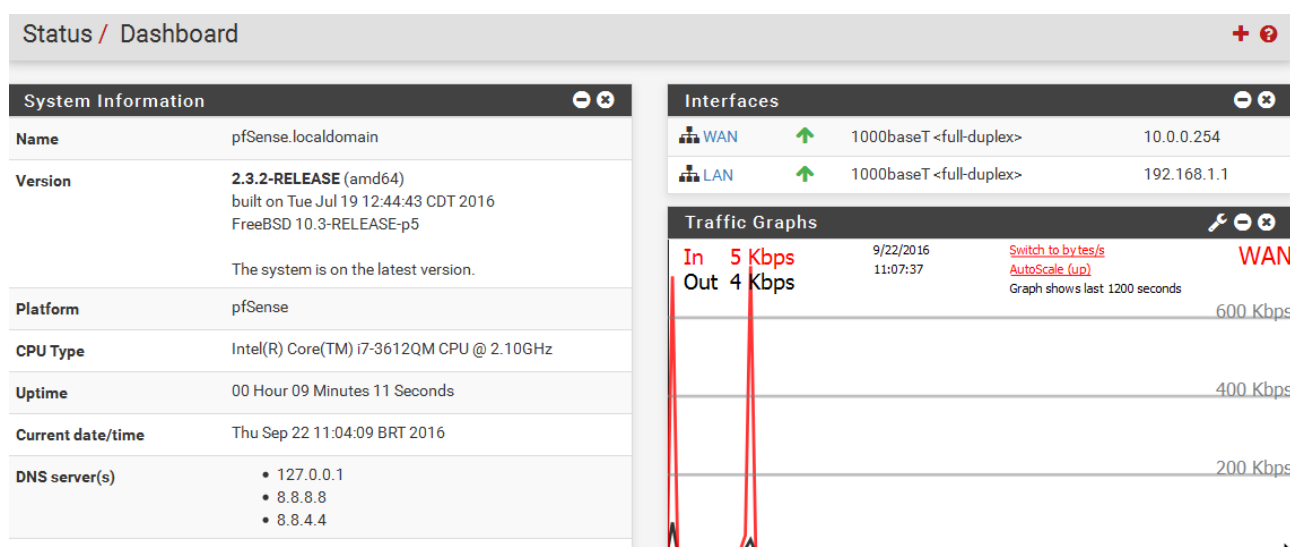
DIAGNOSTICS → Reboot – para reiniciar o firewall

DIAGNOSTICS → Routes – mostra as rotas cadastradas no sistema

DIAGNOSTICS → Test Ports – para testar se um servidor está respondendo por uma porta

PERSONALIZANDO O DASHBOARD

STATUS → DASHBOARD – clica no botão + e adicionar os widgets disponíveis, como por exemplo os gráficos. Para retirar do dashboard, basta clicar no botão x.



Clicando na barra de título do Widget, vai para a tela de origem do gráfico.

No Dashboard também aparece os dados do sistema, como uso de CPU, memória RAM, disco do servidor.

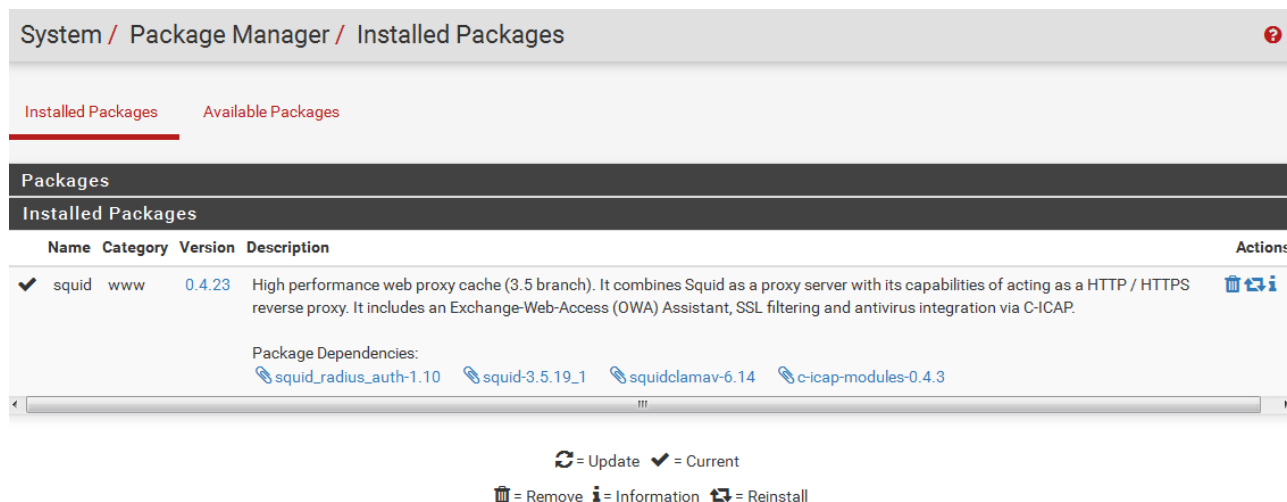
DNS server(s)	<ul style="list-style-type: none">127.0.0.18.8.8.88.8.4.4
Last config change	Thu Sep 22 11:00:40 BRT 2016
State table size	0% (71/98000) Show states
MBUF Usage	2% (1016/61600)
Load average	0.01, 0.10, 0.12
CPU usage	6%
Memory usage	12% of 989 MiB
SWAP usage	0% of 1023 MiB
Disk usage (/)	58% of 992MiB - ufs
Disk usage (/var/run)	3% of 3.4MiB - ufs in RAM

Bom colocar o widget Service Status que mostra o Status dos serviços oferecidos no PFSense.

Widget picture, para colocar a logo da Empresa no dashboard. Você pode mover os widgets arrastado os títulos.

AULA 12 – PROXY SQUID

Para instalar SYSTEM → Package Manager, guia Available Packages. Vai aparecer agora um menu chamado Services → Squid Proxy Server. Depois de instalado aparecerá como na figura abaixo na guia Installed Packages.



TransparentProxy: marcando essa opção o seu proxy será transparente. Não havendo a necessidade de configurações adicionais no navegador dos clientes.

Bypass proxy for these source IPs: Essa opção poderá ser preenchida caso haja a necessidade de um ou mais computadores na rede não passarem pelo proxy. Todo o acesso a esses dispositivos aqui cadastrados será liberados e não há nenhum tipo de filtro de acesso para esses endereços. Lembrem-se de usar o “;” para cadastrar mais de um endereço.

Enabled Logging: Habilitar essa opção para geração de logs de acesso/bloqueio que será lido pelo pacote Lightsquid.

Rotate Logs – define a qtd de dias em que os logs serão armazenados

Guia Cache Management

Hard Disk Cache Size: Aqui preenchemos o tamanho total do cache que será armazenado no disco rígido. Alterar o tamanho da Cache de disco, digamos 3000 ou 4000 (3GB ou 4GB), para acomodar os arquivos cacheados no disco. Lembrado de que não é recomendado deixar esse valor exceder o tamanho de 5000 (5GB) pois pode acarretar queda de desempenho.

Hard Disk Cache System: Sistema de arquivos que será usado pelo disco para armazenar os dados de cache. Deixe o padrão UFS.

Hard Disk Cache Location: Local de armazenamento do cache. Padrão /var/squid/cache.

MemoryCache Size: Tamanho reservado pelo sistema para alocar na memória os arquivos cacheados. Preencher esse campo com no máximo 50% de memória total de ser servidor. EX: servidor possui 1024MB de memória RAM. Nesse caso devemos usar no máximo 512MB de memória para cache. Lembre-se que MemoryCache Size e Hard Disk Cache Size são reservas de armazenamento porém trabalham de formas diferentes. Enquanto o primeiro armazena na memória RAM do servidor os arquivos cacheados o outro armazena em disco rígido os arquivos que são retirados da memória pelo squid.

MinimumObjectSize: Tamanho mínimo do objeto que será armazenado na memória RAM para cache. Padrão " 0 ".

Maximum ObjectSize: Tamanho máximo do objeto que será armazenado na memória RAM para cache. EX: ao preencher o campo com 40000 (40BM) todos os arquivos e downloads com o tamanho menor que 40BM será armazenado na memória até que a mesma fique cheia. Caso o arquivo tenha o valor maior que 40MB o mesmo será descartado pelo squid.

Maximum ObjectSizein RAM: Quantidade máxima de objetos armazenados dentro da memória Ramdo servidor. Padrão 32 objetos. EX: 40.000/32 = 1.250 objetos armazenados na memória para cache.

MemoryReplacementPolicy: A política de substituição de memória determina quais objetos são removidos da memória quando o espaço é necessário. A política padrão para troca de memória é GDSF.

Do NotCache: Aqui podemos preencher quais domínios, IP's que não serão cacheados pelo nosso servidor. EX: www.bb.com.br, 201.38.233.143, etc.

GUIA ACCESS CONTROL

AllowedSubnets: Aqui preenchemos a rede que usará o proxy. No exemplo acima a rede 192.168.105.0/24 é a rede cadastrada para tal finalidade. Lembrando de coloca o IP da rede e não o IP do servidor ou de outra máquina qualquer. Verificar no nosso exemplo que com a mascara é 255.255.255.0 ou /24 o endereço de rede é com o final .0/24. Se no nosso exemplo a rede fosse 192.168.105.xxx/25 onde teríamos o ip 192.168.105.128/25 representando nosso endereço de rede. Para maiores detalhes de cálculos visitar <http://www.joao.pro.br/aplicativos/netcalc.htm>

Blacklist: Aqui serão colocados as palavras chave de bloqueio por url. Todas palavra que estiver cadastrada e coincidir com a palavra digitada pelo host cliente no browser a mesma será bloqueada, não havendo assim a necessidade de preencher toda a url.

No Squid, na seção de Blacklists aceitam-se o uso de expressões regulares.

GUIA TRAFFIC MANAGER

Utiliz esta guia para definir limites para download e upload

Package / Proxy Server: Traffic Management / Traffic Mgmt

General

Remote Cache

Local Cache

Antivirus

ACLs

Traffic Mgmt

Authenticati

Squid Traffic Managment Settings

Maximum Download Size

Limit the maximum total download size to the size specified here (in kilobytes).
Set to 0 to disable.

Maximum Upload Size

Limit the maximum total upload size to the size specified here (in kilobytes).
Set to 0 to disable.

Overall Bandwidth Throttling

This value specifies the bandwidth throttle for downloads (in kilobytes per second).
Users will gradually have their download speed decreased according to this value.
Set to 0 to disable.

INSTALANDO ANTIVÍRUS NO PROXY

Será instalado o HAVP Antivírus na tela de packages.

Para Configurar o Antivirus devemos ir em Services | Antivirus | HttpProxy

- 1 Enable
- 2 Proxy Mode—Parent for Squid
- 3 Proxy interfaces —Lan
- 4 Language—Brasil
- 5 Enable Ram

Depois na guia Settings selecione qto tempo leva para ele atualizar a base de vírus.

Não consegui instalar e ele recomenda o CLAMAV. Depois verificar como se faz a instalação em squidclamav.darold.net

Acesse o site eicar.org e baixe um arquivo de teste com vírus que será exibida a mensagem com o bloqueio.

RELATÓRIOS DE ACESSO

Vamos baixar agora o LightSquid

Vá em Status | Proxy Report

Altere a Linguagem para Português do Brasil

Base Cor escolha uma cor

Report Schema deixa como NovoSea ou NovoPF

Refresh Scheduler deixe um tempo para geração automática (10 minutos)

Save e mande dar um Refresh Now

Ele vai gerar uma guia chamada Squid report com o relatório.

INSTALANDO O SARGE

Podemos instalar também o pacote Sarge e acessá-lo pelo menu Status → Sarge reports.

AUTENTICAÇÃO DE USUÁRIOS

Para configurar acesso autenticado devemos ir em Services | Proxy Services, selecionar a aba Auth Settings e escolher em Authentication method **Local**

“Authentication prompt”: Texto que vai ser exibido na janela que pede o usuário e a senha. **“Authentication processes”**: Número de autenticações simultâneas. Ajuste conforme preciso. **“Authentication TTL”**: Este campo define o tempo de vida da sessão de um usuário autenticado.

Nas configurações do proxy na aba **“Local Users”**, vamos cadastrar os usuários para utilizarmos no nosso exemplo. Para cadastrar um usuário clique no ícone correspondente.

Na tela que se abre, temos 2 campos obrigatórios: **“Username”** e **“Password”**. Já o campo **“Description”** é opcional, porém é muito útil para caráter administrativo. No nosso exemplo eu usei esse campo para definir qual departamento o usuário pertence. Clicamos em **“Save”** para finalizar essa etapa de cadastro.

AUTENTICAÇÃO DE GRUPOS

Vamos no menu **“Diagnostics > Edit File”**. No campo que aparece vamos digitar: **“/usr/local/pkg/squid.inc”** e apertar no botão **“Load”**. Uma vez conteúdo do arquivo carregado, vamos procurar (Control + F) pelo seguinte conteúdo: **“acl password proxy_auth REQUIRED”** (sem as aspas).

O SQUID.CONF É um arquivo que é utilizado para gerar o arquivo squid.conf qdo se inicia o sistema.

Definição ACLs dos Grupos com Seus Respectivos Usuários

```
acl COMERCIAL proxy_auth user "/var/squid/acl/usuarios_comercial.acl"
```

```
acl FINANCEIRO proxy_auth "/var/squid/acl/usuarios_financeiro.acl" acl ADMINISTRATIVO
```

```
proxy_auth "/var/squid/acl/usuarios_administrativo.acl"
```

Definição das ACLs dos Sites Liberados para Cada Grupo

```
acl SITES_COMERCIAL url_regex "/var/squid/acl/sites_comercial.acl"
acl SITES_FINANCEIRO url_regex "/var/squid/acl/sites_financeiro.acl"
acl SITES_ADMINISTRATIVO url_regex "/var/squid/acl/sites_administrativo.acl"
```

Liberação do Acesso para os Grupos

```
http_access allow password COMERCIAL SITES_COMERCIAL
http_access allow password FINANCEIRO SITES_FINANCEIRO
http_access allow password ADMINISTRATIVO SITES_ADMINISTRATIVO
http_access deny all
```

Agora salvamos o arquivo "**squid.inc**" alterado.

Iremos repetir os processos acima para os grupos restantes e suas respectivas listas de sites liberados:

Grupos:

```
/var/squid/acl/usuarios_financeiro.acl
/var/squid/acl/usuarios_administrativo.acl
```

Sites Liberados:

```
/var/squid/acl/sites_financeiro.acl
/var/squid/acl/sites_administrativo.acl
```

```
acl grupo1 proxy_authuserstato
acl grupo2 proxy_authuserjoao
acl sites1 url_regex -i pfsensestato
acl sites2 url_regex -i itauSantander
http_access allow sites1 grupo1
http_access allow sites2 grupo2
http_access deny all
```

O squid trabalha com #dstdomain,src , time, mime_type, ulr_regex, outros módulos autenticação, ntlm, pam_unix, ldap, etc...