

Instituto de Ensino Superior de Brasília - IESB

Projeto Integrador - Implementação de Segurança

Projeto de Segurança

Objetivo

Implementar uma rede de segurança para proteção de servidores web.

Justificativa

O avanço das tecnologias criou um novo cenário onde a maioria dos serviços são providos via web.

A proteção em várias camadas, aliada a boas políticas de rede trazem uma maior segurança as infraestruturas de servidores.

Se a normatização adota no Brasil e internacionalmente, no caso de sites que provêem serviços na internet, garantem uma padronização de configurações que garantirão o melhor desempenho das aplicações, a disponibilidade, confiabilidade e integridade das comunicações feitas com estes servidores.

Etapas

Será implementado um pfSense como firewall, um serviço de páginas web com o Apache 2 e um proxy reverso com o Squid.

Todos os servidores ficarão atrás do proxy Reverso e do Firewall.

Softwares Usados:

pfSense versão 2.4.3

Squid versão 4.2

Apache versão 2

Virtualbox versão 5.2.18

Instalação e configuração da infraestrutura

Foram instaladas quatro máquinas virtuais, sendo uma como firewall (pfSense), uma como proxy reverso (Debian 9), uma como servidor web (Debian 9) e uma como cliente (Debian 9).

Máquinas Virtuais:
Firewall - pfSense
Revproxy - Squid
WebServer - Apache
Clientedeb - Debian 9

Oracle VM VirtualBox Gerenciador

Arquivo (F) Grupo Ajuda (H)



Novo



Configurações



Descartar



Iniciar (T)

Detalhes

Ferramentas

Novo grupo

Projeto Integrador de Segurança



Firewall - pfSense



RevProxy - Squid



WebServer - Apache



clientedeb



Geral

Nome: Firewall - pfSense
Sistema Operacional: Other/Unknown (64-bit)
Grupos: Projeto Integrador de Segurança

Sistema

Memória Principal: 2048 MB
Ordem de Boot: Disquete, Óptico, Disco Rígido
Aceleração: VT-x/AMD-V, Paginação Aninhada, PAE/NX

Geral

Nome: RevProxy - Squid
Sistema Operacional: Debian (64-bit)
Grupos: Projeto Integrador de Segurança

Sistema

Memória Principal: 256 MB
Ordem de Boot: Disquete, Óptico, Disco Rígido
Aceleração: VT-x/AMD-V, Paginação Aninhada, Paravirtualização KVM

Geral

Nome: WebServer - Apache
Sistema Operacional: Debian (64-bit)
Grupos: Projeto Integrador de Segurança

Sistema

Memória Principal: 256 MB
Ordem de Boot: Disquete, Óptico, Disco Rígido
Aceleração: VT-x/AMD-V, Paginação Aninhada, Paravirtualização KVM

Geral

Nome: clientedeb
Sistema Operacional: Debian (64-bit)
Grupos: Projeto Integrador de Segurança

Sistema

Memória Principal: 2048 MB
Ordem de Boot: Disquete, Óptico, Disco Rígido
Aceleração: VT-x/AMD-V, Paginação Aninhada, Paravirtualização KVM

Virtual Box

Redes internas:

projeto1 - rede dos usuários 192.168.1.0/24

projeto2 - rede dos servidores 192.168.2.0/24



Configuração das Máquinas Virtuais

Firewall

Interfaces de rede:

Eth0 - 192.168.1.1

Eth1 - 192.168.2.1

Eth2 - Bridge na rede da máquina física para acesso a internet

A screenshot of the pfSense web configurator interface. The title bar reads 'Firewall - pfSense [Executando] - Oracle VM VirtualBox'. The main menu includes 'Arquivo', 'Máquina', 'Visualizar', 'Entrada', 'Dispositivos', and 'Ajuda'. Below the menu, it shows 'FreeBSD/amd64 (pfSense.localdomain) (ttyv0)'. The main content area displays the pfSense 2.4.3-RELEASE-p1 (amd64) configuration. It shows three interfaces: INTERNET (wan) connected to em2 with IP v4/DHCP4: 10.0.4.15/24; CLIENTES (lan) connected to em0 with IP v4: 192.168.1.1/24; and SERVIDORES (opt1) connected to em1 with IP v4: 192.168.2.1/24. A list of 16 numbered options is provided for management:

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

The message 'Enter an option:' is displayed at the bottom, followed by a log entry: 'Message from syslogd@pfSense at Sep 15 19:52:46 ... pfSense php-fpm[321]: /services_unbound.php: Successful login for user 'admin' from: 192.168.1.2'

Configurações de firewall(semanalmente revisadas):

- Bloqueado tráfego IPV4/IPV6 de pacotes com IPs inválidos na internet para saída pela porta Eth2.
- Bloqueado o tráfego IPV4/IPV6 TCP e UDP vindos da rede dos clientes diretamente para a rede dos servidores.
- Habilitado o tráfego IPV4/IPV6 TCP de toda rede de usuários pela porta 80 para a rede dos servidores
- Habilitado qualquer tipo de tráfego saindo e entrando para a interface Eth2 com destino a rede dos usuários.
- Habilitado saída de pacotes TCP e UDP da rede dos servidores para a rede dos clientes.

pfSense.localdomain - Firewall: Rules: INTERNET - Mozilla Firefox

Projeto Integrador: Implementar | +

Back Forward Stop Home 192.168.1.1/firewall_rules.php

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics

Firewall / Rules / INTERNET

Floating INTERNET CLIENTES SERVIDORES

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue
X	0 /57 KiB	*	RFC 1918 networks	*	*	*	*	*
X	0 /0 B	*	Reserved Not assigned by IANA	*	*	*	*	*
✓	0 /0 B	IPv4 TCP	CLIENTES net	*	INTERNET address	*	*	none

Add

i

pfSense is © 2004 - 2018 by Rubicon Communications, LLC (Netgate). All Rights Reserved.

[Terminal] pfSense.localdomain - F...

pfSense.localdomain - Firewall: Rules: CLIENTES - Mozilla Firefox

pfSense.localdomain - Fin X Projeto Integrador: Implementar X | +

← → C ⌂ 192.168.1.1/firewall_rules.php?if=lan

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnos...

Firewall / Rules / CLIENTES

Floating INTERNET CLIENTES SERVIDORES

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Sch...
<input checked="" type="checkbox"/>	2 /7.45 MiB	*	*	*	CLIENTES Address	80	*	*	
<input type="checkbox"/>	3 /37.82 MiB	IPv4 *	CLIENTES net	*	*	*	*	*	none
<input type="checkbox"/>	0 /0 B	IPv6 *	CLIENTES net	*	*	*	*	*	none

Add

i

pfSense is © 2004 - 2018 by Rubicon Communications, LLC (Netgate). All Rights Reserved.

[Terminal] pfSense.localdomain - F...

pfSense.localdomain - Firewall: Rules: SERVIDORES - Mozilla Firefox

pfSense.localdomain - Fin X Projeto Integrador: Implementar X | +

← → C ⌂ 192.168.1.1/firewall_rules.php?if=opt1

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnos...

Firewall / Rules / SERVIDORES

Floating INTERNET CLIENTES SERVIDORES

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue
	✓ 0 / 0 B	IPv6 *	SERVIDORES net	*	*	*	*	none
	✓ 4 / 5.76 MiB	IPv4 *	SERVIDORES net	*	*	*	*	none

Add

pfSense is © 2004 - 2018 by Rubicon Communications, LLC (Netgate). All Rights Reserved.

[Terminal] pfSense.localdomain - F...

The screenshot shows a Mozilla Firefox browser window with the URL `192.168.1.1/system_gateways.php`. The page title is "pfSense.localdomain - System: Routing: Gateways". The pfSense logo is visible in the top left. The main content area displays the "Gateways" section of the configuration. There are three tabs at the top: "Gateways" (which is selected), "Static Routes", and "Gateway Groups". Below is a table listing three gateways:

Name	Interface	Gateway	Monitor IP	Description
gw_clientes	CLIENTES	192.168.1.1	192.168.1.1	
gw_servers	SERVIDORES	192.168.2.1	192.168.2.1	
INTERNET_DHCP (default)	INTERNET	10.0.4.2	10.0.4.2	Interface

At the bottom of the page, a footer note reads: "pfSense is © 2004 - 2018 by Rubicon Communications, LLC (Netgate). All Rights Reserved". The browser's address bar shows the URL again, and the taskbar at the bottom includes icons for Terminal and the current tab.

Servidor Web

Enp0s3 - 192.168.2.10
Serviço Web rodando em Apache 2

WebServer - Apache [Executando] - Oracle VM VirtualBox

Arquivo Máquina Visualizar Entrada Dispositivos Ajuda

```
root@webserver:/var/www/html# service apache2 status
● apache2.service - The Apache HTTP Server
  Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor pres
  Active: active (running) since Sat 2018-09-15 19:22:30 EDT; 56min ago
    Process: 799 ExecStop=/usr/sbin/apachectl stop (code=exited, status=0/SUCC
    Process: 827 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCC
  Main PID: 831 (apache2)
    Tasks: 55 (limit: 4915)
   CGroup: /system.slice/apache2.service
           ├─831 /usr/sbin/apache2 -k start
           ├─832 /usr/sbin/apache2 -k start
           └─833 /usr/sbin/apache2 -k start

Sep 15 19:22:30 webserver systemd[1]: Starting The Apache HTTP Server...
Sep 15 19:22:30 webserver apachectl[827]: AH00558: apache2: Could not reliably
Sep 15 19:22:30 webserver systemd[1]: Started The Apache HTTP Server.
lines 1-15/15 (END)
```

Proxy Reverso

Enp0s8 - 192.168.2.100

Serviço de proxy reverso rodando em Squid

Regras do proxy reverso:

- Todo tráfego que chega pela porta 80 é verificado seu "payload" e entregue as informações solicitadas dos servidores requeridos.

RevProxy - Squid [Executando] - Oracle VM VirtualBox

Arquivo Máquina Visualizar Entrada Dispositivos Ajuda
GNU nano 2.7.4 File: squid.conf Modifi

```
# Squid normally listens to port 3128
http_port 192.168.2.100:80 vhost vport
...
cache_peer 192.168.2.10 parent 80 0 originserver default
...
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
http_access allow valid_dst
...
httpd_suppress_version_string on
```

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Li


Cliente

Enp0s3 - 192.168.1.2

clientedeb [Executando] - Oracle VM VirtualBox

Arquivo Máquina Visualizar Entrada Dispositivos Ajuda

Applications Places System



Computer



root's Home



Trash

Terminal

File Edit View Search Terminal Tabs Help

Terminal

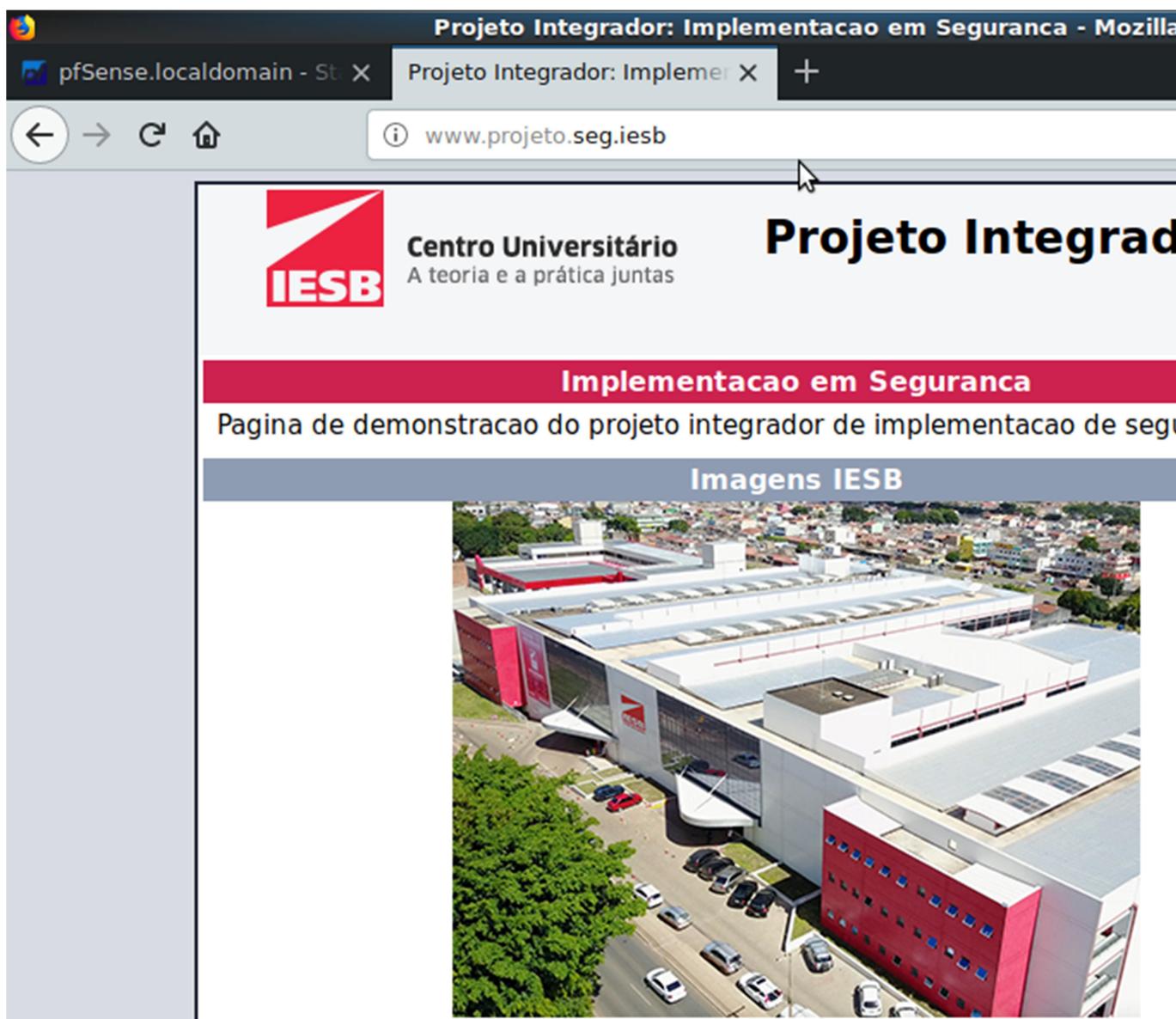
X

Terminal

```
root@cliente:~/Pictures# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UN
t qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pf
group default qlen 1000
    link/ether 08:00:27:83:f2:0b brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.2/24 brd 192.168.1.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe83:f20b/64 scope link
        valid_lft forever preferred_lft forever
root@cliente:~/Pictures#
```

Terminal

[Projeto Integrador: Imp...]



[Terminal]



Projeto Integrador: Impl...

Conclusão

Concluído o projeto todos os clientes somente acessarão os serviços por intermédio do proxy reverso. Todo tráfego vindo da interface dos usuários ou da internet será filtrado pelo firewall e repassado ao proxy reverso que intermediará as solicitações feitas aos servidores. Este tipo de implementação trás maior segurança para as aplicações que rodam

no servidor, garantindo
a disponibilidade para todos os usuários e maior performance dos serviços.