

Implantação - VM Cliente PoP

1. Implantação

1.1 Requisitos de Hardware recomendado

- 1 vCPU
- 1 GB RAM
- 10 GB HD
- 2 NICs, cada uma com um IP público
 1. Acesso remoto
 2. Testes isolados
- Sistema Operacional: GNU/Linux Debian 7
 - Utilizar hostname no seguinte formato: **client-pop-<Estado onde o cliente está sendo implantado>**
Ex: client-pop-go, client-pop-rj, client-pop-mg...

1.2 Processo de implantação

1. Subir a VM do cliente do PoP com os requisitos de hardware recomendados utilizando o software de virtualização a escolha;
2. Configurar as interfaces de rede da VM conforme especificado na seção 1.2.1;
3. Instalar os pacotes necessários listados na seção 1.2.2;
4. Configurar o firewall da VM conforme especificado na seção 1.2.3;
5. Configurar o servidor ssh conforme especificado na seção 1.2.4;
6. Criar uma conta ater conforme especificado na seção 1.2.5.

1.2.1 Configuração das interfaces de rede

1. Adote o seguinte padrão para as interfaces:

| Interface | Descrição |
|-----------|--|
| eth0 | Interface de acesso remoto para o cliente do PoP |
| eth1 | Interface de testes isolados do ATER |

Certifique-se que as bridges da VM do cliente do PoP estão configuradas para seguirem este padrão.

2. Para configurar as interfaces de rede no Debian 7 devemos modificar o arquivo de interfaces contido em "/etc/network/interfaces";
3. Abra o arquivo "/etc/network/interfaces" com o seu editor de preferência:

```
# nano /etc/network/interfaces
```

4. Configure o arquivo seguindo o seguinte padrão:

```

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# Interface de acesso remoto
auto eth0
iface eth0 inet static
address <IP público para acesso remoto>
netmask <Máscara do IP>
gateway <Gateway da rede>
dns-nameservers <Servidor de DNS primário> <Servidor de DNS secundário>

# Interface de testes isolados
auto eth1
iface eth1 inet static
address <IP público para testes isolados>
netmask <Máscara do IP>

```

Substitua as seguintes variáveis da interface eth0:

| | Descrição |
|--|---|
| <IP público para acesso remoto> | Endereço de IP público para o acesso remoto da VM do cliente do PoP |
| <Máscara do IP> | Máscara de subrede do IP público |
| <Gateway da rede> | Endereço IP do gateway para o acesso a internet |
| <Servidor de DNS primário> | Endereço do servidor de nomes primário |
| <Servidor de DNS secundário> | Endereço do servidor de nomes secundário (opcional) |

Substitua as seguintes variáveis da interface eth1:

| | Descrição |
|--|--|
| <IP público para acesso remoto> | Endereço de IP público para execução dos testes isolados do ATER |
| <Máscara do IP> | Máscara de subrede do IP público |

5. Após modificar o arquivo e deixá-lo de acordo com o padrão salve-o e feche o editor;
6. Reinicie as configurações de interface:

```
# /etc/init.d/networking restart
```

7. Efetue os seguintes testes:

| | Comando | Resultado esperado |
|---------------------------------|------------------------|--|
| Conexão com a internet | # ping 8.8.8.8 -c 5 | 5 packets transmitted, 5 received, 0% packet loss... |
| Resolução de nomes (DNS) | # ping google.com -c 5 | 5 packets transmitted, 5 received, 0% packet loss... |

1.2.2 Instalação dos pacotes necessários

1. Atualize a lista de repositórios do sistema:
 - a. No Debian 7 o arquivo de repositórios fica localizado em "/etc/apt/sources.list";
 - b. Abra o arquivo "/etc/apt/sources.list" com o seu editor de preferência:

```
# nano /etc/apt/sources.list
```

- c. Deixe o arquivo da seguinte forma:

```
deb http://ftp.br.debian.org/debian/ wheezy main
deb-src http://ftp.br.debian.org/debian/ wheezy main

deb http://security.debian.org/ wheezy/updates main
deb-src http://security.debian.org/ wheezy/updates main

# wheezy-updates, previously known as 'volatile'
deb http://ftp.br.debian.org/debian/ wheezy-updates main
deb-src http://ftp.br.debian.org/debian/ wheezy-updates main
```

- d. Assim que o arquivo estiver conforme acima, salve-o e feche o seu editor;
- e. Recarregue a sua lista de diretórios:

```
# apt-get update
```

2. Abaixo a lista de pacotes necessários para a implantação da VM do cliente do PoP:

| Nome do pacote | Descrição | Versão homologada |
|---------------------|---|-------------------|
| iptables | Regras de filtragem de tráfego (firewall) | 1.4.14-3.1 |
| iptables-persistent | Software para persistência das configurações das regras do iptables | 0.5.7 |

| | | |
|---------------|--|--------------------------|
| iperf | Software para transmissão de tráfego entre computadores | 2.0.5-3 |
| ssh | Cliente e servidor de secure shell | 1:6.0p1-4+deb7u2 |
| sudo | Provém poderes limitados de super-usuário (root) a usuários específicos | 1.8.5p2-1+nmu1 |
| ntp | Daemon para sincronismo do relógio | 1:4.2.6.p5+dfsg-2+deb7u1 |
| tcpdump | Ferramenta para análise de tráfego | 4.3.0-1+deb7u1 |
| tcptraceroute | Ferramenta para traçar rotas utilizando pacotes TCP | 1.5beta7+debian-4 |
| traceroute | Ferramenta para traçar a rota dos pacotes em redes IPv4 e IPv6 | 1:2.0.18-3 |
| mtr | Ferramenta de visualização Full screen do traceroute X11 e ncurses | 0.82-3 |
| ethtool | Ferramenta para visualização e configuração de interfaces de rede Ethernet | 1:3.4.2-1 |
| wget | Ferramenta para baixar arquivos da web | 1.13.4-3+deb7u2 |

3. Instale os pacotes necessários listados acima:

```
# aptitude install iptables iptables-persistent iperf ssh sudo ntp tcpdump
tcptraceroute traceroute mtr ethtool wget
```

1.2.3 Configuração do firewall

1. A política do firewall do cliente do PoP recomendada é de:

| Chave | Política |
|---------|--------------|
| INPUT | DROP [0:0] |
| FORWARD | ACCEPT [0:0] |
| OUTPUT | ACCEPT [0:0] |

2. Para configurar o firewall utilizando a ferramenta iptables no Debian 7 devemos modificar o arquivo "/etc/iptables/rules.v4";

3. Abra o arquivo "/etc/iptables/rules.v4" com o seu editor de preferência:

```
# nano /etc/iptables/rules.v4
```

4. Por padrão, seguindo a política descrita acima damos drop em todo pacote que tenta entrar no cliente do PoP, entretanto ele deve aceitar pacotes de:

| | Regra |
|----------------------------------|---|
| Rede local | -A INPUT -i lo -j ACCEPT |
| Rede do INF (UFG) | -A INPUT -s 200.137.197.192/26 -j ACCEPT |
| ICMP | -A INPUT -p icmp -j ACCEPT |
| NTP | -A INPUT -p udp --sport 123 -j ACCEPT |
| Conexões já estabelecidas | -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT |

Aconselhamos a liberar também a conexão para a rede da sua instituição.

5. No final, seu arquivo rules.v4 deve estar parecido com:

```
# Generated by iptables-save v1.4.14 on Tue Jan 20 14:00:00 2015
*filter
:INPUT DROP [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]

# localhost
-A INPUT -i lo -j ACCEPT

# redes e máquinas permitida
-A INPUT -s 200.137.197.192/26 -j ACCEPT

# icmp
-A INPUT -p icmp -j ACCEPT

# ntp
-A INPUT -p udp --sport 123 -j ACCEPT

# established
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# commit
COMMIT
# Completed on Tue Jan 20 14:00:00 2015
```

6. Após modificar o arquivo e deixá-lo de acordo com o padrão salve-o e feche o editor;
7. Para que as regras de firewall sejam aplicadas é necessário que seja dado um reload no iptables-persistent:

```
# /etc/init.d/iptables-persistent reload
```

8. Verifique se as regras foram aplicadas rodando o comando:

```
# iptables -L -n
```

9. Você deverá ter algo semelhante a:

```
Chain INPUT (policy DROP)
target prot opt source destination
ACCEPT all -- 0.0.0.0/0 0.0.0.0/0
ACCEPT all -- 200.137.197.192/26 0.0.0.0/0
ACCEPT icmp -- 0.0.0.0/0 0.0.0.0/0
ACCEPT udp -- 0.0.0.0/0 0.0.0.0/0 udp spt:123
ACCEPT all -- 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
```

1.2.4 Configuração do servidor SSH

1. Para configurar o servidor SSH no Debian 7 devemos modificar o arquivo "/etc/ssh/sshd_config";
2. Abra o arquivo "/etc/ssh/sshd_config" com o seu editor de preferência:

```
# nano /etc/ssh/sshd_config
```

3. Por padrão o cliente do PoP deve ter as seguintes configurações de SSH:

| Configuração | Valor |
|-----------------|-------|
| Port | 6622 |
| PermitRootLogin | no |
| UseDNS | no |

Caso o seu arquivo de configuração não tenha alguma das configurações, basta adicioná-la no final do arquivo.

4. No final, seu arquivo sshd_config deve ter algo semelhante a:

```
# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for

Port 6622

...

# Authentication:

...

PermitRootLogin no

...

UseDNS no
```

5. Após modificar o arquivo e deixa-lo de acordo com o padrão salve-o e feche o editor;
6. Para que as configurações entrem em vigor é necessário reiniciar o servidor ssh:

```
# /etc/init.d/ssh restart
```

1.2.5 Criação da conta ATER

1. Para criar uma conta no Debian 7 você pode utilizar o comando "useradd":

```
# useradd ater -m -s /bin/bash
```

2. A conta deve ter permissão de sudo (deve estar no grupo sudo);
 - a. Para adicionar o usuário no grupo sudo no Debian 7 devemos modificar o arquivo "/etc/group";
 - b. Abra o arquivo "/etc/group" com o seu editor de preferência:

```
# nano /etc/group
```

- c. Procure por algo como:

```
sudo:x:27:
```

O número 27 pode mudar para outro, este é apenas o identificador do grupo no seu sistema.

- d. Adicione o usuário ATER no grupo, para isto basta adicionar o nome do usuário no final da linha:

```
sudo:x:27:ater
```

Caso tenha múltiplos usuários eles devem estar separados por "," (vírgula), por exemplo:

```
sudo:x:27:ater,ater2
```

- e. Após a modificação, salve o arquivo e feche o seu editor;
- 3. Altere a senha da conta para uma senha qualquer (senha segura de preferência);
 - a. Para alterar a senha de um usuário no Debian 7 você deve utilizar o comando "passwd":

```
# passwd ater
```

- 4. Após a criação da conta encaminhe os dados de acesso a nossa equipe ATER.