LABORATÓRIO XIV

VIRTUAL PRIVATE NETWORKS

Redes de Computadores – Da Teoria à Prática com Netkit

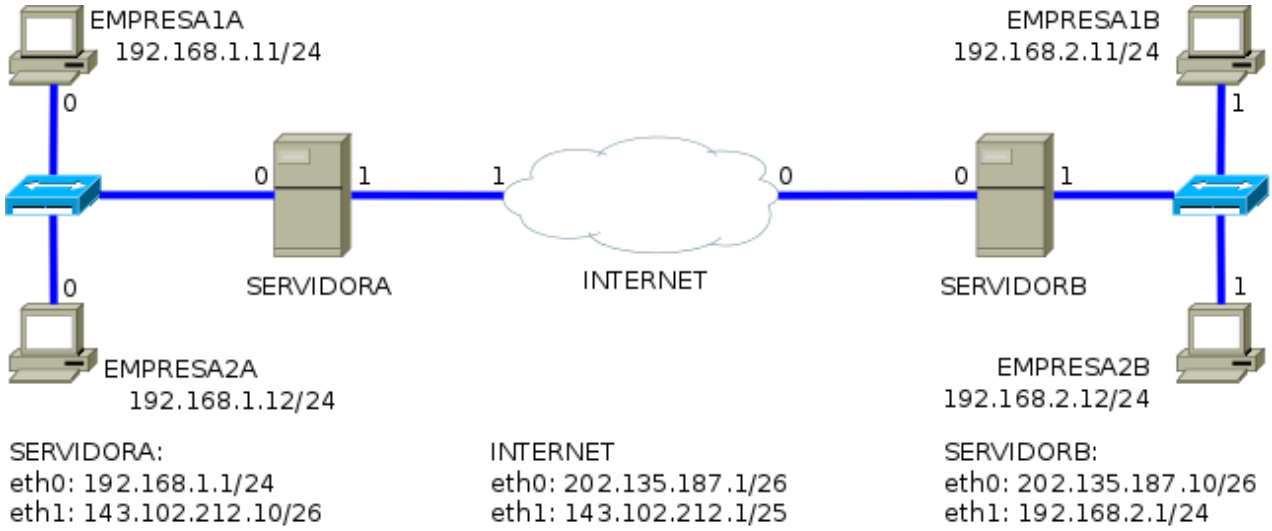
Laboratório XIV – Redes Privadas Virtuais.

Objetivos do laboratório

- Aprender sobre assinatura de chaves e assinaturas
- Compreender conceitos de redes privadas virtuais
- Configurar sistemas com openvpn

Cenário sendo reproduzido

O cenário proposto mostra a rede de duas empresas, redes Empresa A e Empresa B,sendo ligadas pela internet. É desejável que uma rede virtual unindo as duas empresas seja configurada. Uma configuração similar seria possível de realizar utilizando a própria residencia.



Durante a seção **execução do laboratório**, evite fazer experimentos para que os resultados sejam equivalentes aos da saída. Situações de erros são intencionais.

Conhecimentos que você irá adquirir

Ao completar este lab você estará familiarizado com a configuração básica de um sistema de VPN, através da ferramenta openvpn, bem como com a geração de assinaturas digitais.

Os comandos marcados com a tag [real] deverão ser executados no console real. Os demais comandos serão executados dentro das máquinas virtuais. Sempre que exigido a instrução pedirá uma máquina virtual específica.

Execução do laboratório

1. [real] Salve o arquivo netkit_lab14.tar.gz na sua pasta de labs. (/home/seu_nome/nklabs).

2. [real] Use o comando:
```
[seu_nome@suamaquina ~]$ tar -xf netkit_lab14.tar.gz
```
Ele irá criar a pasta lab14 dentro da sua pasta nklabs.

3. [real] Use o comando a seguir:
```
[seu_nome@suamaquina ~]$ lstart -d /home/seu_nome/nklabs/lab14
```

4. Verifique as regras dos firewalls dos servidores A e B com o comando a seguir. Observe que o compartilhamento de internet já foi efetuado.
```
$ iptables –L
```

5. Acione o tcpdump em uma das duas interfaces do micro INTERNET.

6. A partir do computador EMPRESA1A, crie um par de chaves para o usuário joaquim, com o seguinte comando.
```
$ su joaquim
# ssh-keygen -t rsa -b 2048
```

7. Acesse a pasta .ssh, oculta, na pasta do usuário joaquim.
```
# cd /home/joaquim/.ssh
```

8. Existirão dois arquivos, um arquivo id_rsa e outro, id_rsa.pub, que são as chaves privadas e públicas do usuário, respectivamente. Visualize o conteúdo das duas com o comando cat.
```
# cat id_rsa.pub
```

9. Copie o arquivo id_rsa.pub para sua pasta de usuário e depois, copie o arquivo de volta para a pasta do usuário joaquim do servidor. Você precisará sair do usuário “Joaquim” para efetuar este passo, pois o mesmo não terá permissões de escrita na pasta “hosthome”.
```
# cp id_rsa.pub /hosthome
$ su joaquim (a partir do ServidorA)
# cp /hosthome/id_rsa.pub /home/joaquim
```

10. Acrescente o conteúdo do arquivo id_rsa.pub no arquivo de chaves autorizadas. Será necessário criá-lo com o seguinte procedimento:
```
# mkdir /home/joaquim/.ssh
# touch /home/joaquim/.ssh/authorized_keys
# cat ~/id_rsa.pub >> /home/joaquim/.ssh/authorized_keys
```

11. Inicie o serviço SSH no SERVIDOR A, como root (necessário usar exit se estiver logado como Joaquim):
```
# /etc/init.d/ssh start
```

12. A partir do EMPRESA1A, acesse o serviço de ssh com o usuário joaquim. A senha de joaquim é 123joa:
```
# ssh joaquim@192.168.1.1
```

13. A partir do EMPRESA2A, acesse o serviço de ssh com o usuário joaquim. A senha de joaquim é 123joa:

```
# ssh joaquim@192.168.1.1
```

Se tudo correu bem, o computador EMPRESA1A pode acessar a rede sem necessidade de usar a senha. O comando ls mostrará os mesmos resultados.

14. No servidorA, que será a matriz, crie a chave do openvpn com a seguinte instrução:

```
# exit
$ openvpn --genkey --secret /etc/openvpn/minhavpn.key
```

15. Visualize o conteúdo da chave com o comando cat:

```
$ cat /etc/openvpn/minhavpn.key
```

16. Crie o arquivo matriz.conf na pasta /etc/openvpn, com o seguinte conteúdo:

```
remote 202.135.187.10
dev tun
ifconfig 10.0.0.1 10.0.0.2
cd /etc/openvpn
secret minhavpn.key
port 5000
user root
group root
comp-lzo
# Keep alive
ping 15
verb 3
```

17. Execute o sistema openvpn com a seguinte instrução:

```
$ openvpn --config /etc/openvpn/matriz.conf --daemon
```

18. Repita a configuração para o SERVIDORB. As principais diferenças:
A linha remote que deverá utilizar o IP externo do servidor A, e os IPs da linha ipconfig deverão ser invertidos.

19. Copie o arquivo de chave minhavpn.key para o SERVIDORB.

20. Faça o teste de comunicação com ping, entre o servidor A e o servidor B, através da rede 10.0.0.0

21. Se toda a rede foi configurada com sucesso, os computadores das redes A e B estarão em comunicação como se não houvesse a internet entre eles.

22. Caso encontre problemas, tente acrescentar a rota no SERVIDOR B

```
$ route add -net 192.168.2.0/24 gw 10.0.0.2
```

23. Caso encontre problemas, tente acrescentar a rota no SERVIDOR A

```
$ route add -net 192.168.1.0/24 gw 10.0.0.1
```

24. Neste momento, toda a configuração deve estar pronta e o sistema funcionando, caso não funcione, verifique os arquivos de configurações, endereçamento, rotas e chaves.

25. [real] Importante, não encerre o laboratório até concluir os exercícios. Depois disso, utilize:

```
[seu_nome@suamaquina ~]$ lhalt -d /home/seu_nome/nklabs/lab14
```

Exercícios

1. Pesquise outras ferramentas para montar uma vpn.
2. Existe um modo de comunicação chamado TLS, que faz a permuta de chaves. Pesquise e faça a configuração do modo TLS neste laboratório.
3. Qual a vantagem do uso do openvpn sobre o ssh?