Criando VPN's usando o OpenVPN.

Autoria de Matheus Cucoloto
25/09/2006
Última Atualização 28/09/2006

Neste artigo será apresentado a facilidade em que podemos criar redes virtuais privadas (VPN), utilizando o OpenVPN em vários sistemas Operacionais distintos. O OpenVPN se destaca pelo seu suporte a conexões atrás de NAT ou Firewall. Se o servidor se encontra em um ambiente desses é apenas necessário o redirecionamento da porta em que ele esta ouvindo, por padrão na 1194. Já no ambiente do cliente, se o mesmo se encontra em algum dos ambientes mencionados a única exigência é ter pelo menos sua conexão entre ele e o servidor de VPN liberada para que o cliente o servidor troquem informações e levantem a VPN.
Instalando o OpenVPN Bom, a instalação do OpenVPN no FreeBSD é simples, podemos utilizar o pkg_add ou então a arvore Ports. Aqui utilizaremos o Ports e de preferência atualizado.(matheus@internet1)~# cd /usr/ports/security/openvpn
(matheus@internet1)~# make install cleanSerá apresentado um Dialog sobre o PW_SAVE, não precisaremos desta opção então apenas confirmamos pressionando ENTER.Após a compilação e instalação podemos iniciar a configuração dos arquivos do OpenVPN.Configurando o OpenVPNPrimeiramente adicionamos a linha openvpn_enable="YES" e gateway_enable=”YES” no nosso arquivo rc.conf(matheus@internet1)~# echo openvpn_enable="YES" >> /etc/rc.conf
(matheus@internet1)~# echo gateway_enable="YES" >> /etc/rc.confDepois de instalado vamos alterar o nome do script de inicialização do OpenVPN no diretório /usr/local/etc/rc.d(matheus@internet1)~# cd /usr/local/etc/rc.d
(matheus@internet1)~# mv openvpn openvpn.shAgora criaremos o diretório de arquivos de configuração do OpenVPN:(matheus@internet1)~# mkdir -p /usr/local/etc/openvpn
(matheus@internet1)~# cd /usr/local/etc/openvpnCriada a pasta vamos criar o arquivo openvpn.conf e preenche-lo com as configurações necessárias.(matheus@internet1)~# ee openvpn.conf----------DADOS DO ARQUIVO----------

```
# Interface da VPN
dev tun
# Ouvir em que endereço (Esta comentado ouvirá em todos os ips)
;local a.b.c.d
# Ouvir em que porta
port 1194
# Protocolo TCP ou UDP
proto udp
# Tornar o servidor de VPN seu gateway padráo para a internet
# Rede e Classe de Rede entre Clientes e Servidor
server 10.8.0.0 255.255.255.0
# Arquivo aonde fica armazenado os ips dos clientes
ifconfig-pool-persist ipp.txt
# Certificados para a autenticação da VPN
ca /usr/local/etc/openvpn/easy-rsa/keys/ca.crt
cert /usr/local/etc/openvpn/easy-rsa/keys/servidorvpn.crt
key /usr/local/etc/openvpn/easy-rsa/keys/servidorvpn.key
dh /usr/local/etc/openvpn/easy-rsa/keys/dh1024.pem
# As rotas que o cliente deve pegar
push "route 192.168.0.0 255.255.255.0"
# Usar compressão na VPN
comp-lzo
# Reestabelece a conexão se por ventura a mesma falhar
ping-timer-rem
persist-tun
persist-key
# Rodar o OpenVPN como Daemon mas com privilégios de usuario nobody
group nobody
daemon
# não repetir muitas vezes o mesmo erro
mute 20
```

----------DADOS DO ARQUIVO----------

Criando os arquivos de CertificaçãoQuando instalamos o OpenVPN é criado no diretório /usr/local/share/doc/openvpn/ arquivos de exemplos vamos copiar deste local o diretório easy-rsa. Nesta pasta existe scripts que tornam a criação das chaves SSL facíl.(matheus@internet1)~# cd /usr/local/share/doc/openvpn
(matheus@internet1)~# cp -r easy-rsa /usr/local/etc/openvpn/
(matheus@internet1)~# cd /usr/local/etc/openvpn/easy-rsaBom, para quem não usa o shell SH, vai ter que usar pelo menos nesta parte para usar os scripts, pois os mesmos foram feitos para o SH e necessitam da shell ativa, para criar variáveis e coisas afins.(matheus@internet1)~# shVamos editar algumas variáveis contidos no arquivo vars.# ee

varsAs variáveis que nos interessa estão no final do arquivo e são as seguintes:

export KEY_COUNTRY=BR -> Pais;
export KEY_PROVINCE=PR -> Estado;
export KEY_CITY=CASCAVEL -> Cidade;
export KEY_ORG="VPN-BACKUP" -> Organização, empresa;
export KEY_EMAIL="matheuscucoloto@gmail.com"Alterando as mesmas evitamos repetir varias vezes a mesma informação. Agora podemos carregar as variáveis:# . vars
./clean-allCriando a CA, nesta parte será feita perguntas referentes as variáveis que editamos anteriormente e outras como “Organizational Unit Name” = comentário referente a empresa e “Common Name” = FQDN da maquina ex: srv-vpn2.dominio.com.br:# ./build-ca Criar chaves do Servidor, nesta parte será feito as mesmas perguntas do comando anterior mas adicionando mais 2 variáveis as mesmas não precisam necessariamente de informação:# ./build-key-server servidorvpn Criando as chaves do(s) cliente(s), neste caso criamos apenas 1, mas nada impede depois de você crie outras chaves, apenas deve diferenciar a variável “Common Name” de cada chave, para evitar problemas. “filialbh” é o nome que sera dado para a chave criada, altere conforme o seu ambiente. # ./build-key filialbhGerando parâmetros Diffie Hellman para o OpenVPN:# ./build-dh Feito todo este procedimento, podemos voltar ao nosso shell de preferência:# returnIniciando o servidor OpenVPNPara tornar nossa administração mais fácíl vamos informar ao syslog para ele logar todos os eventos do OpenVPN em um arquivo /var/log/openvpn.log(matheus@internet1)~# ee /etc/syslog.conf Adicione as seguintes informações neste arquivo:----------DADOS DO ARQUIVO----------!openvpn
. /var/log/openvpn.log----------DADOS DO ARQUIVO----------Criamos o arquivo:(matheus@internet1)~# touch /var/log/openvpn.log Agora vamos reiniciar o syslog:(matheus@internet1)~# /etc/rc.d/syslogd restartE iniciamos o OpenVPN:(matheus@internet1)~# /usr/local/etc/rc.d/openvpn.sh startVamos verificar se o serviço levantou:(matheus@internet1)~# sockstat -4l | grep openvpnPor Padrão o OpenVPN escuta na porta 1194 no protocolo UDP, mas nada impede que você use outra porta ou o protocolo TCP, apenas especifique no arquivo de configuração, mais informações você pode conseguir nos arquivos de exemplo na pasta /usr/local/share/doc/openvpn.Configurando o lado Cliente da coisaCliente FreeBSDSupondo que a maquina que ira se conectar ao nosso servidor de VPN seja um FreeBSD, instalamos o OpenVPN como fizemos anteriormente usando o Ports. Feita a instalação vamos seguir os passos seguintes:Criaremos o diretório de arquivos de configuração do OpenVPN:

(matheus@internet1-filialbh)~# mkdir -p /usr/local/etc/openvpn
(matheus@internet1-filialbh)~# cd /usr/local/etc/openvpnCriada a pasta vamos criar o arquivo openvpn.conf e preenche-lo com as configurações necessárias.(matheus@internet1-filialbh)~# ee openvpn.conf----------DADOS DO ARQUIVO----------
client
remote ipdoservidorvpn 1194
dev tun
comp-lzo
ca ca.crt
cert filialbh.crt
key filialbh.key
group nobody
daemon
verb 3
mute-replay-warnings
mute 20
----------DADOS DO ARQUIVO----------Feito o arquivo de configuração agora devemos buscar os arquivos de chave para fazer a autenticação da VPN. Necessitamos do arquivofilialbh.crt filialbh.key e ca.crt que foram criados anteriormente e estão em /usr/local/etc/openvpn/easy-rsa/keys no servidor que acabamos de criar. Estes arquivos devem ser copiados para a pasta /usr/local/etc/openvpn da máquina da filial. Cabe a você a forma de transportar o arquivo (scp, www, ftp, samba, disquete, cd, dvd e afins...), tenha certeza que esses arquivos estejam seguros, pois quem tiver essa chave poderá se autenticar na VPN.Adicionamos a linha openvpn_enable="YES" e gateway_enable=”YES” no nosso arquivo rc.conf(matheus@internet1-filialbh)~# echo openvpn_enable="YES" >> /etc/rc.conf
(matheus@internet1-filialbh)~# echo gateway_enable="YES" >> /etc/rc.confAlteramos o nome do script de inicialização do OpenVPN no diretório /usr/local/etc/rc.d(matheus@internet1-filialbh)~# cd /usr/local/etc/rc.d
(matheus@internet1-filialbh)~# mv openvpn openvpn.shE iniciamos o OpenVPN:(matheus@internet1-filialbh)~# /usr/local/etc/rc.d/openvpn.sh startAgora verificaremos se existe a interface e faremos um teste de ping em um host do outro lado:(matheus@internet1-filialbh)~# ifconfig tun0
tun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1500
inet 10.8.0.6 --> 10.8.0.5 netmask 0xffffffff
Opened by PID 56202
(matheus@internet1-filialbh)~# ping 192.168.254.254
64 bytes from 192.168.254.254: icmp_seq=0 ttl=64 time=1.665 ms
64 bytes from 192.168.254.254: icmp_seq=1 ttl=64 time=1.448 ms
64 bytes from 192.168.254.254: icmp_seq=2 ttl=64 time=1.379 msCliente WindowsSe temos do outro lado uma maquina

com Windows, precisaremos baixar o OpenVPN para windows no seguinte endereço:http://openvpn.net/download.htmlFeita a instalação, vamos ao Windows Explorer (ctrl+e), e navegamos até a pasta C:\Arquivos de programas\OpenVPN\config. Lá iremos criar um arquivo chamado openvpn.ovpn e preencheremos ele com o seguinte conteúdo:----------DADOS DO ARQUIVO----------client
remote ipdoservidorvpn 1194
dev tun
comp-lzo
ca ca.crt
cert filialbh.crt
key filialbh.key
group nobody
daemon
verb 3
mute-replay-warnings
mute 20
----------DADOS DO ARQUIVO----------Feito o arquivo de configuração agora devemos buscar os arquivos de chave para fazer a autenticação da VPN. Necessitamos do arquivofilialbh.crt filialbh.key e ca.crt que foram criadas anteriormente estão em /usr/local/etc/openvpn/easy-rsa/keys no servidor que acabamos de criar. Estes arquivos devem estar presentes na pasta C:\Arquivos de programas\OpenVPN\config da maquina Windows da filial. Cabe a você a forma de transportar o arquivo (scp, www, ftp, samba, disquete, cd, dvd e afins...), tenha certeza que esses arquivos estejam seguros, pois quem tiver essa chave poderá se autenticar na VPN.Depois disso já podemos levantar a VPN, clique com o botão direito do Mouse e selecione a opção “Start OpenVPN on this config file”. É possível também levantar a VPN utilizando o GUI que vem junto com a instalação, ele cria um ícone no canto do relógio, apenas 2 cliques e estará conectado.Para testarmos entre no DOS e digite ipconfig, lá ira aparecer uma nova conexão local ou um novo dispositivo com endereço IP e tudo mais, ai é só pingar o outro lado para verificar se a conexão esta OK.

ConclusãoO OpenVPN é uma solução bastante flexível, que pode auxiliar muito em ambientes com sistemas operacionais diferentes sem abrirmos mão da segurança e da redução de custos, pois o mesmo consegue trabalhar normalmente atrás de conexões NAT ou com Firewall. Com uma simples ADSL é possível estabelecer uma VPN.Matheus Cucoloto
email: matheuscucoloto@gmail.com