선결 요건
FreeBSD 10.2
루트 권한
1 단계 - 시스템 업데이트
설치를 시작하기 전에 시스템이 최신 버전인지 확인하십시오. 업데이트하려면 "freebsd-update"를 사용하십시오 :

```
freebsd-update fetch
freebsd-update install
```

2 단계 - OpenVPN 설치
"/ usr / ports / openvpn /"디렉토리에 freebsd 포트를 통해 열린 vpn을 설치하거나 "pkg"명령을 사용하여 바이너리 패키지 방법으로 설치할 수 있습니다. 이 튜토리얼에서는 pkg 명령을 사용합니다. 다음 명령으로 설치하겠습니다 :

```
pkg install openvpn
```

이 명령은 openvpn에 필요한 " easy-rsa "및 " lzo2 "패키지를 설치합니다.
3 단계 - 서버 인증서 및 키 생성
우리는 서버 키와 인증서를 생성하기위한 "easy-rsa"패키지가 필요하며 우리의 freebsd에 설치되어 있습니다.

이제 openvpn과 우리의 키를위한 새로운 디렉토리를 만드십시오 :

```
mkdir -p / usr / local / etc / openvpn /
```

그런 다음 "/ usr / local / share /"에있는 easy-rsa 디렉토리를 openvpn 디렉토리로 복사하십시오.

```
cp -R / usr / local / share / easy-rsa / usr / local / etc / openvpn / easy-rsa /
```

openvpn easy-rsa 디렉토리로 이동하여 "chmod"명령으로 모든 파일을 쓸모 없게 만듭니다.

```
cd / usr / local / etc / openvpn / easy-rsa /
chmod + x *
```

easy-rsa 디렉토리에 암호화 인증서를 생성해야합니다.

```
. ./vars
```

참고 : ./clean-all 을 실행하면 / usr / local / etc / openvpn / easy-rsa / keys에서 rm -rf를 수행하게됩니다.

```
./clean-all
```

다음으로 4 키와 인증서를 생성합니다.

CA (인증 기관) 키
서버 키 및 인증서
클라이언트 키 및 인증서
DIFFIE-HELLMAN 매개 변수 (SSL / TLS 연결의 서버 끝 부분에 필요)
ca.key 생성

easy-rsa 디렉토리에서 위의 명령을 실행하십시오.

./build-ca

주, 국가, 이메일 등에 관한 정보를 입력하십시오. "Enter"키를 눌러 기본값을 사용할 수 있습니다. 이 명령은 "keys /"디렉토리에 ca.key 및 ca.crt를 생성합니다.

서버 키 및 인증서 생성

"build-key-server nameofserverkey"를 사용하여 서버 키를 생성하십시오 . 우리는 서버 이름으로 " server "를 사용 합니다.

./build-key-server 서버

주, 국가, 이메일 등에 관한 정보를 입력하십시오. "Enter"키를 눌러 기본값을 사용할 수 있습니다. 모든 정보를 확인하려면 "y"를 입력하십시오.

클라이언트 키 및 인증서 생성

easy-rsa 디렉토리에서 "build-key nameofclientkey"명령으로 클라이언트 키와 인증서를 생성하십시오. 이 튜토리얼에서는 위 이름이 "클라이언트"를 사용합니다.

./build-key 클라이언트

주, 국가, 이메일 등에 관한 정보를 입력하십시오. "Enter"키를 눌러 기본값을 사용할 수 있습니다. 모든 정보를 확인하려면 "y"를 입력하십시오.

dh 매개 변수 생성

dh 매개 변수에 대한 freebsd 10.2의 기본 키 크기는 2048 비트 키입니다. 강력하지만 4096 비트 키를 사용하여보다 안전하고 강력하게 만들 수 있지만 핸드 셰이크 프로세스가 느려집니다.

./build-dh
DH 파라미터 생성, 2048 비트 안전 프라임, 제너레이터 2 이것은 오랜 시간이 걸릴 것입니다.

이제 모든 인증서는 키 디렉토리 (" / usr / local / etc / easy-rsa / keys / ") 아래에 만들어집니다. 마지막으로 키 디렉토리를 openvpn에 복사해야합니다.

cp -R keys ../../

cd ..
ll

총 40
drwxr-xr-x 4 뿌리 바퀴 512 Sep 21 00:57 easy-rsa
drwx ------ 2 뿌리 바퀴 512 Sep 21 00:59 키

4 단계 - OpenVPN 구성
이 단계에서는 이전에 만든 모든 키와 인증서로 openvpn을 구성합니다. "/ usr / local / share / examples / openvpn / sample-config-files /"디렉토리의 openvpn 구성 파일을 openvpn 디렉토리 "/ usr / local / etc / openvpn /"에 복사해야합니다.

c p

/usr/local/share/examples/openvpn/sample-config-files/server.conf/usr/local/etc/openvpn/server.conf
cd / usr / local / etc / openvpn /

다음으로, " server.conf "파일을 nano로 편집 하십시오. 그렇지 않다면, 명령으로 설치하십시오 :

pkg install nano

이제 파일을 편집하십시오.

nano -c server.conf

주 : 나노 편집기에서 행 번호 표시를 위해 -c를 입력 하십시오 .

에서 라인 (32) , 당신은 OpenVPN을 사용하는 포트를 구성해야합니다. 기본 포트를 사용합니다.

포트 1194

내가 UDP 프로토콜, 기본 구성, 라인 36 :

프로토콜 UDP

그런 다음 78 행으로 이동 하여 인증 기관 (CA), 서버 키, 클라이언트 키 및 dh 매개 변수를 구성합니다.

ca /usr/local/etc/openvpn/keys/ca.crt
cert /usr/local/etc/openvpn/keys/server.crt
키 /usr/local/etc/openvpn/keys/server.key #our 서버 키
dh /usr/local/etc/openvpn/keys/dh2048.pem

그리고 openvpn과 그 네트워크의 클라이언트가 사용하는 사설 IP를 설정하십시오 . 101 번 라인으로 가십시오 . 나는 기본 IP를 그대로 둘 것이다.

서버 10.8.0.0 255.255.255.0

마지막으로 280 행 의 로그 파일을 구성하십시오 . 로그 파일을 " / var / log / openvpn / "디렉토리에 저장합니다.

status /var/log/openvpn/openvpn-status.log

과의 라인 289 :

log /var/log/openvpn/openvpn.log

저장 및 종료. 그리고 이제 로그를 저장할 파일을 만드십시오.

mkdir -p / var / log / openvpn /
touch / var / log / openvpn / {openvpn, openvpn-status} .log

5 단계 - 포트 전달 활성화 및 OpenVPN을 시작에 추가
FreeBSD에서 포트 forwrding을 사용하려면 sysctl 명령을 사용할 수 있습니다 :

sysctl net.inet.ip.forwarding = 1

"rc.conf"파일을 편집하여 openvpn을 부팅 시간에 추가하십시오 :

nano rc.conf

아래 줄 끝에 추가 :

gateway_enable은 = "YES"
openvpn_enable = "YES"
openvpn_configfile = "/ usr / 지방은 / etc /하는 OpenVPN / server.conf"
openvpn_if = "탭"

저장 및 종료.

6 단계 - OpenVPN 시작
openvpn wit service 명령을 시작하십시오 :

서비스 openvpn start

openvpn이 사용하는 포트를 확인하여 openvpn이 실행 중인지 확인하십시오.

sockstat -4 -l

openvpn이 포트 1194 를 열고 사용하고 있음을 볼 수 있습니다 .

7 단계 - 클라이언트 구성
클라이언트로서 인증서 파일을 다운로드하십시오.

ca.crt
client.crt
client.key
이 세 파일을 홈 디렉토리에 복사하고 사용자 권한으로 사용 권한을 ssh로 로그인하도록 변경하십시오.

cd / usr / local / etc / openvpn / keys /
cp ca.crt client.crt 클라이언트. 키 / home / myuser /
cd / home / myuser /
chown myuser : myuser ca.crt client.crt client.key

그리고 클라이언트에 cetificate를 다운로드하십시오, 저는 scp 명령으로 다운로드 할 필요가 있기 때문에 여기에서 리눅스를 사용합니다 :

scp myuser@192.168.1.100 ~ ~ / ca.crt myvpn /
scp myuser@192.168.1.100 ~ ~ / client.crt myvpn /
scp myuser@192.168.1.100 ~ ~ / client.key myvpn /

클라이언트 파일 구성을 작성하십시오.

nano client.ovpn

아래 코드를 추가하십시오 :

클라이언트
dev에 tun
proto udp
원격 192.168.1.100 1194 # serverIP 및 openvpn에 의해 사용되는 포트
resolv-retry 무한
nobind
사용자 nobody
지속 키
persist-tun
mute-replay-warnings
ca ca.crt
cert client.crt
key client.key
ns-cert -type server
comp-lzo
동사 3

저장 및 종료.

이제 클라이언트에 속한 파일을 볼 수 있습니다.

어울리다

총 20K
-rw-r-r--. 1 myuser myuser 1.8K Sep 21 03:09 ca.crt
-rw-r - r--. 1 myuser myuser 5.4K Sep 21 03:09 client.crt
-rw -------. 1 myuser myuser 1.7K Sep 21 03:09 client.key
-rw-rw-r--. 1 myuser myuser 213 Sep 20 00:13 client.ovpn

8 단계 - OpenVPN 테스트
이것은 시간 테스트 openvpn입니다, 우리는 openvpn 파일과 openvpn 서버에 연결하십시오. 그리고 명령과 연결 :

cd myopenvpn /
sudo openvpn --config client.ovpn

그리고 우리는 vpn과 연결되어 있고 개인 IP도 있습니다 : 10.8.0.6.

Openvpn 성공적으로.

다른 테스트 :

freebsd 서버에서 클라이언트에 대해 개인용 IP를 ping합니다.

ping 10.8.0.6

클라이언트에서 openvpn 10.8.0.1을 실행하는 개인 IP로 freebsd 서버에 연결합니다.

ssh myuser@10.8.0.1

그리고 모든 것이 성공적으로 연결되었습니다.

결론

VPN 또는 가상 사설망은 공용 네트워크 (인터넷)의 안전하고 사적인 네트워크입니다. Openvpn은 가상 사설망 기술을 구현하는 오픈 소스 프로젝트이며 Openvpn은 트래픽을 보호하고 OpenSSL Libraries를 사용하여 암호화합니다. OpenVPN은 자신의 서버에 쉽게 설치 및 설치할 수 있으므로 온라인 "개인 정보 보호"를 보호하려는 경우이 솔루션이 가장 좋습니다.