SMK_HARAPAN BANGSA_Depok_OpenVPN_HARDENING_Stabil

📜 11. Pengujian OpenVPN

🚨 Install OpenVPN di Ubuntu Server 24.04.2 LTS

✅ 1. Update Sistem

Update paket agar semua repositori dan sistem up-to-date:

```
sudo apt update && sudo apt upgrade -y
```

✅ 2. Install OpenVPN dan Easy-RSA

Ubuntu 24.04 sudah punya paket `openvpn` dan `easy-rsa` di repo resmi:

```
sudo apt install openvpn easy-rsa -y
```

Paket ini juga akan otomatis menarik dependensi:

- `openssl`, `libssl`: TLS/SSL
- `lzo`, `lz4`: kompresi data
- `iptables`, `nftables`: NAT & routing
- `pkcs11-helper`, `libtirpc`: tambahan autentikasi/token support

✅ 3. Install Utility Tambahan (Opsional Tapi Disarankan)

```
sudo apt install net-tools iproute2 curl wget unzip tar firewalld -y
```

- `net-tools`: ifconfig, netstat, dll.
- `iproute2`: untuk `ip`, `ss`, dll.
- `firewalld`: manajemen firewall lebih mudah.
- `curl`, `wget`, `unzip`, `tar`: bantu download & ekstrak config/certs.

✅ 4. Aktifkan Kernel Module TUN/TAP

Pastikan interface virtual TUN aktif:

```
lsmod | grep tun
```

Kalau kosong, load manual:

```
sudo modprobe tun
```

Lalu pastikan modul selalu aktif:

```
echo 'tun' | sudo tee -a /etc/modules
```

✅ 5. Setup Easy-RSA dan Buat Sertifikat

```
make-cadir ~/openvpn-ca
cd ~/openvpn-ca
```

Inisialisasi PKI:

```
./easyrsa init-pki
./easyrsa build-ca
```

Generate request dan key server:

```
./easyrsa gen-req server nopass
./easyrsa sign-req server server
```

Generate Diffie-Hellman:

```
./easyrsa gen-dh
```

Generate TLS key untuk Hardening:

```
openvpn --genkey --secret ta.key
```

✅ 6. Salin Semua File ke Direktori OpenVPN

```
sudo cp pki/ca.crt pki/private/server.key pki/issued/server.crt ta.key
pki/dh.pem /etc/openvpn/server/
```

✅ 7. Buat File Konfigurasi Server

Contoh dasar file config:

```
sudo nano /etc/openvpn/server/server.conf
```

Isi contoh config minimal:

```
port 1194
proto udp
dev tun
ca ca.crt
cert server.crt
key server.key
dh dh.pem
auth SHA256
tls-auth ta.key 0
topology subnet
server 10.8.0.0 255.255.255.0
push "redirect-gateway def1 bypass-dhcp"
push "dhcp-option DNS 8.8.8.8"
keepalive 10 120
cipher AES-256-CBC
persist-key
persist-tun
status openvpn-status.log
verb 3
```

✅ 8. Aktifkan IP Forwarding

```
echo 'net.ipv4.ip_forward=1' | sudo tee -a /etc/sysctl.conf
sudo sysctl -p
```

✅ 9. Konfigurasi NAT dengan iptables

Ganti `enp0s3` dengan interface jaringan ke internet kamu (cek dengan `ip a`):

```
sudo iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o enp0s3 -j MASQUERADE
```

Biar persistent:

```
sudo apt install iptables-persistent -y
sudo netfilter-persistent save
```

✅ 10. Konfigurasi Firewall

```
sudo systemctl enable firewalld
sudo systemctl start firewalld

sudo firewall-cmd --add-port=1194/udp --permanent
sudo firewall-cmd --add-masquerade --permanent
sudo firewall-cmd --reload
```

✅ 11. Start dan Enable OpenVPN

```
sudo systemctl enable openvpn-server@server
sudo systemctl start openvpn-server@server
```

Cek status:

```
sudo systemctl status openvpn-server@server
```

✅ 12. Buat Client Certificate (dari ~/openvpn-ca)

```
cd ~/openvpn-ca
./easyrsa gen-req client1 nopass
./easyrsa sign-req client client1
```

Salin file ke direktori client config:

```
mkdir -p ~/client-configs/keys
cp pki/issued/client1.crt pki/private/client1.key pki/ca.crt ta.key
~/client-configs/keys/
```

✅ 13. Buat File `.ovpn` untuk Client (Windows)

```
mkdir -p ~/client-configs/files
nano ~/client-configs/files/client1.ovpn
```

Isi `.ovpn` file:

```
client
dev tun
proto udp
remote [IP_Public_atau_Bridged_IP_Server] 1194
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
auth SHA256
cipher AES-256-CBC
verb 3
key-direction 1

<ca>
...isi dari ca.crt...
</ca>
<cert>
...isi dari client1.crt...
</cert>
<key>
...isi dari client1.key...
</key>
<tls-auth>
...isi dari ta.key...
</tls-auth>
```

NOTE: File ini bisa langsung dikopi ke Windows Client dan dipakai di OpenVPN GUI.

✅ 14. Koneksi Antar VM dan Host

- **Bridged Adapter** di Ubuntu Server = dapat IP real dari router, bisa diakses Windows Host.
- **Host-Only Adapter** = akses lokal VM-host, cocok buat test tanpa koneksi luar.

Pastikan Windows Host:

- Sudah install OpenVPN GUI.
- File `.ovpn` disimpan di `C:\Users\<username>\OpenVPN\config\`.
- Jalankan OpenVPN GUI sebagai Administrator.

✅ Ringkasan Paket yang Diinstall di Ubuntu Server 24.04.2

```
sudo apt update && sudo apt install openvpn easy-rsa iptables-persistent \
    firewalld curl wget unzip tar net-tools iproute2 -y
```

Isi File: `/etc/openvpn/server/server.conf`

```
port 1194
proto udp
dev tun
ca ca.crt
cert server.crt
key server.key
dh dh.pem
auth SHA256
tls-auth ta.key 0
topology subnet
server 10.8.0.0 255.255.255.0
push "redirect-gateway def1 bypass-dhcp"
push "dhcp-option DNS 8.8.8.8"
keepalive 10 120
cipher AES-256-CBC
persist-key
persist-tun
status openvpn-status.log
verb 3
```

Isi File: `/root/client-configs/files/client1.ovpn`

```
/etc/openvpn/server/server.conf
port 1194
proto udp
dev tun
ca ca.crt
```

```
cert server.crt
key server.key
dh dh.pem
auth SHA256
tls-auth ta.key 0
topology subnet
server 10.8.0.0 255.255.255.0
push "redirect-gateway def1 bypass-dhcp"
push "dhcp-option DNS 8.8.8.8"
keepalive 10 120
cipher AES-256-CBC
persist-key
persist-tun
status openvpn-status.log
verb 3
root@ubuntu-server:/home/ubuntu/scripts# cat /root/client-
configs/files/client1.ovpn
client
dev tun
proto udp
remote 172.16.50.24 1194
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
auth SHA256
cipher AES-256-CBC
verb 3
key-direction 1

<ca>
-----BEGIN CERTIFICATE-----
MIIDQjCCAiqgAwIBAgIUarEfgBjvTNU8TNGR6ssKI2dkh1QwDQYJKoZIhvcNAQEL
BQAwEzERMA8GA1UEAwwIQ2hhbmdlTWUwHhcNMjUwNjExMDg1MjEzWhcNMzUwNjA5
MDg1MjEzWjATMREwDwYDVQQDDAhDaGFuZ2VNZTCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBANkSYh5zmys0QksCtPIQqrwqgd12JUyH+Q3bhfHOnVbBkzjb
5AolACTfMvA3iEdZaOQKU6M6pQlXctB7z8ZwoBcyA5pemG3VDsDWHt4f72sgir4t
FcxKXUeS/ipbx0Fiy1gsYFoOwI7whGRhSSquon56aFyGYRmDcS0wOPCGFmfVOUT6
pR5HGdS6Z3HFLh+aCEafWtIVIFCyse5TowUP+E1+6sSBSO2WpCdTK2XEhwTPiG7x
csnYjvF7YCfSCv3Lw+pFpqgKJeTu+gx3mj01w/8kzatR7swBEZMZY+jE7T5JJCz3
RJoagr7Tr6aiBAnNHMOdvUJsFzfHKHQXnlw2Fj8CAwEAAaOBjTCBijAdBgNVHQ4E
FgQUV1Km9ovtXb7Sr5AYTbPJZasKd6MwTgYDVR0jBEcwRYAUV1Km9ovtXb7Sr5AY
TbPJZasKd6OhF6QVMBMxETAPBgNVBAMMCENoYW5nZU1lghRqsR+AGO9M1TxM0ZHq
ywojZ2SHVDAMBgNVHRMEBTADAQH/MAsGA1UdDwQEAwIBBjANBgkqhkiG9w0BAQsF
AAOCAQEAhfVeU1nYBqaXNUCdYQvHj1F90rmY/mXD0xkQXzFm/L20atMHzRN/UWQj
LdbYtLA3TYa0Dp5aLkx2XPcybMAhU3r0RC8oDZpH2uECiaR8cKFGLX1B8bLSSVl+
VwLUvurGdsvDvboUqnHpxYCufEhlT2s0qTmf50ZZKUd90rXyQya453rZgOU0aGcU
yzyEguUWEW30kYERwfwk0Fc+WXk9qcNcI0NUCH/zbj1vL9YibcS77JaZVL43uxng
WMJ4FI3NprYegTuU8MhnqdPZRStpFYHX6zG4dKUyS8yj7Ote+TC6tltYOb+f/sD8
```

```
Mz9Tfj5hQikMCWZvSdA7SjGQkflAXA==
-----END CERTIFICATE-----
</ca>
<cert>
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            10:07:fb:dd:28:6c:0d:69:91:eb:ed:99:ca:90:6f:bf
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=ChangeMe
        Validity
            Not Before: Jun 11 08:53:34 2025 GMT
            Not After : Sep 14 08:53:34 2027 GMT
        Subject: CN=ChangeMe
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:82:73:b2:db:87:6c:a6:d5:c2:5c:de:17:50:fe:
                    a6:e3:a5:05:60:1a:a5:95:3c:91:5c:10:01:6a:9d:
                    53:53:70:4e:5c:e5:54:e5:98:0b:b9:84:ec:bf:6d:
                    46:0f:61:15:9e:d0:53:c8:26:37:c9:b1:4c:a2:79:
                    cc:7a:44:5c:e2:1e:d9:ac:d1:8d:19:86:d7:6f:4b:
                    5c:e4:03:91:84:60:1c:92:74:c1:ac:28:fd:05:b7:
                    4b:de:45:b3:85:cd:60:96:ec:56:32:61:5b:11:a1:
                    02:80:48:7a:6c:9e:a8:d3:ed:89:6a:76:ff:36:f1:
                    b4:0e:41:8c:82:81:9c:d8:a1:30:52:85:f9:5d:f6:
                    24:dd:d7:75:49:78:92:68:12:06:d1:4e:f0:26:fc:
                    fe:b9:c5:12:d7:5f:1c:44:ed:b0:92:d3:a2:25:e2:
                    6e:2b:c5:44:74:d7:65:33:42:e7:df:9a:d3:ac:57:
                    90:95:de:87:b3:d2:de:fd:64:b8:03:4e:4c:24:3e:
                    5a:2e:ce:73:f6:71:ab:e8:b4:f8:84:d9:a3:2a:39:
                    67:39:74:a0:f3:4d:c0:1b:5f:28:63:c7:cd:9c:85:
                    dd:08:6e:d6:d7:9f:6f:76:fd:fc:3f:54:80:f0:6e:
                    38:b3:05:f0:0e:2c:65:d5:c7:f1:a8:1e:d3:cd:6b:
                    ba:2d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Key Identifier:
                D6:2B:61:38:EE:E8:1C:48:78:70:1D:4E:9B:C5:DE:AF:94:C7:B2:41
            X509v3 Authority Key Identifier:

keyid:57:52:A6:F6:8B:ED:5D:BE:D2:AF:90:18:4D:B3:C9:65:AB:0A:77:A3
                DirName:/CN=ChangeMe

serial:6A:B1:1F:80:18:EF:4C:D5:3C:4C:D1:91:EA:CB:0A:23:67:64:87:54
            X509v3 Extended Key Usage:
```

```
                TLS Web Client Authentication
            X509v3 Key Usage:
                Digital Signature
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        69:92:fa:d3:f4:a4:7b:00:c5:a2:46:79:00:05:9e:12:ac:db:
        bf:29:c2:4d:c0:30:dd:83:6f:32:6d:7c:63:c8:6f:e6:82:d0:
        62:9b:47:9b:41:a4:4e:18:4a:06:54:3c:76:7d:a7:5c:3c:c6:
        23:36:5d:7f:59:06:13:a8:48:80:f8:8e:d3:3f:f6:f3:44:77:
        3f:86:05:9a:25:a8:a4:55:df:cf:49:e2:bd:4a:64:1c:34:c3:
        24:8c:e2:3a:ec:13:88:e4:29:94:a4:dc:b2:2f:04:f3:49:42:
        58:d8:c1:98:52:21:63:35:15:44:f0:f7:c9:bd:1c:61:66:b5:
        7f:81:37:3d:ed:0d:3a:6b:14:ea:e9:07:f3:05:73:37:6d:e3:
        36:de:a6:7f:a0:3c:14:d9:74:b6:14:0d:8e:15:21:76:7b:c5:
        ef:1b:c1:80:88:b4:cb:4b:f5:96:cf:54:c8:d9:f0:a2:a7:c4:
        61:57:1a:93:5c:1b:65:cc:93:d1:10:ef:35:0f:84:08:99:ca:
        94:b9:5f:65:6b:9e:98:a3:4a:8a:9f:6d:a8:d4:9a:57:8d:ca:
        e0:4f:02:5f:37:94:28:9b:7a:3a:af:9a:ca:bf:a6:a6:5a:de:
        27:ea:57:f2:3f:5d:33:61:ed:2a:a2:76:b3:eb:2c:01:23:9f:
        93:7b:a1:5b
-----BEGIN CERTIFICATE-----
MIIDUDCCAjigAwIBAgIQEAf73ShsDWmR6+2ZypBvvzANBgkqhkiG9w0BAQsFADAT
MREwDwYDVQQDDAhDaGFuZ2VNZTAeFw0yNTA2MTEwODUzMzRaFw0yNzA5MTQwODUz
MzRaMBMxETAPBgNVBAMMCENoYW5nZU1lMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAgnOy24dsptXCXN4XUP6m46UFYBqllTyRXBABap1TU3BOXOVU5ZgL
uYTsv21GD2EVntBTyCY3ybFMonnMekRc4h7ZrNGNGYbXb0tc5AORhGAcknTBrCj9
BbdL3kWzhc1gluxWMmFbEaECgEh6bJ6o0+2Janb/NvG0DkGMgoGc2KEwUoX5XfYk
3dd1SXiSaBIG0U7wJvz+ucUS118cRO2wktOiJeJuK8VEdNdlM0Ln35rTrFeQld6H
s9Le/WS4A05MJD5aLs5z9nGr6LT4hNmjKjlnOXSg803AG18oY8fNnIXdCG7W159v
dv38P1SA8G44swXwDixl1cfxqB7TzWu6LQIDAQABo4GfMIGcMAkGA1UdEwQCMAAw
HQYDVR0OBBYEFNYrYTju6BxIeHAdTpvF3q+Ux7JBME4GA1UdIwRHMEWAFFdSpvaL
7V2+0q+QGE2zyWWrCnejoRekFTATMREwDwYDVQQDDAhDaGFuZ2VNZYIUarEfgBjv
TNU8TNGR6ssKI2dkh1QwEwYDVR0lBAwwCgYIKwYBBQUHAwIwCwYDVR0PBAQDAgeA
MA0GCSqGSIb3DQEBCwUAA4IBAQBpkvrT9KR7AMWiRnkABZ4SrNu/KcJNwDDdg28y
bXxjyG/mgtBim0ebQaROGEoGVDx2fadcPMYjNl1/WQYTqEiA+I7TP/bzRHc/hgWa
JaikVd/PSeK9SmQcNMMkjOI67BOI5CmUpNyyLwTzSUJY2MGYUiFjNRVE8PfJvRxh
ZrV/gTc97Q06axTq6QfzBXM3beM23qZ/oDwU2XS2FA2OFSF2e8XvG8GAiLTLS/WW
z1TI2fCip8RhVxqTXBtlzJPREO81D4QImcqUuV9la56Yo0qKn22o1JpXjcrgTwJf
N5Qom3o6r5rKv6amWt4n6lfyP10zYe0qonaz6ywBI5+Te6Fb
-----END CERTIFICATE-----
</cert>
<key>
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQCCc7Lbh2ym1cJc
3hdQ/qbjpQVgGqWVPJFcEAFqnVNTcE5c5VTlmAu5hOy/bUYPYRWe0FPIJjfJsUyi
ecx6RFziHtms0Y0ZhtdvS1zkA5GEYBySdMGsKP0Ft0veRbOFzWCW7FYyYVsRoQKA
SHpsnqjT7Ylqdv828bQOQYyCgZzYoTBShfld9iTd13VJeJJoEgbRTvAm/P65xRLX
XxxE7bCS06Il4m4rxUR012UzQuffmtOsV5CV3oez0t79ZLgDTkwkPlouznP2cavo
tPiE2aMqOWc5dKDzTcAbXyhjx82chd0IbtbXn292/fw/VIDwbjizBfAOLGXVx/Go
HtPNa7otAgMBAAECggEAELz5sRNSTkHW24WfpkPWdBUjeG5S2rA30oE3PU/MdkNN
```

```
uruuRftZXceBfRpvR9/kH0mJxn+o3tdCBwLryrBk3pqowXTtzt2vXNdlptgSXtLa
N6yFgSqNNKONN4rn+v4cK6FNeg9l2QA4yu8BzlgZP4AWBrQYERu4R6//cGtjDaSK
Ihk6yI3XhUdto8M0AmFYudcBXT5ETgej9aYM+FvZbeu6HGrUnh66v0y4MEIoSayg
c1JXL+d1hfaZwnAXkxzB4tFVe8vcMcsrVWIeDeg6TAiYVc1gXxDhn3moQ198NQ7O
BCPcapRIPgSdebSPkgewik6bVWhAl713AWshWzEjnQKBgQC3rMejkvUjMQPg8hZI
CodyeCv9ju5u582mLfXZ3pGBQfhlQCHLB+frki7cgacMnqjacvPsKajF89ZRTgkb
oDCPCAeXhR/CU3LB7bWFZCnfULPZOCempa3DWqo5WRkBN7P8he7/qcEjotjE3IDe
TXZ+Hlf2anyuvQlrVCYvE3kPBwKBgQC10dCTDVJJ4jIUKwhOZYmCvwJGhPMVw0tb
kvlUeIpX/tYu62Lmg2LQ3NRT0GBxxZcoFBJfdebdUae/AJ3DrwB7hGpiLuScF9uI
4QvTsaZ5OXuuBQYJ99uTKeF7DQER2XqvMV75mPKTui5s/Mdbr2F48c1QAeQzL1Tk
rRscyTcsKwKBgApyuaiEY41s7FuPadUPREUusNHrn4SPixM46hNKpdxEdGzOCR4T
hQ3Rcvj4JxiArfo/L8DvXbpk9HwLhFkd86UvP79Ow0+6j3yYmQrNd9RMMu7YUukX
45qJPcWlW9bF5Gco9z9z2Ji+WrZYFLyQi30BHN/XjuAhwLdqQgHLicdhAoGAWJx9
Dm37oM6AoZunXK3XqsT0kvHQltarL2Id6bElm2UzdYJ6nOWDj09Qm9h+aHRoCrxd
h/CqJ0rYehoOyYPMtGYAgwFfoUNvVvJ3FSELhSEiydjg7JLDjKFoptPbpZtcU224
X+TOtHiUj8FSV7jNxGf0K/3//YIf2aMUB595KCkCgYB9l1vOa0DSrW+3UoGmfICx
3wVgWCEn6ERzlPfPKIdPfuPfm9EjRZYu1sTXnnzJMCfwi5Ind9rj0xhk+0w0vwW8
8sbROQ3mq//Brlkx5jHCuphireidcc5rsaO3TiuIgAIfSUc9RuED75thgAHS0jfM
dWV4ffd/LKZCG8wK/VZqMg==
-----END PRIVATE KEY-----
</key>
<tls-auth>
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
687f2cf005cb82f698ab223730a18243
d3d3effab09f5f5212412fdc5b2f0fa4
9d53b7a0acce9c7e88ad462276f5ba8b
884c1d91f45fc9b347a314953f83bba9
269ed7f82e9eedd404f89623fcd344aa
774e31f9d5f234fdf36058c5e5f026d2
27ccd0b056c339fcd6612168a07d96ef
064843434a0b1d2c78f06e43d0b2b01a
97ab256a622726a395eaba814d302f57
5bfe66980d7739f18b41f6e86f937201
a7bfa9bf1fba14662a142b3303841aa4
b5980921d85d99fcacca8b003e288f75
6db7a0f00443b3f8d5f018002d4c0e5d
509a2b435c9c2a2b1295347766e50f9d
1b38f84673f3b4d25f8f4fa39a9c9439
1988dfe4a4a919ce7c526d769667f697
-----END OpenVPN Static key V1-----
</tls-auth>
```

✅ Hasil Pengujian OpenVPN

```
root@ubuntu-server:/home/ubuntu/scripts# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    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 fq_codel state UP group default qlen 1000
    link/ether 08:00:27:c5:86:d3 brd ff:ff:ff:ff:ff:ff
    inet 172.16.50.24/24 metric 100 brd 172.16.50.255 scope global dynamic enp0s3
       valid_lft 1066sec preferred_lft 1066sec
    inet6 fe80::a00:27ff:fec5:86d3/64 scope link
       valid_lft forever preferred_lft forever
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
    link/none
    inet 10.8.0.1/24 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::89ac:6a4b:b9bd:e321/64 scope link stable-privacy
       valid_lft forever preferred_lft forever
root@ubuntu-server:/home/ubuntu/scripts#
```