# Openvpn Testing Scenarios in StromNode Environment

Keys:

<https://github.com/sureshkvl/HOWTOs/tree/master/openvpn>

Reference Document :

<https://github.com/sureshkvl/HOWTOs/blob/master/openvpn/config_examples.md>

Test Environement:

Stormnode is installed as KVM VM in ubuntu 14.04 Laptop. Latest Openvpn-storm is installed in the stormnode images.

# Test Scenario 1 :

One Server and Multiple Clients, authenticated via certificates). Clients all traffic will be directed to the Server.

StormNode1 will act as a server. Stormnode2,3 are Clients.

## Server Config:

POST <http://192.168.122.134:5000/openvpn/server>

{

"port": 7001,

"dev": "tun1",

"proto": "udp",

"ca": "ca.crt",

"dh": "dh1024.pem",

"cert": "server.crt",

"key": "server.key",

"server": "172.172.172.0 255.255.255.0",

"auth": "SHA1",

"cipher": "AES-256-CBC",

"comp-lzo": "no",

"keepalive": "3 15",

"management": "127.0.0.1 2020",

"max-clients": 254,

"mlock": true,

"persist-key": true,

"persist-tun": true,

"push": [ "comp-lzo no", "redirect-gateway def1", "dhcp-option 8.8.8.8","route-delay 5" ],

"rcvbuf": 262144,

"replay-window":"512 15",

"route": null,

"route-gateway": "172.172.172.1",

"script-security": "3 system",

"sndbuf": 262144,

"status": "/var/log/server-status.log",

"tls-cipher": "DHE-RSA-AES256-SHA",

"topology": "subnet",

"txqueuelen": 500,

"verb": 3,

"certificates": [{

"name":"ca",

"data":""

},

{

"name":"dh",

"data":"LS0tLS1CRUdJTiBESCBQQVJBTUVURVJTLS0tLS0NCk1JR0hBb0dCQUtjWGxIS2t5NC9JWTlkNldydkRheW5uMi96a3dqWDlFdDdjV2VKNVFhd1U4Q0pzcDI1RjdOWk8NCkJ3Z3AxNTh2NDRPQnNGWjloWU1lV3ZncGN3bXJpVk04Szhka244d1pTbUtTZlVBVnV0Z1prYU5wMUU3dG95cmINCldwQkc0WE1RKzBPcnRmTUJNSFpjcUNxMkFxZEhJM2hJcU96dHhKeGN0aDUxKzlRc2dMS3pBZ0VDDQotLS0tLUVORCBESCBQQVJBTUVURVJTLS0tLS0="

},

{

"name":"cert",

"data":""

},

{

"name":"key",

"data":""

}

]

}

## Client1 Config:

POST <http://192.168.122.125:5000/openvpn/client>

{

"client": true,

"remote": "192.168.122.134 7001",

"dev": "tun1",

"proto": "udp",

"ca": "ca.crt",

"dh": "dh1024.pem",

"cert": "client1.crt",

"key": "client1.key",

"cipher": "AES-256-CBC",

"comp-lzo": "no",

"persist-key": true,

"persist-tun": true,

"tls-cipher": "DHE-RSA-AES256-SHA",

"verb": 3,

"certificates": [{

"name":"ca",

"data":""

},

{

"name":"dh",

"data":"LS0tLS1CRUdJTiBESCBQQVJBTUVURVJTLS0tLS0NCk1JR0hBb0dCQUtjWGxIS2t5NC9JWTlkNldydkRheW5uMi96a3dqWDlFdDdjV2VKNVFhd1U4Q0pzcDI1RjdOWk8NCkJ3Z3AxNTh2NDRPQnNGWjloWU1lV3ZncGN3bXJpVk04Szhka244d1pTbUtTZlVBVnV0Z1prYU5wMUU3dG95cmINCldwQkc0WE1RKzBPcnRmTUJNSFpjcUNxMkFxZEhJM2hJcU96dHhKeGN0aDUxKzlRc2dMS3pBZ0VDDQotLS0tLUVORCBESCBQQVJBTUVURVJTLS0tLS0="

},

{

"name":"cert",

"data":""

},

{

"name":"key",

"data":""

}

]

}

## Client2 Config:

POST <http://192.168.122.236:5000/openvpn/client>

{

"client": true,

"remote": "192.168.122.134 7001",

"dev": "tun1",

"proto": "udp",

"ca": "ca.crt",

"dh": "dh1024.pem",

"cert": "client2.crt",

"key": "client2.key",

"cipher": "AES-256-CBC",

"comp-lzo": "no",

"persist-key": true,

"persist-tun": true,

"tls-cipher": "DHE-RSA-AES256-SHA",

"verb": 3,

"certificates": [{

"name":"ca",

"data":""

},

{

"name":"dh",

"data":"LS0tLS1CRUdJTiBESCBQQVJBTUVURVJTLS0tLS0NCk1JR0hBb0dCQUtjWGxIS2t5NC9JWTlkNldydkRheW5uMi96a3dqWDlFdDdjV2VKNVFhd1U4Q0pzcDI1RjdOWk8NCkJ3Z3AxNTh2NDRPQnNGWjloWU1lV3ZncGN3bXJpVk04Szhka244d1pTbUtTZlVBVnV0Z1prYU5wMUU3dG95cmINCldwQkc0WE1RKzBPcnRmTUJNSFpjcUNxMkFxZEhJM2hJcU96dHhKeGN0aDUxKzlRc2dMS3pBZ0VDDQotLS0tLUVORCBESCBQQVJBTUVURVJTLS0tLS0="

},

{

"name":"cert",

"data":""

},

{

"name":"key",

"data":""

}

]

}

## Test Scenario2 :

Site to Site to VPN using Preshared Staic KEY

Diagram : Same Test1 diagram

Site to Site VPN will be established between the Server (192.168.122.134) and the Client (192.168.122.125)

Server:

POST <http://192.168.122.134:5000/openvpn/server>

{

"dev": "tun1",

"local":"192.168.122.134",

"remote":"192.168.122.125",

"lport": 10000,

"rport": 10000,

"proto": "udp",

"keepalive": "10 60",

"persist-key": true,

"persist-tun": true,

"ifconfig": "10.20.10.1 10.20.10.2",

"secret" : "static.key",

"certificates": [{

"name":"secret",

"data":""

}]

}

Client 1:

POST <http://192.168.122.125:5000/openvpn/client>

{

"dev": "tun1",

"remote": "192.168.122.134",

"local": "192.168.122.125",

"lport":10000,

"rport":10000,

"proto": "udp",

"persist-key": true,

"persist-tun": true,

"ifconfig": "10.20.10.2 10.20.10.1",

"secret" : "static.key",

"certificates": [{

"name":"secret",

"data":""

}]

}