Ubuntu as a Gateway router and NAT and OpenVPN

vim /etc/sysctl.conf

הסר את הסימן #
לפני

#net.ipv4.ip_forward=1

אחרי

net.ipv4.ip_forward=1

הוסף את השורות הבאות ל

vim /etc/rc.local
iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE
iptables --append FORWARD --in-interface eth1 -j ACCEPT

חסימת פינג מהתחנה נחוצה

```
iptables -A OUTPUT -p icmp --icmp-type echo-request -j DROP
```

OR

```
iptables -A OUTPUT -p icmp --icmp-type 8 -j DROP
```

```
1  iptables -F
2  iptables --table nat --append POSTROUTING --out-interface eth0 -j
3  MASQUERADE
4  iptables --append FORWARD -p icmp -i eth1 --icmp-type echo-request -j
5  DROP
   iptables --append FORWARD --in-interface eth1 -j ACCEPT
   iptables -A INPUT -p icmp -i eth1 --icmp-type echo-request -j DROP
```

הסבר
לפי מספרי השורות:

1. מחיקת/ניקוי כל חוקי חומת האש.
2. **איפשור טכנולוגיית NAT דרך כרטיס הרשת eth0.**
3. **חסימת פינג מהראוטר החוצה.**
4. **איפשור יציאה החוצה (גלישה בכל הפורטים לכל תחנות הקצה)**
5. **חסימת פינג לשרת עצמו**

התקנת OpenVPN

```
apt-get install openvpn

mkdir /etc/openvpn/easy-rsa/

cp -r
/usr/share/doc/openvpn/examples/easy-rsa/2.0/* /etc/openvpn/easy
-rsa/
sudo chown -R $USER /etc/openvpn/easy-rsa/
```

ערוך את הקובץ

```
vim /etc/openvpn/easy-rsa/vars

export KEY_COUNTRY="US"
export KEY_PROVINCE="NC"
export KEY_CITY="Winston-Salem"
export KEY_ORG="Example Company"
export KEY_EMAIL="steve@example.com"
```

Enter the following to create the server certificates:

```
cd /etc/openvpn/easy-rsa/
source vars
./clean-all
./build-dh
./pkitool --initca
./pkitool --server server
cd keys
openvpn --genkey --secret ta.key
cp server.crt server.key ca.crt dh1024.pem ta.key /etc/openvpn/
```

יצירת משתמשים

```
cd /etc/openvpn/easy-rsa/
source vars
./pkitool hostname

groupadd nobody
```

server.conf

```
local 10.23.198.32
port 1194
proto udp
;dev tun
dev tap

ca /etc/openvpn/easy-rsa/keys/ca.crt
cert /etc/openvpn/easy-rsa/keys/server.crt
key /etc/openvpn/easy-rsa/keys/server.key    # This file should be kept secret
dh /etc/openvpn/easy-rsa/keys/dh1024.pem
client-to-client                # To allow clients to see each other
server 10.200.0.0 255.255.255.0      # Set to virtual network and subnet mask
ifconfig-pool-persist ipp.txt
push "route 192.168.0.0 255.255.255.0"
push "dhcp-option DNS 10.200.0.1"
push "dhcp-option DOMAIN benory.com";
push "dhcp-option SEARCH benory.com";
push "dhcp-option ROUTE 10.200.0.1";
keepalive 10 120
cipher AES-128-CBC   # AES
comp-lzo
persist-key
persist-tun
user nobody
group nobody
status openvpn-status.log
#crl-verify crl.pem
verb 3
```

Client Windows

## #####	client ;dev tun
# Sample client-side OpenVPN 2.0 config file #	**dev tap**
# for connecting to multi-client server. #	dev-node MyTap
# #	proto udp
# This configuration can be used by multiple #	remote 10.23.198.32 1194 # use real name
# clients, however each client should have #	or IP address of the server
# its own cert and key files. #	resolv-retry infinite
# #	nobind
# On Windows, you might want to rename this #	persist-key
# file so it has a .ovpn extension #	persist-tun

```
############################################
#####

# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client

# Use the same setting as you are using on
# the server.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
dev tap
;dev tun

# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel
# if you have more than one.  On XP SP2,
# you may need to disable the firewall
# for the TAP adapter.
dev-node MyTap
#tls-auth ta.key 1
# Are we connecting to a TCP or
# UDP server?  Use the same setting as
# on the server.
;proto tcp
proto udp

# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
;remote 10.8.1.2
remote 10.23.198.32
;remote my-server-2 1194

# Choose a random host from the remote
# list for load-balancing.  Otherwise
# try hosts in the order specified.
;remote-random

# Keep trying indefinitely to resolve the
# host name of the OpenVPN server.  Very useful
# on machines which are not permanently
connected
# to the internet such as laptops.
resolv-retry infinite

# Most clients don't need to bind to
# a specific local port number.
nobind

# Downgrade privileges after initialization
```

```
ca ca.crt
cert ttt.crt
key ttt.key
cipher AES-128-CBC   # AES
comp-lzo
verb 3
```

סקריפט לשינוי ה
DNS Suffix

```
strComputer = "."
arrNewDNSSuffixSearchOrder =
Array("example.com")

Set objWMIService =
GetObject("winmgmts:" _
 & "{impersonationLevel=impersonate}!\\" &
strComputer & "\root\cimv2")
Set colNicConfigs =
objWMIService.ExecQuery _
 ("SELECT * FROM
Win32_NetworkAdapterConfiguration WHERE
IPEnabled = True")

Set objNetworkSettings = _
 objWMIService.Get("Win32_NetworkAdapter
Configuration")
intSetSuffixes = _
 objNetworkSettings.SetDNSSuffixSearchOrd
er(arrNewDNSSuffixSearchOrder)
```

```
(non-Windows only)
;user nobody
;group nobody

# Try to preserve some state across restarts.
persist-key
persist-tun

# If you are connecting through an
# HTTP proxy to reach the actual OpenVPN
# server, put the proxy server/IP and
# port number here.  See the man page
# if your proxy server requires
# authentication.
;http-proxy-retry # retry on connection failures
;http-proxy [proxy server] [proxy port #]

# Wireless networks often produce a lot
# of duplicate packets.  Set this flag
# to silence duplicate packet warnings.
;mute-replay-warnings

# SSL/TLS parms.
# See the server config file for more
# description.  It's best to use
# a separate .crt/.key file pair
# for each client.  A single ca
# file can be used for all clients.
ca "f:\\program files\\openvpn\\config\\ca-ns.crt"
cert "f:\\program
files\\openvpn\\config\\benor-ns.crt"
key "f:\\program
files\\openvpn\\config\\benor-ns.key"

# Verify server certificate by checking
# that the certicate has the nsCertType
# field set to "server".  This is an
# important precaution to protect against
# a potential attack discussed here:
#  http://openvpn.net/howto.html#mitm
#
# To use this feature, you will need to generate
# your server certificates with the nsCertType
# field set to "server".  The build-key-server
# script in the easy-rsa folder will do this.
;ns-cert-type server

# If a tls-auth key is used on the server
# then every client must also have the key.
; tls-auth ta.key 1

# Select a cryptographic cipher.
# If the cipher option is used on the server
```

# then you must also specify it here. ;cipher x # Enable compression on the VPN link. # Don't enable this unless it is also # enabled in the server config file. comp-lzo # Set log file verbosity. verb 5 # Silence repeating messages ;mute 20 ;remote-cert-tls server	