Routing IPSec Tunnels to OpenVPN networks using OpenSWAN.

Lance Buttars

http://www.obscuritysystems.com/

OpenVPN and IPSec

- OpenVPN is not compatible with IPSec!
- OpenVPN != IPSec
- VPN does not always mean using IPSec
  - (but that is what the majority thinks)
- Using OpenSWAN you can bridge an OpenVPN network to a IPSec tunnel.

OpenVPN vs IPSec

OpenVPN

- Client Server
- Single Port
  - You pick the port
- Easy to setup.
- Easy to Troubleshoot
- More Secure than a standard PSK 3-DES
- Works in OpenVZ

IPSec

- Peer to Peer
- Multiple Ports
  - 50 for ESP or AH
  - 500 for ISAKMP
  - 4500 for NAT-T
- Does not work well with NAT
- Complicated
- Mostly uses PSK which can become outdated.
- Does not work in OpenVZ

OpenVPN Positive

- Easy RSA scripts can quickly and easily create certificates to issue connectivity.
- Server / Client infrastructure one point controls configuration and forces all others to comply.
- Uses a single port can switch between UDP and TCP.
- Compression can lead to faster Internet Connections.
- NAT is not a problem for OpenVPN.

OpenVPN Negative

- Not supported with most equipment.
- Not compatible with IPsec.
- Not understood well by people who don't use it.
- No RFC Number as of yet.

IPSec Positive

- Works on older equipment.
- Most places already have one version of it or another.
- Secure if setup correctly.
- RFC standard.

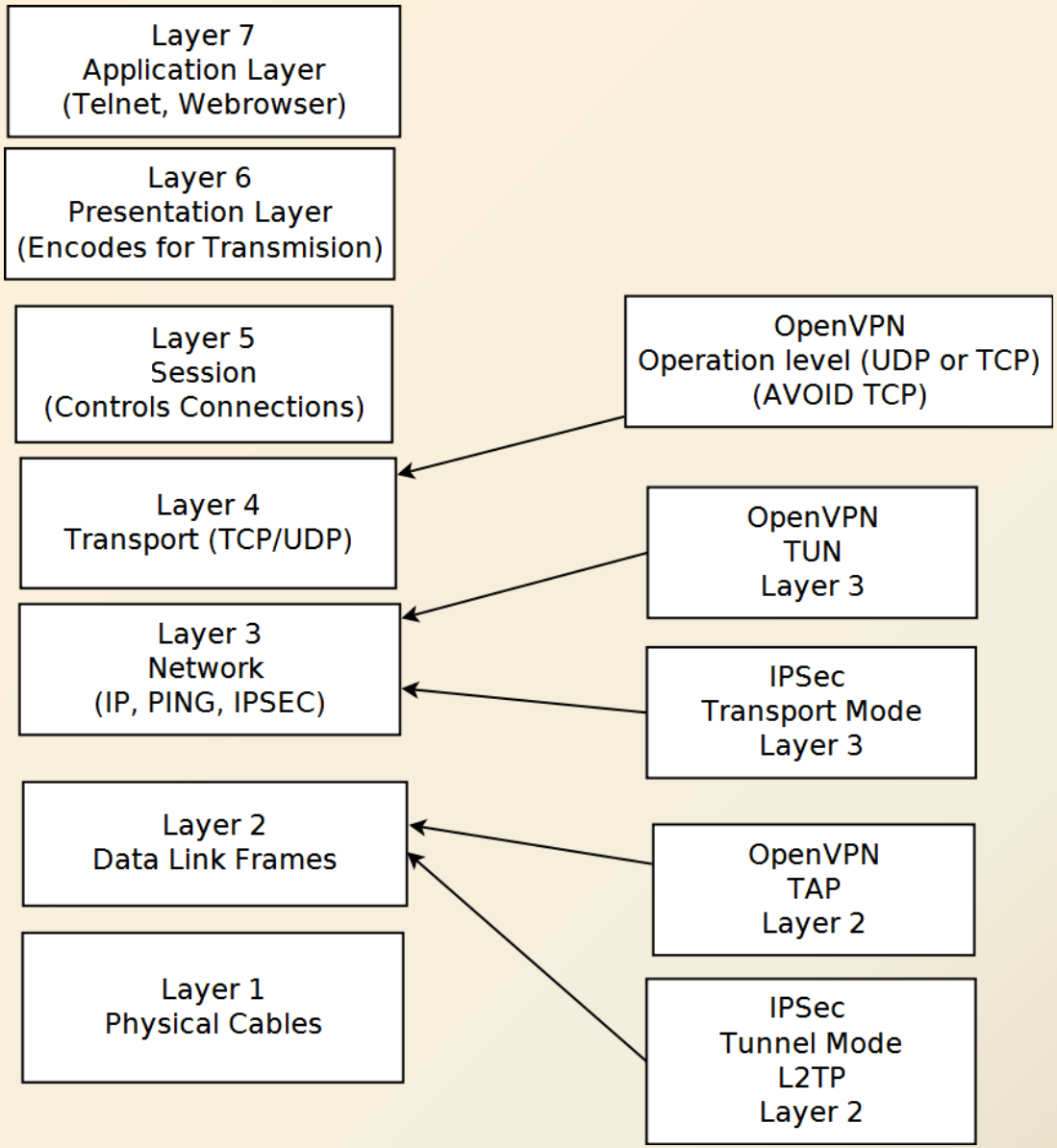
IPSec Negatives

- Hard to configure.
- Too many options.
- Hates NAT and NAT hates it.
- Peer to Peer architecture makes connection setup between two parties difficult.
- PSK results in insecure communication channels.
- Not compatible with OpenVPN.
- L2TP required for road warrior setup.

PPTP
(Point-to-Point Tunneling Protocol)

- DON'T USE IT!
- Requires GRE which can cause configuration issues.
- Can easily be broken by capturing DataStream.
- Lack of Two face authentication.
- After learning OpenVPN you will never need it.
- Uses MSCHAP2

ISO Layers


Layer 7
Application Layer
(Telnet, Webrowser)
Layer 6
Presentation Layer
(Encodes for Transmision)
Layer 5
Session
(Controls Connections)
Layer 4
Transport (TCP/UDP)
Layer 3
Network
(IP, PING, IPSEC)
Layer 2
Data Link Frames
Layer 1
Physical Cables
OpenVPN
Operation level (UDP or TCP)
(AVOID TCP)
OpenVPN
TUN
Layer 3
IPSec
Transport Mode
Layer 3
OpenVPN
TAP
Layer 2
IPSec
Tunnel Mode
L2TP
Layer 2

OpenVPN Setup

- **Debian Path**
- **cd /usr/share/doc/openvpn/examples/easy-rsa/2.0/**

- **vim vars (Edit file)**
  - **Fill this file out like a form**
- **Source var**
  - **Loads environmental settings**
- **./clean-all**
  - **WARNING: Only run once cleans key directory**
- **./build-ca**
  - **Builds a Certificate Authority**
- **./build-key-server server**
  - **Builds OpenVPN server certificate and key**
- **./build-key client1**
  - **Builds client key and certificate**
- **./build-dh**
  - Diffie-Hellman

Security Files

- ca.crt
  - Given to every client to use to validate connection.
- ca.key
  - Keep Private (Keys to the VPN Kingdom)
- dh{n}.pem
  - server only Diffie Hellman parameters
- server.crt
  - Server Certificate
- server.key
  - Server Key
- client1.crt
  - Certificate for client
- client1.key
  - Key for client key private for client used to connect.

Open Settings /etc/openvpn/server.conf

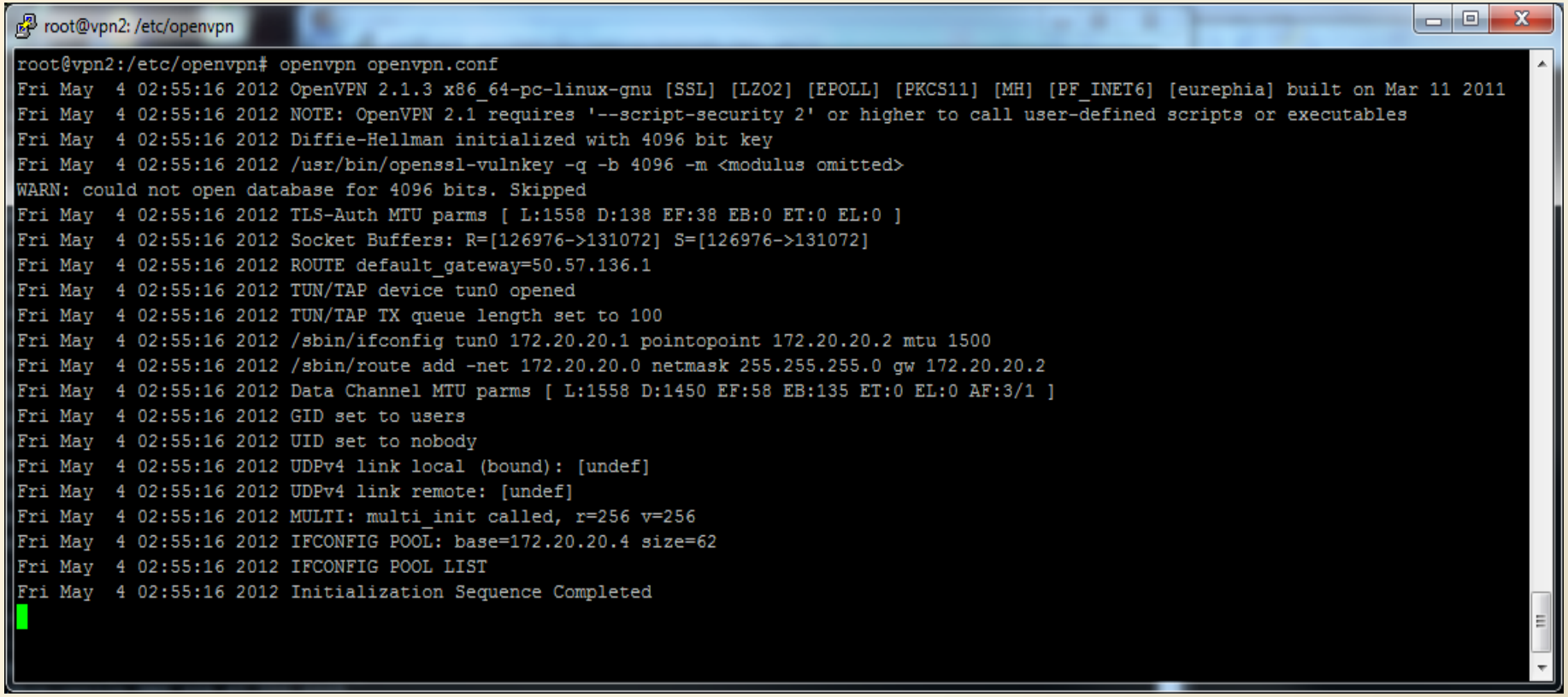
- port 1923
  - Port Used to connect to Server
- proto udp
  - proto tcp /udp
    - ALWAYS USE UDP IF YOU CAN
      - TCP does not work well with tcp over tcp.
- dev tun
  - TAP/TUN
    - Type of VPN Tunnel Layer 3 or Layer 2
- ca /etc/openvpn/ca.crt
  - Certificate Path
- cert /etc/openvpn/test.crt
  - Certificate for Server
- key /etc/openvpn/test.key
  - Key for server
- dh /etc/openvpn/dh2048.pem
  - Dihellmen key for server

OpenVPN Setting Part 2

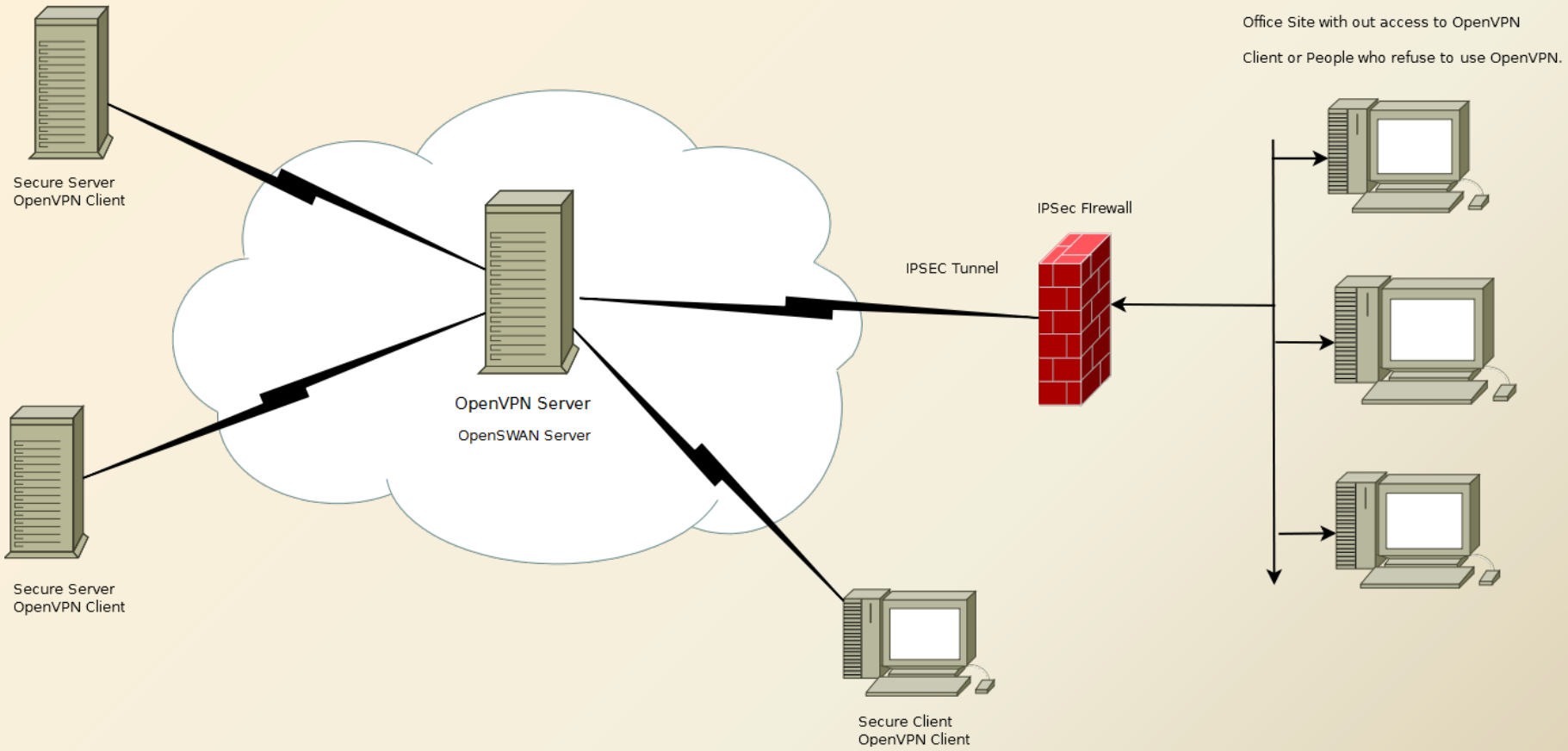
- server 172.16.x.x 255.255.255.0
  - Ip address pool
- ifconfig-pool-persist ipp.txt
  - Ip address pool log
- keepalive 10 120
  - Pings to check to see if other side is still up
- comp-lzo
  - Use comp-lzo compression
- user nobody
  - Service user
- group users
  - Service group
- status openvpn-status.log
  - verb 3

OpenVPN Setting Part 3

- client-to-client
- push "redirect-gateway def1 bypass-dhcp“
  - Only use if your setting up road warrior NATt’ed setup will change default gateway for all clients
- push "dhcp-option DNS 208.67.222.222"
- push "dhcp-option DNS x.x.x.1"
- push "route 172.x.x.0 255.255.255.0"
- push "route 10.x.x.0 255.255.225.0


root@vpn2: /etc/openvpn
root@vpn2:/etc/openvpn# openvpn openvpn.conf
Fri May 4 02:55:16 2012 OpenVPN 2.1.3 x86_64-pc-linux-gnu [SSL] [LZO2] [EPOLL] [PKCS11] [MH] [PF_INET6] [eurephia] built on Mar 11 2011
Fri May 4 02:55:16 2012 NOTE: OpenVPN 2.1 requires '--script-security 2' or higher to call user-defined scripts or executables
Fri May 4 02:55:16 2012 Diffie-Hellman initialized with 4096 bit key
Fri May 4 02:55:16 2012 /usr/bin/openssl-vulnkey -q -b 4096 -m <modulus omitted>
WARN: could not open database for 4096 bits. Skipped
Fri May 4 02:55:16 2012 TLS-Auth MTU parms [L:1558 D:138 EF:38 EB:0 ET:0 EL:0]
Fri May 4 02:55:16 2012 Socket Buffers: R=[126976->131072] S=[126976->131072]
Fri May 4 02:55:16 2012 ROUTE default_gateway=50.57.136.1
Fri May 4 02:55:16 2012 TUN/TAP device tun0 opened
Fri May 4 02:55:16 2012 TUN/TAP TX queue length set to 100
Fri May 4 02:55:16 2012 /sbin/ifconfig tun0 172.20.20.1 pointopoint 172.20.20.2 mtu 1500
Fri May 4 02:55:16 2012 /sbin/route add -net 172.20.20.0 netmask 255.255.255.0 gw 172.20.20.2
Fri May 4 02:55:16 2012 Data Channel MTU parms [L:1558 D:1450 EF:58 EB:135 ET:0 EL:0 AF:3/1]
Fri May 4 02:55:16 2012 GID set to users
Fri May 4 02:55:16 2012 UID set to nobody
Fri May 4 02:55:16 2012 UDPv4 link local (bound): [undef]
Fri May 4 02:55:16 2012 UDPv4 link remote: [undef]
Fri May 4 02:55:16 2012 MULTI: multi_init called, r=256 v=256
Fri May 4 02:55:16 2012 IFCONFIG POOL: base=172.20.20.4 size=62
Fri May 4 02:55:16 2012 IFCONFIG POOL LIST
Fri May 4 02:55:16 2012 Initialization Sequence Completed

Bridging and Routing between OpenSWAN and IPSec



IPSec Nuts and Bolts

- Encryption 3DES AES
  - Always use AES ,3DES has known attacks
- Diffie-Hellman Key Exchange
  - Keeps keys safe
- AH / ESP
  - Packet types
- Transport and Tunnel Mode
  - Layers
- Aggressive Mode /Main Mode
- Inter Key Exchange
  - Phase 1 / Phase 2
- The NAT Problem
  - NAT -t
- IKE daemon called Pluto.
- NETKEY, the 2.6 IPsec Stack
- Perfect Forward Secrecy

Authentication Header (AH)

- Guarantees connectionless integrity and data origin authentication of IP Packets
- Protects against replay attacks.
- Security Parameter Index(SPI)
  - Uniquely Identifies connection
- Sequence Number(SN)
  - Uniquely sets number for every packet.
- A cryptographic checksum. Integrity
  - check value (ICV)
  - MD5 or SHA1
- Hash Message Authentication Code (HMAC)
  - SPI + SN= ICV
- AH only provides authentication and does not encrypt the payload
- Since AH on its own does not offer encryption, it is hardly used at all.

Encapsulating Security Payload (ESP)

- Encrypts and Protects replay.
- Has SPI,SN and ICV.
- ESP now provides authentication.
- The only reason AH is separate form ESP is because of the US Export Restriction that were in effect when they were created.
- ESP is better.
- There is little or no need for AH.

IPSec Security Authority (SA)

- Contract Between two communicating entities.
  - Contains database for SPI
  - Sequence Number
  - Lifetime
  - Mode
  - Tunnel
  - Contains all configuration options

Internet Key Exchange (IKE)

- Phase 1 ISAKMP SA
  - Phase 1 deals with obtaining privacy through a Diffie-Hellman key exchange,
- Phase 2 Quick Mode
  - Establishes what Ciphers to use.
  - Which tunnel mode to use so on forth.
- Main Mode
  - Slower mode packets more fault tolerant
- Aggressive Mode
  - Faster less packets more error prone
- Pluto
  - Handles IKE Enable Pluto Debugging to trouble shoot IKE problems in great depth.

IPSec Modes

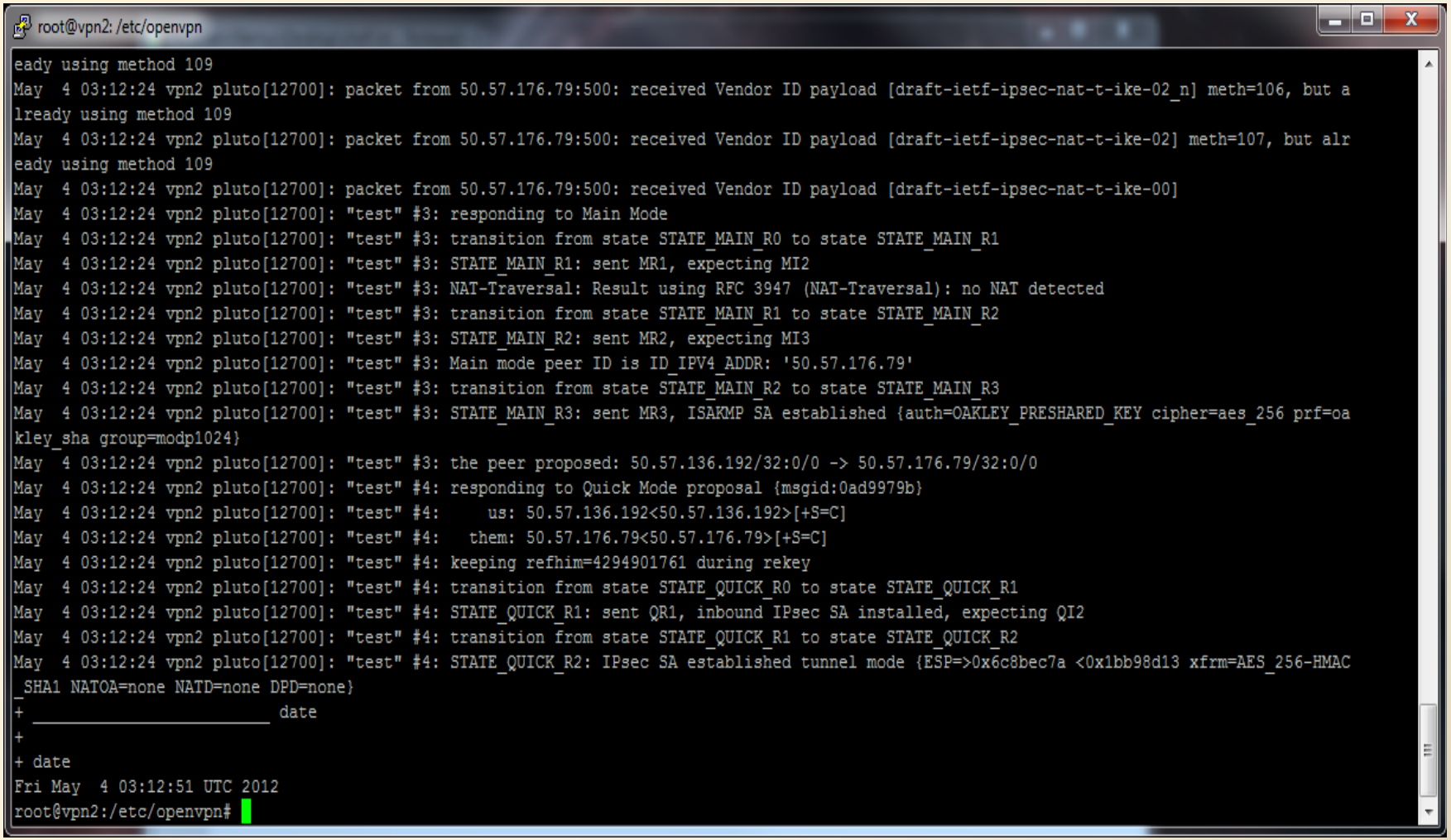
- Tunnel Mode
  - Used in most cases
  - Connection between two routers
  - Also know as an Encrypted route
- Transport Mode
  - Is used for LT2P
  - Used for transporting Layer 2 traffic.
  - only the payload of the IP packet is encrytped and authenticated.
  - The routing is intact, since the IP header is not modified or Encrypted

KLIPS vs NETKEYS

- Klips
  - Most compile OpenSWAN requires kernel modules
  - NETKEYS
    - A little confusing
    - Comes installed by default
    - Cannot view routes from netstat -r command
    - Does not create virtual interface.

L2TP

- Point to Point Protocol
  - Needs IPSEC for security
- Supported by Windows , Apple and almost all mobile devices.
- Hard to configure
- Uses port 1701


root@vpn2: /etc/openvpn
eady using method 109
May 4 03:12:24 vpn2 pluto[12700]: packet from 50.57.176.79:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02_n] meth=106, but a
lready using method 109
May 4 03:12:24 vpn2 pluto[12700]: packet from 50.57.176.79:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02] meth=107, but alr
eady using method 109
May 4 03:12:24 vpn2 pluto[12700]: packet from 50.57.176.79:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-00]
May 4 03:12:24 vpn2 pluto[12700]: "test" #3: responding to Main Mode
May 4 03:12:24 vpn2 pluto[12700]: "test" #3: transition from state STATE_MAIN_R0 to state STATE_MAIN_R1
May 4 03:12:24 vpn2 pluto[12700]: "test" #3: STATE_MAIN_R1: sent MR1, expecting MI2
May 4 03:12:24 vpn2 pluto[12700]: "test" #3: NAT-Traversal: Result using RFC 3947 (NAT-Traversal): no NAT detected
May 4 03:12:24 vpn2 pluto[12700]: "test" #3: transition from state STATE_MAIN_R1 to state STATE_MAIN_R2
May 4 03:12:24 vpn2 pluto[12700]: "test" #3: STATE_MAIN_R2: sent MR2, expecting MI3
May 4 03:12:24 vpn2 pluto[12700]: "test" #3: Main mode peer ID is ID_IPV4_ADDR: '50.57.176.79'
May 4 03:12:24 vpn2 pluto[12700]: "test" #3: transition from state STATE_MAIN_R2 to state STATE_MAIN_R3
May 4 03:12:24 vpn2 pluto[12700]: "test" #3: STATE_MAIN_R3: sent MR3, ISAKMP SA established {auth=OAKLEY_PRESHARED_KEY cipher=aes_256 prf=oa
kley_sha group=modp1024}
May 4 03:12:24 vpn2 pluto[12700]: "test" #3: the peer proposed: 50.57.136.192/32:0/0 -> 50.57.176.79/32:0/0
May 4 03:12:24 vpn2 pluto[12700]: "test" #4: responding to Quick Mode proposal {msgid:0ad9979b}
May 4 03:12:24 vpn2 pluto[12700]: "test" #4:   us: 50.57.136.192<50.57.136.192>[+S=C]
May 4 03:12:24 vpn2 pluto[12700]: "test" #4:   them: 50.57.176.79<50.57.176.79>[+S=C]
May 4 03:12:24 vpn2 pluto[12700]: "test" #4: keeping refhim=4294901761 during rekey
May 4 03:12:24 vpn2 pluto[12700]: "test" #4: transition from state STATE_QUICK_R0 to state STATE_QUICK_R1
May 4 03:12:24 vpn2 pluto[12700]: "test" #4: STATE_QUICK_R1: sent QR1, inbound IPsec SA installed, expecting QI2
May 4 03:12:24 vpn2 pluto[12700]: "test" #4: transition from state STATE_QUICK_R1 to state STATE_QUICK_R2
May 4 03:12:24 vpn2 pluto[12700]: "test" #4: STATE_QUICK_R2: IPsec SA established tunnel mode {ESP=>0x6c8bec7a <0x1bb98d13 xfrm=AES_256-HMAC
_SHA1 NATOA=none NATD=none DPD=none}
+ _____ date
+
+ date
Fri May 4 03:12:51 UTC 2012
root@vpn2:/etc/openvpn#

OpenSWAN Setup

- apt-get install openswan
- apt-get install lsof
- ipsec verify
- ipsec setup start
- ipsec.secrets
  - /etc, or /etc/ipsec/
  - Stores RSA keys and preshared secrets (PSKs)
- ipsec.conf
  - /etc, or sometimes in /etc/ipsec
  - Contains all configuration options

```
#!/bin/bash

# Disable send redirects
echo 0 > /proc/sys/net/ipv4/conf/all/send_redirects
echo 0 > /proc/sys/net/ipv4/conf/default/send_redirects
echo 0 > /proc/sys/net/ipv4/conf/eth0/send_redirects
echo 0 > /proc/sys/net/ipv4/conf/eth1/send_redirects
echo 0 > /proc/sys/net/ipv4/conf/lo/send_redirects
echo 0 > /proc/sys/net/ipv4/conf/ppp0/send_redirects

# Disable accept redirects
echo 0 > /proc/sys/net/ipv4/conf/all/accept_redirects
echo 0 > /proc/sys/net/ipv4/conf/default/accept_redirects
echo 0 > /proc/sys/net/ipv4/conf/eth0/accept_redirects
echo 0 > /proc/sys/net/ipv4/conf/eth1/accept_redirects
echo 0 > /proc/sys/net/ipv4/conf/lo/accept_redirects
echo 0 > /proc/sys/net/ipv4/conf/ppp0/accept_redirects
```

- # /etc/ipsec.conf - Openswan IPsec configuration file
  config setup

Debug-logging controls: "none" for (almost) none, "all" for lots.

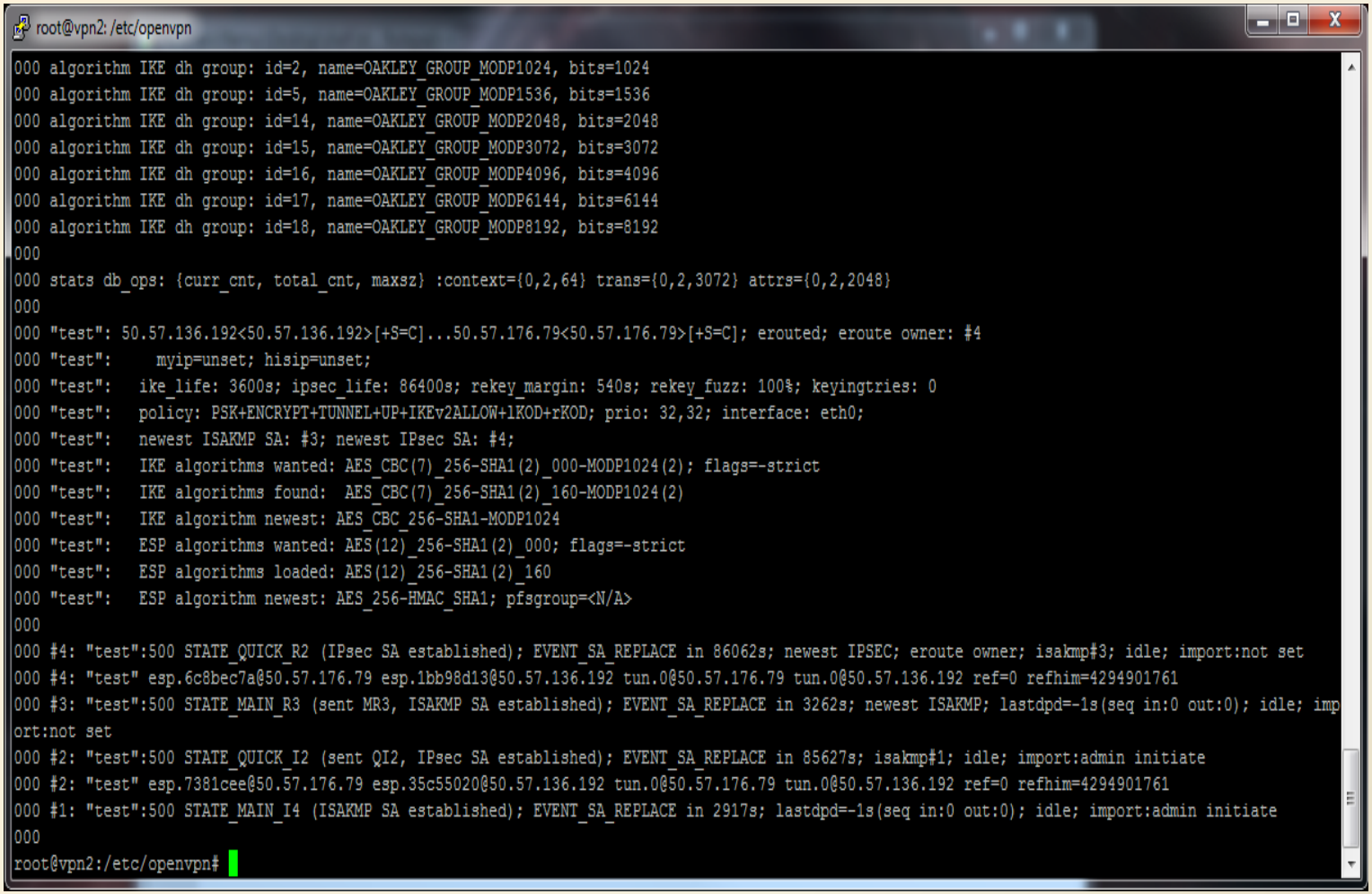
- # klipsdebug=none
- #plutodebug="control parsing"
- # For Red Hat Enterprise Linux and Fedora, leave protostack=netkey

  nat_traversal=yes
- virtual_private=
- oe=off
- # Enable this if you see "failed to find any available worker"
- nhelpers=0
- #You may put your configuration (.conf) file in the "/etc/ipsec.d/"

```
conn test
        type=tunnel
        authby = secret
        left = x.x.x.36
        leftsubnet =x.x.x.36/32
        leftsourceip = x.x.x.x36 (OpenVPN Network)
        leftid=x.x.x.181
        leftnexthop=%defaultroute
        rightid=x.x.x.38
        right=x.x.x.92
        rightsubnet=x.x.x.15/24 #(OpenSWAN Network)
        esp=aes256-sha1
        ike="aes256-sha1-modp1024"
        keyexchange = ike
        pfs = no
        auto = start
        lifetime=86400s
        aggrmode=no
```

Trouble Shooting OpenSWAN IPSec

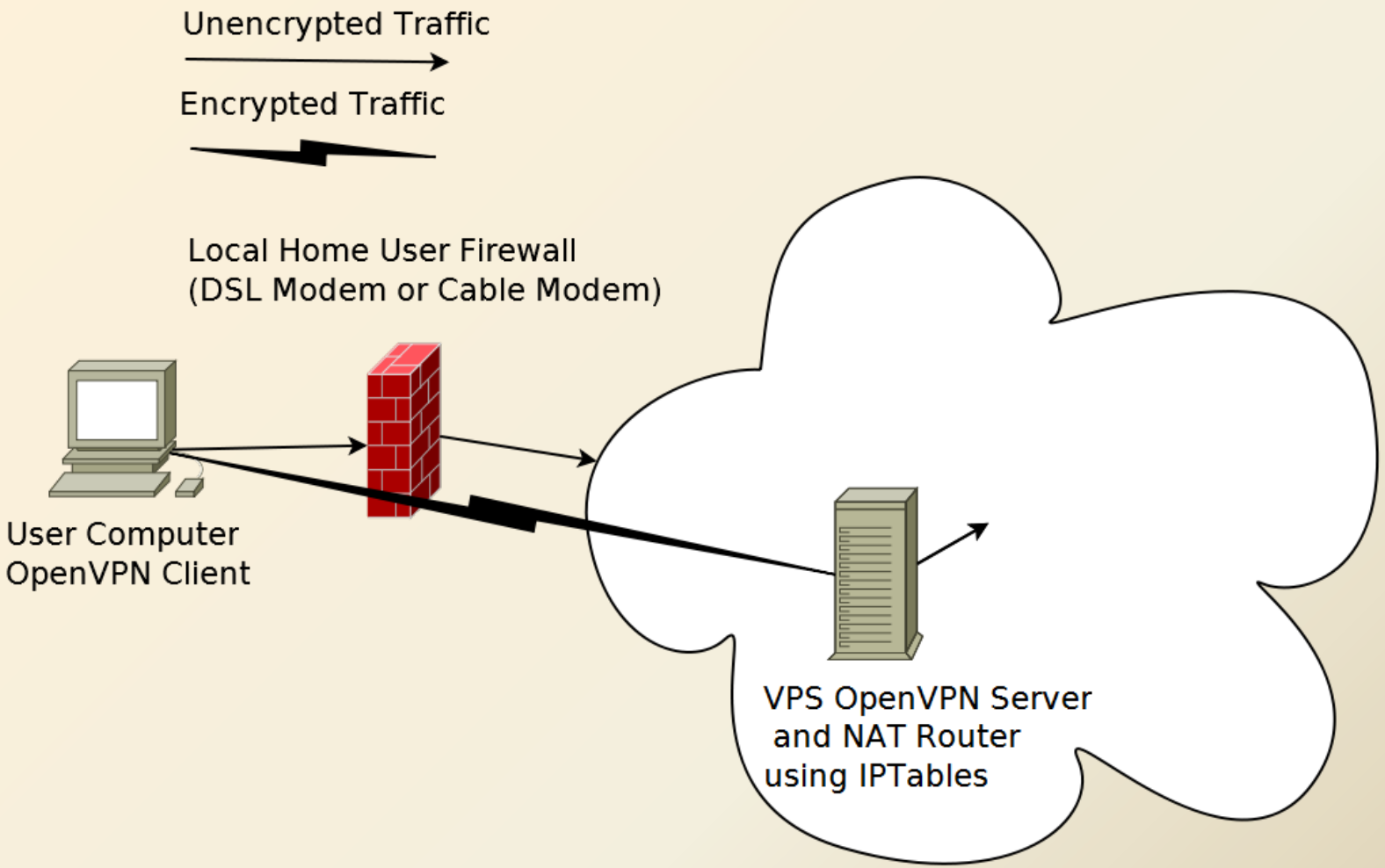
- Ipsec barf
- Ipsec auto --status
- Enabling pluto debug or disable pluto debuging.


root@vpn2: /etc/openvpn
000 algorithm IKE dh group: id=2, name=OAKLEY_GROUP_MODP1024, bits=1024
000 algorithm IKE dh group: id=5, name=OAKLEY_GROUP_MODP1536, bits=1536
000 algorithm IKE dh group: id=14, name=OAKLEY_GROUP_MODP2048, bits=2048
000 algorithm IKE dh group: id=15, name=OAKLEY_GROUP_MODP3072, bits=3072
000 algorithm IKE dh group: id=16, name=OAKLEY_GROUP_MODP4096, bits=4096
000 algorithm IKE dh group: id=17, name=OAKLEY_GROUP_MODP6144, bits=6144
000 algorithm IKE dh group: id=18, name=OAKLEY_GROUP_MODP8192, bits=8192
000
000 stats db_ops: {curr_cnt, total_cnt, maxsz} :context={0,2,64} trans={0,2,3072} attrs={0,2,2048}
000
000 "test": 50.57.136.192<50.57.136.192>[+S=C]...50.57.176.79<50.57.176.79>[+S=C]; erouted; eroute owner: #4
000 "test":   myip=unset; hisip=unset;
000 "test":   ike_life: 3600s; ipsec_life: 86400s; rekey_margin: 540s; rekey_fuzz: 100%; keyingtries: 0
000 "test":   policy: PSK+ENCRYPT+TUNNEL+UP+IKEv2ALLOW+lKOD+rKOD; prio: 32,32; interface: eth0;
000 "test":   newest ISAKMP SA: #3; newest IPsec SA: #4;
000 "test":   IKE algorithms wanted: AES_CBC(7)_256-SHA1(2)_000-MODP1024(2); flags=-strict
000 "test":   IKE algorithms found: AES_CBC(7)_256-SHA1(2)_160-MODP1024(2)
000 "test":   IKE algorithm newest: AES_CBC_256-SHA1-MODP1024
000 "test":   ESP algorithms wanted: AES(12)_256-SHA1(2)_000; flags=-strict
000 "test":   ESP algorithms loaded: AES(12)_256-SHA1(2)_160
000 "test":   ESP algorithm newest: AES_256-HMAC_SHA1; pfsgroup=<N/A>
000
000 #4: "test":500 STATE_QUICK_R2 (IPsec SA established); EVENT_SA_REPLACE in 86062s; newest IPSEC; eroute owner; isakmp#3; idle; import:not set
000 #4: "test" esp.6c8bec7a@50.57.176.79 esp.1bb98d13@50.57.136.192 tun.0@50.57.176.79 tun.0@50.57.136.192 ref=0 refhim=4294901761
000 #3: "test":500 STATE_MAIN_R3 (sent MR3, ISAKMP SA established); EVENT_SA_REPLACE in 3262s; newest ISAKMP; lastdpd=-1s(seq in:0 out:0); idle; imp
ort:not set
000 #2: "test":500 STATE_QUICK_I2 (sent QI2, IPsec SA established); EVENT_SA_REPLACE in 85627s; isakmp#1; idle; import:admin initiate
000 #2: "test" esp.7381cee@50.57.176.79 esp.35c55020@50.57.136.192 tun.0@50.57.176.79 tun.0@50.57.136.192 ref=0 refhim=4294901761
000 #1: "test":500 STATE_MAIN_I4 (ISAKMP SA established); EVENT_SA_REPLACE in 2917s; lastdpd=-1s(seq in:0 out:0); idle; import:admin initiate
000
root@vpn2:/etc/openvpn#

OpenVPN Case Studies

- Virtual Private Servers
  - Interserver (http://www.interserver.net/)
    - 3mb up and down 376 mb ram $6.00 a month.
      - » Los Angles ,CA
      - » Secaucus, NJ
    - Santrex (http://www.santrex.net/vps-hosting.php)
      - OffShore VPS $9.00
        - **Be Very Careful of Terms and Laws when crossing borders!**
          - **France**
          - **Germany**
          - **Luxembourg**
          - **Netherlands**
          - **Romania**
          - Etc..

Road warrior Setup / Proxy setup



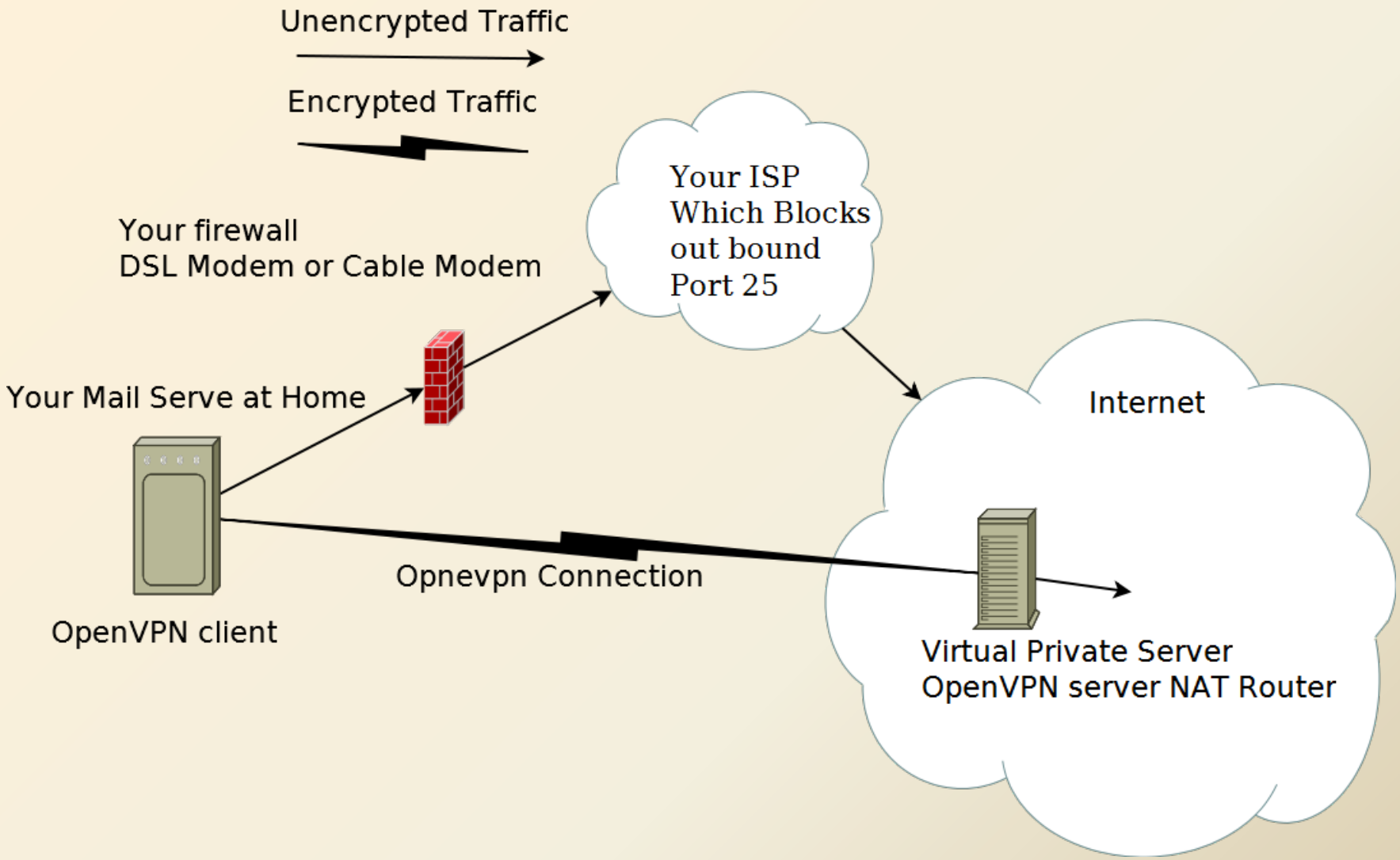
IPTables NATing OpenVPN Network

- iptables -t nat -A POSTROUTING -s 172.18.x.x/24 -j SNAT --to x.x.x.x
- iptables -A INPUT -p udp -m udp --dport 1074 -m state --state NEW -j ACCEPT
- iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
- iptables -A FORWARD -s 172.18.x.x/24 -j ACCEPT
- iptables -A FORWARD -j REJECT

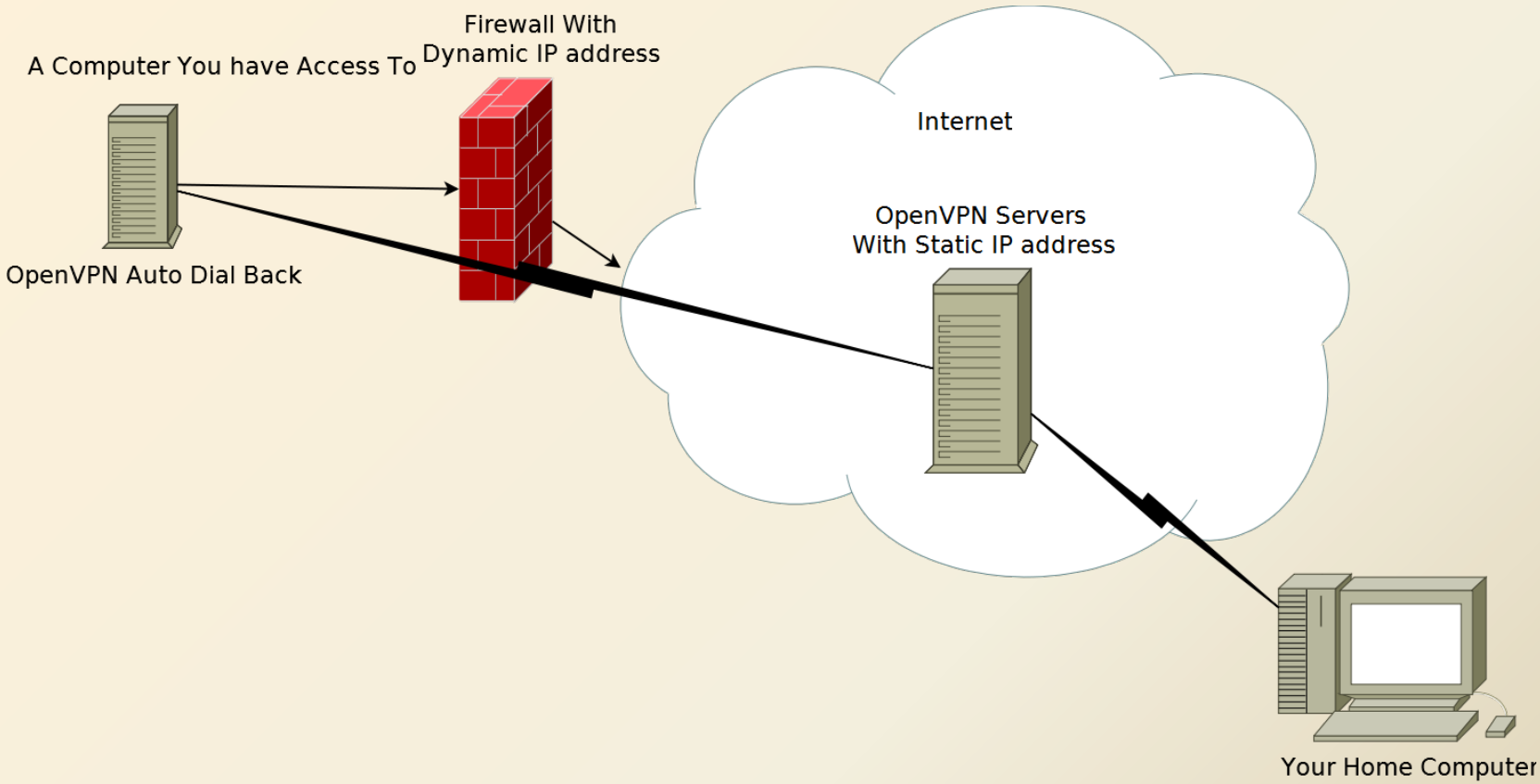
Routing in Linux

- vim /etc/sysctl.conf
- # Controls IP packet forwarding
- net.ipv4.ip_forward = 1
- Systcl –p
- (don’t always turn this on is off for a reason)

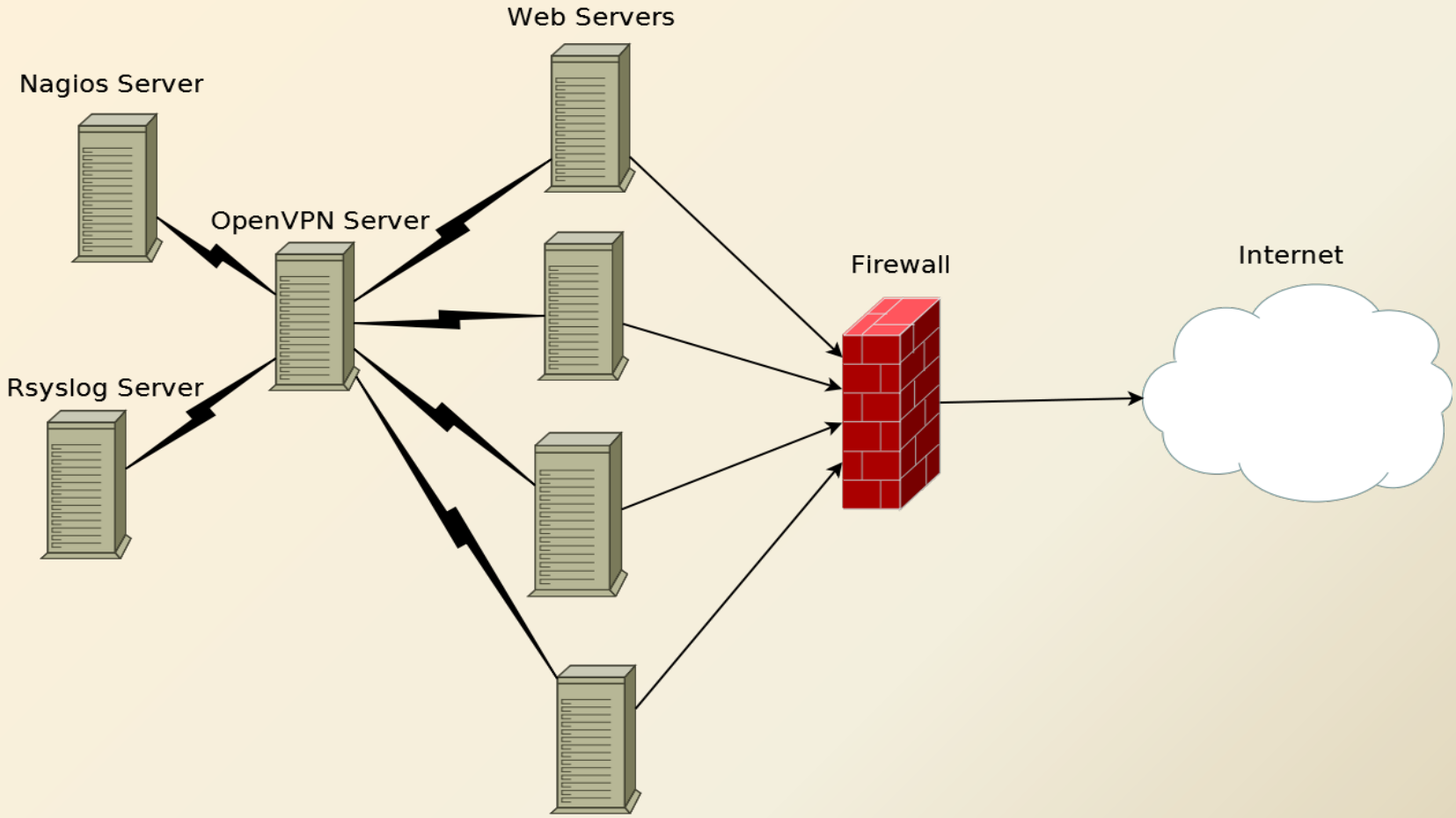
Server Tethering To OpenVPN Cloud Server.



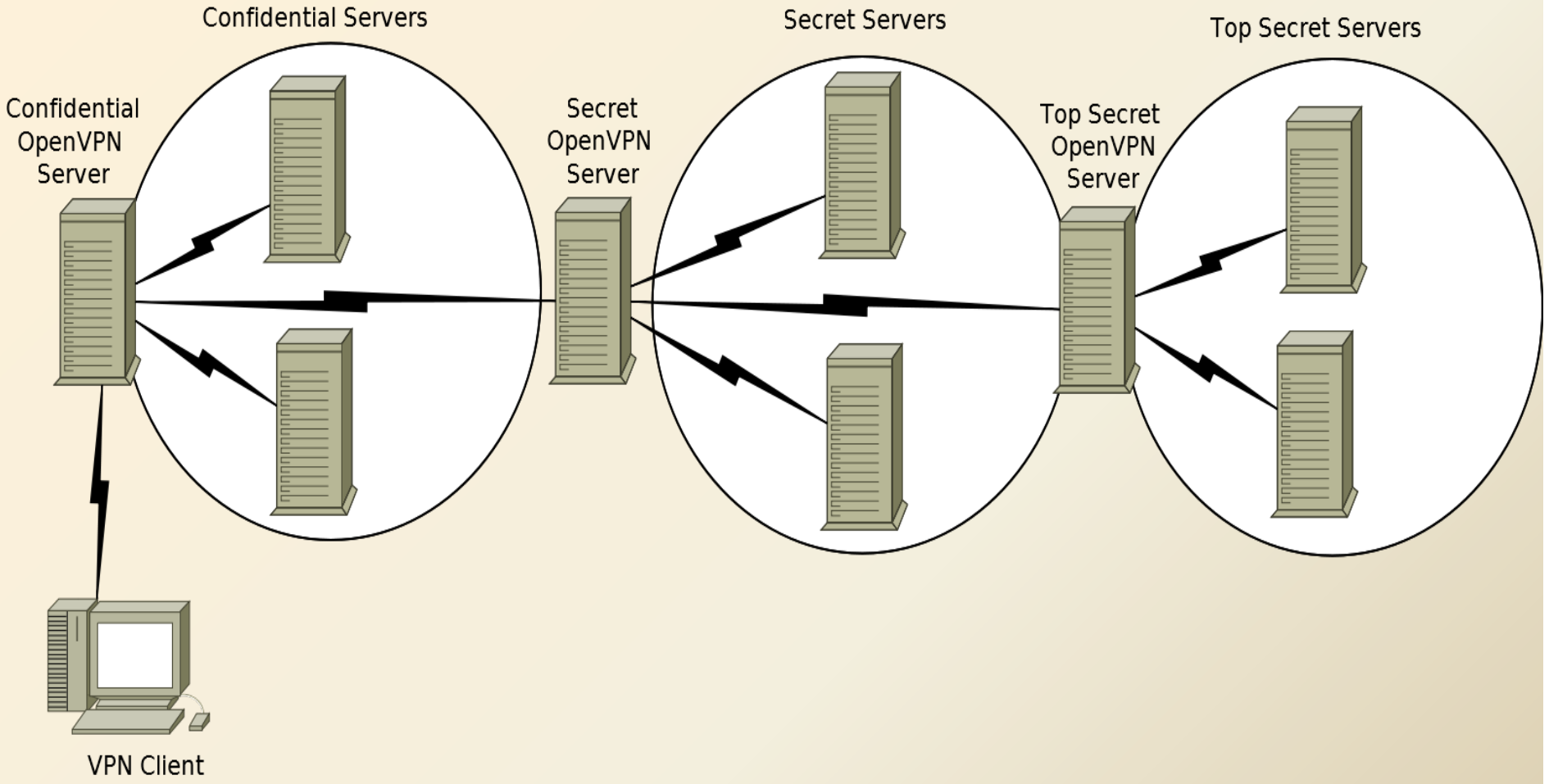
OpenVPN Dial Back



Monitoring Services



OpenVPN Inception Layers?



Stunnel

- Encrypts Layer 4 in TLS/SSL RSA Encryption
  - openssl req -new -x509 -days 365 -nodes -config stunnel.cnf -out stunnel.pem -keyout stunnel.pem
  - **openssl rsa -in *original.pem* -out *new.pem***

stunnel.conf

- cert = /etc/stunnel/stunnel.pem
  setuid = nobody
  setgid = nobody
  pid = /tmp/stunnel.pid
  debug = 7
  output = stunnel.log
  [mysqls]
  accept = 3309
  connect = 3306

Obscurity Systems

- For Consulting or More Info My
  - Website
    - http://www.obscuritysystems.com/
  - Email
    - nemus@grayhatlabs.com
    - info@obscuritysystems.com
  - Phone Number
    - 801-828-3184
- Sllug Mailing list http://www.sllug.org/