

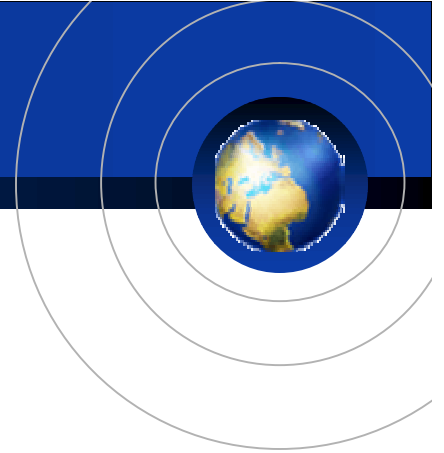
卒業研究  
Virtual Private Network



1ADT1217 中岩 正洋

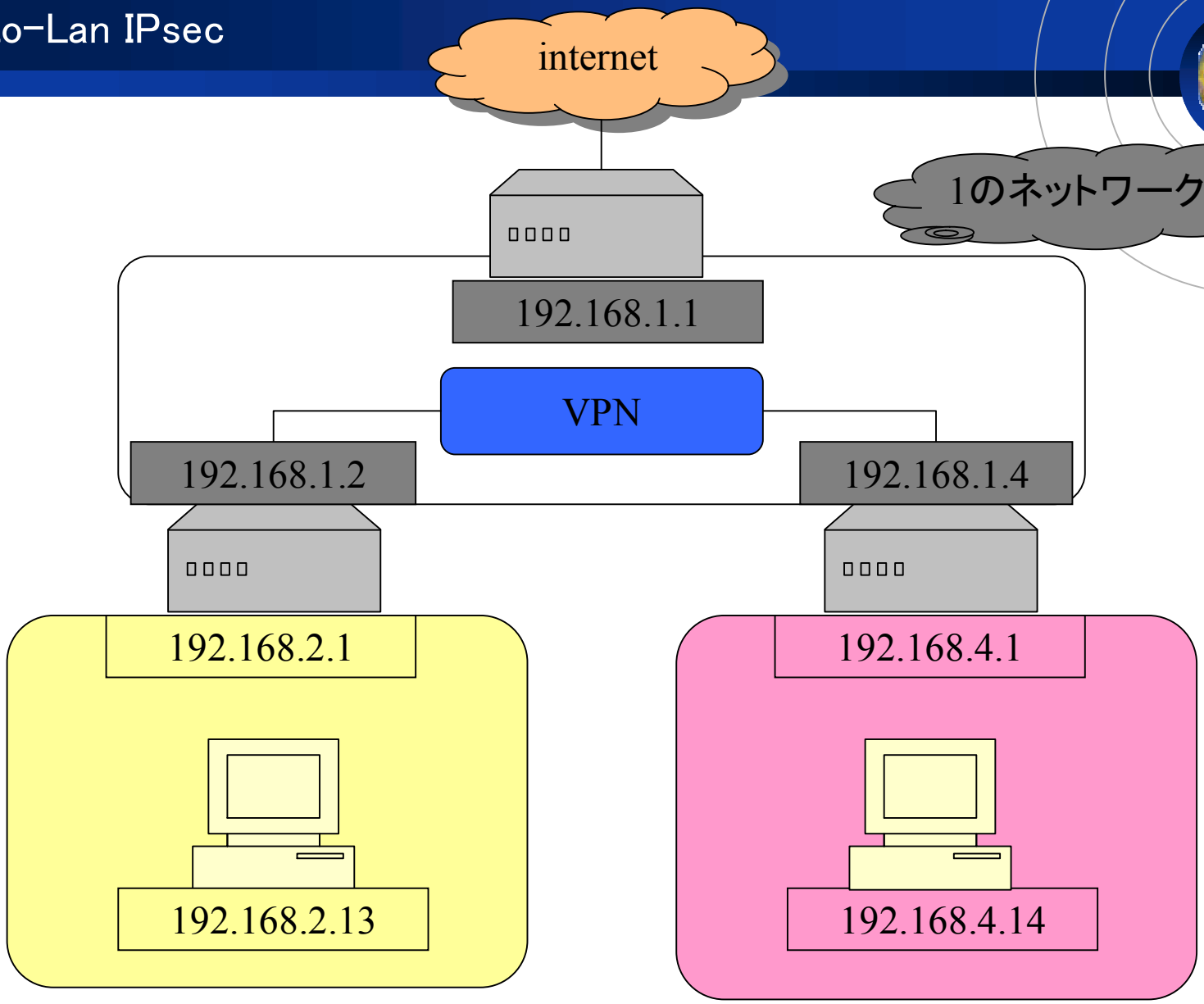
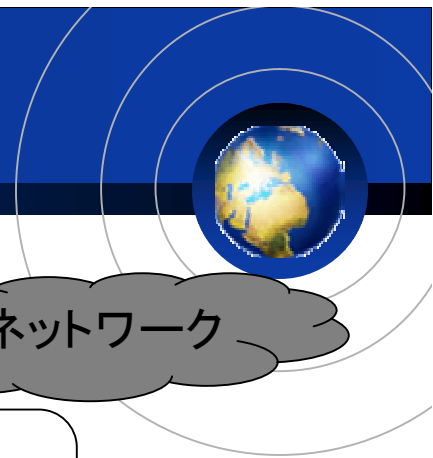
**Logo**

# 今年一年の取り組み

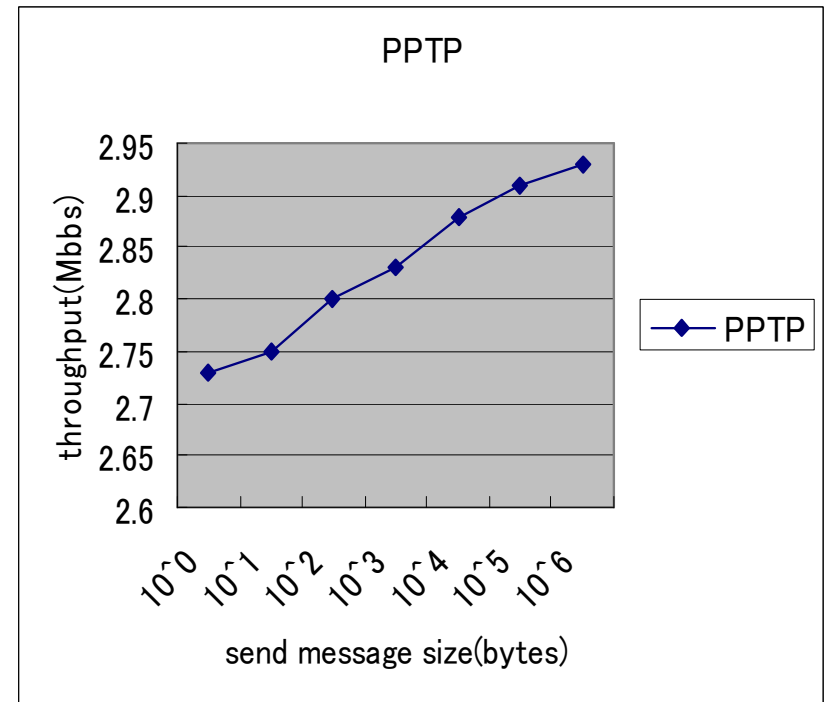
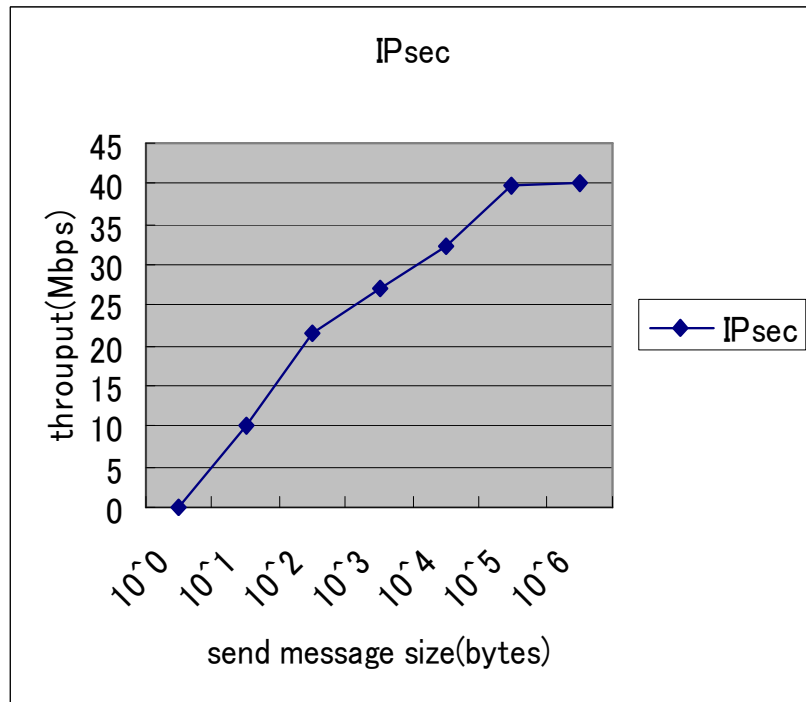


- Red Hat Linux 8.0 to WindowsXP  
FreeS/WAN(transport mode)
- YAMAHA RTX1000 Routerを用いてのVPN  
IPsec(LAN間接続) , PPTP(LAN間接続)
- WindowsXP(pro)によるVPN  
PPTP(remote access)
- Fedora Core2 によるVPN  
IPsec-tools(transport mode)
- Fedora Core3 によるVPN  
IPsec-tools(transport mode , tunnel mode)  
Openswan(transport mode , tunnel mode)

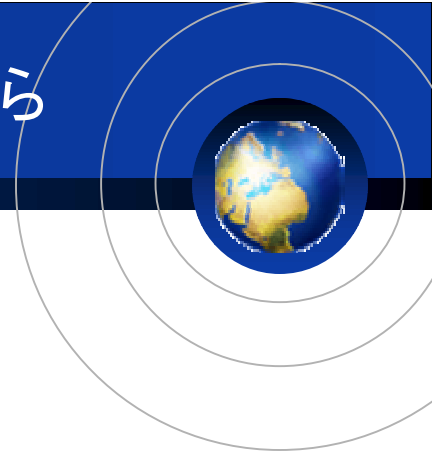
# YAMAHA RTX1000 Router Lan-to-Lan IPsec



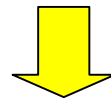
# YAMAHA RTX1000 Routerによる VPNのthroughput比較



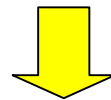
# YAMAHA RTX1000によるVPNのthrough put比較から



IPsecを使った場合(LAN間接続)  
through putは最大約40Mb/sec  
PPTPを使った場合(LAN間接続)  
through putは最大約3Mb/sec



この差は何？  
YAMAHAに問い合わせてみると...

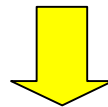


IPsecはハードウェア処理の為に高速  
PPTPはソフトウェア処理の為に低速

# ソフトウェア処理VPN



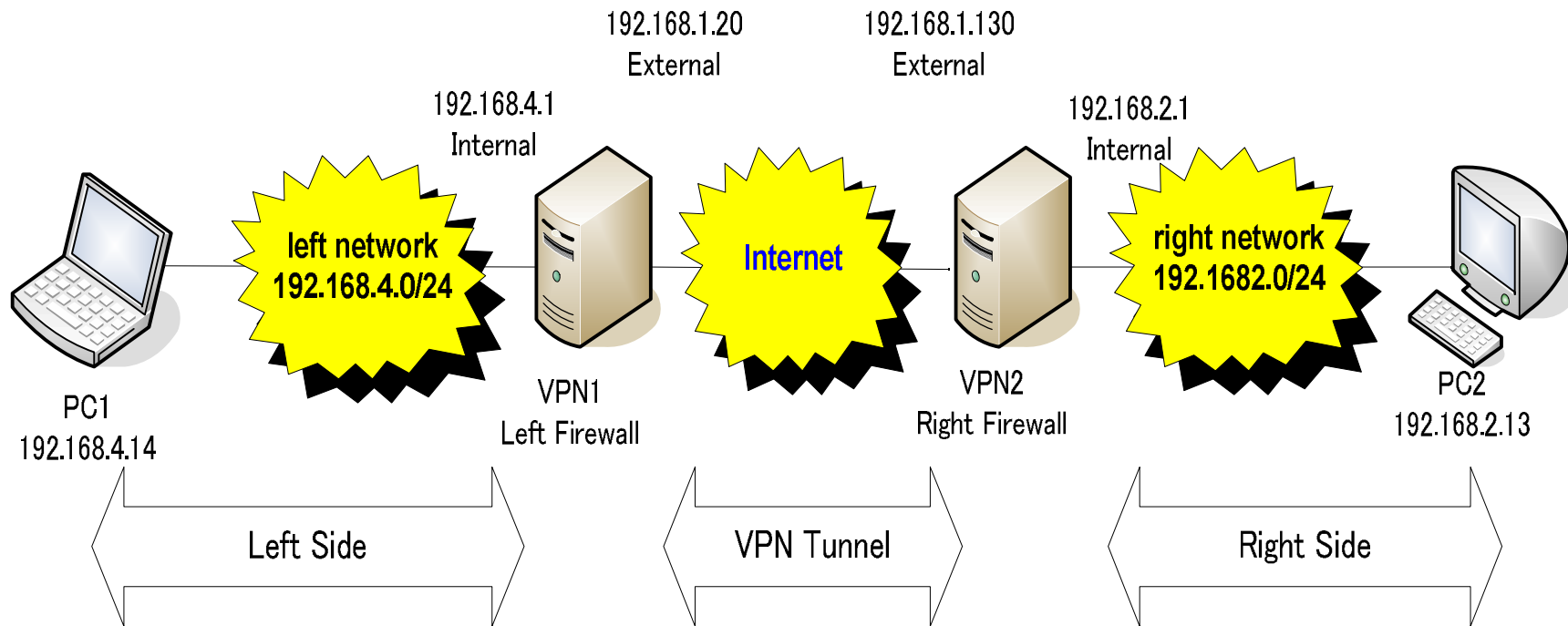
- ソフトウェア処理で動くVPNを探すo(.\_.=.\_.)o キョロキョロ
- Internetのスタンダードとして考えると、「PPP over SSH」「PPTP」「L2tpd」「IPsec」などが考えられる。
- 他にも、「OpenVPN」「SoftEther」「TinyVPN」「StrongS/WAN」「Openswan」「ipsec-tools」「VTun」「Cipe」「Stunnel」「AmeritaVPN」「LinVPN」「Tinc」などがある。



- IPsecを構築してみようということで「ipsec-tools」or「Openswan」をFedora Core3に実装してIPsecを行うことに。



# IPsec VPN Topology Diagram



# IPsec-tools利用時のtcpdumpでのcapture



## IPsec(Host to Host)の場合(←pingがおかしい)

```
05:08:27.766837 IP leftVPN20.com > rightVPN130.com: AH(spi=0x10e0bcc9, seq=0xc): ESP(spi=0x66814a24, seq=0xc)
05:08:28.766689 IP leftVPN20.com > rightVPN130.com: AH(spi=0x10e0bcc9, seq=0xd): ESP(spi=0x66814a24, seq=0xd)
05:08:29.766547 IP leftVPN20.com > rightVPN130.com: AH(spi=0x10e0bcc9, seq=0xe): ESP(spi=0x66814a24, seq=0xe)
05:08:30.766398 IP leftVPN20.com > rightVPN130.com: AH(spi=0x10e0bcc9, seq=0xf): ESP(spi=0x66814a24, seq=0xf)
05:08:31.766251 IP leftVPN20.com > rightVPN130.com: AH(spi=0x10e0bcc9, seq=0x10): ESP(spi=0x66814a24, seq=0x10)
05:08:32.766106 IP leftVPN20.com > rightVPN130.com: AH(spi=0x10e0bcc9, seq=0x11): ESP(spi=0x66814a24, seq=0x11)
05:08:33.765960 IP leftVPN20.com > rightVPN130.com: AH(spi=0x10e0bcc9, seq=0x12): ESP(spi=0x66814a24, seq=0x12)
05:08:34.765814 IP leftVPN20.com > rightVPN130.com: AH(spi=0x10e0bcc9, seq=0x13): ESP(spi=0x66814a24, seq=0x13)
05:08:35.765669 IP leftVPN20.com > rightVPN130.com: AH(spi=0x10e0bcc9, seq=0x14): ESP(spi=0x66814a24, seq=0x14)
05:08:36.765522 IP leftVPN20.com > rightVPN130.com: AH(spi=0x10e0bcc9, seq=0x15): ESP(spi=0x66814a24, seq=0x15)
```

## IPsec(Host to Host)の場合(←理想)

```
05:13:34.547033 IP leftVPN20.com > rightVPN130.com: AH(spi=0x10e0bcc9, seq=0x10c): ESP(spi=0x66814a24, seq=0x10c)
05:13:35.544472 IP rightVPN130.com > leftVPN20.com: AH(spi=0x10e0bcc9, seq=0x38): ESP(spi=0x66814a24, seq=0x38)
05:13:35.546880 IP leftVPN20.com > rightVPN130.com: AH(spi=0x10e0bcc9, seq=0x10d): ESP(spi=0x66814a24, seq=0x10d)
05:13:36.544321 IP rightVPN130.com > leftVPN20.com: AH(spi=0x10e0bcc9, seq=0x39): ESP(spi=0x66814a24, seq=0x39)
05:13:36.546732 IP leftVPN20.com > rightVPN130.com: AH(spi=0x10e0bcc9, seq=0x10e): ESP(spi=0x66814a24, seq=0x10e)
05:13:37.544168 IP rightVPN130.com > leftVPN20.com: AH(spi=0x10e0bcc9, seq=0x3a): ESP(spi=0x66814a24, seq=0x3a)
05:13:37.546585 IP leftVPN20.com > rightVPN130.com: AH(spi=0x10e0bcc9, seq=0x10f): ESP(spi=0x66814a24, seq=0x10f)
05:13:38.544016 IP rightVPN130.com > leftVPN20.com: AH(spi=0x10e0bcc9, seq=0x3b): ESP(spi=0x66814a24, seq=0x3b)
05:13:38.546439 IP leftVPN20.com > rightVPN130.com: AH(spi=0x10e0bcc9, seq=0x110): ESP(spi=0x66814a24, seq=0x110)
05:13:39.543865 IP rightVPN130.com > leftVPN20.com: AH(spi=0x10e0bcc9, seq=0x3c): ESP(spi=0x66814a24, seq=0x3c)
```

### [設定]

固定鍵付きの手動暗号化

認証鍵(A) 66f3b1b73a2d66ac5926

暗号鍵(E) f46ed43a6dd7711d0e8f4c52

# Openswan : Determine the Tunnel Status



- **IKE Section** : Defines the various encrypted key exchange algorithms and their parameters.

Phase 1 parameters

- **ESP Section** : Defines the various data encryption algorithms and their parameters.

Phase 2 parameters

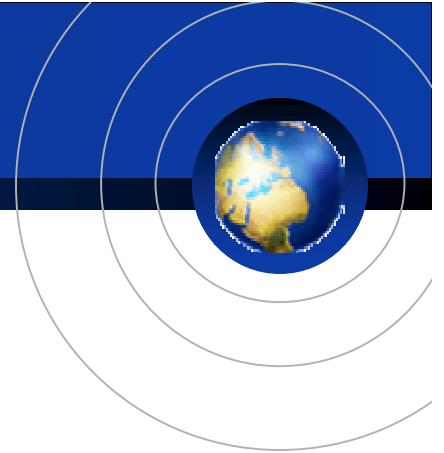
- **VPN Section** : This is usually prefaced by the name of the VPN tunnel , in this case “net-to-net”

# The “ipsec auto –status” command provides a status on Openswan running on vpn device



```
000 algorithm ESP encrypt: id=2, name=ESP_DES, ivlen=8, keysize=64, keysize=64
000 algorithm ESP encrypt: id=3, name=ESP_3DES, ivlen=8, keysize=192, keysize=192
000 algorithm ESP encrypt: id=7, name=ESP_BLOWFISH, ivlen=8, keysize=40, keysize=448
000 algorithm ESP encrypt: id=11, name=ESP_NULL, ivlen=0, keysize=0, keysize=0
000 algorithm ESP encrypt: id=12, name=ESP_AES, ivlen=8, keysize=128, keysize=256
000 algorithm ESP encrypt: id=252, name=ESP_SERPENT, ivlen=8, keysize=128, keysize=256
000 algorithm ESP encrypt: id=253, name=ESP_TWOFISH, ivlen=8, keysize=128, keysize=256
000 algorithm ESP auth attr: id=1, name=AUTH_ALGORITHM_HMAC_MD5, keysize=128, keysize=128
000 algorithm ESP auth attr: id=2, name=AUTH_ALGORITHM_HMAC_SHA1, keysize=160, keysize=160
000 algorithm ESP auth attr: id=5, name=AUTH_ALGORITHM_HMAC_SHA2_256, keysize=256, keysize=256
000 algorithm ESP auth attr: id=251, name=(null), keysize=0, keysize=0
000
000 algorithm IKE encrypt: id=7, name=OAKLEY_AES_CBC, blocksize=16, keydeflen=128
000 algorithm IKE encrypt: id=5, name=OAKLEY_3DES_CBC, blocksize=8, keydeflen=192
000 algorithm IKE hash: id=2, name=OAKLEY_SHA1, hashsize=20
000 algorithm IKE hash: id=1, name=OAKLEY_MD5, hashsize=16
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.c: {curr_cnt, total_cnt, maxsz} :context={0,0,0} trans={0,0,0} attrs={0,0,0}
000
000 "packetdefault": 0,0,0,0/0===192.168.1.130[%myid]---192.168.1.1...%opportunistic: prospective erouted: eroute owner: #0
000 "packetdefault": srcip=unset; dstip=unset
000 "packetdefault": ike_life: 3600s; ipsec_life: 3600s; rekey_margin: 540s; rekey_fuzz: 100%; keyingtries: 3
000 "packetdefault": policy: RSASIG+ENCRYPT+TUNNEL+PFS+DONTREKEY+OPPORTUNISTIC+failurePASS+IKOD+rKOD; prio: 0,0; interface: eth0;
000 "packetdefault": newest ISAKMP SA: #0; newest IPsec SA: #0;
...
```

# Using RSA Keys (Opportunistic Encryption DNS Checks) Using Pre-Shared Keys (PSK)



```
[root@leftVPN20 ~]# service ipsec restart
ipsec_setup: Stopping Openswan IPsec...
ipsec_setup: stop ordered, but IPsec does not appear to be running!
ipsec_setup: doing cleanup anyway...
ipsec_setup: Starting Openswan IPsec 2.3.0...
ipsec_setup: insmod /lib/modules/2.6.10-1.741_FC3/kernel/net/key/af_key.ko
ipsec_setup: insmod /lib/modules/2.6.10-1.741_FC3/kernel/net/ipv4/xfrm4_tunnel.ko
[root@leftVPN20 ~]# ipsec verify
Checking your system to see if IPsec got installed and started correctly:
Version check and ipsec on-path [OK]
Linux Openswan U2.3.0/K2.6.10-1.741_FC3 (netkey)
Checking for IPsec support in kernel [OK]
Checking for RSA private key (/etc/ipsec.secrets) [OK]
Checking that pluto is running [OK]
Two or more interfaces found, checking IP forwarding [OK]
Checking NAT and MASQUERADEing
Checking for 'ip' command [OK]
Checking for 'iptables' command [OK]
Checking for 'setkey' command for NETKEY IPsec stack support [OK]

Opportunistic Encryption DNS checks:
  Looking for TXT in forward dns zone: leftVPN20.com [MISSING]
  Does the machine have at least one non-private address? [FAILED]
```