IPSec How-to Debian
Category: How-to's

IPSec How-to Debian

Introduction

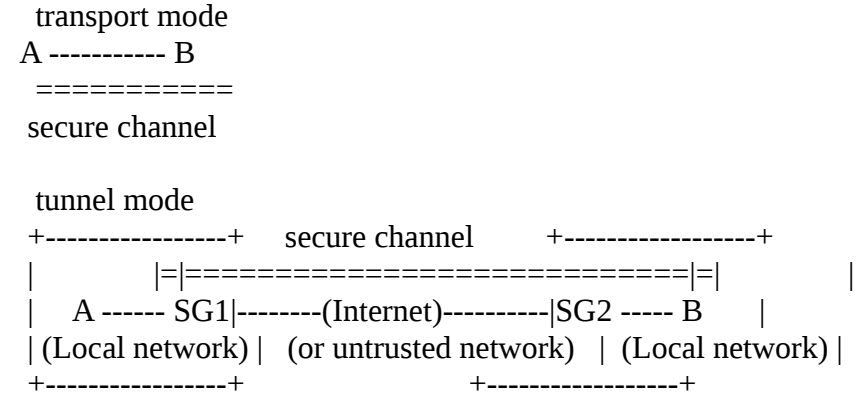
This HOWTO will explain a common scenario, where you have to connect two networks using a VPN IPSec tunnel. We'll be using Debian GNU/Linux as a base OS, Linux 2.6 native IPSec stack and racoon as an IKE daemon.

IPSec protocol suite

IPSec is designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6 as stated in RFC2401. It's an extension to the IP protocol, which provide access control,data origin authentication, integrity and confidentiality to IP, and upper-level protocols. To do it's magic, IPSec needs some help from few protocols – Authentication Header (AH), Encapsulating Security Payload (ESP), IP Payload Compression (IPcomp) and Internet Key Exchange (IKE). AH provides data origin authentication, connectionless integrity, and offers anti-replay service to help against denial of service attacks. So with AH you get the guarantee, when you receive a packet from host that you share a secret key, this packet is coming from the peer that you expect it to come from and it's not modified in transit. ESP gives you confidentiality guarantee that your packets will not be wiretapped(monitored by third party), it also can provide authentication. AH and ESP may be used alone or in combination with each other to accomplish a desired level of security service. IPcomp provides compression to IP datagrams, before they are encrypted. IKE is a hybrid protocol, a mixture of ISAKMP framework and Oakley and SKEME protocols. It provides a secure way for peers' to negotiate keys as needed by AH and ESP. AH, ESP and IPcomp are implemented at the kernel level, while IKE is in userland as a daemon process.

IPSec modes

There are two modes of operation of IPSec(AH,ESP,IPcomp), tunnel and transport mode. In transport mode, the protections is for the upper-level protocols and is used to secure the traffic between two hosts. Tunnel mode provides protection to the tunneled IP datagrams, and is used on security gateways to encrypt traffic between networks or hosts behind them.



The Setup

First, because this HOWTO is Debian oriented, you should do a base install of Debian GNU/Linux on both machines that will act as security gateways. Both must have at least two NICs each, one for the internal network, and the other for the untrusted WAN or Internet. We will use the stock kernel that

ships with Debian (as of the time of writing – 2.6.15.1). For sake of simplicity, let's define some stuff:

Network A
network: 172.16.10.0/24
SG hostname: alfa
SG wan ip addr: 1.2.3.4

Network B
network: 172.16.23.0/24
SG hostname: bravo
SG wan ip addr: 2.3.4.5

Again, for simplicity, we'll use PSK based authentication, instead of x.509 sertificates. Note that generally x.509 sertificates are preferrable, and of course more secure.

Install racoon and ipsec-tools
After all the initial settings and setup is done, you have to install raccoon and ipsec-tools:

~# aptitude install racoon ipsec-tools

Reading package lists… Done
Building dependency tree… Done
Reading extended state information
Initializing package states… Done
Building tag database… Done
The following NEW packages will be installed:
ipsec-tools racoon
0 packages upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 390kB of archives. After unpacking 1184kB will be used.
Writing extended state information… Done
Get:1 http://ftp.bg.debian.org unstable/main ipsec-tools 1:0.6.3-1 [81.3kB]
Get:2 http://ftp.bg.debian.org unstable/main racoon 1:0.6.3-1 [309kB]
Fetched 390kB in 5s (77.0kB/s)
Preconfiguring packages …
Selecting previously deselected package ipsec-tools.
(Reading database … 106748 files and directories currently installed.)
Unpacking ipsec-tools (from …/ipsec-tools_1%3a0.6.3-1_i386.deb) …
Selecting previously deselected package racoon.
Unpacking racoon (from …/racoon_1%3a0.6.3-1_i386.deb) …
Setting up ipsec-tools (0.6.3-1) …

Setting up racoon (0.6.3-1) …
Starting IKE (ISAKMP/Oakley) server: racoon.

~#

Configure racoon and ipsec-tools
Note that a debconf script will pop up, asking for the way you will configure racoon. For now choose `direct' over `racoon-tool'. Here is what debconf says:

“Racoon can now be configured two way.
The traditional one (direct), which is for direct editing of /etc/racoon/racoon.conf and setup of the SPD using setkey via a shell script written by the systems administrator. You will have to make sure that the kernel has all required modules loaded or the racoon daemon can exit with a ‘failed to parse configuration file’ error.
The new one is the racoon-tool administration front end which configures both, as well as handling module loading and can handle most common setups. Please read /usr/share/doc/racoon/README.Debian for more details.”

Now that we’ve installed both racoon and ipsec-tools, we should configure them. Let’s edit /etc/ipsec-tools.conf on alfa:

```
#!/usr/sbin/setkey -f

## Flush the SAD and SPD
#
flush;
spdflush;

# Create policies for racoon
spdadd 172.16.23.0/24 172.16.10.0/24 any -P in ipsec
esp/tunnel/2.3.4.5-1.2.3.4/require;

spdadd any 172.16.10.0/24 172.16.23.0/24 -P out ipsec
esp/tunnel/1.2.3.4-2.3.4.5/require;
```

and /etc/racoon/racoon.conf:

```
path pre_shared_key “/etc/racoon/psk.txt”;

# bravo SG
remote 2.3.4.5 {
exchange_mode main;
proposal {
encryption_algorithm 3des;
hash_algorithm md5;
authentication_method pre_shared_key;
dh_group modp1024;
}
}

sainfo anonymous {
pfs_group modp768;
encryption_algorithm 3des;
authentication_algorithm hmac_md5;
compression_algorithm deflate;
}
```

/etc/racoon/psk.txt:

2.3.4.5 Queedeethohw2Ozi9ohCaiNgohm4pig6Ahtai3aerei9oohoPa

Now configure the same things on bravo:

/etc/ipsec-tools.conf:

```
#!/usr/sbin/setkey -f

## Flush the SAD and SPD
#
flush;
spdflush;

# Create policies for racoon
spdadd 172.16.10.0/24 172.16.23.0/24 any -P in ipsec
esp/tunnel/1.2.3.4-2.3.4.5/require;

spdadd any 172.16.23.0/24 172.16.10.0/24 -P out ipsec
esp/tunnel/2.3.4.5-1.2.3.4/require;
```

and /etc/racoon/racoon.conf:

```
path pre_shared_key “/etc/racoon/psk.txt”;

# alfa
remote 1.2.3.4 {
exchange_mode main;
proposal {
encryption_algorithm 3des;
hash_algorithm md5;
authentication_method pre_shared_key;
dh_group modp1024;
}
}
```

/etc/racoon/psk.txt

```
1.2.3.4 Queedeethohw2Ozi9ohCaiNgohm4pig6Ahtai3aerei9oohoPa
```

Now on *both* security gateways, ensure proper file permissions:

```
chmod 600 /etc/ipsec-tools.conf /etc/racoon/racoon.conf /etc/racoon/psk.txt
```

Routing and firewalling issues

Although IPSec and Netfilter are two different things, they need to co-operate and play well together. In majority of cases our security gateway will act as firewall, and also SNAT-ing the internal network as it has non-routable addresses. Few things should be done and checked to be sure everything is OK:

1. Make sure you have turned on ip_forwarding
2. Don’t SNAT or MASQUERADE esp and ah. Look at this fragment:

iptables -t nat -A POSTROUTING -o $EXT_IF -p esp -j ACCEPT
iptables -t nat -A POSTROUTING -o $EXT_IF -p ah -j ACCEPT

iptables -t nat -A POSTROUTING -o $EXT_IF -j SNAT –to-source $ext_ip_addr or
iptables -t nat -A POSTROUTING -i $EXT_IF -j MASQUERADE

3. Set the MTU of the network interface to around 1380-1400
ip link set dev ethX mtu 1380 , or
ifconfig ethX mtu 1380 , or better put it into /etc/network/interfaces

auto ethX
iface ethX inet static
address 192.168.1.2
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
mtu 1380

If you want to set TCP MSS for a particular network, port, etc. you can do it with iptables:
iptables -t mangle -A FORWARD -s $NETA -d $NETB -i ethX -p tcp -m tcp –tcp-flags SYN,RST SYN -j TCPMSS –set-mss 1380

Start
Now, after everything is configured, it’s time for testing. Set up security policies:
/etc/init.d/setkey start

Start racoon:
/etc/init.d/racoon start

you should see something like this is /var/log/syslog:
Jan 17 00:56:16 helene racoon: INFO: @(#)ipsec-tools 0.6.3 (http://ipsec-tools.sourceforge.net)
Jan 17 00:56:16 helene racoon: INFO: @(#)This product linked OpenSSL 0.9.8a 11 Oct 2005 (http://www.openssl.org/)
Jan 17 00:56:17 helene racoon: INFO: 127.0.0.1[500] used as isakmp port (fd=7)
Jan 17 00:56:17 helene racoon: INFO: 127.0.0.1[500] used for NAT-T
Jan 17 00:56:17 helene racoon: INFO: 217.18.246.110[500] used as isakmp port (fd=8)
Jan 17 00:56:17 helene racoon: INFO: 217.18.246.110[500] used for NAT-T
Jan 17 00:56:17 helene racoon: INFO: 192.168.0.1[500] used as isakmp port (fd=9)
Jan 17 00:56:17 helene racoon: INFO: 192.168.0.1[500] used for NAT-T
Jan 17 00:56:17 helene racoon: INFO: 192.168.1.1[500] used as isakmp port (fd=10)
Jan 17 00:56:17 helene racoon: INFO: 192.168.1.1[500] used for NAT-T

Now

Jan 17 00:56:41 helene racoon: INFO: IPsec-SA request for 213.169.63.98 queued due to no phase1 found.
Jan 17 00:56:41 helene racoon: INFO: initiate new phase 1 negotiation:

217.18.246.110[500]<=>213.169.63.98[500]
Jan 17 00:56:41 helene racoon: INFO: begin Identity Protection mode.
Jan 17 00:56:41 helene racoon: INFO: received Vendor ID: DPD
Jan 17 00:56:41 helene racoon: INFO: ISAKMP-SA established 217.18.246.110[500]-
213.169.63.98[500] spi:1ea07af90e201e2e:5abce7641fb2acd3
Jan 17 00:56:42 helene racoon: INFO: initiate new phase 2 negotiation:
217.18.246.110[500]<=>213.169.63.98[500]
Jan 17 00:56:42 helene racoon: INFO: IPsec-SA established: ESP/Tunnel 213.169.63.98[0]-
>217.18.246.110[0] spi=71657333(0×4456775)
Jan 17 00:56:42 helene racoon: INFO: IPsec-SA established: ESP/Tunnel 217.18.246.110[0]-
>213.169.63.98[0] spi=233700488(0xdedfc88)

Hint: Establishing tunnel
Sometimes you want to test the tunnel, but you don’t have access to any mashine behind the firewall, so
you need special hint. If you spoof request for connection from computer in your local network(for example net:A) the tunnel will be established.

Issue the next command on alfa:
nmap -S 172.16.10.129 -sP 172.16.23.0/24 -e eth0

To run this command you need root privilegies because of -S option, which means to spoof
the address 172.16.10.129. We are using eth0 as output interface. In this example nmap will try
to scan network 172.16.23.0/24 for any reacheable hosts.

Resources

http://www.netbsd.org/Documentation/network/ipsec/

http://www.networksorcery.com/enp/protocol/esp.htm

http://www.networksorcery.com/enp/protocol/ah.htm

http://www.networksorcery.com/enp/topic/ipsecsuite.htm http://www.faqs.org/rfcs/rfc2401.html

http://www.ipsec-howto.org/x197.html
1 comment
1 Comment so far

ANKIT April 30th, 2010 9:35 am

Hi,
I have a problem regarding accessibilty of multiple remote hosts from one local host.
The scenario is that, i have three debian routers. shorewall and racoon are installed. Now i want to connect hosts to each routers and each host must ping remote hosts. How should i configure these routers, if using Racoon?
Please reply soon.
Thanking you.