Linux to IPsec VPN Hints

* Contents

- Introduction
- Links
- Routing tips
- Firewalling tips

* Introduction

This Nano-HowTo was made when connecting a Linux Gateway to a
WatchGuard X6000 VPN appliance using IKE, IPsec, ESP, 3DES, MD5, PF2.
The actual target was Ö-Ticket, Austria's largest event ticket company.

Since linux kernel 2.6 introduced ipsec to the vanilla kernel ("26sec"),
there are plenty of methods to connect Linux to an IPsec based VPN.

This text describes how to connect to Oe-Ticket's VPN with 2 solutions:
- isakmpd (originating from OpenBSD)
- racoon & ipsec-tools (AKA KAME-tools)

The hints in the tips sections would have saved me 2 long work days!

* Important Links:

Main IPsec-HowTo, Introduction and (too) short examples:
www.ipsec-howto.org
especially:
KAME
isakmpd

Firewalling problems and strategies:
IPseconLinux.pdf

Introduction and samples in German:
kernel-ipsec.html

Raccoon error message decoder ring:
www.fefe.de/racoon.txt

* Routing Tips

Since 26sec, you don't have a ipsec0 interface and you do not see the
ipsec tunnel in the netstat -rn output. This sucks, but do not try to
add weird routes!

When having routing or even ping'ing problems, do not forget that
traffic from the gateway itself is treated differently than traffic
from the tunneled internal network!

If you want to connect from the ipsec'ing, you must not use the default
source interface (i.e. the world interface that hosts the ipsec tunnel)
but have to use an source address within the tunneled internal network.
Use e.g.
ping -I 10.0.1.1 10.0.2.1
or
telnet -b 10.0.1.1 10.0.2.1 80
etc. (I don't know the squid hack yet)

* Firewalling Tips

If you run netfilters (iptables), know these:
- you have to accept port 500 and 4500 udp+tcp traffic (from the VPN server) for IKE key exchange
- you have to accept -p esp traffic! (from the VPN server) to be able to receive answers
- some TCP applications have problems with too large packets, so force down the MTU size for tunneled packets, using something like this:
iptables -A FORWARD -p tcp --tcp-flags SYN,RST SYN -d 10.1.1.0/24 -j TCPMSS --set-mss 1300

From: IBCL BLog.
Originally posted: 2006-09-21