Subject: Re: Re: IPsec packets from VEs sent to wrong interface
Posted by marcusb on Tue, 24 Jun 2008 07:39:11 GMT
View Forum Message <> Reply to Message

Hi,

Denis V. Lunev wrote:
> I think the problem is in you routing setup.

I've checked but don't see anything suspicious. The routing setup is very simple.

[host:~]# ip route
172.16.2.2 dev eth0 scope link src 172.16.1.1
172.16.1.101 dev venet0 scope link
x.y.z.0/25 dev eth0 proto kernel scope link src x.y.z.w
172.16.1.0/24 dev br0 proto kernel scope link src 172.16.1.1
default via x.y.z.1 dev eth0

[host:~]# ip route get 172.16.2.2
172.16.2.2 dev eth0 src 172.16.1.1
    cache expires 21334342sec mtu 1500 advmss 1460 hoplimit 64

(Public IP addresses have been altered.)

ping from 172.16.2.2 to 172.16.1.1 works, but the other direction does not. When trying, the host node sends out ARP requests for 172.16.2.2 unencrypted on eth0, ignoring IPsec policy.

[host:~]# setkey -DP
172.16.2.2[any] 172.16.1.0/24[any] any
        in ipsec
        esp/tunnel/a.b.c.d-x.y.z.w/unique#16397
        created: Jun 24 09:03:28 2008 lastused: Jun 24 09:16:11 2008
        lifetime: 0(s) validtime: 0(s)
        spid=1656 seq=1 pid=2200
        refcnt=1
172.16.1.0/24[any] 172.16.2.2[any] any
        out ipsec
        esp/tunnel/x.y.z.w-a.b.c.d/unique#16397
        created: Jun 24 09:03:45 2008 lastused: Jun 24 09:33:20 2008
        lifetime: 0(s) validtime: 0(s)
        spid=1673 seq=2 pid=2200
        refcnt=3
172.16.2.2[any] 172.16.1.0/24[any] any
        fwd ipsec
        esp/tunnel/a.b.c.d-x.y.z.w/unique#16397
        created: Jun 24 09:03:28 2008 lastused:
        lifetime: 0(s) validtime: 0(s)
        spid=1666 seq=3 pid=2200

refcnt=1

Cheers,

Marcus