

Re: Encrypt some services with ipsec

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-09/0044.html>

From: Bigby Findrake (*bigby_at_ephemeron.org*)

Date: 09/25/05

Date: Sat, 24 Sep 2005 21:57:57 -0700 (PDT)
To: "carlopmart@gmail.com" <carlopmart@gmail.com>

On Sat, 24 Sep 2005, carlopmart@gmail.com wrote:

> *Hi all,*
>
> *I have two prodction servers with FreeBSD 5.4 (all security patches*
> *are applied). They running some services like dns, ssh, http, ftp, etc.*
> *But I would like to encrypt some services for some hosts with ipsec when*
> *it is accessed. For example:*
>
> *– DNS resolution: not encrypted.*
> *– DNS replication master–slave: encrypted by ipsec.*
> *– Telnet: encrypted by ipsec for some hosts. Deny for the rest.*
> *– SSH: not encrypted for some hosts, encrypted by ipsec for the rest.*
> *– FTP: encrypted by ipsec.*
> *– HTTP: encrypted by ipsec.*
>
> *is it possible to encrypt only certains services under ipsec tunnel??*

Someone please check my work.

>*From the man page on setkey, it looks like you can specify ports for the*
security policies, so you could specify certain ports to encrypt, and not
specify a blanket/default host–to–host policy for all other traffic, so
that all other unspecified traffic is unencrypted.

For example:

```
-----BEGIN /ETC/IPSEC.CONF-----  
#  
# encrypt all dns traffic between master host A (1.1.1.1) slave host B  
# (1.1.1.2)  
spadd 1.1.1.1 1.1.1.2[53] any -P out ipsec esp/transport//use;  
spadd 1.1.1.2[53] 1.1.1.1 any -P in ipsec esp/transport//use;  
  
spadd 1.1.1.1[53] 1.1.1.2 any -P out ipsec esp/transport//use;  
spadd 1.1.1.2 1.1.1.1[53] any -P in ipsec esp/transport//use;
```

FreeBSD-Security: Re: Encrypt some services with ipsec

```
#
# encrypt telnet traffic between server A (1.1.1.1) and client C (1.1.1.3)
spadd 1.1.1.1[23] 1.1.1.3 any -P out ipsec esp/transport//use;
spadd 1.1.1.3 1.1.1.1[23] any -P in ipsec esp/transport//use;

#
# encrypt http traffic between server A (1.1.1.1) and client D (1.1.1.4)
spadd 1.1.1.1[80] 1.1.1.4 any -P out ipsec esp/transport//use;
spadd 1.1.1.4 1.1.1.1[80] any -P in ipsec esp/transport//use;

#
# and all other traffic is unencrypted.
-----END /ETC/IPSEC.CONF-----
```

```
/-----/
I used to hate weddings; all the Grandmas would poke me and
say, "You're next sonny!" They stopped doing that when i
started to do it to them at funerals.
```

```
finger://bigby@ephemeron.org
http://www.ephemeron.org/~bigby/
news://news.ephemeron.org/alt.lemurs
/-----/
```

freebsd-security@freebsd.org mailing list
<http://lists.freebsd.org/mailman/listinfo/freebsd-security>
To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"