

## Re: dynamic IPSEC

**Source:** <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2003-08/0127.html>

---

**From:** Christian Kratzer ([ck-lists\\_at\\_cksoft.de](mailto:ck-lists_at_cksoft.de))

**Date:** 08/12/03

Date: Tue, 12 Aug 2003 09:06:17 +0200 (CEST)  
To: [questions@freebsd.org](mailto:questions@freebsd.org), [security@freebsd.org](mailto:security@freebsd.org)

Hi,

On Mon, 11 Aug 2003, Kent Hauser wrote:

> *Hi Mike,*  
>  
> *Had any progress? I've also been stymied for a clean solution. Previously, I*  
> *used a simple SED script from executed from "/etc/ppp/ppp.linkup" to edit a*  
> *"setkeys" script which then negotiated with the office ascend router/gw & all*  
> *was VPN heaven. However, I now need to negotiate mobile(FreeBSD) to*  
> *static(FreeBSD) & that is proving problematic. Executing a SED script after*  
> *DHCP of mobile is easy, but it seems I also need to SED the static host's SPD*  
> *-- ie no wildcards allowed as in the ascend router situation. Needless to*  
> *say, allowing "unauthenticated" hosts (read anyone) to modify the SPD on a*  
> *machine so that it can be authenticated strikes me as putting the cart before*  
> *the horse.*  
>  
> *When I install a "wildcard" host (0.0.0.0) on the static side, racoon only*  
> *negotiates the mobile->static SAD...which is useless & expires. Seems to me*  
> *that racoon needs to update kernel SPDs with wildcards to support mobile*  
> *VPNs. At least that's all I've been able to come up with.*  
>  
> *Have you found a silver bullet?*

Solution 1:

the silver bullet to allow roaming clients with dynamic address to connect to your racoon is to have no policy at all defined for them and use an anonymous section your racoon.conf with

```
generate_policy on;
```

This way your clients connect and racoon sets up any policy they request.

This is a bit ugly as you have to trust them not to screw up your policy but seems to be the only solution currently available with racoon.

## FreeBSD-Security: Re: dynamic IPSEC

You will also want to use certificates instead of preshared keys for authentication unless you are comfortable with having a single preshared key for all your roaming users.

Solution 2:

We have a setup where we have 3 offices each with dynamic ip's and freebsd boxes as their gateways. The boxes all run scripts to register their dynamic ip address at a colocated box with a static ip. The boxes also resolve each others ip addresses every 5 minutes and generate a new ipsec.conf and install it if it differs from the previous one. The system is now very stable and we have ispec tunnels between all 3 offices.

If something changes they rewire themselves on the fly.

Greetings  
Christian

--

CK Software GmbH  
Christian Kratzer,                      Schwarzwaldstr. 31, 71131 Jettingen  
Email: ck@cksoft.de  
Phone: +49 7452 889-135      Open Software Solutions, Network Security  
Fax:    +49 7452 889-136      FreeBSD spoken here!

---

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"