Simple VPN

Shreyas Srivatsan

Maritza Johnson

Steven M. Bellovin

IPsec is Impossible to Configure

- There are $O(\aleph_0)$ different options
- (Maybe more than that; I can't count how many there are, and they keep inventing more of them)
- If you can't understand it, you can't configure it (let alone configure it correctly)

Jon Postel on the IETF, circa 1998

"It's perfectly appropriate to be upset. I thought of it in a slightly different way --- like a space that we were exploring and, in the early days, we figured out this consistent path through the space: IP, TCP, and so on. What's been happening over the last few years is that the IETF is filling the rest of the space with every alternative approach, not necessarily any better. Every possible alternative is now being written down. And it's not useful."

The Problem

- *Many* different options
- Different configuration for gateways, hosts, etc
- Different for each platform
- 95% (or more) of the options are completely irrelevant to 95% (or more) of the potential users

Simple VPN

- One configuration file for an entire network
- One policy decision
- One option
- You specify the topology and the platforms – the code generates config files for your platform (three different ones supported now), plus X.509 certificates (no PKI needed)
- You even get a picture of your configuration

No PKI Needed

- We don't need PKI for IPsec, we need pki
- We *certainly* don't need more options for IPsec
- Solution: Simple VPN generates public/private key pairs; no passwords needed
- Why not? They're just access tokens, and the administrator controls access anyway

Sample Configuration File

```
access "direct"
type "racoon"
authgen
vpn sample {
    nodes "ubuntu"{
        host 128.59.11.1, 128.59.12.1
        gw 128.59.13.1{
            subnet 128.59.13.0/24
        }
    }
}
```
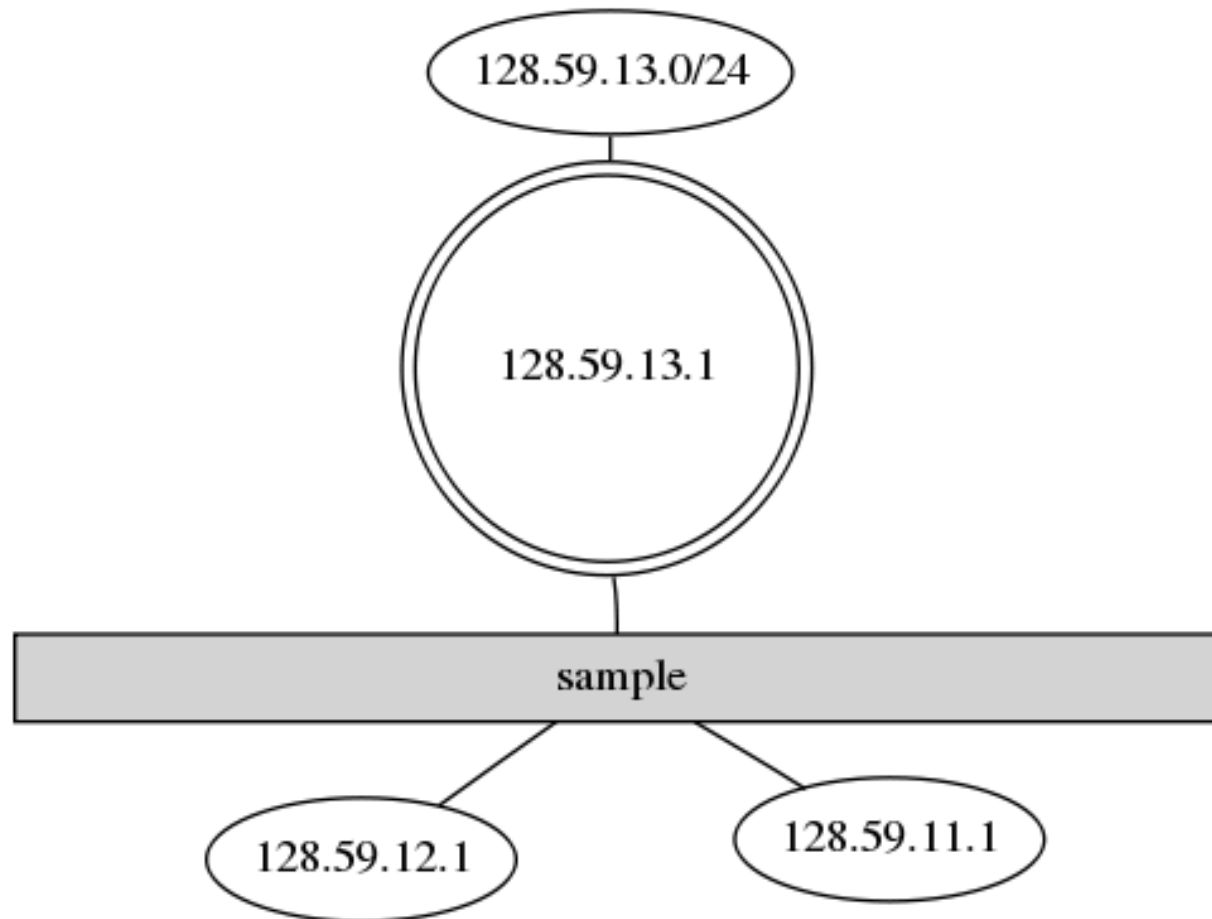
Your Move

- Code (BSD license):
  http://sourceforge.net/projects/simple-vpn/

- Tech report:
  http://mice.cs.columbia.edu/
  getTechreport.php?techreportID=1433

- Currently supports Openswan, Strongswan, and Racoon, on Linux

- Contributions welcome