

Building Linux Based Virtual Private Networks

Brian Elliott Finley, Sr. Area Engineer, VA Linux
<http://www.valinux.com/>

This session will cover building and using software based virtual private networks with Linux. It will include a presentation on VPN basics, how they work, and instructions on how to set up your own VPN for free.

Executive Summary

Linux is rapidly becoming a very popular platform for deploying virtual private networks (VPNs). Because of the firewalling capabilities built in to the Linux kernel, its interoperability, and due to the wide availability and choice offered by open source solutions, many companies and organizations are choosing Linux for the deployment of their VPNs.

What is a Linux VPN anyway? And why would I want one? Many companies have yet to realize the advantages of using VPNs for secure connectivity to and from remote sites. We will cover the basics of VPNs on Linux and will discuss some of their applications and benefits.

Different Linux based hardware and software VPN solutions will also be discussed. We will delve into some of the issues in implementing virtual private networks such as firewalling to make sure your virtual network is really private.

You will be shown how to create your own Linux VPN as we configure a live VPN using freely available tools and utilities. We will then use this VPN to access resources securely on a server across the Internet. You will be given all the information and references you need to go back to your job and set one up yourself.

Questions will be answered throughout the session.

Outline

VPN basics

- What is a VPN?
- Service based encrypted tunnels (HTTPS) versus VPNs
- What does a VPN do for me?
- Extending the LAN to remote office locations
- Less expensive than long distance charges
- More flexible than point to point leased lines

VPN building blocks

- Three networks
- Local office
- Remote office (or single user)
- Internet (or other connecting network)
- Firewalls at both ends
- It doesn't matter that your VPN is secure if someone has physical access to your site.
- Encryption over the connecting network

Building and using Linux based VPNs

- Why use Linux?
- Much less expensive than dedicated hardware
- Firewalling capabilities built into the kernel (expensive commercial software not necessary)
- More flexible -- change it as new software comes out
- Some Linux based VPN products
- Watchguard firebox (commercial product)
- vpnd
- vtun
- stunnel (service based tunnels)
- PoPToP
- SSH -- make your own
- There are most certainly others...

Demonstration

- Connect to Internet and show the network interfaces on the local firewall.
- Demonstrate that local machine can't access the remote intranet web server.

- Start up the VPN.
 - Demonstrate that local machine can now access the remote intranet web server.
 - Attempt to explain how it all works!
-

References

- Linux information: <http://linux.com/>
- The Linux HOWTO pages: <http://www.caldera.com/LDP/HOWTO/>
- The VPN HOWTO: <http://www.caldera.com/LDP/HOWTO/VPN-HOWTO.html>
- You can get SSH v1 from: <ftp://ftp.zedz.net/pub/crypto/ssh/ftp.ssh.fi/>
- vpnd homepage: <http://matrix.crosswinds.net/nuremberg/~anstein/unix/vpnd.html>
- vtun homepage: <http://vtun.sourceforge.net/>
- stunnel homepage: <http://opensores.thebunker.net/pub/mirrors/stunnel/index.html>
- OpenSSH homepage: <http://www.openssh.com/>
- Ipchains HOWTO:
<http://www.caldera.com/LDP/HOWTO/IPCHAINS-HOWTO.html>
- PoPToP homepage: <http://www.moretonbay.com/vpn/pptp.html>
- Watchguard: <http://www.watchguard.com/>

(Questions and Answers throughout)