

## IPCop: Net-Net VPN

Robert Munds, Network Admin  
Clinton Schools

### VPN?

- Virtual Private Network
  - Some of the links between nodes are carried by open connections
  - The link-layer protocols of the virtual network are said to be tunneled
  - One common application is secure communications through the public Internet

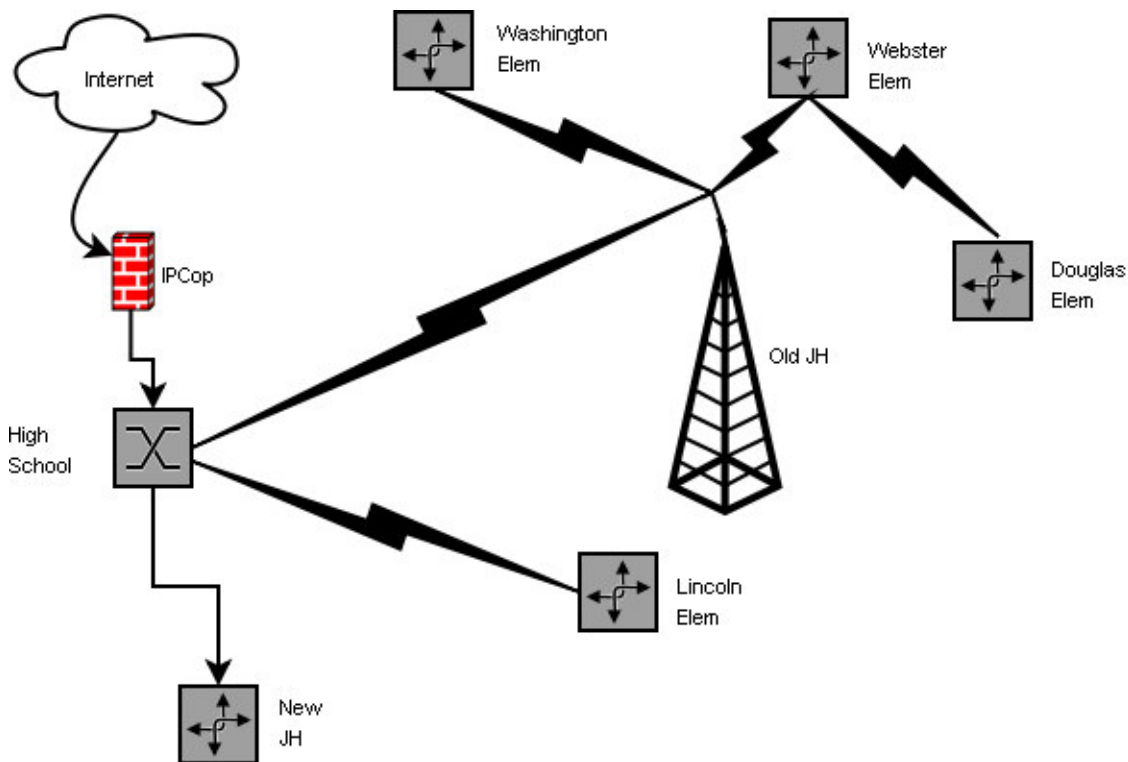
### IPCop

- **IPCop** is a Linux distro which provides a easy to manage firewall
- A fork of the Smoothwall Linux firewall
- IPCop includes a simple user managed mechanism

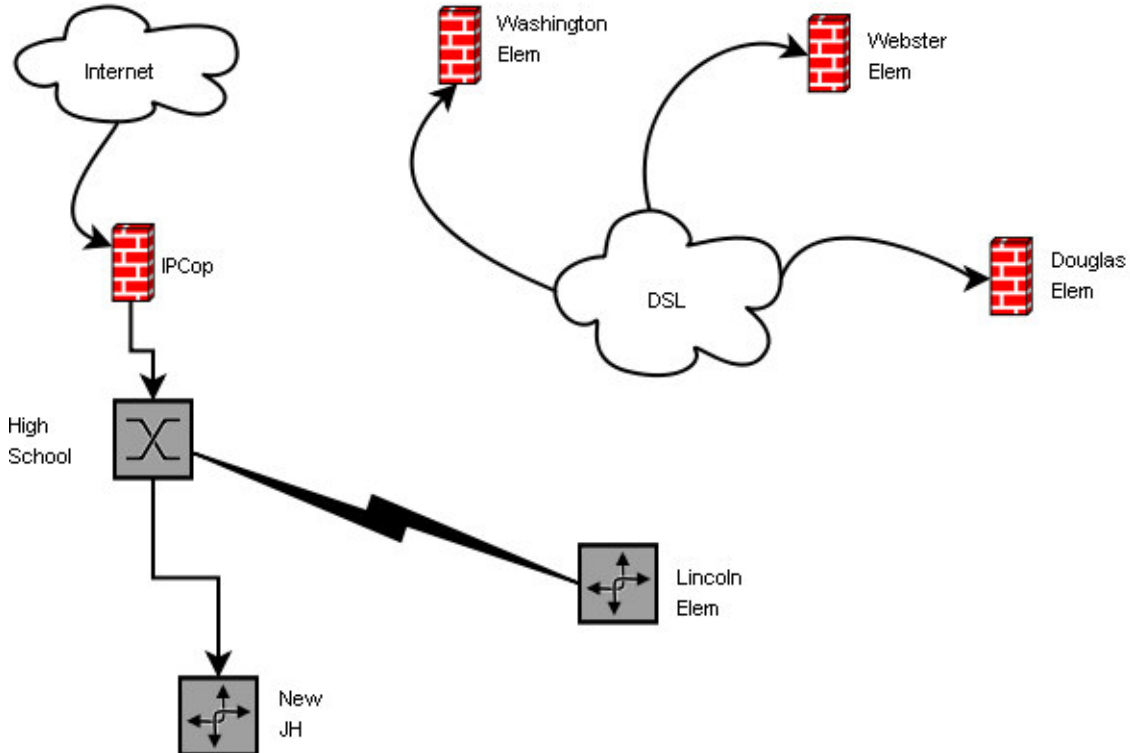
### Why VPN's?

- Formerly point-point wireless connections between buildings
- Demolition of old Jr. High eliminated central tower housing several antennas
- Vendor slow to install replacement wireless system
- Implemented DSL to 3 buildings on interim basis

### Previous Config



## Current Config



## Issues

- 3 elem buildings have internet access
- Netware servers unable to communicate
  - No eDirectory synchronization
- Main post office server cannot communicate with remote PO's
  - Staff cannot access e-mail
  - The Horror!

## Priorities

- Staff access to e-mail
- Netware servers “talk” to each other
- Network configured to function as if nothing had changed
  - New configuration transparent

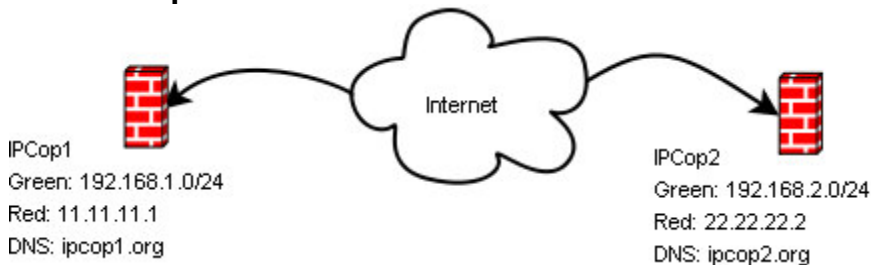
## How to implement

- Setup 2 IPCop boxes
  - Current version 1.4.21
- Setup an IPSec VPN between these boxes
  - Internet Protocol Security (IPSec)
  - A suite of protocols for securing IP communications by authenticating and encrypting

## Synchronize clocks

- Important note
  - It is essential to have clocks synchronized on both machines
- Here is one case
  - One clock was a few hours ahead
  - The certs generated were yet to become valid
  - A very uninformative failure that the CA was not available for my host verification
- To set: Services/Time Server

## Initial Setup



## Remove previous

- Remove all CA and certs
  - If any have been previously created
- Set “Local VPN Hostname/IP” public IP Address or DNS host name
- Check “Enabled”
- Click Save
- Reboot
  - just in case

## Generate Certificates

- On ipcop1: Hit “Generate Root/Host Certificates” fill the following values:
  - ipcop1 as the “Organization name”
  - ipcop1.org as the “IPCop's Hostname” (this will be filled in for you)
- Specify your Country
- Click “Generate Root/Host Certificates” button
  - This will generate the certificates (patience!) and will take you back to the VPN configuration page
- Click the “Download Root Certificate” button (icon like a floppy disk).
- You will be prompted for the file name to save.
- The default file name is cacert.pem.
- Just so there is no confusion change the name to cacert.1.pem
- Click the “Download Host Certificate” button
  - You will be prompted for the file name to save.
  - The default file name is hostcert.pem.
  - Just so there is no confusion change the name to hostcert.1.pem
- Repeat on IPCop2

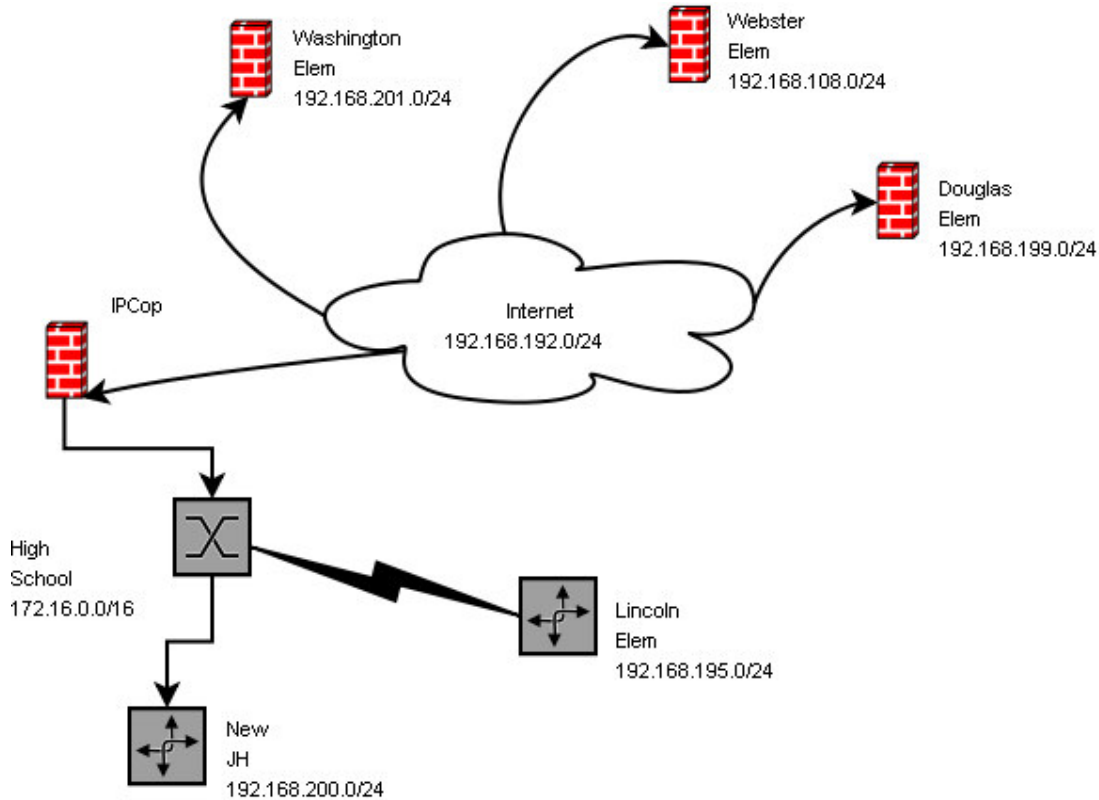
### **Update the CA Certificates**

- Let the 2 IPCop boxes know about the other CA (Certificate Authority)
  - They can trust the certificates issued by the other box
- On ipcop1:
  - Fill ipcop2 as the “CA name”
  - Browse and select the cacert.2.pem file
  - hit the “Upload CA Certificate” button
  - This will upload the CA certificate from ipcop2 to ipcop1 and it will show in the “Certificate Authorities” section
- Repeat on IPCop2

### **Create Connections**

- On ipcop1: Hit the “Add” button
- Select “Net-to-Net Virtual Private Network” for the “Connection type”
- Fill the following values:
  - ipcop2 as the “Name”
  - left as the “IPCop side”
  - 192.168.1.0/24 as the “Local subnet”
  - ipcop2.org as the “Remote Host/IP”
    - Or 22.22.22.2
  - 192.168.2.0/24 as the “Remote subnet”
- In the “Authentication” section select “Upload a certificate”
  - Check “Upload a certificate” and browse to the hostcert.2.pem file
- Click the “Save” button
- Repeat on IPCop2
  - Reverse addresses

## Multiple Buildings



## Multiple VPN's

- Configure VPN links for:
  - Main – Douglas
  - Main – Webster
  - Main – Washington
  - Douglas – Webster
  - Douglas – Washington
  - Webster - Washington

## Main IPCop Routing Table

- Next hops to:
  - Default:gateway (eth1)
  - Lincoln: 192.168.192.195
  - JH: 192.168.192.200
  - HS: 192.168.192.244
  - Douglas: gateway (ipsec)
  - Webster: gateway (ipsec)
  - Washington: gateway (ipsec)

## **Houston, ...**

- Server at Webster cannot communicate with host at HS, Lincoln or JH
- There is a problem with the routing table on each IPCop box
- TraceRt Webster server -> HS server
  - Not in local network
  - IPCop
  - 172.16.2.5 not in routing table
  - Sends to default route – the internet
  - DIES!

## **Solution**

- Add IPsec routes Webster IPCop
  - Web172 (to HS)
  - Web195 (Lincoln)
  - Web200 (JH)
- All have remote destination the Main IPCop
- Same for all IPCop boxes

## **Another TraceRt**

- TraceRt Webster server -> HS server
  - Not in local network
  - IPCop
  - 172.16.2.5 in routing table
    - IPsec route to 172.16.0.0/16 network
  - Sends to IPsec port on main IPCop
  - 172.16.0.0/16 in routing table
    - Forwards to 192.168.192.244

## **Three Step Solution**

- ONE – access e-mail
  - Port forward rules sending e-mails from main PO to public address of IPCop
- TWO – Sync eDirectory
  - Implement VPN
  - Main server can sync, but HS, JH & Lincoln servers can't see Douglas, Webster & Wash
- THREE – Completely transparent
  - Multiple VPN's
- All this took was three weeks of experiments!

## **Problem**

- Asynchronous nature of DSL
  - 7M bps down
  - 768K bps up
- Copy files (backup?) from remote sites now takes days instead of hours

## **Solution**

- Replace DSL with faster links
- We've chosen wireless
- 150M bps point-point (Motorola)
- New water tower next to HS
  - No need to have our own tower!

## **References**

- IPCop: [www.ipcop.org](http://www.ipcop.org)
- [www.databrokers.net/opensource/ipcop/vpn-to-vpn-detailed-how-to.html](http://www.databrokers.net/opensource/ipcop/vpn-to-vpn-detailed-how-to.html)