Firewalling an advertising company

Using FreeBSD to provide Firewall and
VPN services for an advertising agency

Head office goals and challenges

- Secure workstations
- Secure hosted machines
- Secure hostile machines
- Provide VPN endpoint for colo, branches and suppliers
- Reduce costs, and if possible, improve existing solution

- Branches not ready to move to FreeBSD, so must be able to provide VPN endpoint for them

Colocation goals

- Secure hosted services
- Provide VPN endpoint for Head Office machines
- Provide VPN endpoint for clients

Reasons for choosing FreeBSD

- Standards compliant
- IPSec implementation interoperates well with Checkpoint and Symantec
- Costs
- Have skills in-house

Firewalling the office

- 2U server with 4 100Mb network cards running FreeBSD 5.2.1
- IPFW for firewalling
- IPSec and Racoon for VPN solution
  - Card 1 -> Internet connection
  - Card 2 -> Workstations, using natd via card 1
  - Card 3 -> Hosted servers (mail, dns, etc)
  - Card 4 -> Hostile servers

Firewalling the colocation facility

- 2U server with 3 100Mb Intel network cards running FreeBSD 5.2.1
- IPFW for firewalling
- IPSec and Racoon for VPN solution
  - Card 1 -> Internet connection
  - Card 2 -> Hosted servers switch
  - Card 3 -> Private network switch for VPN's

Preparing the machine for IPFW

- Add the following lines to your kernel config:
  - options IPFIREWALL
  - options IPFIREWALL_VERBOSE
  - options IPFIREWALL_VERBOSE_LIMIT=10
  - options IPFIREWALL_DEFAULT_TO_ACCEPT
- If you want to do NAT as well (as we do at Head office,) also add
  - options IPDIVERT

Preparing the machine for IPFW

- Add the following lines to /etc/rc.conf
  - firewall_enable="YES"
  - firewall_logging="YES”
  - firewall_quiet="YES"
  - firewall_script="/etc/firewall/ipfw.harden"
- If you want to do NAT (as we do at the Head Office), also add
  - natd_enable="YES”
  - natd_interface="193.30.111.243”
  - natd_flags="-s -u -m"

Preparing the machine for IPSec

- Add the following lines to your kernel
  - options IPSEC
  - options IPSEC_ESP
- While you are testing, you might also want to add
  - options IPSEC_DEBUG

IPFW - Next steps

- Create firewall rules script
  - Setup ipfw command (quiet or not, depending on rc.conf)
  - Flush existing rules
  - Setup loopback and allow outgoing traffic on relevant interfaces
  - Deny private networks on your Internet connection
  - Include anti-spoofing rules
  - Add individual rules to allow access to relevant services on machines
  - Include a rule to deny with tcp-rst to your smtp server, port 113 for faster mail handshakes
  - Ensure that last rule is to deny all
- Copy firewall rules script into /etc/firewall (or wherever you specified in /etc/rc.conf)

VPN - Next steps

- Setup /etc/ipsec.conf
  - Flush all SAD and SPD entries
  - Setup rules for each Tunnel as follows

spdadd our.internal.net/mask their.internal.net/mask any -P out ipsec esp/tunnel/our.public.ip-their.public.ip/require ;

spdadd their.internal.net/mask our.internal.net/mask any -P in ipsec esp/tunnel/their.external.ip-our.external.ip/require;

VPN - Next steps

- Install racoon from ports
- Set permissions on /usr/local/etc/racoon/psk.txt (600)
- Make any changes to /usr/local/etc/racoon/racoon.conf

Final step

- Re-compile your kernels
- Reboot the machines
- Attempt to access a forbidden service
- Attempt to access a provided service
- Attempt to connect from one private network to another over VPN

What if it doesn’t work - FW

- First, check /var/log/security - attempt the connection and see what is produced there
- Check your firewall rules
  - # ipfw list
- Ensure that the firewall is running
  - # sysctl net.inet.ip.fw.enable

    should produce

    net.inet.ip.fw.enable: 1

What if it doesn’t work - VPN

- Ensure that both endpoint machines can make connections to 500/udp on the other endpoint
- Check your SAD and SPD entries
  - setkey -DP; setkey -DP
- Increase the debug level in the racoon conf by changing the
  - log notify;

    to

    log debug;
- Check your racoon log in /var/log/racoon

Benefits - Cost

- A FreeBSD firewall / VPN solution has a software and licensing cost of GBP0.00 + install time.
- Symantec Firewall version 7 costs GBP2,500.00 per year
- With some commercial firewalls, If you need more outgoing web connections, you have to pay more
- With some commercial you need a higher level of encryption than des (i.e. 3des), you have to pay more

Benefits - Flexibility

- With FreeBSD, you can firewall connections from a VPN site on the destination side. This does not appear to be possible in Symantec
- We've been able to act as a VPN endpoint for more different VPN devices than the Symantec solution. They were unable to inter-operate with Checkpoint or Checkpoint-NG
- Logging is far better, and faults are easier to diagnose and rectify

Conclusion

- The operating system that we are running on can be locked down, so the firewall is running on a solid base
- We've been able to provide a more flexible solution at a lower cost
- All of this should be possible on the BSD of your choice

Still to do

- Add transparant proxy for outgoing web traffic
- Add a FreeBSD mail server before the Exchange server to do spam filtering and anti-virus