



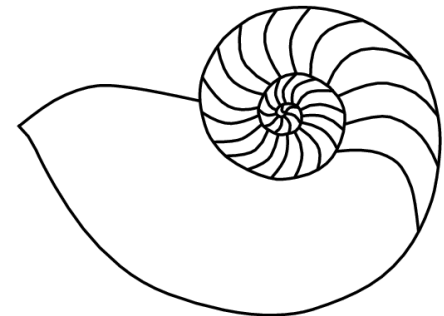
UNIVERSITY
OF MANITOBA

Computer Science

Firewall Software for UNIX

Gilbert Detillieux

February 10, 2009
MUUG Meeting

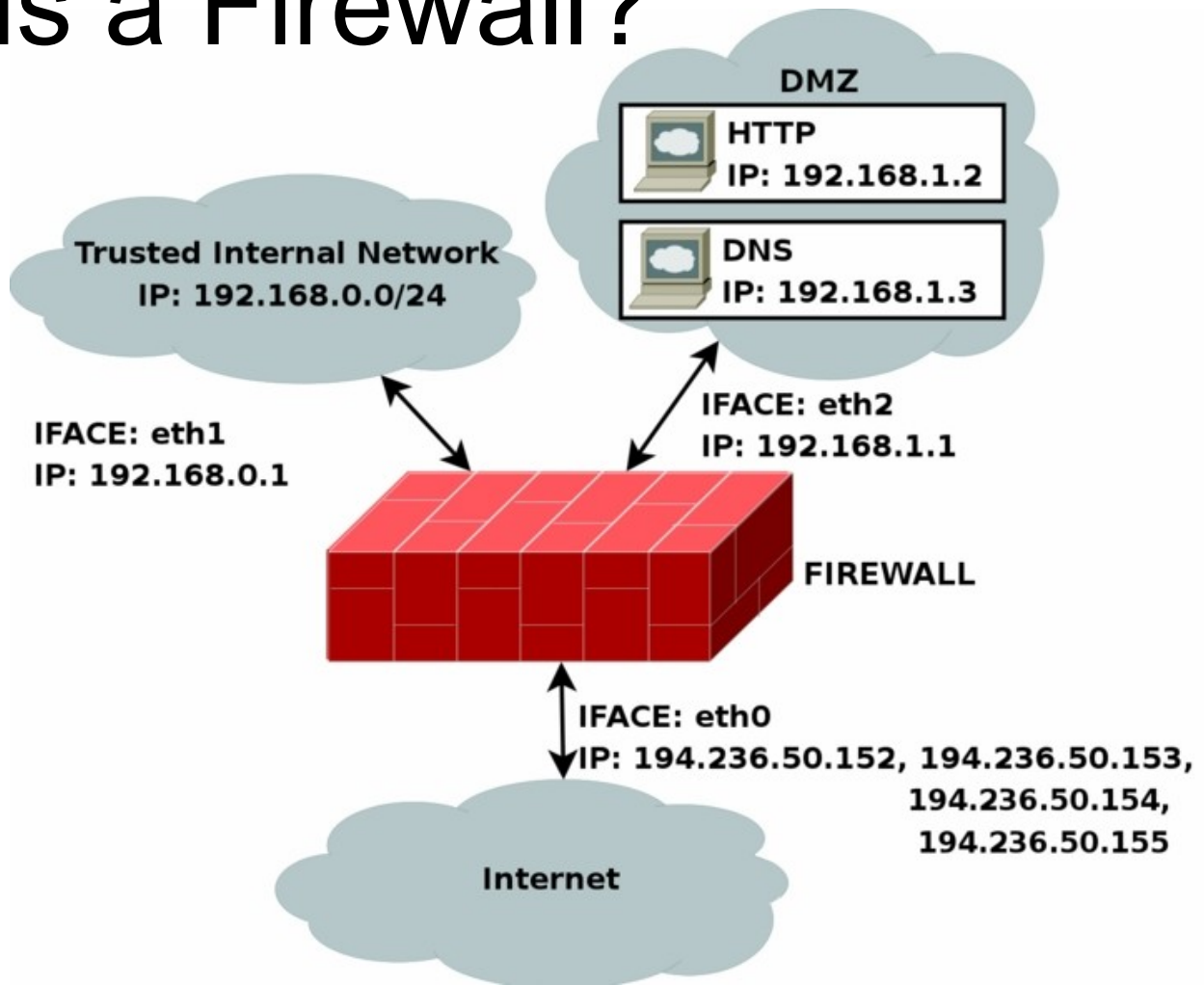




What is a Firewall?

- Typically, a dedicated box
- Can either be special hardware or a generic computer
- Mediates network traffic between internal network and external (Internet)
- Blocks undesirable traffic (in one or both directions)

What is a Firewall?





Enterprise Firewall Limitations

- No protection from internal attacks
 - E.g. internal hosts compromised by virus
- Hard to protect DMZ hosts
- Hard to deal with complex networks
 - E.g. campuses with lots of servers
 - Performance issues under high traffic loads

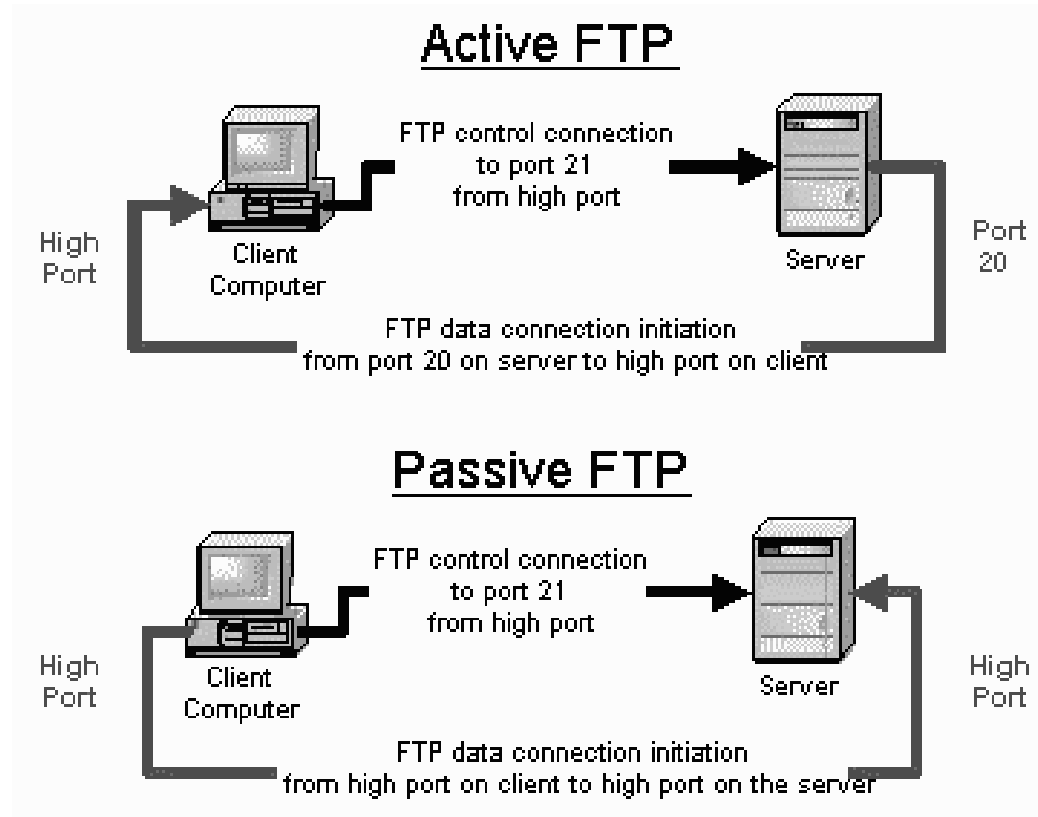
What is a Software Firewall?

- Typically, an in-kernel packet filter
- Configured via user-mode
 - Commands
 - Configuration files
 - Possibly with a GUI front-end
- Rules to match IP source/dest *address*, *s/d port*, *proto*, *direction* (in/out), *interface*, etc.
- Allow/accept/pass/permit desirable packets
- Block/deny/drop undesirable packets, or...
- Reject/return packets
- Stateless or stateful operation

What is Connection Tracking?

- State tracking
 - Remember src/dest addr/port/proto of desired traffic in one direction
 - Allow replies to these through as well
- This isn't enough...
 - What about broadcast requests?
 - What about related connections on other ports?

Why is FTP a Problem?



What Else Is a Problem?

- Broadcast-based traffic
 - NetBIOS Name Services (e.g. in Samba)
- Other services with related connections
 - Amanda backup service
 - IRC
 - H323, SCTP, SIP
 - PPTP
- NAT

IPFilter (or “ipf”)

- Included in Solaris 10 and OpenSolaris
- Available for Linux, BSD-based & other UNIX flavours
- Rules read from one file (ipf.conf)
- ***Last*** matching rule is applied
 - Can use “**quick**” keyword to stop search
- No GUI in Solaris, but **fwbuilder** available

IPFilter Rules (ipf.conf)

- **block/pass in/out [log] [quick] [on *i/f*] [proto tcp/udp/icmp] [all]/[from *addr* [port = *port*] to *addr* [port = *port*]] [flags *f*] [with *opt*] [keep state]**
- Examples:
 - pass in quick on lo0 all
 - block in on bge0 all
 - pass out proto tcp/udp from any to any keep state

IPFilter Example Rules (ipf.conf)

```
# Block any packets which are too short to be real
block in log quick all with short
# drop and log any IP packets with options set in them.
block in log all with ipopts
# Allow all traffic on loopback.
pass in quick on lo0 all
pass out quick on lo0 all
# Public Network.  Block everything not explicitly allowed.
block in all
#block out all
# Allow ICMP in/out.
pass in quick proto icmp all keep state
pass out quick proto icmp all keep state
# Allow outbound state related packets.
pass out quick proto tcp/udp from any to any keep state
# allow ssh from anywhere
pass in quick proto tcp from any to any port = 22 flags S keep state
```

What About NetBIOS Name Service Request Broadcasts?

- State table contains outbound request to a broadcast address
- Incoming replies will be to our own address
- Crude ipf.conf solution:
 - pass in quick proto udp from 192.168.1.0/24 to any port = 137
 - pass in quick proto udp from 192.168.1.0/24 port = 137 to any
 - pass out quick proto udp from any to any port = 137

What About FTP Server (Passive Mode)?

- Problem: Need to accept incoming data connections from/to unknown port numbers
- Restrict port range in FTP server, e.g. vsftpd:
 - `pasv_min_port=7000`
 - `pasv_max_port=7999`
- Crude ipf.conf solution:
 - `pass in quick proto tcp from any to <thishost> port = 21 flags S keep state`
 - `pass in quick proto tcp from any to <thishost> port 6999 >< 8000 flags S keep state`

Enabling IPFilter on Solaris

- Make sure package is installed...
 - Solaris 10: **SUNWipfu, SUNWipfr**
 - OpenSolaris: **SUNWipf**
- Edit **/etc/ipf/ipf.conf**
- **# svcadm enable network/ipfilter**
- To reload after file change:
 - **# svcadm refresh network/ipfilter**
 - **# /lib/svc/method/ipfilter reipf**

Monitoring IPFilter

- To check hit counts (*summary or by rule*):
 - # **ipfstat -h[io][n]**
- To view state table (*statistics or list*):
 - # **ipfstat -s[I]**
 - # **ipfstat -t[C]** (*state top mode*)
- To monitor log device:
 - # **ipmon**

IPFilter Resources

■ General:

- <http://en.wikipedia.org/wiki/IPFilter>
- <http://coombs.anu.edu.au/~avalon/ip-filter.html>
- <http://www.phildev.net/ipf/>
- <http://www.obfuscation.org/ipf/>
- <http://home.claranet.nl/users/guido/bsdcon2000/index.html>

■ Solaris:

- <http://docs.sun.com/app/docs/doc/819-3000/eupsq?a=view>
- <http://docs.sun.com/app/docs/doc/819-3000/etmhi?a=view>
- http://www.softpanorama.org/Net/Network_security/Firewalls/ip_filter.shtml
- http://www.homepage.montana.edu/~unixuser/031705/create_solaris_ipf.html
- <http://ma.yer.at/fwbuilder/>

IPFirewall (or “ipfw”)

- Included in Mac OS X 10.3 and later
- Available for FreeBSD
- Ported to Windows 2000 & later (**wipfw**)
- Rules added by command or config files
- Rule # specified to determine order
- Different GUI for different Mac OS X version
- Third-party GUI's also available

IPFW Rules

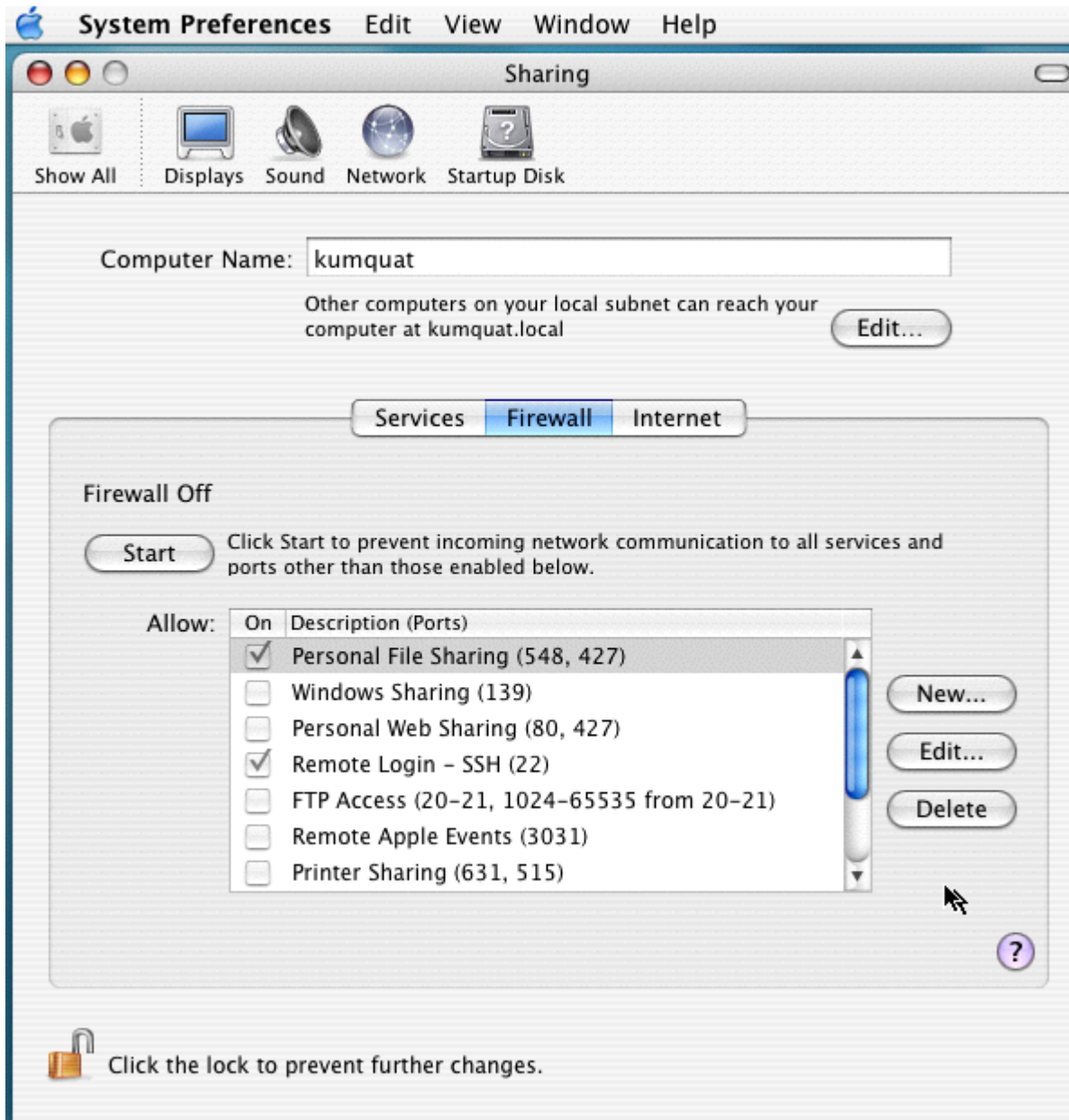
- **add *rulenum***
allow/accept/pass/permit/deny/drop [log]
[*proto* from *addr* [*port*] to *addr* [*port*]] [*options*]
- **Examples:**
 - add 1000 allow all from any to any via lo0
 - add 12300 allow tcp from any to any established
 - add 12301 allow tcp from any to any out
 - add 12302 allow tcp from any to any 22
 - add 12303 allow udp from any to any out keep-state
 - add 65534 deny log ip from any to any



IPFW Features & Limitations

- Similar functionality to IPFilter
- State table mechanism has similar limitations:
 - No connection tracking for related ports
 - Replies to broadcast requests also won't match saved state
- Rules can match in/out packets (or both)
- Ranges & lists allowed for IP addresses & ports:
 - `add 12334 allow tcp from any to any 5900-5906`

Mac OS X 10.3: System Preferences / Sharing



Mac OS X 10.5: System Preferences / Security

The screenshot shows the 'Security' window in Mac OS X 10.5, with the 'Firewall' tab selected. The window title is 'Security'. The menu bar includes 'System Preferences', 'Edit', 'View', 'Window', and 'Help'. The window has standard Mac OS X window controls (red, yellow, green buttons) and a 'Show All' button. A search field is visible in the top right corner. The 'Firewall' tab is active, showing three radio button options: 'Allow all incoming connections' (selected), 'Allow only essential services', and 'Set access for specific services and applications'. Below these options is a text box containing 'File Sharing (AFP)', 'Remote Login (SSH)', and 'Screen Sharing'. At the bottom of the window, there is a lock icon with the text 'Click the lock to prevent further changes.' and a help icon (question mark).

System Preferences Edit View Window Help

Security

Show All

General FileVault Firewall

Allow all incoming connections

Allow only essential services

Set access for specific services and applications

Mac OS X normally determines which programs are allowed incoming connections. Select this option if you want to allow or block incoming connections for specific programs.

File Sharing (AFP)
Remote Login (SSH)
Screen Sharing

+ -

Advanced...

Click the lock to prevent further changes.

Mac OS X 10.5 Server: Server Admin / Firewall

The screenshot shows the Server Admin application window for the 'aluminum.cs.umanitoba.ca' server, specifically the Firewall configuration page. The 'Services' tab is selected, showing a list of services to be allowed or blocked. The 'Edit Services for:' dropdown is set to 'any'. The 'Allow only traffic from "any" to these ports:' radio button is selected. The table below lists various services with their respective ports and protocols.

Server Admin:aluminum.cs.umanitoba.ca:Firewall

Address Groups Services Logging Advanced

Edit Services for: any

Allow all traffic from "any"

Allow only traffic from "any" to these ports:

Allow	Description	Ports	Protocol
<input checked="" type="checkbox"/>	TCP (outgoing)		TCP UDP
<input checked="" type="checkbox"/>	TCP (established)		TCP UDP
<input checked="" type="checkbox"/>	UDP Fragments		TCP UDP
<input checked="" type="checkbox"/>	UDP outbound and responses to same port		TCP UDP
<input type="checkbox"/>	UDP inbound and responses to same port		TCP UDP
<input type="checkbox"/>	GRE - Generic Routing Encapsulation protocol		GRE
<input type="checkbox"/>	ESP - Encapsulating Security Payload protocol		ESP
<input checked="" type="checkbox"/>	IGMP - Internet Group Management Protocol		IGMP
<input type="checkbox"/>	ICMP - all messages		ICMP
<input type="checkbox"/>	Amanda Backup Services	10080	TCP UDP
<input type="checkbox"/>	Password Server	106,3659	TCP UDP
<input type="checkbox"/>	WebObjects	1085	TCP UDP
<input type="checkbox"/>	Remote RMI and RMI/IIOP access to JBoss	1099,8043	TCP UDP
<input type="checkbox"/>	Mail: POP3	110	TCP UDP
<input type="checkbox"/>	RPC - Remote Procedure Call (rpcbind)	111	TCP UDP
<input checked="" type="checkbox"/>	Authentication service	113	TCP UDP
<input type="checkbox"/>	SFTP - Simple File Transfer Protocol	115	TCP UDP
<input type="checkbox"/>	NNTP - Network News Transfer Protocol	119	TCP UDP
<input checked="" type="checkbox"/>	OTSS web administration	1220	TCP UDP

Buttons: +, [icon], -, [icon]

Buttons: Stop Firewall, Revert, Save

Enabling IPFW on MacOS X Server

- Use Server Admin / Firewall GUI
 - Modifies **/etc/ipfilter/ipfw.conf.apple**
 - Starts/stops daemon
- Add manual overrides to **/etc/ipfilter/ipfw.conf**
- To reload after file changes:
 - **# ipfw flush**
 - **# ipfw /etc/ipfilter/ipfw.conf.apple**
 - **# ipfw /etc/ipfilter/ipfw.conf**

Monitoring IPFW on MacOS X Server

- Use Server Admin / Firewall GUI
- To check rule hit counts:
 - # **ipfw show**
- To view dynamic (state table) rules too:
 - # **ipfw -d [-e] show**
- To monitor log:
 - # **tail -f /var/log/ipfw.log**



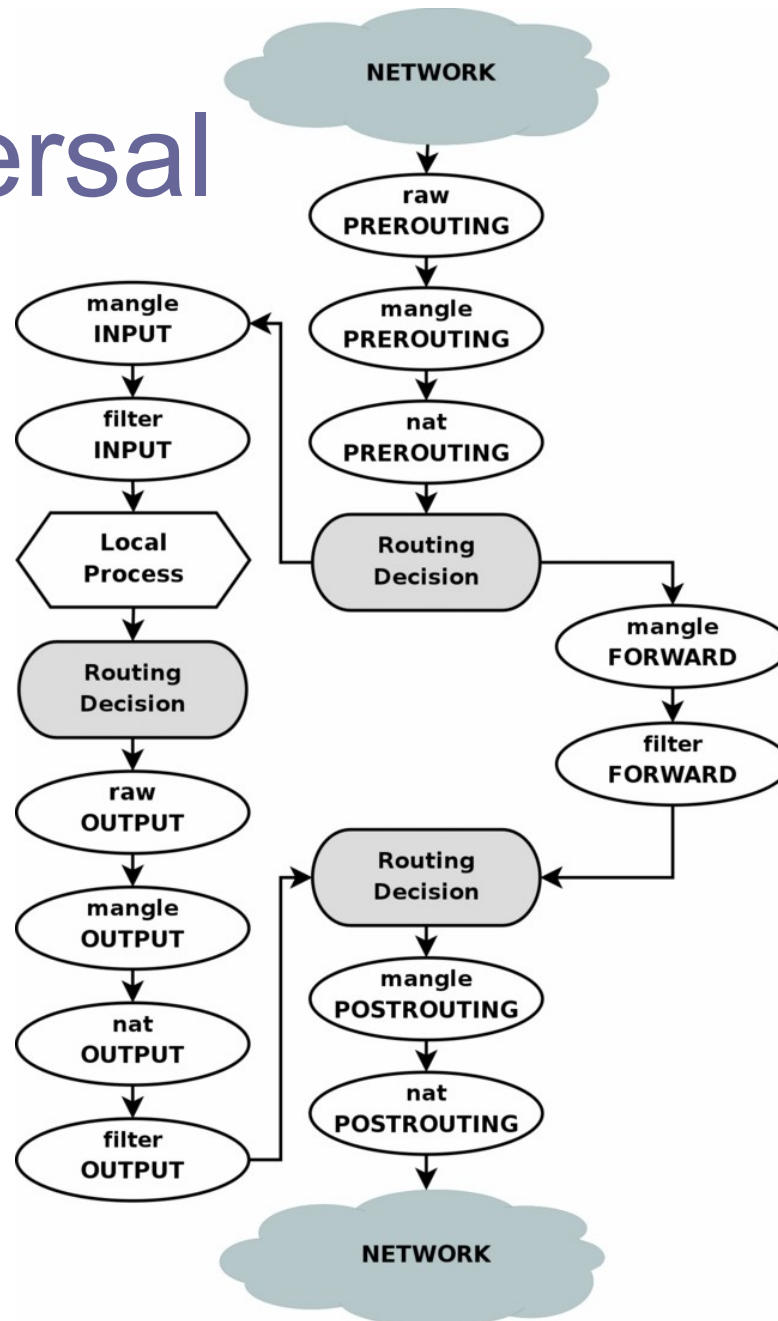
IPFirewall Resources

- <http://en.wikipedia.org/wiki/Ipfirewall>
- <http://www.freebsd-howto.com/HOWTO/Ipfw-HOWTO>
- <http://securosis.com/2007/11/16/ipfw-rules-20071116-revision/>
- <http://www.hanynet.com/waterroof/>
- <http://wipfw.sourceforge.net/>

Netfilter/iptables

- Included in Linux 2.4 or later kernels
- Replaces older **ipchains** filter
- Maintains state information *and* does related-connection tracking
- Can add filter rules to pre-defined chains for **INPUT**, **OUTPUT**, *and* **FORWARD**
- Can also add user-specified chains (like subroutines)
- Also supports other tables/chains for more complex operations, such as NAT support

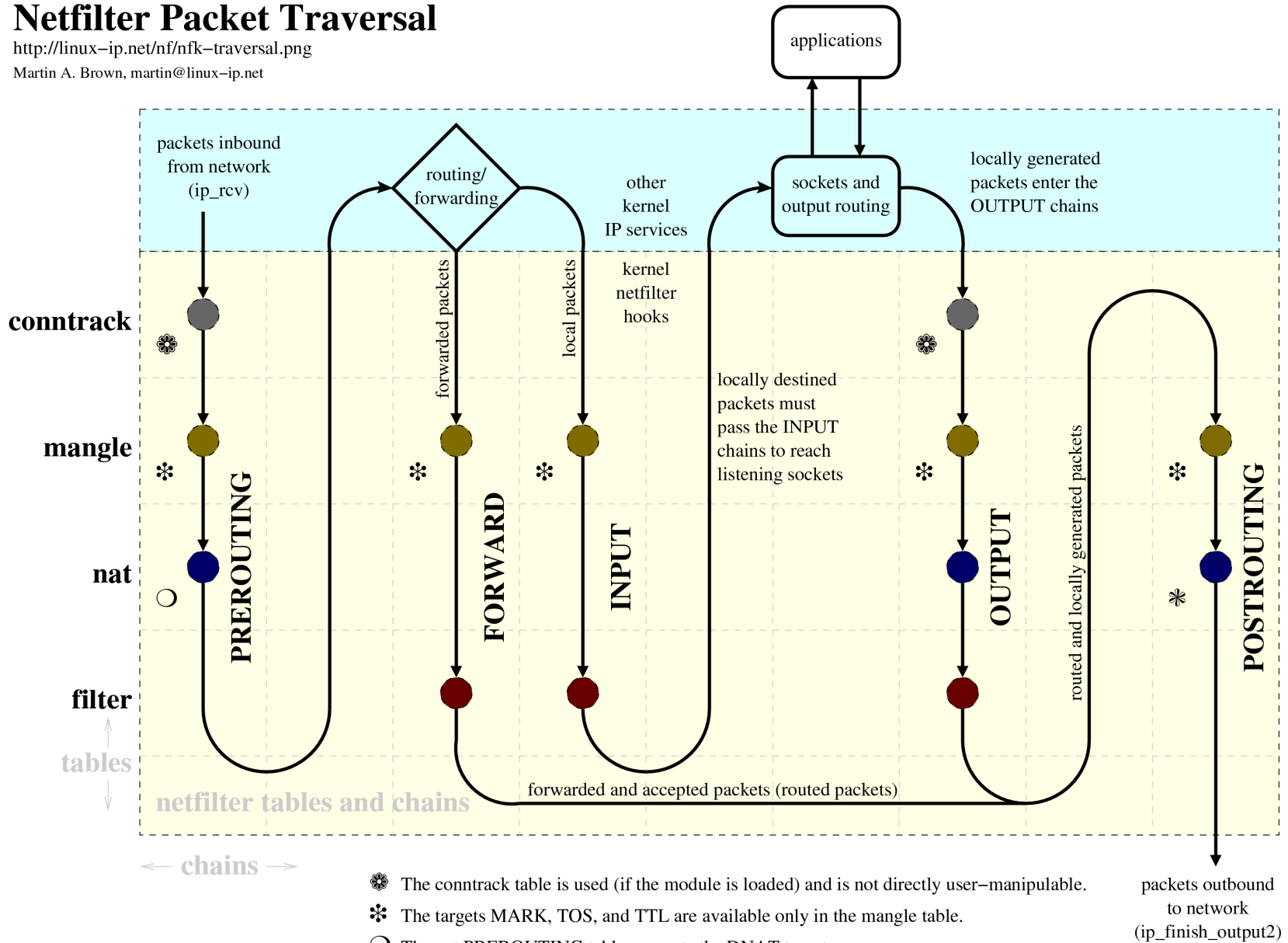
Packet Traversal



Netfilter Packet Traversal

<http://linux-ip.net/nf/nfk-traversal.png>

Martin A. Brown, martin@linux-ip.net



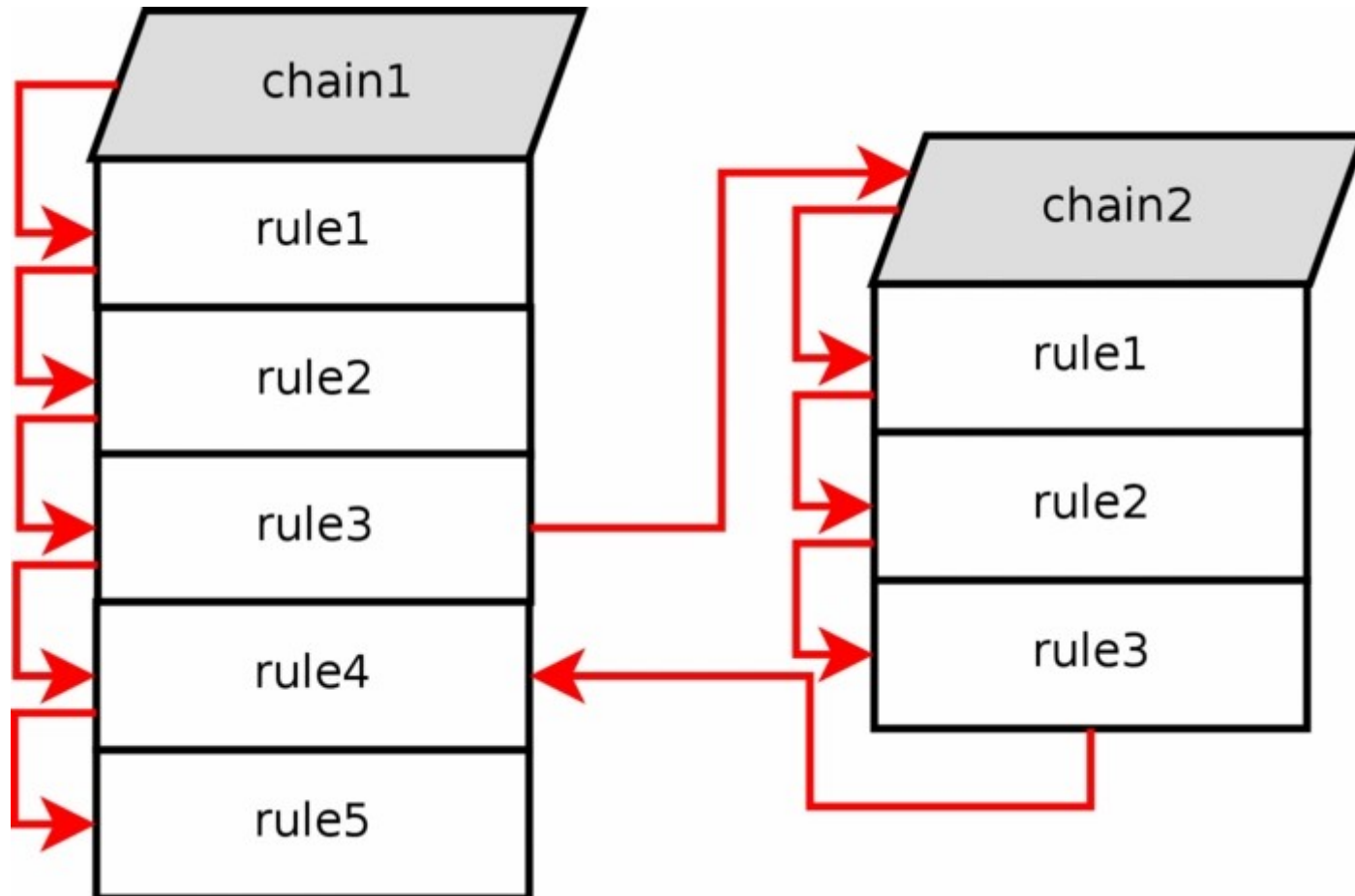
cf. <http://www.docum.org/qos/kptd/>

cf. http://open-source.arkoon.net/kernel/kernel_net.png

cf. <http://iptables-tutorial.frozentux.net/>

* The nat POSTROUTING table supports SNAT and MASQUERADE targets.

User-Specified Chains



Iptables commands

- Add a chain:
 - # **iptables** [-t/--table *table*] -N/--new-chain *chain*
- Set policy (default action) on a chain:
 - # **iptables** [-t *table*] -P *chain target* [*options*]
- Append/insert a rule to a chain:
 - # **iptables** [-t *table*] -A/I *chain rule-specification* [*options*]
- Rule specification:
 - [-p *proto*] [-s *addr[/mask]*] [-d *addr[/mask]*] [-i/o *interface*]
[-j *target*]
- Rules can include extended packet matching modules:
 - E.g.: -m **tcp** [--source-port *port[:port]*] [--dport *port[:port]*]
- Target is either a user-specified chain or...
 - **ACCEPT, DROP, RETURN, REJECT, or LOG**

iptables-save and iptables-restore

- Save a defined set of tables/chains:
 - # **iptables-save** [-c] [-t *table*] > *file*
- Restore a saved set:
 - # **iptables-restore** [-c] [-n] < *file*
- **-c** to save/restore packet & byte counters
- **-n** to not flush previous table contents
- **-t** to limit output to named table
(default is all tables)

Fedora Firewall Configuration GUI

The screenshot shows the Fedora Firewall Configuration GUI. The main window is titled "Firewall Configuration" and has a menu bar with "File", "Options", and "Help". Below the menu bar are icons for "Wizard", "Apply", "Reload", "Enable", and "Disable". The "Enable" button is highlighted with a red circle, indicating the firewall is active. The "Trusted Services" section is selected in the left sidebar. The main area contains a table of services and their ports, with "Samba Client" and "SSH" checked. A warning icon and text at the bottom of the table state "Allow access to necessary services, only." The system menu on the right shows the "Firewall" option highlighted.

System menu items:

- Preferences
- Administration
- Help
- About GNOME
- Authentication
- Date & Time
- Display
- Firewall**
- Language
- Logical Volume Management
- Network

Firewall Configuration window:

File Options Help

Wizard Apply Reload Enable Disable

Trusted Services

Other Ports

Trusted Interfaces

Masquerading

Port Forwarding

ICMP Filter

Custom Rules

Here you can define which services are trusted. Trusted services are accessible from all hosts and networks.

Service	Port/Protocol
<input type="checkbox"/> NFS4	2049/tcp, 2049/udp
<input type="checkbox"/> OpenVPN	1194/udp
<input type="checkbox"/> POP-3 over SSL	995/tcp
<input type="checkbox"/> RADIUS	1812/udp, 1813/udp
<input type="checkbox"/> Samba	137/udp, 138/udp, 139/tcp, 445/tcp
<input checked="" type="checkbox"/> Samba Client	137/udp, 138/udp
<input type="checkbox"/> Secure WWW (HTTPS)	443/tcp
<input checked="" type="checkbox"/> SSH	22/tcp
<input type="checkbox"/> WWW (HTTP)	80/tcp

⚠ Allow access to necessary services, only.

The firewall is enabled.

/etc/sysconfig/iptables

```
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p ah -j ACCEPT
-A INPUT -p esp -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 631 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 137 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 138 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

Iptables Connection Tracking

- Handled by (application-specific) kernel modules:
 - `# modprobe ip_conntrack_ftp`
 - `# modprobe ip_conntrack_netbios_ns`
- RedHat/Fedora: define in `/etc/sysconfig/iptables-config`:
 - `IPTABLES_MODULES="ip_conntrack_ftp ip_conntrack_netbios_ns"`

Enabling iptables in RedHat/Fedora

- Use the Firewall Configuration GUI
 - Start Configuration Wizard or Load Default Configuration (**Options** menu)
 - Define trusted services, etc.
 - Enable/Disable Firewall service
- Edit **/etc/sysconfig/iptables{-config}**
- Reload after file changes:
 - **# service iptables restart ...or...**
 - **# iptables -F INPUT ; **
iptables-restore /etc/sysconfig/iptables

Monitoring iptables in RedHat/Fedora

- To view rules with packet & byte counters:
 - **# iptables-save -c [-t *table*]**
- To view logs:
 - **# tail -f /var/log/messages | fgrep kernel:**
- To view connection-tracking state info:
 - **# less /proc/net/ip_conntrack ...or...**
 - **# less /proc/net/nf_conntrack**
(depending on kernel version)

Getting Fancy: SSH probe filtering

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22  
-m recent --name sshprobe --set
```

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22  
-m recent --name sshprobe --rcheck --seconds 60  
--hitcount 8 -j DROP
```

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22  
-m recent --name sshprobe --rcheck --seconds 60  
--hitcount 4 -j LOG --log-prefix "SSH-REJECT: "
```

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22  
-m recent --name sshprobe --rcheck --seconds 60  
--hitcount 4 -j REJECT --reject-with tcp-reset
```

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22  
-j ACCEPT
```

Netfilter/iptables Resources

- <http://en.wikipedia.org/wiki/Netfilter/iptables>
- <http://en.wikipedia.org/wiki/Iptables>
- <http://www.netfilter.org/>
- <http://iptables-tutorial.frozentux.net/>
- <http://security.maruhn.com/>
- <http://linux-ip.net/nf/>
- http://ornellas.apanela.com/dokuwiki/pub:firewall_and_adv_routing
- <http://easyfwgen.morizot.net/gen/>
- <http://www.muug.mb.ca/pub/muuglines/pdf/muug0804.pdf>
- <http://www.teaparty.net/technotes/ssh-rate-limiting.html>
- <http://www.linuxjournal.com/video/mastering-iptables-part-i>
- <http://www.linuxjournal.com/video/mastering-iptables-part-2>
- <http://www.linuxjournal.com/video/mastering-iptables-final-installment>



Questions?