

Typical roles

- Dedicated firewall host based on standard Red Hat.
- Packet-filtering gateway.
- Two, three, or four zones.



The Acacia Firewall

Richard Keech
Chief Instructor
Red Hat Asia-Pacific



Why not an existing tool?

- Special-purpose firewall distros do not suit (personal preference).
- Existing config tools did not give same features.
- Wanted very succinct parametric configuration.
- Wanted extensibility.
- Wanted better logging.
- Wanted re-usable, upgradable configurations.



What is Acacia?

- IP tables-based packet filter configuration for multi-port firewalls.
- Easy configuration.
- Extensible.
- Improved logging.
- Access control lists and blacklist.
- Advanced routing integration.
- Statefull.



Package outline

Packages: acacia, ulogd

System services: acacia, ulogd

Config files: /etc/acacia/
 acacia.conf
 acacia.acl
 acacia.blacklist
 /etc/ulogd.conf

Log files: /var/log/acacia/
 acacia.log
 summaries/



Design approaches

- **First-order:**
 effort -> rules
- **Second-order:**
 effort -> config tool -> rules
- **Third-order:**
 effort -> config -> rule generator -> rules



Simple two-port config

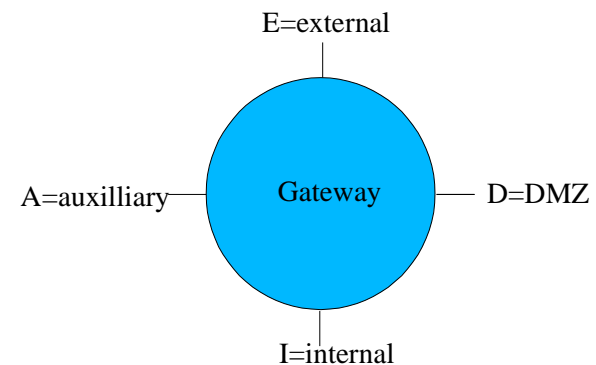
/etc/acacia/acacia.conf

```
IF[$E]=ppp0
IF[$I]=eth0
NUM_INTERFACES=2
ALLOWED_INWARDS_TCP_SERVICES="ssh domain"
ALLOWED_INWARDS_UDP_SERVICES="domain"
```



Acacia's zone model

Up to four zones supported



Flow complexity problem

Packets forwarded from one interface to another are a **flow**.

Two ports: *two flows*

Three ports: *six flows*

Four ports: *twelve flows*

With one big forward chain:

design scales poorly with number of ports, and performance suffers.



Managing flow complexity

Iptables allows rules in forward chain like:

```
iptables -A FORWARD -i eth0 -o eth1 -j TARGET
```

Targets can be custom chains.

Acacia has a custom chain for every flow.

All policy for access in a particular flow is in a **single smaller chain**.

Reduces complexity, improves performance.



Simple three-port config

/etc/acacia/acacia.conf

```
IF[$E]=ppp0
IF[$D]=eth1
IF[$I]=eth0
NUM_INTERFACES=3
ALLOWED_INWARDS_TCP_SERVICES="ssh domain"
ALLOWED_INWARDS_UDP_SERVICES="domain"
MAILSERVER=123.123.12.1
DMZWEBSERVER=123.123.123.2
```



Simple four-port config

/etc/acacia/acacia.conf

```
IF[$E]=ppp0
IF[$D]=eth1
IF[$A]=eth2
IF[$I]=eth0
NUM_INTERFACES=4
ALLOWED_INWARDS_TCP_SERVICES="ssh"
ALLOWED_INWARDS_UDP_SERVICES=""
MAILSERVER=123.123.12.1
DMZWEBSERVER=123.123.123.2
```



DMZ hosts

Config variables identify hosts of common DMZ services:

NAMESERVER
DMZWEBSERVER
DMZWPC
MAILSERVER
FTPSERVER
TIMESERVER



Admin access

Administrative access to the firewall limited by:

ADMINHOST internal
EXTERNALADMINHOST like it says
TELEMETRY_ACCESS=true

Allows HTTP and SNMP inbound from a designated host.



Base policy

Acacia's base rules apply the following:

- Mostly closed access policy;
- Negligible access EI, IA, DI, AE, AD;
- Masquerading of IE, IA traffic;
- Connection tracking;
- Blocks invalid packets;
- Allows access to named services in DMZ.
- IE traffic restricted to HTTP, FTP



Relaxed exit rules

RELAXED_EXIT_RULES=true
allows for out-going access to most services.

Following services still restricted:
NFS, X11, Squid, Socks, Openwindows, lockd.



Logging

- Standard logging uses syslogger.
- Logs to `/var/log/messages` by default.
- Difficult to have a dedicated log file for firewall.
- Acacia uses userspace logger (`ulogd`).
- Use `-j ULOG` instead of `-j LOG`.
- Acacia logs to `/var/log/acacia/acacia.log`.
- Logs rotated daily.



Blacklist

- Can specify bad guys by IP address.
- `/etc/acacia/acacia.blacklist`.



On-firewall services

Use with care!

Access from DMZ and internal:
DHCP_ON_FIREWALL=true
WPC_ON_FIREWALL=true
DNS_ON_FIREWALL=true

Where external access is required:

```
ALLOWED_INWARDS_TCP_SERVICES="ssh"  
ALLOWED_INWARDS_UDP_SERVICES="ntp"
```



Extensions

Arbitrary additional rules.

Allows flexibility to deal with special cases.

All done from config file, eg

```
extra_chain_E () {  
    $FW -A E --dport 3600 -j ACCEPT  
}
```



Where?

- <http://people.redhat.com/rkeech>
- <http://www.acaciafirewall.org/>



The future

- A serious code review for 1.0.
- Re-write rule generator in Python.
- Integrate the logger daemon.
- Builds for other distros.
- Advanced reporting.



ACL

- Can specify good guys by IP address.
- `/etc/acacia/acacia.acl`.
- Default use applies to smtp, imap and pop access to mailserver in DMZ.
- Can be applied more generally through extension rules.



IP Routing

- `iproute` package.
- Can tie routing to packet filtering through packet marking.
- Useful for dealing with channel separation in multi-homed networks.

