Identity-based firewalling

Eric Leblond, Vincent Deffontaines, Sebastien Tricaud

INL
15 rue Berlier
75013 Paris, France

Hack.lu, Luxembourg 2008

Security policy

Definition

The set of management statements that documents an organization’s philosophy of protecting its computing and information assets, or the set of security rules enforced by the system’s security features.

- Components of an organisation:
  - Information assets
  - Network resources
  - Individuals
- Security enforcement point:
  - Doors
  - Switches, Firewalls
  - Applications

New network usages

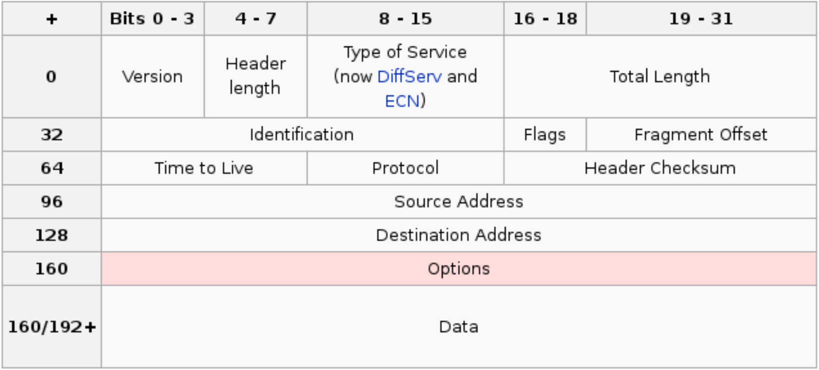
What is new?

- Every organisation user now works on a computer
- Everyone gets mobile

The old stronghold model

- Inside == good, outside == bad
- This doesn’t work well with massive, and mobile usages
- Security policy bypasses come from inside too

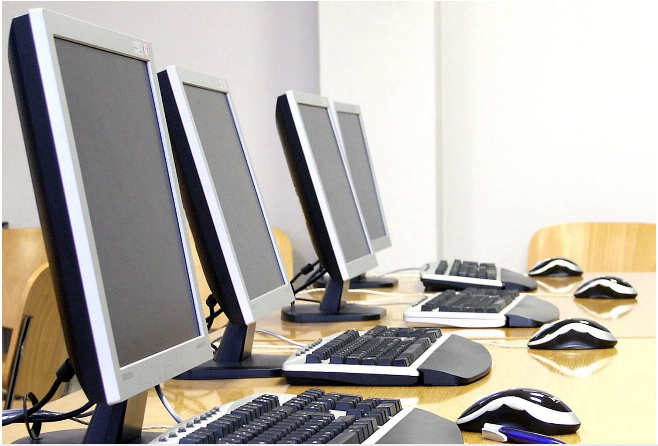
What firewalls focus on



+	Bits 0 - 3	4 - 7	8 - 15	16 - 18	19 - 31
0	Version	Header length	Type of Service (now DiffServ and ECN)	Total Length	
32	Identification			Flags	Fragment Offset
64	Time to Live		Protocol	Header Checksum	
96	Source Address				
128	Destination Address				
160	Options				
160/192+	Data				

Something has been forgotten

How firewalls view a company:



Something has been forgotten

How security officers view a company:

Identity-based packet filtering

- Security policy is mainly about role-based constraints on behavior of members of the organization.
- Security officer needs to differentiate users at the access level.

Policy statements that classical firewalls can’t handle

- A teacher and a student in the same classroom should not have the same rights on the network.
- Only accountants should access the telnet based application installed on a AS400.

Network application pre authentication vulnerabilities

Where is user authentication needed ?

- Applications suffer from pre authentication vulnerabilities.
- User authentication at application level is not enough.

2007-2008 examples

- IIS authentication bypass [a]
- Solaris telnet bypass [b]
- Permission bypass on Oracle Application Server Portal [c]

[a] http://isc.sans.org/diary.html?storyid=2915

[b] http://www.kb.cert.org/vuls/id/881872

[c] http://www.securityfocus.com/bid/29119/discuss

No good existing solution

- All firewalls on the market bind user identities with low level elements of the OSI layer.
- This is formally wrong...
- ... and practically it opens the way to many attacks or security policy bypasses.

1. **Introduction**
2. **Existing solutions**
3. **NuFW algorithm**
4. **NuFW usage**
5. **Conclusion**

Static IP/User binding

The trick

- Static User to IP mapping
- Based on some belief:
  - an IP can not be stolen
  - Microsoft Windows IP conflict detection
- Subject to easy attack:
  - Simple IP stealing
  - Disconnect connected computer

Exploit

```
# arpspoof -t target host
```

Static MAC/IP/User binding

Another trick

- Static User to IP/MAC mapping
- Based on some **strong** belief:
  - a MAC address can not be changed
- Subject to easy attack
  - Mac address change

Exploit

```
# macchanger --mac=01:23:45:67:89:AB eth1
```

Dynamic IP/User binding

Yet another trick

- Dynamically bind user and IP
- Based on some **strong** belief:
  - a MAC address can not be changed
  - an IP address can not be stolen
- Subject to easy attack
  - IP address change

Exploit

```
# macchanger --mac=01:23:45:67:89:AB eth1
# arpspoof -t target host
```

Dynamic user/IP binding, a dangerous "security" feature

- Marketing efforts to convince administrators:
  - Identity-based rules are announced in the middle of various *secure* technologies
  - Most product documentations hide limitations of used technology
- A dangerous gap exists
  - Administrators use their firewall interface to design per-user rules
  - They have no clue about firewall bindings like "User == IP" in the backend
  - But that's how things "work" ! [1]

[1] http://seclists.org/bugtraq/2003/Jun/0218.html

You’re doing it wrong !

Multiuser limitations

One for all and all for one

- First user logged on firewall gets his rules
- Subsequent users from the same IP get the same rules

Typical example : Kerio Wingate case

- Identification done at first HTTP proxy use [a]
- Valid as long as firewall receives traffic from computer
- Timeout is 3 hours
- Virtually full time for a terminal server
- Admin usually connects first after a reboot

[a] http://download.kerio.com/dwn/kwf6-en.pdf

IP = User with NAT ?

- Everyone behind NAT router is seen with the same IP address
- IP or MAC based authentication can not work
- All NATed computers are seen as first authenticated user
- A common problem:
  - Netscreen authentication (bugtraq mailing-list)
  - Authpf
  - etc

802.1x

Method

- Associate switch port with user
- Advanced authentication mechanism
- Requires support on all equipments

Drawback/Caveats

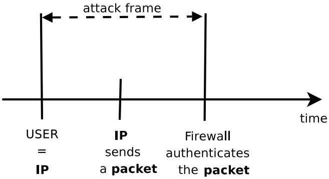
- Needs hardware that supports authentication
- This still assumes "one computer == one user", which is formally wrong
- No support for multiuser systems (Citrix, TSE, Linux, ...)
- No fine-grained (per protocol, per user role) filtering or logging. Just pushes a switch port into a VLAN.

Shared attacks

What they all do is *A priori* authentication

- IP = User
  - Static (Unlimited)
  - Dynamic (Time-based, ...)
- Session has to be kept alive to maintain the User/IP association
- All in all, what it takes to steal a user’s identity on the network is to spoof an IP address

Timeout attacks



- Substitute network parameter during keep alive
- Can be done on all systems
- Slightly difficult for 802.1x because of physical down link detection
  - Put hub between switch and user
  - Wait for user association before substituting

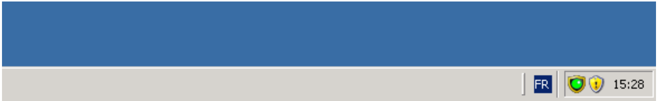
NuFW: A strict authenticating firewall

Strict authenticating firewall principles

- No "IP==user" or "MAC==user" binding at all
- Every connection is authenticated by their emitting user
  - The UserID is checked and validated strictly
  - At the opening time of the connection
- Client
  - Authenticates on the user directory (AD, LDAP, ...)
  - Secure channel from user to firewall
- Respect TCP/IP RFCs
  - No alteration of standard network flows

Consequences

- NuFW requires an Agent on the client computer
  - To authenticate
  - To send requested information
- Interaction with host system



"A posteriori" connection authentication

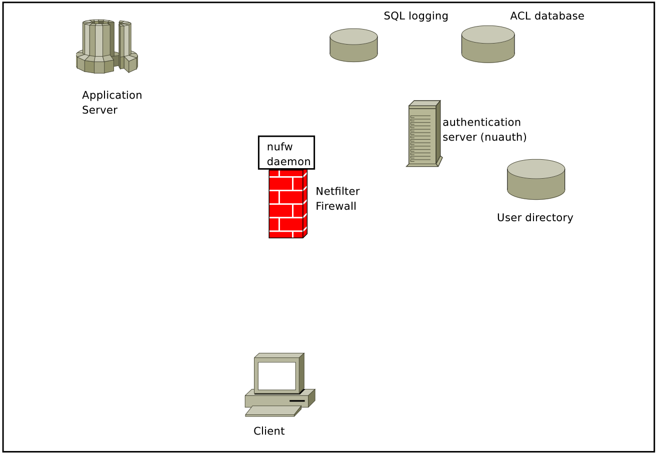
"A posteriori"

- Authentication is done after packet emission
- User is requested to prove that he has emitted the packet
- Avoids timeout attacks

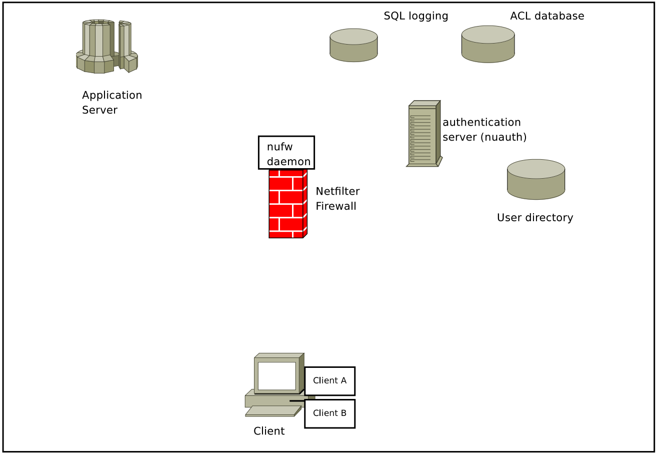
Per connection

- Authenticates each connection individually
- Brings multiuser system support

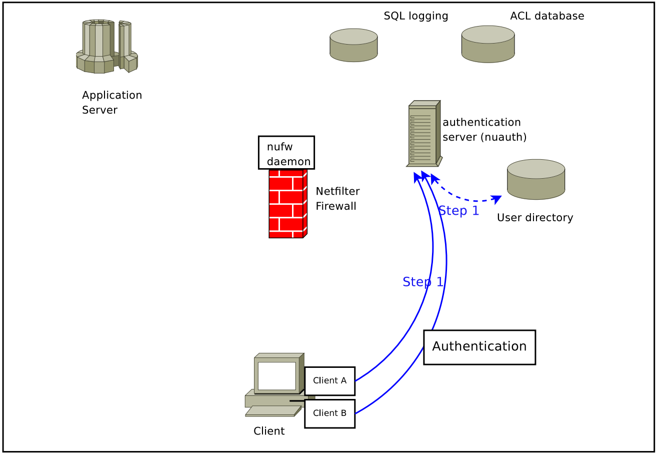
NuFW algorithm



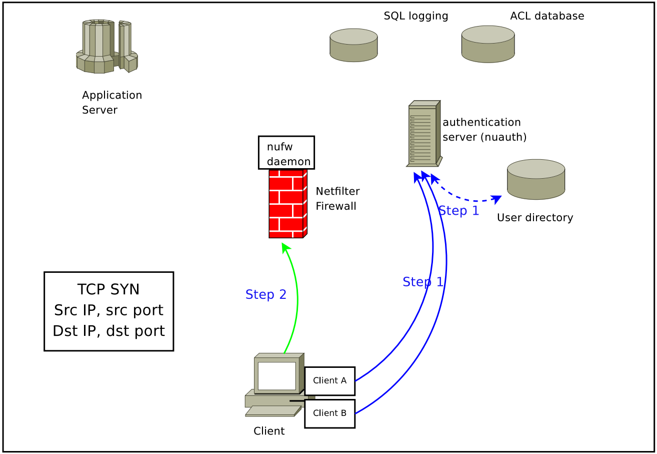
NuFW algorithm



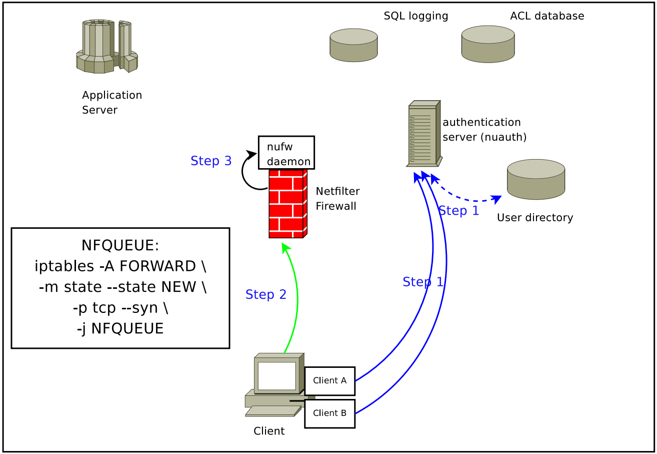
NuFW algorithm



NuFW algorithm

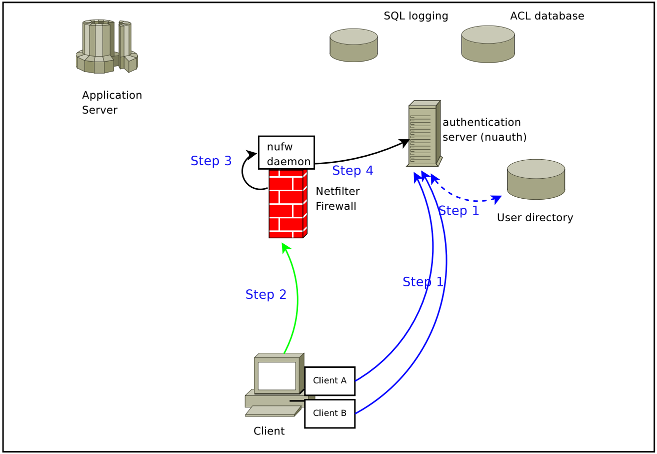


NuFW algorithm

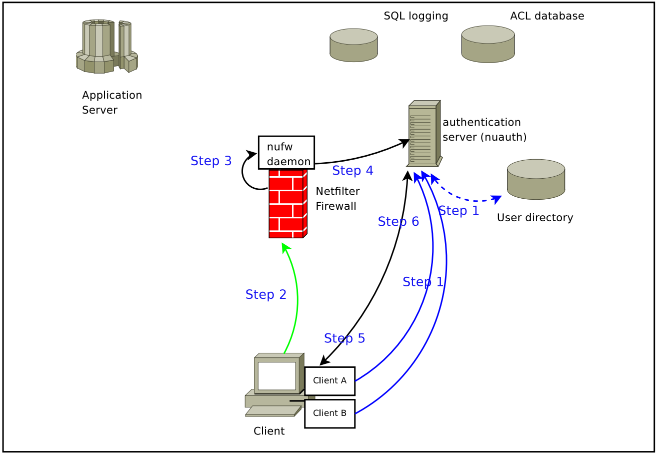


```
NFQUEUE:
iptables -A FORWARD \
-m state --state NEW \
-p tcp --syn \
-j NFQUEUE
```

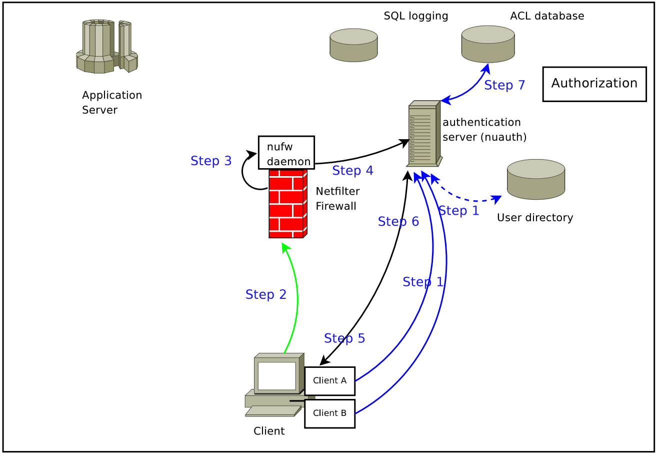
NuFW algorithm



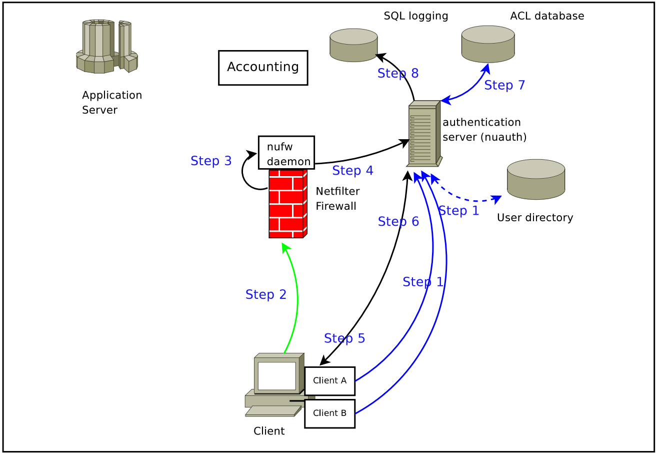
NuFW algorithm



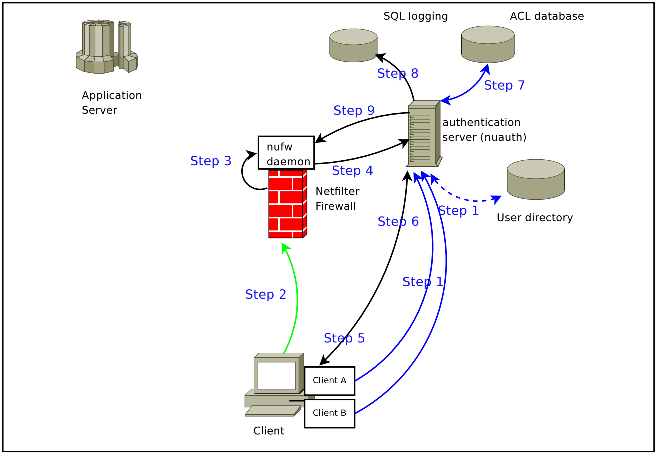
NuFW algorithm



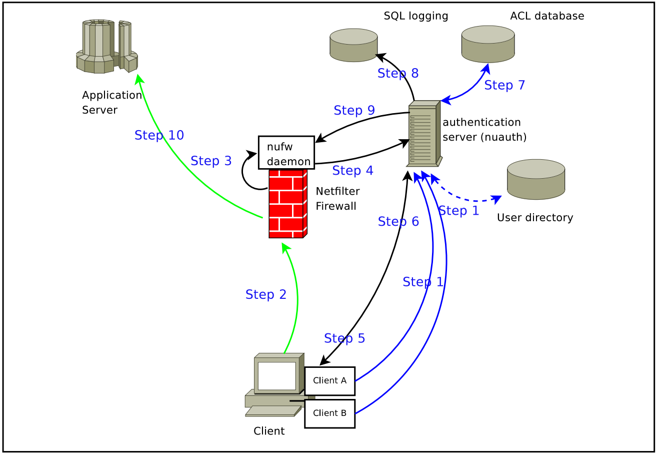
NuFW algorithm



NuFW algorithm



NuFW algorithm



Implementation

NuFW runs on Linux firewalls

- NuFW uses userspace decision system provided by Netfilter (QUEUE or NFQUEUE)
- Linux 2.4 or 2.6 required
- Heavy conntrack usage (>= 2.6.18 recommended)

NuFW and iptables

```
# iptables -A FORWARD -m state \
     --state ESTABLISHED -j ACCEPT
# iptables -A FORWARD -p tcp --dport 23 \
     -m state --state NEW --syn -j NFQUEUE
```

Performances

No impact on bandwith

- Only impacts the opening of authenticated connections
- Conntrack handles all remaining packets (99,98%)

No perceptible delay for user

- Around 15ms to open a new connection

Global performance

- From 2000 to 4000 new authenticated connections/s
- Enough for most networks
- We are working with the Netfilter team to improve performance

NuFW and Network Address Translation

Protocol limitations

- Firewall sees:
  - Source and destination IP, Port
  - Viewed from firewall
- Client sees and announces:
  - Source and destination IP, Port
  - Viewed from client
- Any transformation on IP parameters will cause a failure

NuFW and Network Address Translation

NAT usage

- All address translations have to occur after NuFW authentication
- NuFW firewall itself can do NAT (source or destination)

Supported protocols : TCP and UDP

UDP

- On Linux, unprivileged user cannot get enough information.
- Requires administrative privileges:
  - Available on Windows
  - Can be done for Linux (TODO)

System level connection

- Some connections are established by the kernel
  - ICMP
  - On recent Windows, DNS requests through the svchost.exe service
- Network sharing protocols

Man in the middle attack [2]

- Method
  - Attacker intercepts all packets but lets authentication flows run normally.
  - Client sends a packet to initiate a new connection.
  - Attacker drops the packet and sends a new legit connection with same IP parameters.
  - Client authenticates the packet that reached the gateway.
- However
  - This means legit user does not get its traffic working.
  - It also means the attacker does not choose were to connect.
  - This is a TCP/IP attack, not a NuFW one. Use flow encryption if you don’t trust your network (or anyway you’ll have your passwords sniffed!)

[2] See the Eficaas link in references

Chronology

- 2001-2004: proof of concept, no crypto on exchanges.

Chronology

- 2001-2004: proof of concept, no crypto on exchanges.
- 2005: NuFW 1.0 - First usable, stable release.
  - TLS encryption of exchange
  - Connection to standard user directories via PAM (LDAP, AD, ...)

Chronology

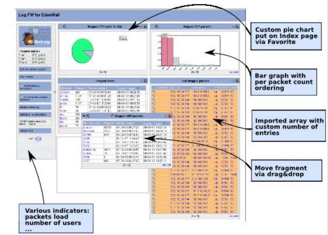
- 2001-2004: proof of concept, no crypto on exchanges.
- 2005: NuFW 1.0 - First usable, stable release.
  - TLS encryption of exchange
  - Connection to standard user directories via PAM (LDAP, AD, ...)
- 2006: NuFW 2.0 - Many "linting" options
  - daemons support reload
  - send ICMP datagram when rejecting a connection
  - Prelude IDS logging support
  - Time-based ACL support

Chronology

- 2001-2004: proof of concept, no crypto on exchanges.
- 2005: NuFW 1.0 - First usable, stable release.
  - TLS encryption of exchange
  - Connection to standard user directories via PAM (LDAP, AD, ...)
- 2006: NuFW 2.0 - Many "linting" options
  - daemons support reload
  - send ICMP datagram when rejecting a connection
  - Prelude IDS logging support
  - Time-based ACL support
- 2007: NuFW 2.2
  - IPv6 support
  - Support for per user routing and QoS
  - Client/Server Protocol enhancements
  - Command mode for interactive administration.

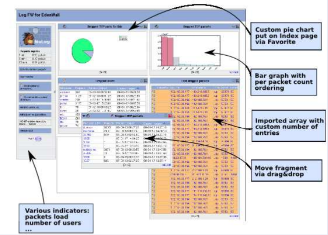
Associated tools

Nulog


Log FW for EdenWall
Custom pie chart put on Index page via Favorite
Bar graph with per packet count ordering
Imported array with custom number of entries
Move fragment via drag&drop
Various indicators: packets load number of users ...

Associated tools

Nulog



Custom pie chart put on Index page via Favorite

Bar graph with per packet count ordering

Imported array with custom number of entries

Move fragment via drag&drop

Various indicators: packets load number of users ...

Other web interfaces

- Nuface: rule management
- Nutrack: connection tracking display and modification

Who uses NuFW ?

Organisations with distinguished user profiles

- Having the network administrator do Human Resources with IP addresses sucks !
- Is your boss fired? Let the HR remove him from the directory. You don’t need to modify the firewall.
- If an intern gets to be a salesman in your organisation, just let the HR set them in the right group.

Who uses NuFW ?

Organisations with distinguished user profiles

- Having the network administrator do Human Resources with IP addresses sucks !
- Is your boss fired? Let the HR remove him from the directory. You don't need to modify the firewall.
- If an intern gets to be a salesman in your organisation, just let the HR set them in the right group.

Advanced logging

- Keep track of who sends network flows
- No need to wonder "Who had that IP address 3 monthes ago?" when problems appear.

A strict approach

Bringing users to IP filter

- NuFW strictly implements security policies
- It opens the way to new usages
  - Links with external applications
  - Interactions with routing and QoS

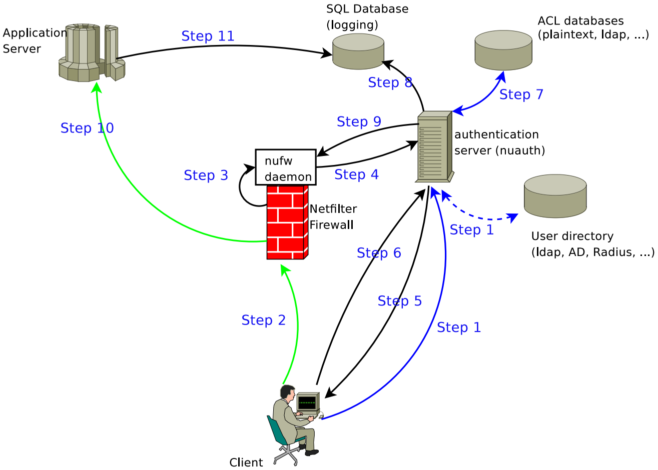
Already used in real life

- Multiple governemental organisations
- Technology shipped in EdenWall UTM appliance

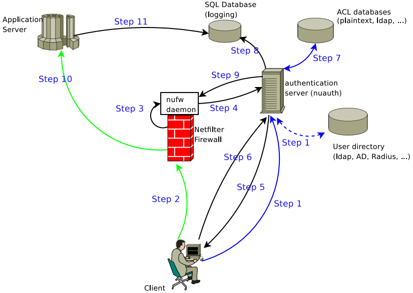
Questions ?

- contacts:
  - mail: nufw-core-team@nufw.org
- links:
  - NuFW: http://www.nufw.org/
  - INL: http://www.inl.fr/
  - EdenWall: http://www.edenwall.com
  - Prelude IDS: http://www.prelude-ids.org/
  - Nuface: http://software.inl.fr/trac/trac.cgi/wiki/EdenWall/NuFace
  - Nulog: http://software.inl.fr/trac/trac.cgi/wiki/EdenWall/NuLog
  - Eficaas: http://www.nufw.org/eficaas/

Detailed NuFW algorithm



Protocol independant Single Sign On



Get username from firewall logging

```
SELECT username FROM log WHERE source_ip=192.168.1.0 AND source_port=2327\
AND destination_ip=192.168.33.3 \
AND destination_port=80 and protocol=6 and state=ESTABLISHED;
```

Working with IDS

Information source for intrusion detection

- The firewall knows the user
- Apache logs the destination user
- Prelude correlator combines both information
  - Alert if srcuser != dstuser
  - React