# The methodology

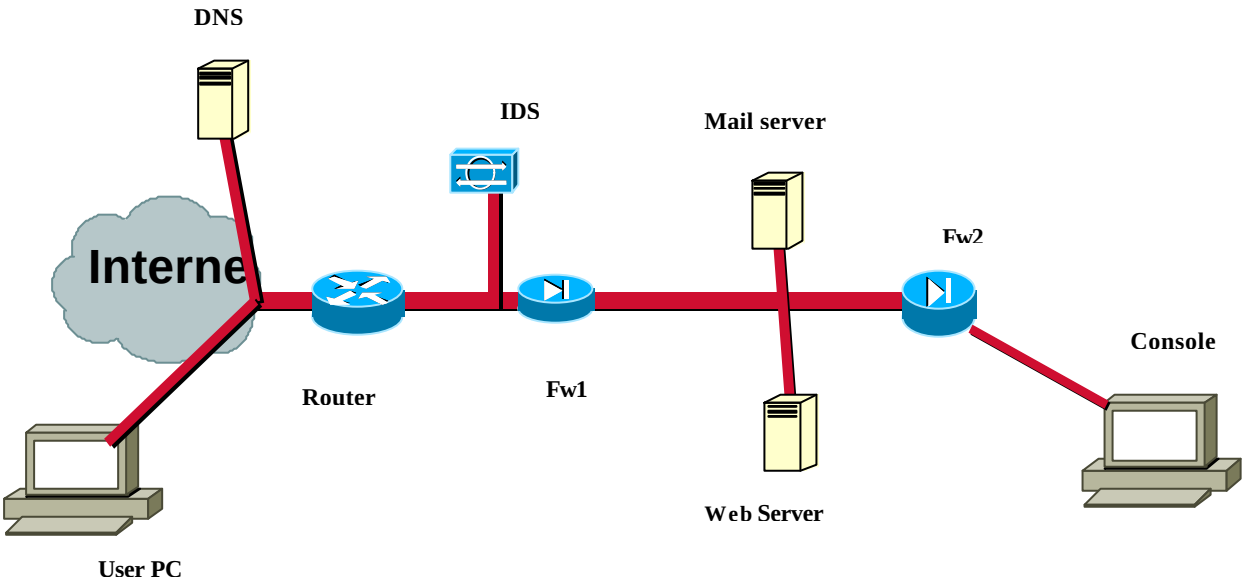
## 1 Introduction

In an ideal world, firewall infrastructures are designed by people with experience, people who have the experience to intuitively know what they are doing. Ideally, these same people will work with the project team to produce a set of firewall rules. In practice often people less experienced may have to produce them.

Having been the latter (hopefully now the former) I produced this simple methodology to help the novice.

Nobody would expect a certified firewall expert to do go through all these stages but if you have to document your processes or produce anomalous IDS patterns, this can be useful.

Example configuration




www.loud-fat-bloke.co.uk

# 2 Stage 1 - Identifying active components – define inventory

The purpose of this stage is to inventorise the components in the configuration. This allows an asset register of all objects to be built.

Typically the list of components will include:

- Database server
- Crypto server
- LDAP Server

For our example we use only

- DNS server
- Mail server
- user Machines
- Maintenance machines
- Front-end router
- web server
- Intrusion detection monitor
- 2nd firewall
- 1st firewall

## 2.1 Order & group active components - define chokepoints

Working from the outside of the configuration, re-order the list of components in the configuration.

Calculate how many chokes or control points in the configuration. Typical examples of these are perimeter router, external firewall, internal firewall and internal router. Group the object list by their relative inter-choke position.

| | |
|---|---|
| Group 1 | Customer PC |
| Group 1 | Internet |
| Group 1 | Primary dns server |

| | |
|---|---|
| Group 1 | Primary dns |
| Group 2 | Front-end router |
| Group 2 | Intrusion detection monitor |
| Group 3 | Front firewall |
| Group 3 | web server |
| Group 3 | mail server |
| ” | |
| ” | |
| ” | |
| .”” | |

## 2.2 Recording the traffic flows- $n^2$ matrix

An example of the $n^2$ matrix is shown below.

| | TO | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Group1 | | | | Group 2 | | | Group 3 | | | | |
| | User PC | dns | Router | | I DS | 1st fw | | web | mail | 2nd fw | | Cons |
| User PC | X | | | | | | | tcp80 | tcp25 | | | |
| dns | | X | | | | | | | | | | |
| router | | | X | | | | | | | | | |
| | | | | X | | | | | | | | |
| IDS | | | | | X | | | | | | | Udp161 Udp69 |
| 1st fw | | | | | | X | | | | | | |
| | | | | | | | x | | | | | |
| web server | | udp53 | | | | | | X | | | | |
| mail server | tcp25 | udp53 | | | | | | | X | | | |
| 2nd fw | | | | | | | | | | X | | |
| | | | | | | | | | | | ) | |
| MGT Cons | | | Tcp22 | | Tcp22 Udp161 | Tcp22 | | Tcp22 | Tcp22 | Tcp22 | | X |

Create a matrix as above with every network object in your inventory. After each choke point (i.e. firewall and router), put a shaded row or column. This represents the perimeter enforced by the device.

www.loud-fat-bloke.co.uk

Once the matrix is complete it will need to be populated. Working from the last item on the vertical, record the traffic(from vertical) to destination on the horizontal by placing ports in the appropriate cell i.e ( mail server will have to resolve dns names udp53 & send email tcp25).

Obviously, this is a long-winded method of recording communications. But it does force you to examine the communication between every object. It also gives you the opportunity to research the behaviour of less known protocols.

## 2.3 Creating access rules

Having created a matrix, it is necessary to document the access list for each choke point. To do this create a table for each choke-point.

If the device is stateful, you will only have to record the out going communication – the state engine of the device will take care of the return connection. If it isn't stateful, you will have to insert the appropriate return connection – quite a problem for RPC or H323

| rule | From Address | From port | To Address | To port | Action | comment |
|---|---|---|---|---|---|---|
| 1 | | | | | | |
| (rtn) | | | | | | |
| 2 | | | | | | |
| (rtn) | | | | | | |
| 3 | | | | | | |

Populate it as follow -Starting from the last row on the vertical. Read along the row, when you find a port, record the destination. Each time the line crosses a shaded control point it will require a logical accesses rule in that control point table. See example

| | User PC | dns | Router | | I DS |
|---|---|---|---|---|---|
| User PC | X | | | | |
| dns | | X | | | |
| router | | | X | | |
| | | | | X | |
| IDS | | | | | X |
| 1st fw | | | | | |
| | | | | | |
| web server | | udp53 | | | |
| mail server | tcp25 | udp53 | | | |
| 2nd fw | | | | | |

## 2.4 Designing access logging rules

This is dependant on the capability of the device. But it is important to actively design the logging option on the rule table and record in the comment section. Define too much logging and you will swap the logs and ruin the performance. Log too little and you'll hide evidence of a hack.

This very device dependant, consider logging

- Explicit deny rule

www.loud-fat-bloke.co.uk

- Administrative access
- Important transactions
- Stealth rule
- Anti Spoofing rules

## 2.5 Designing intrusion detection alerts

Some firewalls have the ability to define alerts. It is a good practice to place such alerts on rules which should never happen. For example, I personally never allow *ssh* to a firewall through the frontend router. Therefore, if a session is attempted from the internet through the router, something has been compromised. This would warrant an alert.

| rule | From Address | From port | To Address | To port | Action | comment |
|---|---|---|---|---|---|---|
| 1 | User PC | ANY | 1st FW | SSh | DENY | Alert |

## 2.6 Add anti-spoofing

Define anti-spoofing to prevent spoofed access. For example on the external routers' external interface

| rule | From Address | From port | To Address | To port | Action | comment |
|---|---|---|---|---|---|---|
| 1 | internal | ANY | internal | Any | DENY | Inward direction |

This blocks any one attempt to be one of my addresses.

## 2.7 Add Stealth rule

No external access to cokes should be allowed. For example on the external routers' external interface we drop any packets as it is obviously a scan attempt.

| rule | From Address | From port | To Address | To port | Action | comment |
|---|---|---|---|---|---|---|
| 1 | external | ANY | internal | Any | Drop | Inward direction |

# 3 Test and enhance for performance

Enhancing for performance is simple. Follow these basic rules:

- Keep the number of rules down
- Keep the most used rules at the top as most devices check them sequentially
- Drop unauthorised traffic early
- Use networks or CIDR groups rather than groups
- Avoid negatives

---