Welcome to

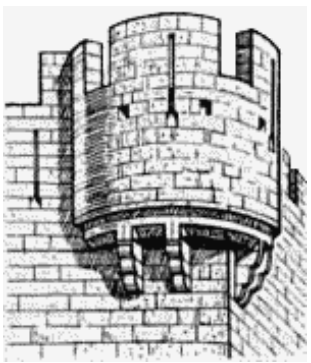
The Modern Firewall Infrastructure

Pruning networks without breaking them

Henrik Kramselund hkj@zencurity.com @kramse

Slides are available as PDF, kramse@Github
troopers20-modern-firewall-infrastructure.tex along with a small paper
Open Source presentation, Alles ist ein Remix - Everything is a Remix

Introduction



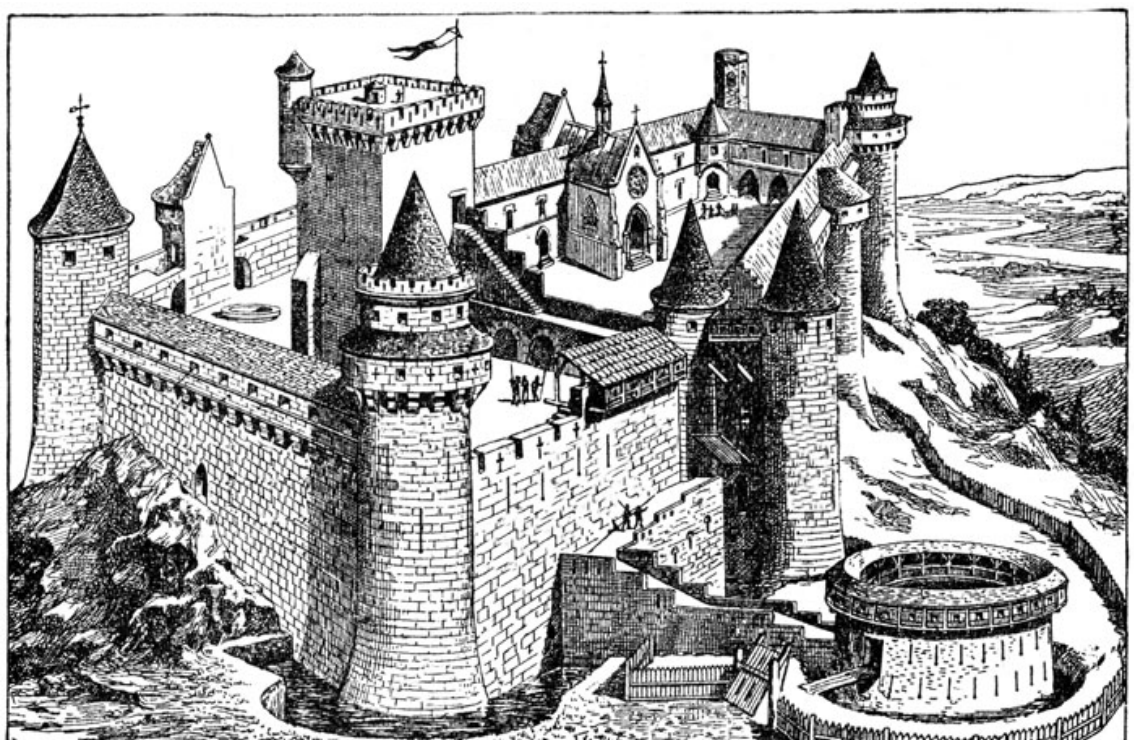
Firewalls are an old concept, we should know this by now

Reality
Networks are increasingly complex and we need **confidentiality**, **integrity** and **availability**
- **while performing service**, upgrading, changing routing, VPNs and make general changes

We dont understand our firewalls
If we cannot **comprehend** our networks => we cannot **maintain** our firewalls

We only see a part of the problem, like the tower shown

Defense in depth Requires an overview

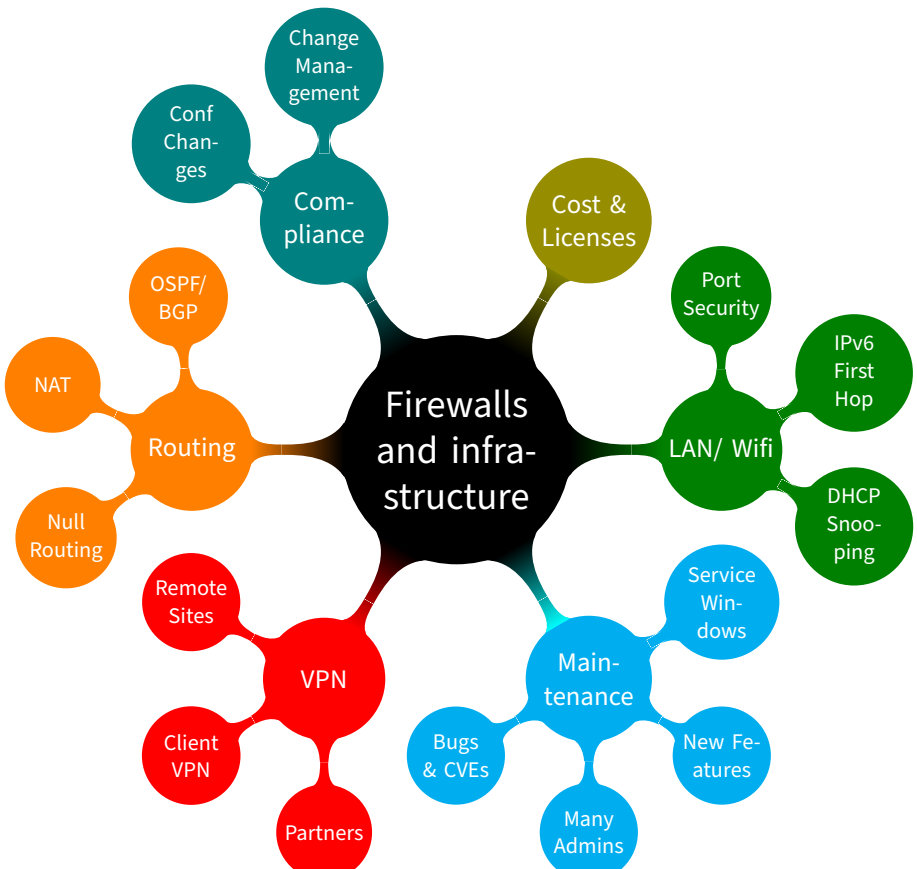


Problems in firewalls, and network security

- Increased threat landscape, World wide networks, attacks from everywhere
- Complexity, adding new rules all the time
- Software quality - firewall software has flaws
- Complexity, so many features put onto a few devices, filtering, proxying, NAT, anti-virus, site-2-site VPN, client VPN, ...
  - how do you upgrade parts without risking the downtime for all

Not a complete list of problems, example today we ignore cost of licenses and hardware

The Modern Firewall Infrastructure - problems



Prerequisites

Level required to understand this are not high, but you need confidence in implementing, so **make the changes in the smallest steps possible.**

A main expectation is that **networks grow in size**, and these hints are for the places where things are getting out of hands.

All vendors are ready to sell you their nextgen - often it will only complicate matters by adding more features to the same box, but only **one firmware upgrade file with all Software contained** (Virus definitions may be downloaded seperately)

Core problem making changes may break something,
and sometimes far inside your own network.

Dedicated devices in a secure infrastructure

My main idea, identify and de-couple the functions - use dedicated systems

Photo by Julie Fader on Unsplash

Definitions

Multiple definitions for firewalls exist, below are a few examples to illustrate some of the variations that exist.

The first book about firewalls used this definition:

> We define a firewall as a collection of components placed between two networks that collectively have the following properties:
>
> - All traffic from inside to outside, and vice-versa, must pass through the firewall.
> - Only authorized traffic, as defined by the local security policy, will be allowed to pass.
> - The firewall itself is immune to penetration.
>
> We should note that these are design goals; a failure in one aspect does not mean that the collection is not a firewall, simply that it is not a very good one.

Source: *Firewalls and Internet Security; Repelling the Wily Hacker.* by Cheswick og Bellovin 1994

We will consider this a firewall, but we know today that both inside and outside at meaningless, since we have multiple networks inside, we have partner network connections etc.

Another short definition that encapsulates this is found on Wikipedia, and may suffice in many situations. Again there will typically be multiple networks, zones or areas of the networks with varying degrees of trust.

> In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.[1] A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.[2]

Source: Wikipedia `https://en.wikipedia.org/wiki/Firewall_(computing)`

- **Firewall Technology:** *Mechanism to help enforce access policies about communication traffic entering or leaving networks.*

Source: “A Reference Model for Firewall Technology and its Implications for Connection Signaling” by Lyles og Schuba 1996

Another definition

I am also fond of this longer and technical definition from RFC4949:

> $ firewall
>
> 1. (I) **An internetwork gateway that restricts data communication traffic to and from one of the connected networks** (the one said to be ”inside”the firewall) and thus protects that network’s system resources against threats from the other network (the one that is said to be ”outside”the firewall). (See: guard, security gateway.)
> 2. (O) **A device or system that controls the flow of traffic between networks using differing security postures.** Wack, J. et al (NIST), ”Guidelines on Firewalls and Firewall Policy”, Special Publication 800-41, January 2002.
>
> Tutorial: A firewall typically protects a smaller, secure network (such as a corporate LAN, or even just one host) from a larger network (such as the Internet). The firewall is installed at the point where the networks connect, and the firewall applies policy rules to control traffic that flows in and out of the protected network.

Another definition

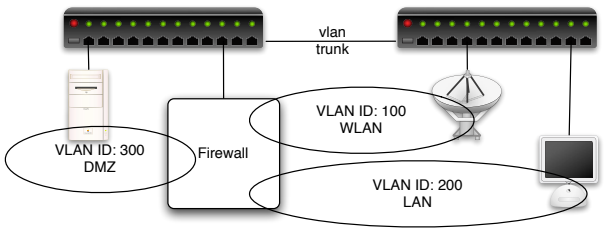
$ firewall, continued

A firewall is not always a single computer. For example, a firewall may consist of a pair of filtering routers and one or more proxy servers running on one or more bastion hosts, all connected to a small, dedicated LAN (see: buffer zone) between the two routers.

The external router blocks attacks that use IP to break security (IP address spoofing, source routing, packet fragments), while proxy servers block attacks that would exploit a vulnerability in a higher-layer protocol or service. The internal router blocks traffic from leaving the protected network except through the proxy servers.

The difficult part is defining criteria by which packets are denied passage through the firewall, because a firewall not only needs to keep unauthorized traffic (i.e., intruders) out, but usually also needs to let authorized traffic pass both in and out.

The firewall is not a single device



Important point: **the firewall devices are not alone**

Security of the network already relies on multiple other devices and functions:

- The routers in front, first line of defense, make use of them
- The switches and routers on the inside, especially VLANs and routing between sites are important
- Also wifi, port security on switches, DHCP snooping, IPv6 First Hop Security

Consider any change to any device related to filtering as a *rule change*
Adding a VLAN is a change, adding a null-route is a rule change, ...

Enterprise Filtering Patterns (EFP)

Definition An *Enterprise Filtering Pattern* (EFP), is an identified pattern in compute networks that describes a common architectural feature. This feature allows us to rationalize and process the architecture and transform it into a more efficient design which may allow higher security, less dependencies on other systems, easier maintenance or other benefits.

I would like to introduce this, and create a library of them

Building castles

Pic by Cayetano cc-by-sa-2.0 https://www.flickr.com/photos/32444077@N00/2779873459

Tools and Hints to Get Started

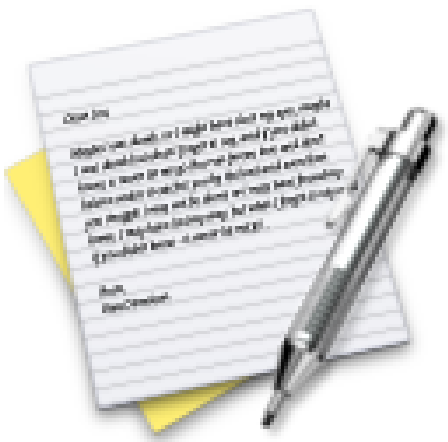
Start by doing this:

- Always keep backup configurations, keep them for a long time, version controlled!
  Detailed information kept, even after deleting a rule. Tool recommendation: Oxidized
- Even better - automate your firewall and filtering configuration changes
  roll out a change, and easy to revert changes. Tool recommendation for filtering routers: Ansible
- Always document all parts, especially VPN connections - partner company and contact information

Then

- Review your configuration regularly, this may be hard see later
- Firewall and filtering rules are more than just the technical parts - also authorized by, date inserted/removed

Design your solution



When was the last time you took 3 hours with a whiteboard and designed your network? - do it, one of the best advise I ever got, know your goals

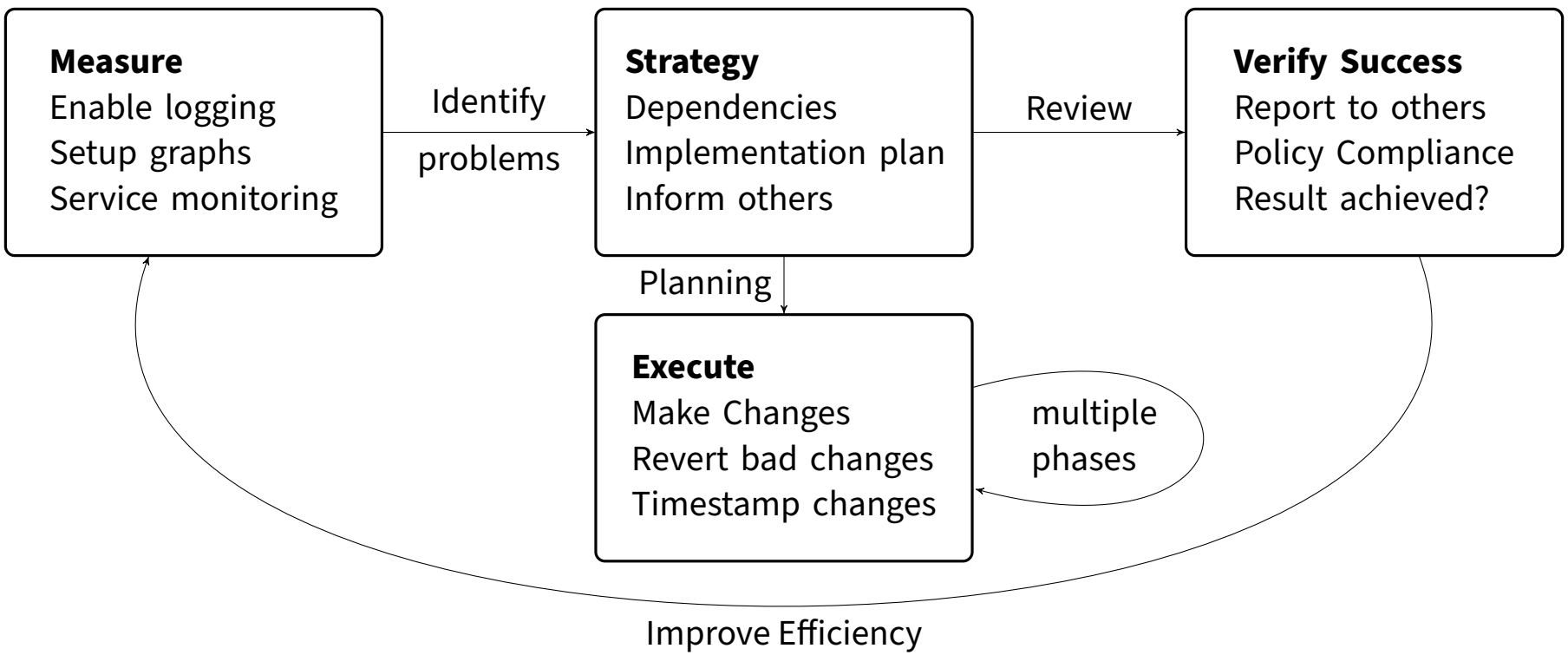
Need a goal to know where you are going

Firewall pruning

1. Measure - enable logging and measurements
2. Identify pattern or problem
3. Write a strategy for updating system
4. Plan update – with fallback planning!
5. Execute change
6. Measure success
7. Move to next item

Make changes incrementally - less risk, less push back when change(s) fails

Make incremental changes



Howto Review Large Rule-sets

Going through a 5.000 line firewall configuration is not easy.

Behind the lines are the whole organisation, the network, the history

First line of attack

- Mark these for deletion Telnet, TFTP
- Mark these as suspicious SMTP, DNS - you want to control these!
- Mark these for review ANY source, ANY destination, especially if both in the same rule

Often you dont actually need to remove these, but make sure they log, and then react when used

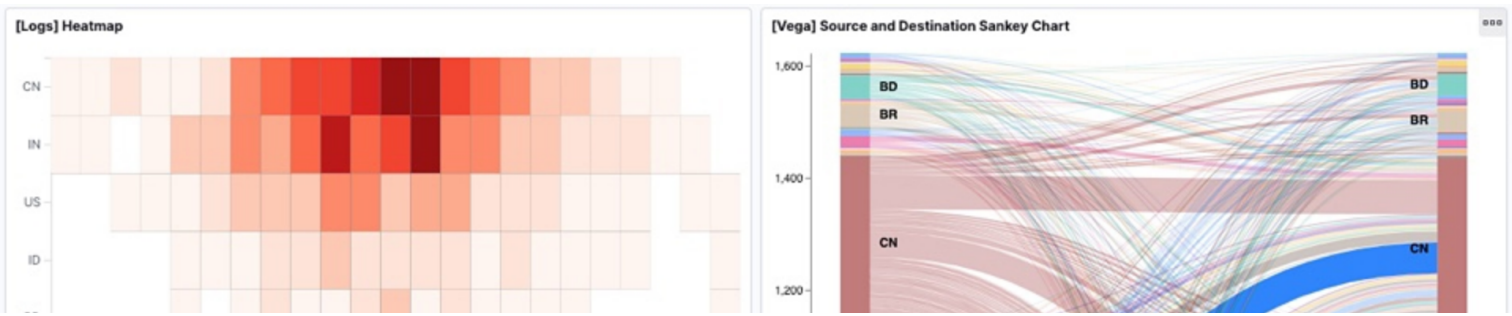
Statistics

So we need to know if dangerous rules are being hit. The business rarely want to risk deleting rules immediately, but if you can provide assurance:

- Deleting a rule can quickly be restored, because we have good configuration backups!
- Noticing if traffic matches this specific rules
- If we can prove the servers and destinations for this rule is not even active in our network

Note: this bind a bit into the IP address management, I use NIPAP, while not perfect it works

How do we know our traffic



Use existing and known methods for traffic insights, Kibana shown

- Firewall logs, all vendors have them, collect it all
- Netflow/sFlow from your network devices, open source solutions exist for parsing/graphing
- Web server logs exist

Added bonus

If the statistics show that your traffic is mostly encrypted, does it make sense to buy and add anti-virus to your firewalls, or would the infrastructure benefit more from secure DNS solutions and web proxies both which can filter on domains, names, URLs, patterns :-D

Maintaining large rule-sets

Goal Rule updating, made more easy
Can I remove this rule, is it used, who owns it, who uses it, can it be updated - made more specific

Decouple the firewall functions

Answer this: There is an important bug in the Client VPN function, can I upgrade the firewall immediately

NO, because our workforce needs the firewall up, the customers need the web site up, the partners need the VPN up for production

Decoupling Functions

Goal

Split your firewall into multiple devices

Divide and conquer

Note: I will NOT go over the financial implications of this, but only say this will enable you to choose the best technology for each function.

Example Decouple VPN Functions

Putting VPN on dedicated boxes allow maintenance for each device independently!

Client VPN often needs more updates!

Photo by KS KYUNG

EFP: Client VPN Decoupling

EFP name: **Client VPN Decoupling**

Process: Move Client VPN functions onto dedicated system. Separating your Client VPN connections from the main firewall system.

Benefits:

☺ Dedicated capacity - known capacity

☺ Isolated from attacks on main firewall device

☺ Software updates decoupled from other devices, allow updates when client VPN needs updates

Disadvantages:

😐 Temporarily need another IP address for testing clients

🚩 More expensive, more switch ports

🚩 More administration

EFP: Client VPN Decoupling Strategy

EFP strategy ⚙ **Client VPN Decoupling Strategy**

This is an example - your network and settings may differ.

Your strategy for decoupling your client VPN from the main firewall system may include the steps below.

1. Measure - enable logging of client VPN use
2. Identify clients using IP address for connections, using DNS name(s)
3. Allocate new IP for Client VPN
4. Plan update – with fallback planning!
5. Execute change
6. Measure success
7. Move to next item

Example Decouple routing

Move routing away from the firewall

Benefits: Can null route your internal network, like 10/8 -> null avoid loops

Leverage RPF Reverse Path Forwarding, only allow non-spoofed inside

Questions?

Henrik Kramselund hkj@zencurity.com @kramse

You are always welcome to send me questions later via email

Email: hlk@zencurity.dk Mobile: +45 2026 6000

Further reading

I have a lot of older presentations, which are open source, copy and find inspiration
https://github.com/kramse/security-courses

- HLK DDoS presentations, advice for configuring routers in front of the networks
- TROOPERS19 HLK VXLAN recommendations about VXLAN, consider your tunnelled protocols for inspection!
- Portscanning - start using portscans in your networks, verify how far malware and hackers can travel, and identify soft systems needing updates or isolation

Network Warrior, recommends designing and working toward a goal, also the GAD maxims