How NOT to Configure Your Firewall:
A Field Guide to Common Firewall Misconfigurations

Avishai Wool

yash@lumeta.com

http://www.lumeta.com/firewall.html

LUMETA

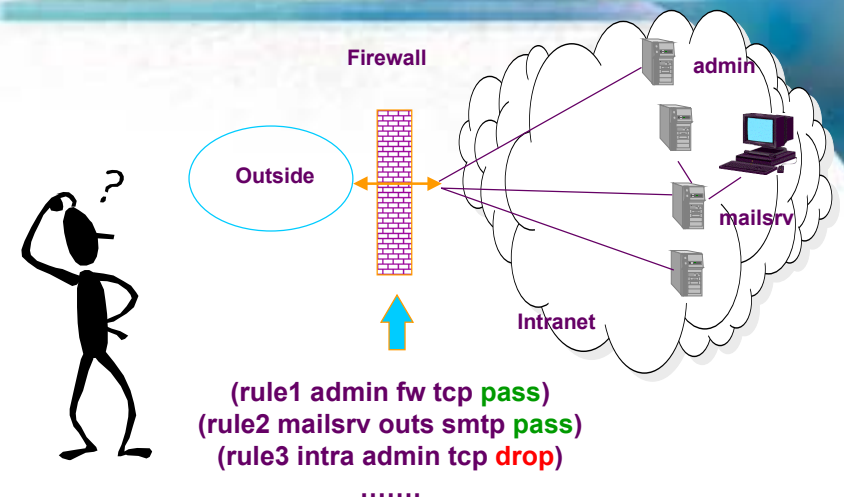
What is your firewall doing?

Firewall admins and auditors face some tough questions:

- Is the firewall *really* enforcing the corporate security policy?
- How will the new admin learn the firewall rules?
- We're acquiring company Y. What does *their* firewall allow?

LUMETA

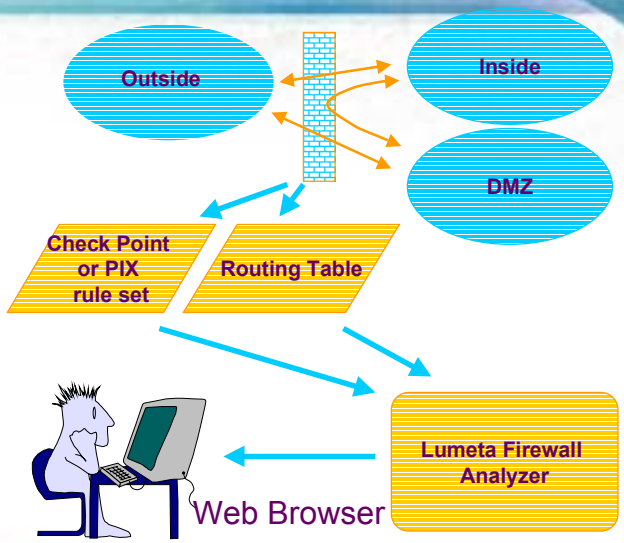
Why are these questions hard?



(rule1 admin fw tcp pass)
(rule2 mailsrv outs smtp pass)
(rule3 intra admin tcp drop)
.....

LUMETA

Lumeta Firewall Analyzer architecture



LUMETA

Common Check Point FireWall-1 Problems

LUMETA

Hidden Implicit Rules

- Separate "Policy → Properties" tab
- User choices create implicit, hidden rules
- Users presume that implicit rules are "safe"
- Services:
  - Domain Name Service (DNS), TCP & UDP
  - ICMP
  - RIP

LUMETA

Implicit Rules are Risky!

- The implicit DNS rules are:
  - From Any, to Any, allow domain-tcp
  - From Any, to Any, allow domain-udp
  - #1 on SANS top-ten risks list
- ICMP rule is:
  - From Any, to Any, allow all icmp types
  - Allows hackers to scan your net
- These are much too open

LUMETA

Default Settings

- Check Point up to v4.0 had risky defaults:
  - Domain TCP ☑
  - Domain UDP ☑
  - ICMP ☑
- In v4.1 the defaults changed – unless you upgraded from an earlier version

LUMETA

Don't Use Implicit Rules

- Disable the properties in the properties tab
- Do you need DNS on TCP at all?
- Write explicit rules, e.g.:
  - Any → MyDNServer : domain-udp
  - MyDNServer → Any : domain-udp
- Check www.phoneboy.com for recipes

LUMETA

Risky Services Access Firewall

- Only use encrypted & authenticated protocols:
  - Yes: Firewall1 (management), ssh
  - No: telnet, ftp, x11, …
  - Don't run listening daemons (ftpd, httpd, portmapper, …)
- Use "scp" (ssh-copy) instead of ftp
- X11 can be tunneled through ssh

LUMETA

Many Machines Access Firewall

- Restrict source IP addresses
- Keep the gui-clients file small
  - (~5 IP addresses)
- Keep those machines secure
- IP addresses should all be internal

LUMETA

Missing Stealth Rule

- Include a rule:
  - From Any, to Firewall, any service, drop
- V4.1 “Policy -> New” wizard creates a stealth rule (unless you upgrade)

LUMETA

Risky Services Allowed in

- Do NOT allow:
  - NetBios (#7 on SANS top 10)
    - Badly named pre-defined service: NBT
  - Sun-RPC (#3 on SANS top 10)
    - No pre-defined service
    - tcp/udp port 111
    - tcp/udp high ports (> 1023)
- V4.1 “Policy -> New” wizard creates a Silent-Services rule (unless you upgrade); RPC still open

LUMETA

Beware of Service=Any

- New rule default is Service=Any
- “Any” is not just the safe services.
- “Any” is ANY:
  - The Good
  - The Bad
  - And the Ugly
- Do NOT allow Service=Any when destination is internal.

LUMETA

Know Your Network Topology

- Check Point rules do not have a direction (don't distinguish between inbound and outbound)
- Every rules applies to ALL interfaces
- Pay attention to which interface IP addresses are behind

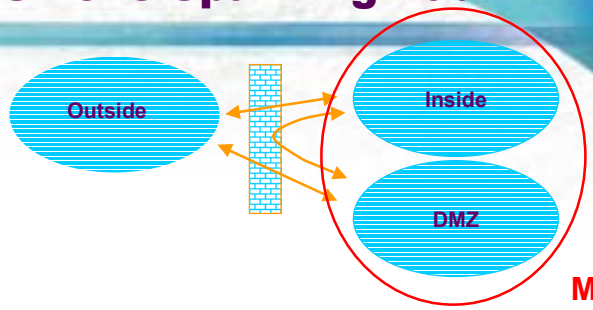
LUMETA

Zone-Spanning Objects

- Destination = Any covers inside, DMZ, and Internet
- Defining "MyNet = inside + DMZ" is asking for trouble

LUMETA

Why is Zone-Spanning Bad

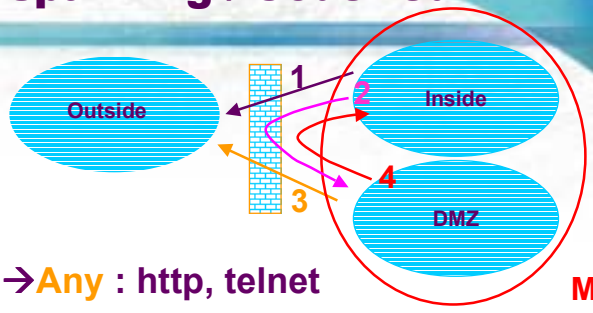


- MyNet = Inside + DMZ
- Any = Outside + Inside + DMZ
- Rule:

  Mynet → Any : http, telnet

LUMETA

Zone spanning / Code red

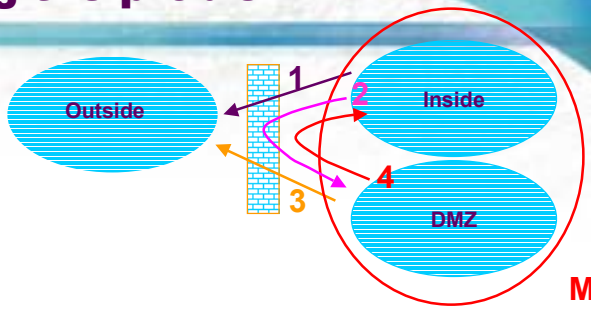


MyNet →Any : http, telnet

- #1 is intended
- #2 allows insiders to telnet into DMZ servers
- #3 Propagates code-red to partners
- #4 Propagates code-red to inside

LUMETA

Fixing the problem



a) DMZ → Any : Any : Drop

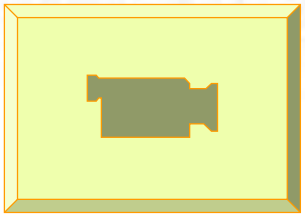
b) MyNet → Any : http

c) Inside → "not in" MyNet : telnet

- (a) drops #3 and #4
- (c) allows on #1, drops #2

LUMETA

Sample output



LUMETA


info@lumeta.com
http://www.lumeta.com/firewall.html
1-866-LUMETA7
That's all, Folks!
LUMETA