NORDSEC 2015

STOCKHOLM, 21 OCTOBER, 2015

CHALLENGES IN MANAGING FIREWALLS

ARTEM VORONKOV, STEFAN LINDSKOG, LEONARDO MARTUCCI
KARLSTAD UNIVERSITY, SWEDEN

OUTLINE

- Introduction
    - Define the problem
    - Related work
- Methodology and interview details
- The results
- Conclusions and limitations

DEFINE THE PROBLEM

- A firewall must be properly configured
- Configuring a firewall is an error-prone task

- To identify the reasons behind firewall misconfigurations => better firewall usability

RELATED WORK

- A. Wool (2004, 2010)
  - Overview of firewall misconfigurations
  - Most of them belong to inbound traffic
- L. Bauer (2009)
  - Policy makers and policy implementers
  - 3 factors to unmanageable access control rule sets

METHODOLOGY AND INTERVIEW DETAILS

- Semi-structured interviews:
  - Respondent's expertise of working with firewalls
  - Efforts to maintain firewalls
  - Difficulties they face
  - Interaction among system administrators
  - Security incidents that have happened
  - Ways of simplifying the management of rule sets

METHODOLOGY AND INTERVIEW DETAILS

Respondents

- 6 system administrators
    - Administration of security devices
    - Experience in creating configuration files
- 40 minutes interviews
- Independent from our research group

- No financial compensation

METHODOLOGY AND INTERVIEW DETAILS

The size of organizations:

- 16,000 – 18,000 for universities
- 2500-3000 for institutes
- More than 100 in the enterprise

Respondent	Experience	Network size	Effort	Organization
#1	12 years	≈50 nodes	1 hour/week	Institute
#2	8 years	≈400 nodes	2 hours/week	Institute
#3	19 years	≈850 nodes	0.5 hour/week	University
#4	17 years	≈450 nodes	9 hours/week	Enterprise
#5	3 years	≈70 nodes	1 hour/week	University
#6	20 years	≈500 nodes	0.5 hour/week	University

THE RESULTS

1. More people not always good
2. A variety of approaches is used to simplify the process of configuring firewalls
3. Firewall misconfigurations are still common
4. Policy creators == policy implementers
5. It is easy to configure a firewall!

THE RESULTS

Approaches to simplify configuring of firewalls

Respondent	Documentation	Comments in configuration files	Firewall management/ testing tools	Revision history	Frequent personal communication
#1	Yes	Yes	No	No	No
#2	Yes	Yes	Yes	No	No
#3	Yes	Yes	No	No	Yes
#4	No	Yes	Yes	Yes	Not applicable
#5	No	Yes	No	No	Yes
#6	No	Yes	No	No	Yes

CONCLUSIONS

- Some results confirm findings from the related work
  - 1st and 3rd points
- 2nd point shows that sysadmins need support
- 4th point deviates from the related work
- The majority thinks that FWs are easy to configure

  BUT:

  Why are there so many misconfigurations?

LIMITATIONS

- Pilot study
- Awareness of inconsistencies of rule sets

Thanks for your attention!

Any questions?