Carnegie Mellon
CyLab
CONFIDENCE FOR A NETWORKED WORLD

Carnegie Mellon CyLab
4720 FORBES AVENUE
CIC BUILDING
PITTSBURGH, PA 15213
PH: 412.268.1870
FX: 412.268.7675
www.cylab.cmu.edu

On the Usability of Firewall Configuration

Tina Wong

Firewalls

- Firewalls are used to protect enterprise internal networks
- Mistakes can lead to serious security, financial and performance implications

Problems

- A quantitative study on firewalls in 37 enterprises found that all of them have some form of misconfigurations
- “Complex rule sets are apparently too difficult for administrators to manage efficiently”
- [Wool 2004]

Why?

- Firewall configuration is a complex and error-prone task
- Configuration languages are like assembly languages – low-level and vendor-specific
- A single change in one firewall can affect the whole network

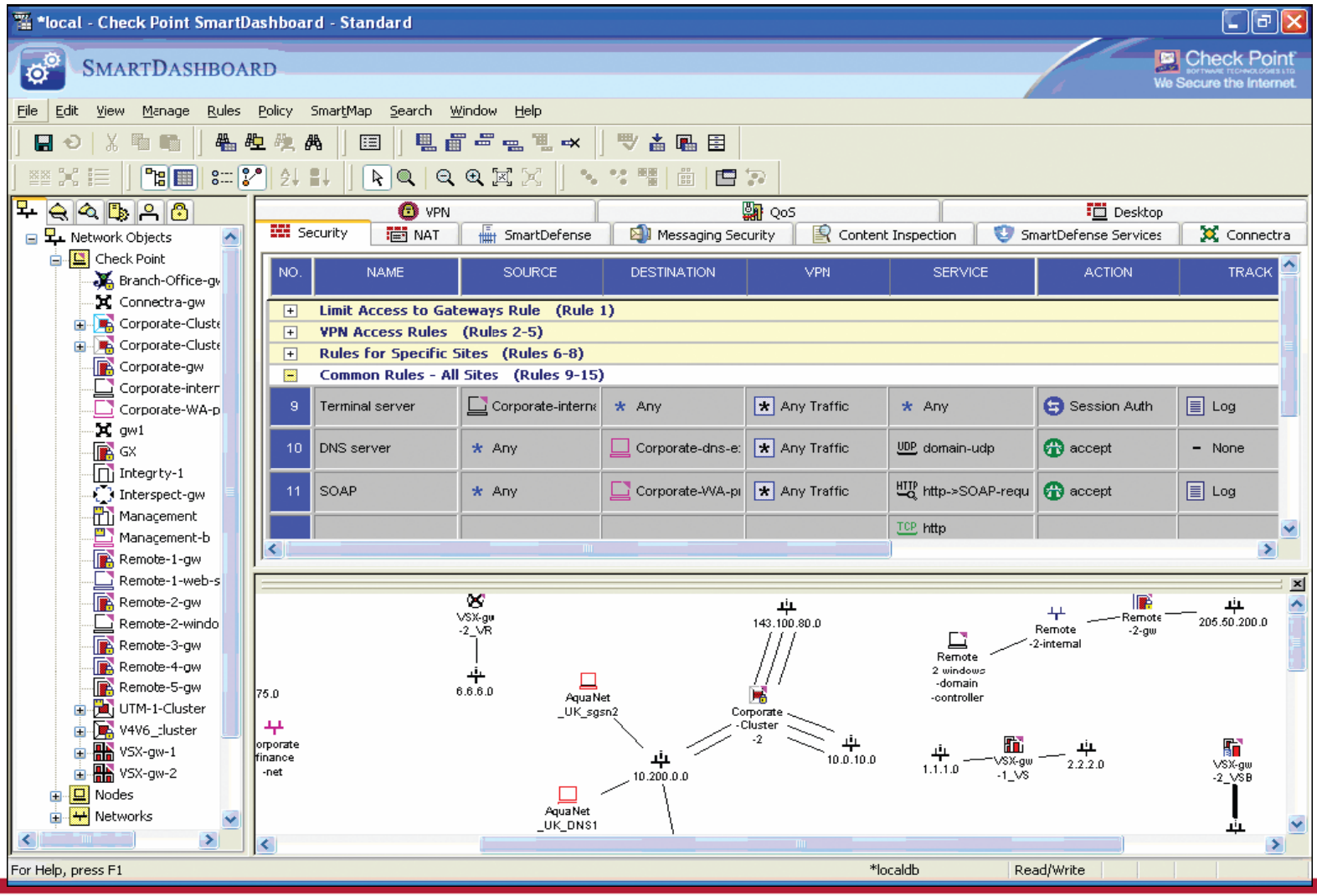
Packet Filters

Also called Access Control Lists (ACLs)

```
access-list name {permit|deny} protocol
  source dest

access-list 101 deny ip 10.0.0.0/8 any
access-list 101 deny ip 127.0.0.0/8 any
access-list 101 deny ip 192.168.0.0/16 any
access-list 101 permit any
```

What about GUI?



Preference on CLI over GUI

- Administrators strongly prefer CLIs over GUIs
- Perceived CLIs as faster, more flexible, trustworthy, reliable, robust and accurate
- GUIs can sometimes hide important details or are buggy
- Administrators face risks in relying solely on GUIs
- “with a plain text editor like vi, the user (administrator) can be confident that what you see is what you get”.
- [Botta et al 2007] [Haber & Bailey 2007]

Contributions

- Models to systematically measure where the complexity lies in firewall configuration – places which lead to heavy mental burdens
- Apply the models to real configuration files from production networks
- Propose tools that can integrate into the configuration process without replacing the CLI as the main user interface

Lexical Complexity

- Program Vocabulary n
  - Sum of number of distinct operators and operands
- Program Volume v
  - v = N * log (n)
  - N is the total number of operators and operands
- Large vocabulary and/or volume size means higher mental demands on the administrator

Example

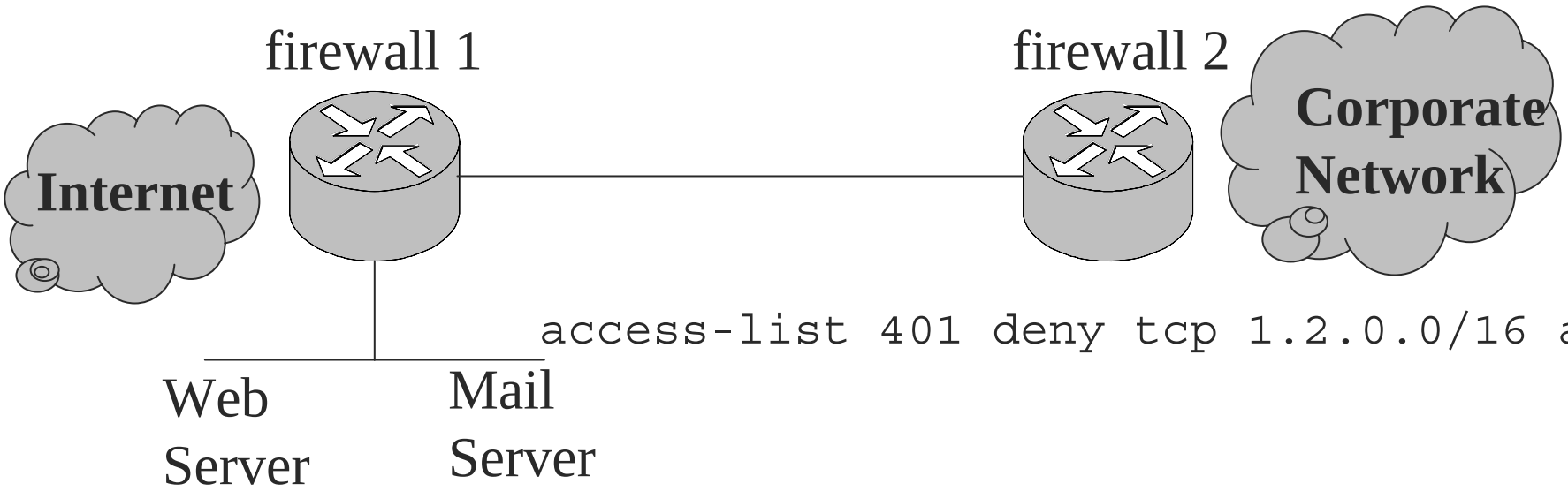
```
access-list 101 deny ip 10.0.0.0/8 any
access-list 101 deny ip 127.0.0.0/8 any
access-list 101 deny ip 192.168.0.0/16 any
access-list 101 permit any
```

- access-list is a keyword thus an operator
- others are parameters thus operands

Structural Complexity

- Measures the number of independent paths in firewall configurations network-wide
- G = <V,E,R>
  - Each firewall rule is a vertex
  - There is an edge e between v1 and v2 if (1) set of packets filtered by v1 intersects with those of v2, or (2) v1 and v2 belong to same packet filter, or (3) v1 and v2 are topologically connected
- SC = E – V + 2p

Example




```
access-list 301 deny tcp 1.2.3.0/24 any
access-list 301 accept tcp any any
```

Study

- Data from a university campus network
- > 50 routers but focus on two border routers and two core routers which implements most of it's firewall functions
- Conclude that should design visualizations to alleviate mental models for the most complex parts of firewall configurations
  - IP addresses, names, interfaces and packet filter interactions

IP addresses

- IP addresses are copied everywhere in firewall configuration
- When writing or reading configuration, intent should be clear
  - internal subnets, private addresses, known malicious networks, etc
- Visualizations fill in details the administrators may not remember
  - Show a global picture of how network treats the addresses

Names

- Ideal case is a central repository for all packet filters – but “the network is the database”
- Packet filters with same name but semantically different
- Packet filters with similar names
  - e.g. Bogon vs bogon
  - Multiple administrators with different coding style
- Topological order

Interactions

- Packet filters for HTTP, SMTP, DNS, and NTP services
  - Defined on border routers on outgoing traffic for accounting purposes
  - Also on incoming traffic for port exceptions
- Visualize to keep with mental images of
  - network topology and interfaces
  - direction of packet filter applications

Information Linking

- [Maclachlan et al 2008] uses explicit linking to coordinate multiple views of related information
- Tie main CLI to related information
  - Administrators only work on a small part of firewall configuration at a time
  - But large amount of relevant information
  - Explicitly link them in side windows
  - An IDE for firewall configuration

Future Work

- Integrate analytics into the configuration environment
- Prototype some of these visualization concepts
- Evaluate them with user studies
- Apply complexity models to routers (e.g. interface definitions, routing protocols, routing policies)

References

- [Wool 2004] A. Wool, A Quantitative Study of Firewall Configuration Errors. IEEE Computer, June 2004
- [Haber & Bailey 2007] E. Haber and J. Bailey, Design Guidelines for System Administration Tools Developed through Ethnographic Field Studies. Proceedings of CHIMIT, March 2007.
- D. Botta et al, Towards Understanding IT Security Professionals and Their Tools. Proceedings of SOUPS, July 2007.
- P. McLachlan et al, LiveRAC: Interactive Visual Exploration of System Management Time-Series Data, In CHI, April 2008.

Thank you

Questions?