Firewall Rule Reviews
Methodologies and Possibilities

Marc Ruef
www.scip.ch
)SCIP(

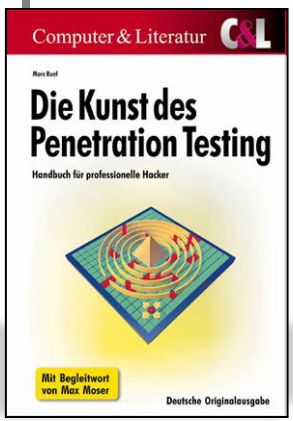
hashdays Security Conference
November 2012
Lucerne, Switzerland

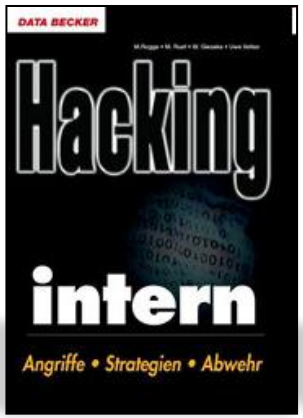
Agenda | Firewall Rule Reviews

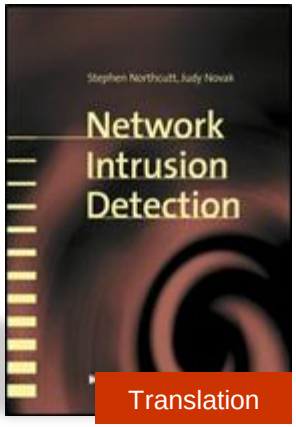
1. Intro	
Introduction	2 min
Who am I?	2 min
What is the Goal?	2 min
2. Firewall Rule Modelling and Review	
Extraction	4 min
Parsing	4 min
Dissection	4 min
Review	10 min
Additional Settings	10 min
Routing Criticality	7 min
Statistical Analysis	5 min
3. Outro	
Summary	2 min
Questions	5 min

Introduction | Who am I?

Name	Marc Ruef
Job	Co-Owner / CTO, scip AG, Zürich
Private Website	http://www.computec.ch
Last Book	„The Art of Penetration Testing“, Computer & Literatur Böblingen, ISBN 3-936546-49-5







Translation

Introduction | What is our Goal?

- A Firewall Rule Review shall determine
  - Insecure rules → Increase security
  - Inefficient rules → Increase performance
  - Wrong rules → Increase quality
  - Obsolete rules → Increase quality
- I will show
  - Different approaches
  - Our methodology
  - Further possibilities

Introduction | Are Firewalls obsolete?

- Multiple sources state, that FWs are/became obsolete (latest «shitstorm» was in May 2012):
  - infoworld.com/d/security/why-you-dont-need-firewall-193153
  - infoworld.com/d/security/the-firestorm-over-firewalls-193409
  - isc.sans.edu/diary.html?storyid=13240
  - networkworld.com/news/2005/070405perimeter.html
- The reasoning behind this would render every additional security measurement obsolete (antivirus, encryption, monitoring, logging, etc.)
- The better the security of your networks/hosts/services/applications is in its core, the more obsolete additional FW restrictions may become
- Layered security is usually still recommended

Introduction | Approach Step-by-Step

1. Extract firewall rules
2. Parse firewall rule sets
3. Dissect
   - Objects
   - Services
   - Actions
   - Relations
4. Determine settings
5. Identify weaknesses
6. Eliminate weaknesses
7. Illustrate risks

Introduction | Files vs. Screenshots

- We prefer exported files
  - Faster
  - More reliable
  - No GUI abstraction layer (better insight)
- Still, screenshots might support the analysis
  - Easier walkthrough («quickview»)
  - Visual enhancement of documentation
  - Verification of parsing (cross-check)
  - Last hope (no export feature, quirky file format, ...)

Extraction | Get the Firewall Rulesets

- iptables
  - Backup: `/usr/sbin/iptables-save`
- Astaro
  - Export: `/usr/local/bin/backup.plx`
  - iptables: `/usr/sbin/iptables-save`
  - Backup: Webadmin / Management / Backup/Restore
- Checkpoint Firewall-1
  - Copy: All files in `%FWDIR%/conf/` (`objects_5.C`, `rulebase.fws`, `*.W`)
  - Export: `cpdb2html/cpdb2web`
- Cisco IOS/PIX/ASA
  - Backup: `show mem`, `show conf`
- Citrix Netscaler
  - Backup: Copy file `/nsconfig/ns.conf` (via SCP)
- Juniper
  - Backup: Admin / Update / Config / Copy&Paste
  - Backup: `request system configuration rescue save` (via FTP)
- McAfee Web Gateway
  - Backup: Configuration / File Management / Configuration Data / Download Configuration Backup
- ...

Parsing | Handle Ruleset Structure

- Apache Directives
  - Apache Reverse Proxies
  - USP Secure Entry Server (Apache-based)
- Arrays
  - Astaro (backup.plx) (alternative is with iptables)
  - Checkpoint (files) (.C, .fws, .W)
  - Fortigate
- Command-line
  - iptables
  - Cisco IOS/PIX/ASA
  - Citrix Netscaler
- INI Files
  - McAfee Web Gateway (base64 encapsulated in XML?!)
  - SonicWALL (base64 encoded string)
- XML Files
  - Airlock
  - Clearswift MIMEsweeper
  - Totemo TrustMail
- ...

Parsing | Access Firewall Rule Attributes (Cisco ASA Example)

```
493 access-list 10 extended permit ip x.x.0.0 255.255.0.0 x.x.39.0 255.255.255.0
494 access-list 10 extended permit ip x.x.0.0 255.255.0.0 xxxxxxxxxxxx 255.255.255.0
495 access-list 10 extended permit ip x.x.0.0 255.255.0.0 xxxxxxxxxxxxx 255.255.255.0
496 access-list 10 extended permit ip x.x.0.0 255.255.0.0 x.x.103.0 255.255.255.0
497 access-list 10 extended permit ip x.x.0.0 255.255.0.0 x.x.101.0 255.255.255.0
498 access-list 10 extended permit ip x.x.0.0 255.255.0.0 x.x.102.0 255.255.255.0
499 access-list 10 remark DMZ to INSIDE
500 access-list 10 extended permit ip x.x.33.0 255.255.255.0 x.x.34.0 255.255.255.0
501 access-list 10 remark DMZ to INSIDE
502 access-list 10 extended permit ip x.x.35.0 255.255.255.0 x.x.34.0 255.255.255.0
503 access-list 10 remark DMZ to INSIDE
504 access-list 10 extended permit ip x.x.40.0 255.255.255.0 x.x.34.0 255.255.255.0
505 access-list 10 remark DMZ to INSIDE
506 access-list 10 extended permit ip x.x.32.0 255.255.255.0 x.x.34.0 255.255.255.0
507 access-list 10 remark LAN-xxxxxxx to INSIDE
508 access-list 10 extended permit ip x.x.33.0 255.255.255.0 x.x.96.0 255.255.255.0
509 access-list 10 remark LAN-xxxxxxxx to INSIDE
510 access-list 10 extended permit ip x.x.33.0 255.255.255.0 x.x.97.0 255.255.255.0
511 access-list 10 extended permit ip x.x.33.0 255.255.255.0 LAN_xxxxxxxxxxxxx 255.255.255.0
512 access-list 10 extended permit ip x.x.35.0 255.255.255.0 LAN_xxxxxxxxxxxxx 255.255.255.0
513 access-list 10 extended permit ip x.x.33.0 255.255.255.0 LAN_xxxxxxxxxx 255.255.255.0
514 access-list 10 extended permit ip x.x.35.0 255.255.255.0 LAN_xxxxxxxxxx 255.255.255.0
515 access-list 10 remark DMZ to INSIDE (xxxxxxxx)
516 access-list 10 extended permit ip x.x.96.0 255.255.255.0 x.x.34.0 255.255.255.0
```

Parsing | Access Firewall Rule Attributes (Firewall-1 Example)

```
30255        : (xxxxxxxxxxxxxxxxxxxx
30256            :AdminInfo (
30257                :chkpf_uid ("{8991278F-A7DB-4049-A7AF-1C18C9DC0195}")
30258                :ClassName (network_object_group)
30259                :table (network_objects)
30260                :LastModified (
30261                    :Time ("Wed May 18 12:58:52 2011")
30262                    :last_modified_utc (1305723532)
30263                    :By (xxxxxx)
30264                    :From (xxxxxxxxxxxxx)
30265                )
30266                :icon ("NetworkObjects/Groups/Group")
30267                :Wiznum (-1)
30268                :name (xxxxxxxxxxxxxxxxxxxx)
30269            )
30270            :ip_convention_object ()
30271            : (ReferenceObject
30272                :Name (xxxxxxxxxx_ftp)
30273                :Table (network_objects)
30274                :Uid ("{54A657BF-5ACE-43A2-99A4-0AB3E854B7EC}")
30275            )
30276            : (ReferenceObject
30277                :Name (xxxxxxxxxxxxxxxx)
30278                :Table (network_objects)
```

Dissection | Access Rule Attributes

- A minimal packet filter rule consists of:
  - Source Host/Net [10.0.0.0/8]
  - Source Port [>1023]
  - Destination Host/Net [192.168.0.10/32]
  - Destination Port [80]
  - Protocol [TCP]
  - Action [ALLOW]
- Additional rule attributes might be (product dependent):
  - ID [42]
  - Active [enabled]
  - Timeframe [01/01/2012 – 12/31/2012]
  - User [testuser2012]
  - Logging [disabled]
  - Priority (QoS) [bandwidth percent 30]
  - ...

Dissection | Example Table

Src Host	Src Port	Dst Host	Dst Port	Protocol	Action
*	>1023	192.168.0.10 /32	80 (http)	TCP	ALLOW
10.0.0.0/8	>1023	*	80 (http)	TCP	ALLOW
...					

Review | Weaknesses Checklist (1/2)

- Allow Rules
  - ANY rules
  - Bi-directional rules
  - Broad definition of zones or port ranges
  - Mash-up of objects
  - Blacklisted traffic (false-negatives)
  - DROP-ALL rule missing
- Insecure Rules
  - Insecure service used (e.g. telnet, ftp, snmp)
  - Overlapping objects
  - Nested objects

Review | Weaknesses Checklist (2/2)

- Obsolete Rules
  - Inactive objects
  - Temporary rules
  - Test rules
  - Obsolete rules
- Documentation Missing
  - No comment/description
  - Whitelisted traffic (reasoning missing)
  - Logging not enabled
- Lockdown missing
  - Lockdown rules missing
  - Stealth rules missing
  - DENY instead of DROP

Review | Example Report Table (Findings)

Src Host	Src Port	Dst Host	Dst Port	Protocol	Action
*	>1023	192.168.0.10 /32	80	TCP	ALLOW
*	* [ANY Rule]	192.168.0.10 /32	23 [Insecure]	TCP	ALLOW
10.0.0.0/8	>1023	*	80	TCP	ALLOW
192.168.0.10 /24	1024-50000 [Inadequate]	10.0.0.0/8	22,902,8443 [Mash-Up]	TCP	ALLOW
* [ANY Rule]	* [ANY Rule]	192.168.0.10 /24	3389	TCP	ALLOW
10.0.0.0/8	0	* [ANY Rule]	0,8	ICMP [Insecure]	ALLOW
...					

Review | Example Report Table (Measures)

Src Host	Src Port	Dst Host	Dst Port	Protocol	Action
*	>1023	192.168.0.10 /32	80	TCP	ALLOW
*	* → >1023	192.168.0.10 /32	23 → 22	TCP	ALLOW
10.0.0.0/8	>1023	*	80	TCP	ALLOW
192.168.0.10 /24	1024-50000 → >1023	10.0.0.0/8	22,902,8443 → 22|902|...	TCP	ALLOW
* → x.x.x.110	* → >1023	192.168.0.10 /24	3389	TCP	ALLOW
10.0.0.0/8	0	* → 192.168. 0.10/24	0,8	ICMP → «Risk Accepted»	ALLOW
...					

Review | Redundant Firewall Environments

Redundant environments usually need to provide «mirrored» rulesets. Every difference is a potential flaw.

Approach:

1. Analyze ruleset FW_A
2. Analyze ruleset FW_B
3. Compare results $FW_A \setminus FW_B$
4. Report all flaws and differences

Review | Multi-Tier Firewall Basics

No FW allows direct connection:

$$A \rightarrow B$$

Single-Tier consists of 1 FW («inline»):

$$A \rightarrow FW \rightarrow B$$

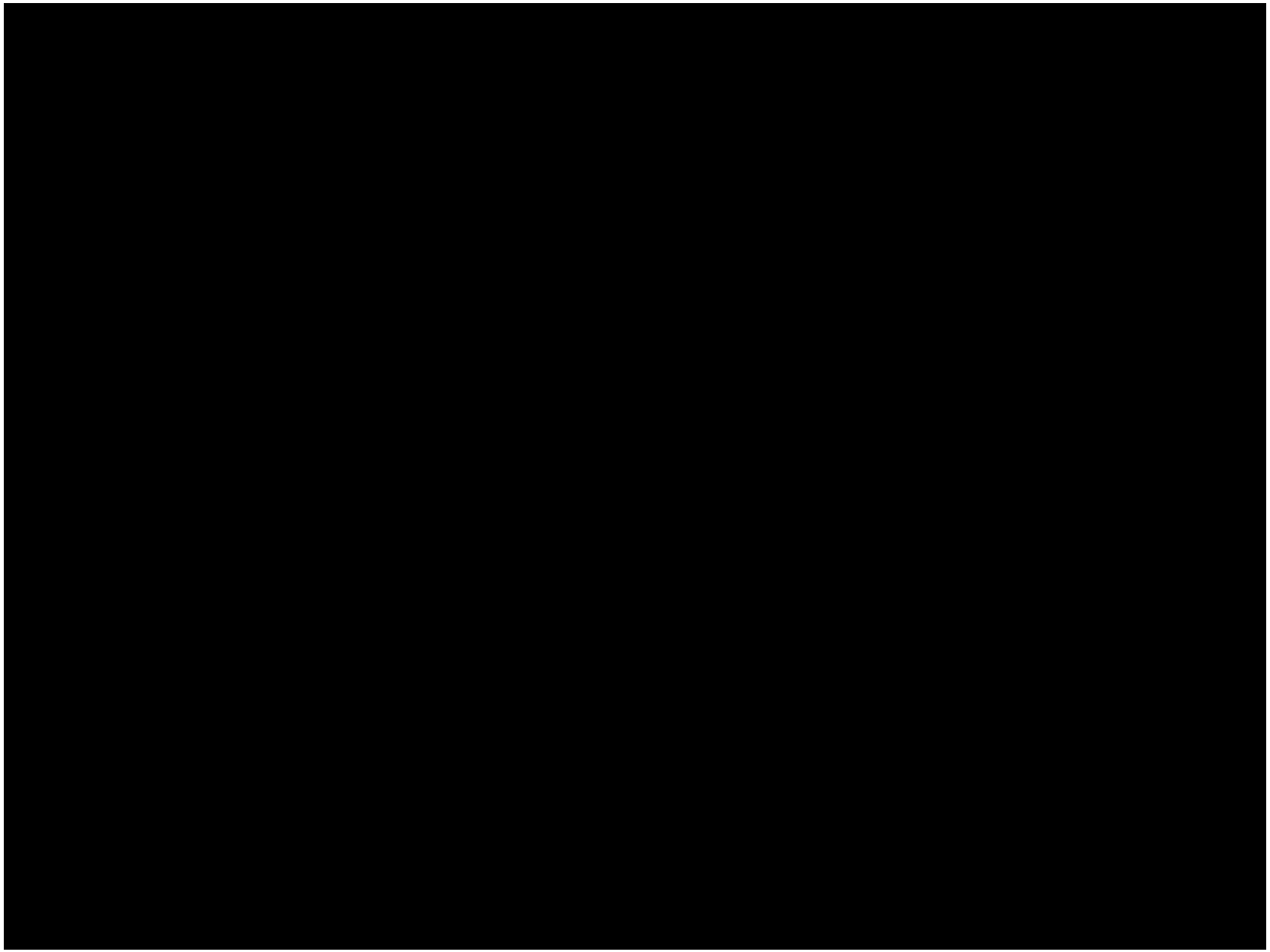
Multi-Tier consists of n FWs. Two-Tier example:

$$A \rightarrow FW_1 \rightarrow FW_2 \rightarrow B$$

Review | Multi-Tier Firewall Rule Cascading

- Consider every tier
- The effort grows exponentially with each new tier
- Respect priorities (what overrides what)
- Additional environmental aspects might influence priorities/actions (e.g. dynamic routing, Intrusion Prevention Systems)

Review | Automated Analysis (Video)



Additional Settings | Workshops recommended

- It is important to consider environmental aspects within an analysis:
  - Network topology
  - Routing
  - Additional security measures (e.g. av, auth, enc)
- It is recommended to discuss aspects with administrators and architects within a workshop

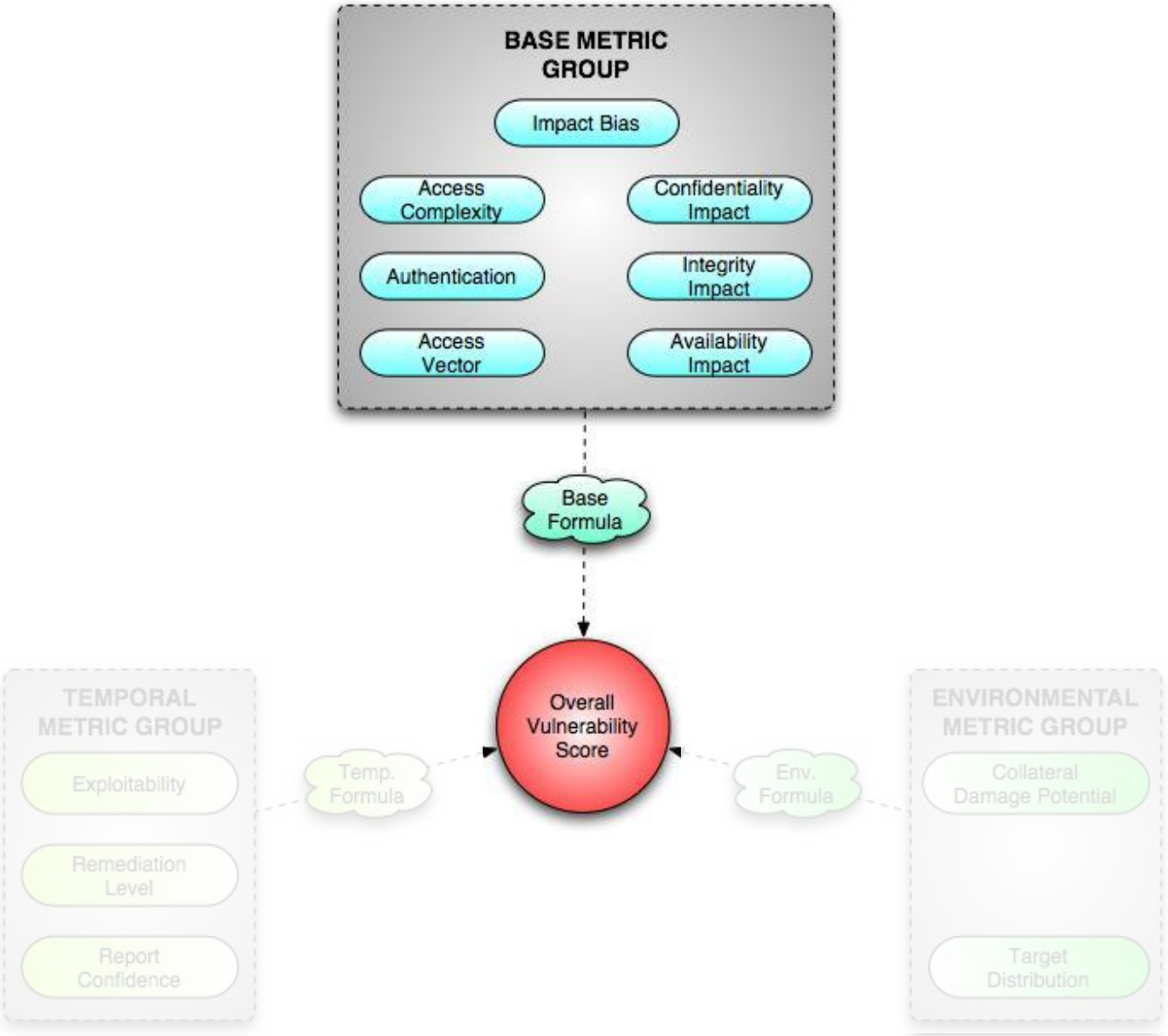
Additional Settings | Global Settings

- Some FWs, especially proxies, introduce additional (global) settings which might affect the rules. Example McAfee Web Gateway:
  - Antivirus
    - Enabled [1=enabled]
    - HeuristicWWScan [0=disabled]
    - AutoUpdate [0=disabled]
  - Caching
    - Enabled [1=enabled]
    - CacheSize [536870912]
    - MaxObjectSize [8192]
  - HTTP Proxy Settings
    - Enabled [1=enabled]
    - AddViaHeader [1=enabled]
    - ClientIpHeader ['X-Forwarded-For']
  - ...

Additional Settings | Example Report Table

ID	Setting	Value	Recommend	Risk
...				
1427	CheckFileSignatures	0	1 (=enabled)	Medium
1428	ChecksumMismatchWeb	'Replace and Quarantine'	'Replace and Quarantine'	Passed
1429	EmbdJavaAppletWeb	'Allow'	'Block'	Medium
1430	ExpiredContentWeb	'Block'	'Block'	Passed
1431	JavaScriptWeb	'Allow'	'Block'	Low
1432	MacroWeb	'Replace document and Quarantine'	'Block Document' (strict approach)	Passed
1433	UnsignedEXEWeb	'Allow'	'Block'	High
...				

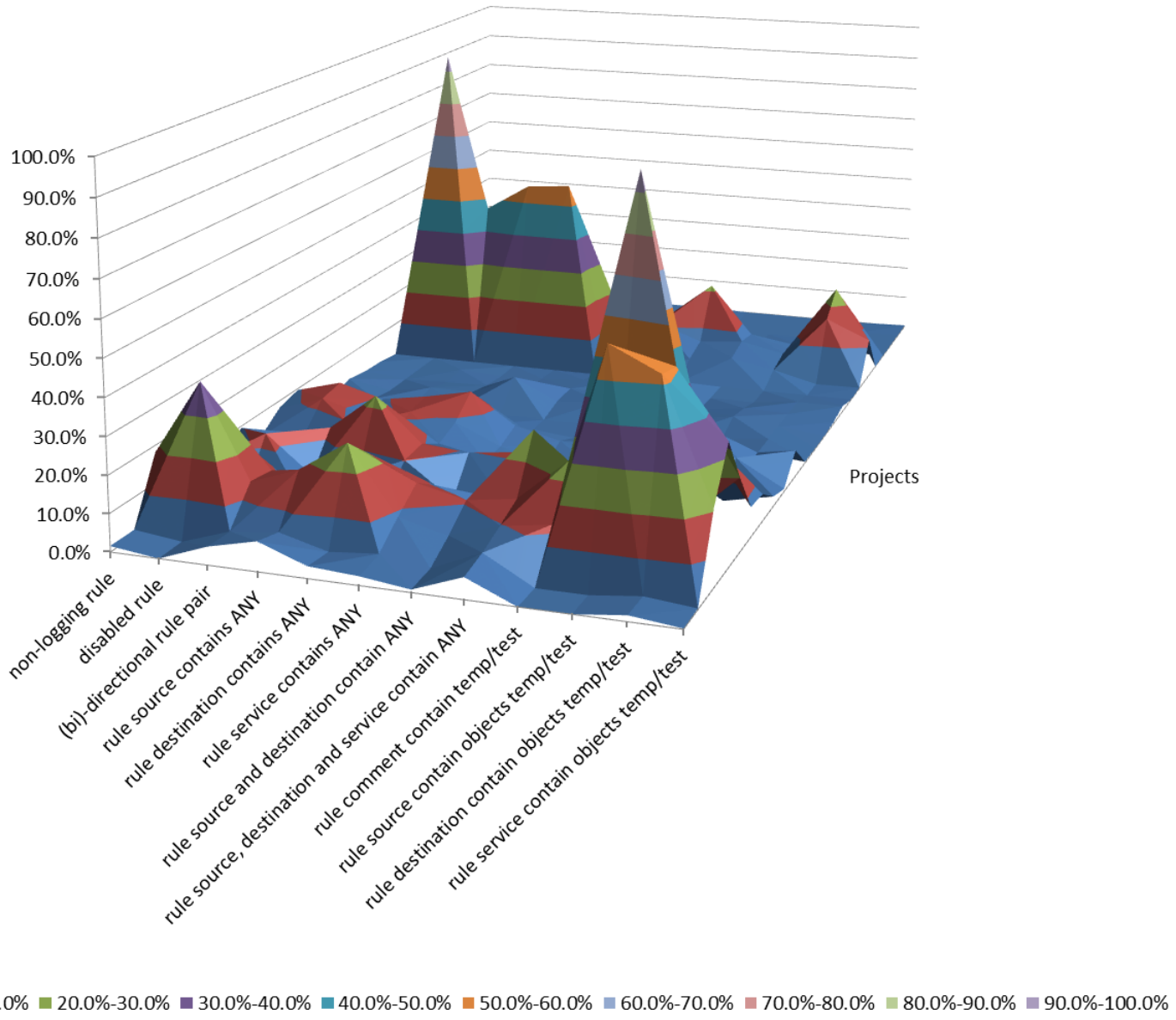
Routing Criticality | CVSSv2 Overview



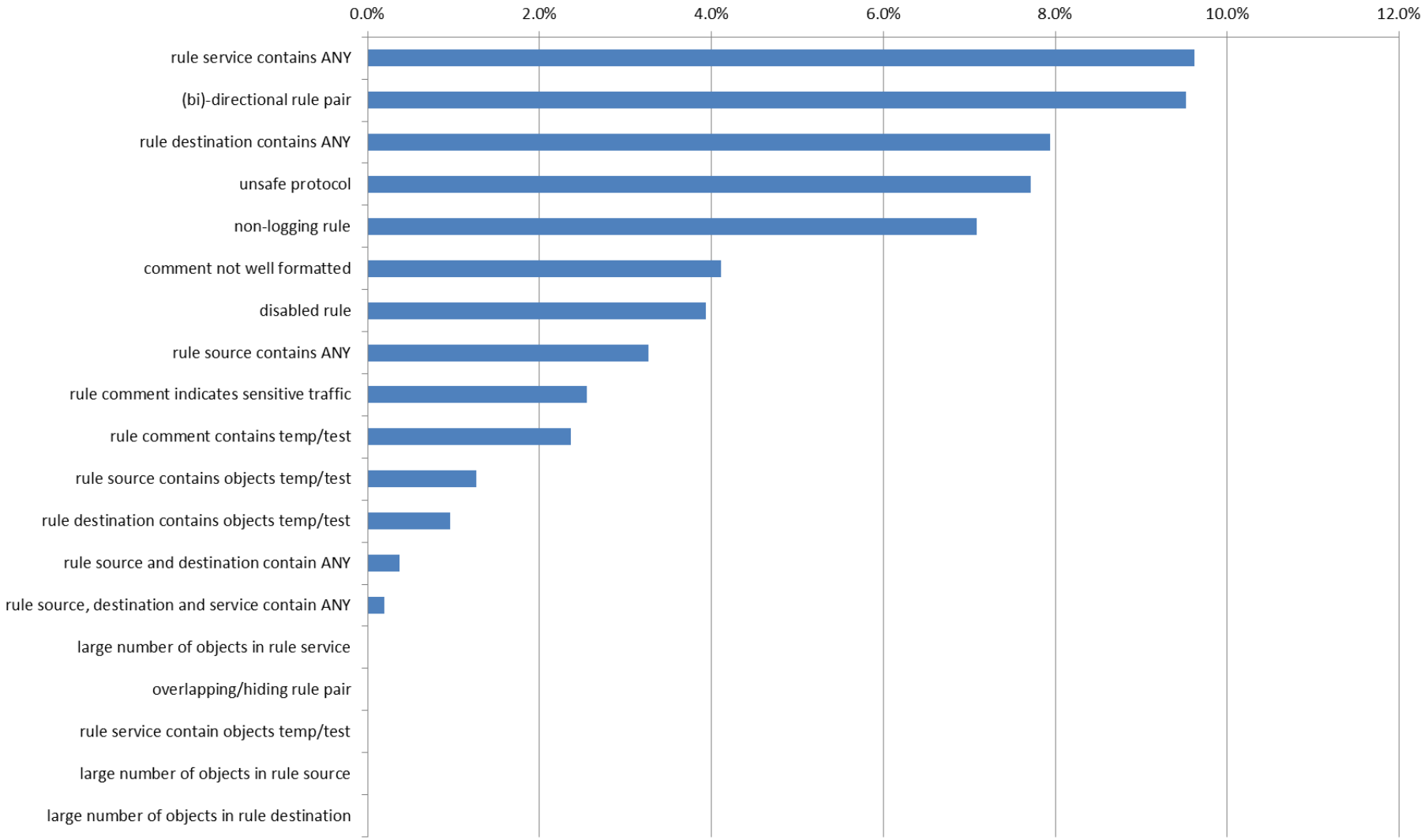
Routing Criticality | Weight Indexing (Experimental Example)

Description	Source	Destination	Port	AV	AC	Au	CI	II	AI	Score
External Web to Web Server	Internet	DMZ	t80	N	L	N	N	C	C	9.4
External Web for Internal Clients (in)	LAN	Internet	t80	N	M	N	C	C	C	9.3
External Web to Customer Site	Internet	DMZ	t443	N	L	S	C	C	C	9.0
External Mail to Public Mail Server	Internet	DMZ	t110	N	M	S	C	C	C	8.5
External Remote Access to Servers	Internet	DMZ	t22	N	M	S	C	C	C	8.5
Internal Access to DNS Servers	LAN	DMZ	u53	L	L	N	C	C	C	7.2
Intranet Access for Internal Clients	LAN	DMZ	t80	L	L	N	P	C	C	6.8
External Web for Internal Clients (out)	LAN	Internet	t80	L	L	S	C	C	C	6.8
Internal Remote Access to Servers	LAN	DMZ	t3389	L	M	S	P	C	P	5.5
Internal ICMP Echo for Servers	DMZ	Internet	i0,8	L	M	S	P	P	C	5.5

Statistical Analysis | Findings per Projects (11 Projects)



Statistical Analysis | Top Findings (Median 11 Projects)



Statistical Analysis | Common Weaknesses

- Common amount of weaknesses determined within analysis of commercial firewalls with approx. 300 rules:
  - First time analysis: 20-30%
  - Annual analysis: 7-10%
- Suggested full analysis frequency: Annually

Statistical Analysis | Reasons for Risks

- There are several possible reasons why FWs are not configured in the most secure way:
  - Mistakes (wrong click, wrong copy&paste, …)
  - Forgetfulness/Laziness ("I will improve that later…")
  - Misinformation (vendor suggests ports 10000-50000)
  - Misunderstanding (technical, conceptual)
  - Unknown features (hidden settings)
  - Technical failure (e.g. broken backup import)
  - Process failure (everyone can do as they please)

Outro | Summary

- Firewall Rule Reviews help to determine weaknesses in firewall rulesets.
- The extraction, parsing and dissection of a ruleset allows a comprehensive analysis.
- Common weaknesses are broad definition of objects, overlapping rules and unsafe protocols.
- Additional quality comes with peripheral aspects like rule comments and logging.

Outro | Literature (German)

- Firewall Rule Analysis
  - Firewall Rule Parsing am Beispiel von SonicWALL, http://www.scip.ch/?labs.20110113
  - Firewall Rule Review - Ansatz und Möglichkeiten, http://www.scip.ch/?labs.20120607
  - Formaler Prozess einer Config Review, http://www.scip.ch/?labs.20121011
- CVSS Scoring
  - Common Vulnerability Scoring System und seine Probleme, http://www.scip.ch/?labs.20101209

Outro | Questions

Security is our Business!

scip AG
Badenerstrasse 551
CH-8048 Zürich

Tel +41 44 404 13 13
Fax +41 44 404 13 14
Mail info@scip.ch
Web http://www.scip.ch
Twitter http://twitter.com/scipag

)SCIP(

☑ Strategy | Consulting
☑ Auditing | Testing
☑ Forensics | Analysis