

User Name: uiadmin

62.8 Hours Saved

Break Down of Saved Hours (ROI)

	Manual	Automated
Per Network Device	1:00:00	00:03
Per Filtering Element*	2:00	< 1 sec
Per Vulnerability	1:00	< 1 sec
Total Time**	62:49:00	1:30

* Explicit/Implicit rules and equivalents

** 24 Hours Format (HH:MM:SS)

56 Important Network Config Check Failures

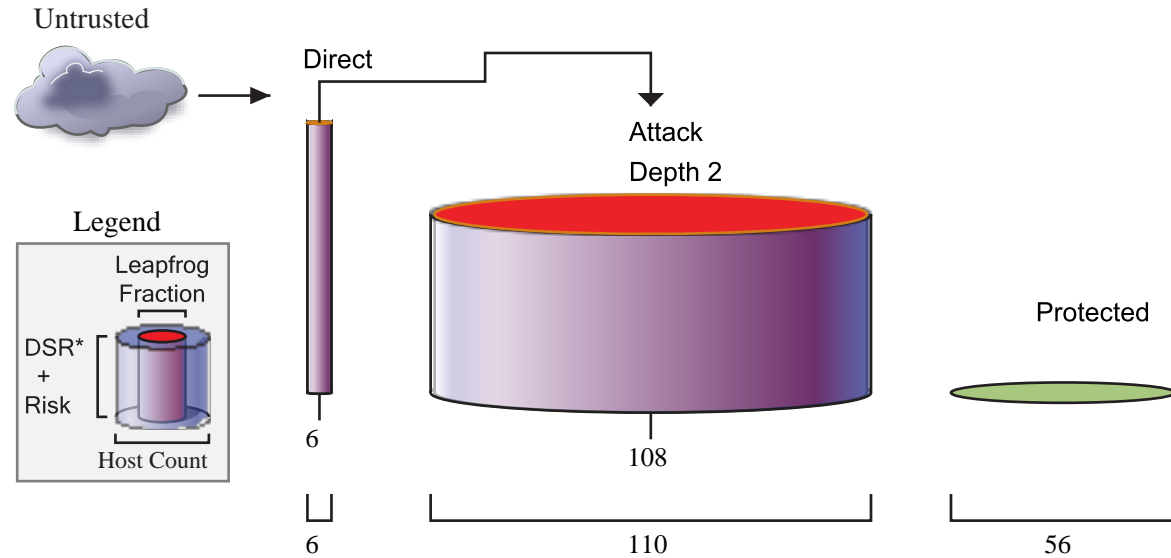
Best Practice Failure Highlights

Avg. Best Practice failures per network device	9.5
Redundant Filter Rules	6
Password Issues Found	24
Risky Services Exposed	33

Information Analyzed

Network Devices	14
Threat Sources	3
Filter Rule Elements	208
NAT Rules	55
Real Hosts	167
Inferred Hosts	5
Total Hosts	172
Vulnerabilities	2403
Unique Vulnerabilities	350
Avg. Vulns / Host	14.0

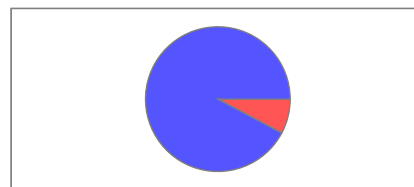
6 hosts out of 172 have been identified as a top priority.



RedSeal's analysis has found 6 of your 172 hosts vulnerable to direct attack from untrusted networks, which could penetrate (leapfrog) deeper into your network (table, page 2). These issues should be given the highest priority to be fixed (i.e. block services, patch vulns, collect additional information).

DSR* - Downstream Risk

Total Attackable Risk: 2,461



- Directly Attackable
- Indirectly Attackable

The impact of Remediation

The total attackable risk found was 2,461, of which 92.24% is not attackable directly from untrusted networks, and is therefore protected by fixing the 6 top priority hosts. This removes the threat path to:

1,893 Indirectly Attackable Vulnerabilities
110 Indirectly Attackable Hosts

Task List For Top Priority Items

The tables prioritize threats and Best Practice failures. The left table, containing up to 20 directly attackable hosts with reachable leapfroggable vulnerabilities, is sorted by downstream risk. The right table, which lists devices, is sorted by number of high-severity failures. In situations where all of the high priority items cannot be fixed, RedSeal Systems can generate a deeper prioritized list. For example, out of the 6 that are most urgently in need of remediation, downstream risk can be used to further prioritize. A host's downstream risk is the sum of the calculated risk scores of all hosts directly or indirectly reachable from the host.

Top Priority Hosts for Remediation

Host Name	Downstream Risk	Risk Score	Value	Exposure	Vulns		
					Conf	Inf	Pres
172.16.3.125	1676	12	20	0.60	2	0	0
B2BWebServ6	378	30	50	0.60	8	0	0
B2BWebServ7	378	30	50	0.60	8	0	0
B2BWebServ8	378	30	50	0.60	8	0	0
B2BWebServ9	378	30	50	0.60	8	0	0
10.5.3.1-10.5.3.253	59	59	60	0.99	0	1	0

Top 20 Network Devices by Number of High Failures

Network Device	High	Medium	Low	Total Failures
SM-ER	8	4	4	16
B2B-ER	8	4	4	16
SM-Users	7	0	4	11
Hamburg	5	4	4	13
Tokyo	4	0	4	8
RemoteOffices	4	0	4	8
SM-DataCenter	4	0	4	8
KarachilR	4	0	4	8
Tokyo-Pix	4	1	6	11
SM-Core	4	0	4	8
Hamburg-NS	3	0	8	11
SM-Pix	2	1	8	11
B2B-Pix	1	1	0	2

Glossary

Network Device: Any system in the model that is not a simple host (e.g., Router, Firewall, Switch, etc).

Filter Rule: A line in an imported network device configuration that is a security rule or access list entry.

Filter Rule Element: A component of a Filter Rule with a single source and destination address or address range.

NAT Rule: A line in an imported network device configuration that is a network address translation rule.