

Product Overview

RedSeal™ Security Risk Manager™

MAP, MEASURE AND MITIGATE YOUR NETWORK'S SECURITY RISK
WITH UNPRECEDENTED EASE AND SPEED

RedSeal SRM provides instant visibility to identify and shut down IT security risk exposures. RedSeal SRM simplifies and automates the process of threat and risk management and provides:

- Network mapping and traffic flow audit
- Infrastructure audits including routers and firewalls
- Threat identification and prioritization for hosts
- Comprehensive risk and compliance reporting

RedSeal SRM drastically reduces the amount of time it takes to audit your network security infrastructure, provides an accurate understanding of your security risk posture, and ensures your organization is in compliance with both internal and external regulations.

RedSeal SRM identifies and prioritizes which vulnerabilities are true threats to your organization by converging networking topology and access rules with security and vulnerability data. Automated router and firewall audits ensure that industry best practices are followed and many compliance requirements are met.

Key Benefits:

- Audits router and firewall configurations based on industry best practices
- Maps network topology
- Automatically identifies the most important risks to remediate
- Reduces workload in analyzing vulnerability data and preparing for audits
- Increases return on existing security investment

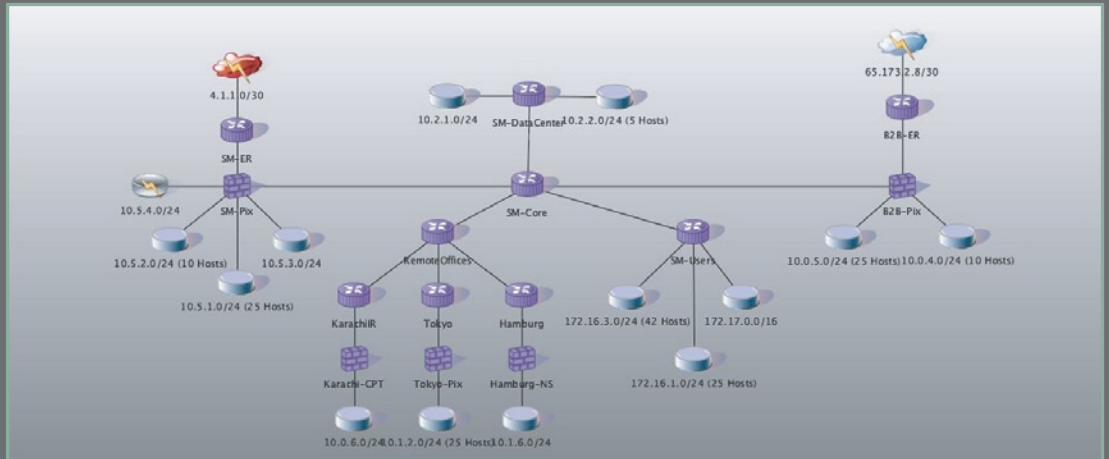
RedSeal SRM maps the entire infrastructure, measures its relevant risk, and mitigates its exposure.



Maps Entire Infrastructure

RedSeal SRM automatically audits your entire network infrastructure including network resources, security devices and hosts to compile an end-to-end and up-to-date map of these resources and their relationships.

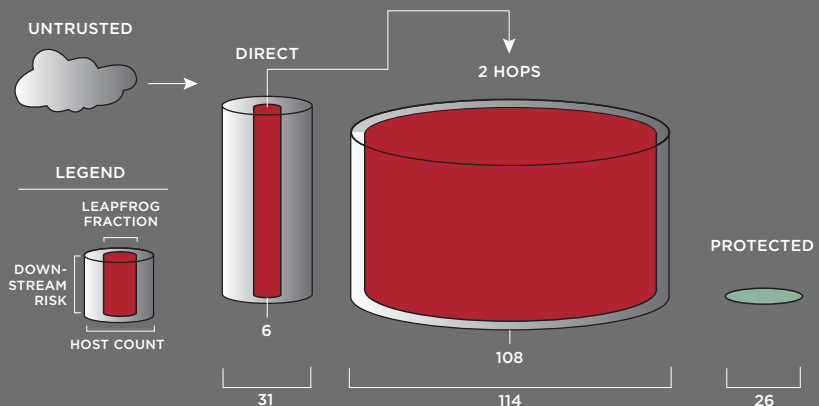
RedSeal SRM automatically collects network device configuration data and uses this information to generate a network topology diagram. This extensive network model provides a unique view of how traffic flows through your network. Using best practices and regulatory requirements, router and firewall configurations are audited in seconds to identify common configuration errors and faulty access policies.



Measures Relevant Risk

RedSeal SRM pinpoints which critical assets are exposed, and which are protected behind firewalls, then assigns a risk value for meaningful measurement. RedSeal SRM combines network policy and host data from vulnerability scanners to identify which vulnerabilities are true threats to the organization. Threat paths provide a network representation of how the exploitation of a chain of vulnerabilities could allow an attacker to gain access to resources that are deeper within the network. Even without host data RedSeal SRM presumed vulnerabilities feature enables organizations to accurately identify potential threats.

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

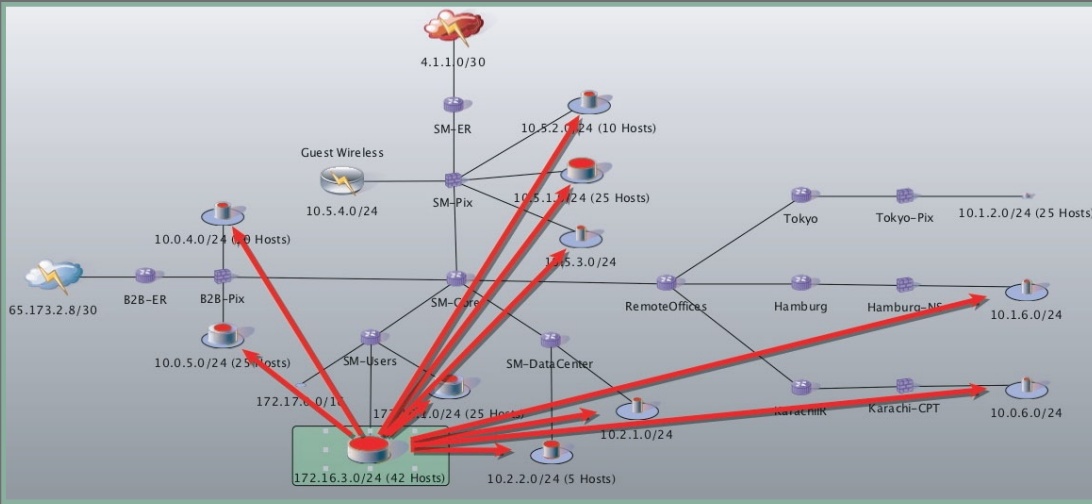


The results of analysis shows this network at 2 hops to death. This is due to the fact that 6 out of the 172 hosts can be directly attacked and then used to attack an additional 113 hosts at hop 2. At this point 100% of the attackable hosts have been accounted for.

“RedSeal SRM is a very good tool to provide an overall view of network threats and risks, and will help you prioritize mitigation measures.”
—Information Security

“Highly Recommended—
This is the first product we
have seen that truly
understands IT risk and
presents it in a manner that
is extremely useful, both to
IT and security teams.”

—SC Magazine



Host Name	IP	Protocols	Ports	Exposure	Value	Downstr...	Vulnerability	Severity	Impact	Patch	Type	Exploitab...
BadSSH	NAT 172.16.3.125	TCP	22	0.58	20	1,838	CVE-2006-5051	HIGH	ACIS	No	PRESUMED	Leapfrog
BadSSH	NAT 172.16.3.125	TCP	22	0.58	20	1,838	CVE-2006-4924	LOW	A	Yes	CONFIRMED	Yes
BadSSH	NAT 172.16.3.125	TCP	22	0.58	20	1,838	CVE-2006-5052	LOW	C	Yes	PRESUMED	Yes
BadSSH	NAT 172.16.3.125	TCP	22	0.58	20	1,838	CVE-2007-2243	LOW	C	No	PRESUMED	Yes

RedSeal presumed vulnerabilities feature correlates past scan results with new threat and vulnerability data to identify new vulnerabilities possible. This map shows new unscanned vulnerability on BadSSH leads to 98% of network being attackable.

Mitigates Exposure

RedSeal SRM prioritizes vulnerabilities that you need to find and fix before an exploit so you can assess your risk profile and focus on the most important assets first.

RedSeal SRM provides a variety of risk measurements and customizable reports so that security administrators can easily prioritize remediation based on business value, internal policy, and regulatory requirements. You can easily determine your network security posture, and identify threats as early as possible to ensure your network security remains in continuous compliance.

redseal
NCC Report by Device

User Name: uladmin
Restriction: Minimum Selected Severity = low; Coverage Date = Jan 14, 1970, 7:04 AM (GMT-08:00) - Jan 14, 1970, 7:04 AM (GMT-08:00);
Notes:

NCC Severity Summary

High	74
Medium	18
Low	56

Summary Data

	Report	Model
Total Network Devices	14	14
Network Devices with 0 Issues	0	0
Avg NCC Failures per Device	10.6	10.6
Unique NCC Failures	49	49
Total NCC Failures	148	148

All Devices > Devices 14 of 131 devices have at least 1 issue

Device: B2B-ER		Instance ID	Config Location	First Noticed	Last Noticed
low	bootp server not disabled	55		Apr 24 2007	Apr 24 2007
high	ip source routing is enabled	66		Apr 24 2007	Apr 24 2007
high	gratuitous arp enabled	57		Apr 24 2007	Apr 24 2007
medium	ip proxy arps allowed on interface "Ethernet0/0"	59	24	Apr 24 2007	Apr 24 2007
medium	ip proxy arps allowed on interface "Ethernet1/0"	62	30	Apr 24 2007	Apr 24 2007
high	ip redirect message allowed on interface "Ethernet1/0"	61	30	Apr 24 2007	Apr 24 2007
high	ip redirect message allowed on interface "Ethernet0/0"	58	24	Apr 24 2007	Apr 24 2007
medium	ip unreachable message allowed on interface "Ethernet1/0"	63	30	Apr 24 2007	Apr 24 2007
medium	ip unreachable message allowed on interface "Ethernet0/0"	60	24	Apr 24 2007	Apr 24 2007
high	no enable secret	51	16	Apr 24 2007	Apr 24 2007
high	no exec timeout set on vty line line vty 0 4	54	52	Apr 24 2007	Apr 24 2007
high	no password for "line console 0"	52		Apr 24 2007	Apr 24 2007
high	no password on vty line vty 0 4	53	52	Apr 24 2007	Apr 24 2007
low	global service pad enabled	56		Apr 24 2007	Apr 24 2007
low	ip global option top keepalives in disabled	64		Apr 24 2007	Apr 24 2007
low	ip global option top keepalives out disabled	65		Apr 24 2007	Apr 24 2007
high	weak community string "public" in the command "snmp-server community public RO"	50	43	Apr 24 2007	Apr 24 2007

Bootp Server Not Disabled

April 24, 2007 15:33
Page 1 of 25

Features

NETWORK TOPOLOGY

- Automated collection of network device configuration data
- Network diagram (exportable to Visio)

NETWORK CONFIGURATION CHECKS

- Baseline check of network device configurations based on industry best practices from vendors and organizations such as NIST, DISA, etc.
- Rule clean-up: redundant rules, non-contiguous wildcards, permit any/any, etc.
- Validate network flows by analyzing network access policies

THREAT IDENTIFICATION AND PRIORITIZATION

- RedSeal Threat Reference Libraries™ is one of the largest current resource library of its kind and as of Jan '08 contains over 28,100 items used to identify exposures and threats
- Identifies which vulnerabilities are threats based on host data from vulnerability scanners, network configuration and authorization policies, and asset values
- Presumed vulnerabilities identifies potential threats between vulnerability scans
- Automated collection of host data from vulnerability scanners and others.

RISK METRICS AND REPORTING

- Determine your security posture and what actions are needed to reduce risk
- Prioritize threats base on internal policy and regulatory requirements
- Generate customizable reports utilizing a variety of risk metrics, including exposure, downstream risk, etc.

NETWORK INFRASTRUCTURE

- Cisco® ASA
- Cisco® FWSM v2 or later
- Cisco® IOS v11.0 or later
- Cisco® PIX v5.x or later
- Cisco® VPN3000 v3.x and v4.x
- Cisco® Aironet v12.3.x and v12.4T(5) or later
- Check Point® Provider-1™
- CheckPoint® SmartCenter™
- CheckPoint® Firewall-1™
- Juniper Networks® Netscreen™ ScreenOS v5.x
- Foundry Networks® FastIron® Ironware™ v7.6 or later

VULNERABILITY ASSESSMENT SYSTEMS

- McAfee® FoundStone™ v5.0 or later
- Qualys® QualysGuard™ v4.6 or later
- Tenable Security® Nessus™ v2.x or later

SERVER REQUIREMENTS

You can purchase RedSeal SRM pre-loaded on the RedSeal SRM appliance or you can use a Microsoft Windows XP SP2 machine or Microsoft Windows Enterprise Server 2003 machine as described

REDSEAL™ SRM™ APPLIANCE

- 1U 19" rack-mount server
- Dual AMD Opteron™ 64bit processors, 8GB RAM
- Hardened Linux®, preloaded software
- 1 10/100/1000 MB Ethernet
- 110-220 V AC Power Supply

MICROSOFT® WINDOWS® Enterprise Server 2003 SP2

- Sun® JRE 6
- 2GB RAM minimum

MICROSOFT® WINDOWS® XP SP 2

- Sun® JRE 1.5
- 2GB RAM minimum

CLIENT REQUIREMENTS

- Sun® JRE 1.5

About RedSeal Systems Inc.

RedSeal provides security risk management solutions that give instant visibility into the threats that leave an open door to valuable company resources.

Evaluate in YOUR environment

It only takes about 30 minutes to try before you buy. You can now download RedSeal Security Risk Management software at no cost or obligation, please go to <http://www.redseal.net/downloads> and you'll see for yourself how easy it is to map, measure and mitigate your security risk posture.



Email eval@redseal.net
Call 1-888-845-8169
Visit www.redseal.net
Download RedSeal SRM at www.redseal.net/downloads/



www.altaware.com
sales@altaware.com
(866) 833-4070
Your RedSeal Systems Reseller

Copyright©2007 RedSeal Systems, Inc. All rights reserved. This publication is protected by copyright and international treaty. No part of this publication may be reproduced in any form by any means, or provided to any third party, without prior written authorization from RedSeal Systems, Inc. The information in this document is confidential to RedSeal Systems and its partners, and is intended for informational purposes only. Information regarding competitive offerings is derived from public sources, and is subject to change without notice.

RedSeal™ Security Risk Manager™, SRM™, RiskMap™, ARA™, and related logos are trademarks of RedSeal Systems, Inc., in the U.S. and/or certain other countries. All other product, service, or company names mentioned herein are trademarks of their respective companies.