



CISCO IPS RISK RATING EXPLAINED

In contrast to simplistic alert rating models that are commonly used in the industry, Cisco IPS Version 5.0 Sensor Software delivers unique Risk Ratings that are assigned to alerts generated from IPS (Intrusion Prevention Systems) sensors. The intent of this risk rating is to provide the user with an indication of the relative risk of the traffic or offending host continuing to access the user's network. This rating can be used either to illuminate the events that require immediate administrator attention in the classic intrusion detection system (IDS) promiscuous mode, or to provide a means for developing risk-oriented event action policies when the sensor is employed in the inline intrusion protection system (IPS) mode.

The risk rating is realized as an integer value in the range from 0 to 100. The higher the value, the greater the security risk of the trigger event for the associated alert. The risk rating is a calculated number that has four primary components—Alert Severity Rating (ASR), Signature Fidelity Rating (SFR), Attack Relevancy Rating (ARR), and Target Value Rating (TVR).

The Risk Rating is calculated using the following formula:

$$RR = \frac{\text{Fidelity} * \text{Severity} * \text{Target-Value-Rating}}{100 * 100 * 100}$$

Signature Fidelity Rating (SFR) = Relative measure of the accuracy of the signature (predefined); 0–100 Set by Cisco Systems, Inc.

Alert Severity Rating (ASR) = Relative result or damage if the attack succeeds (predefined); 25—Information, 50—Low, 75—Medium, 100—High

Target Value Rating (TVR) = Value used to change the risk rating higher or lower based on the target of the attack (user defined); 75—Low Asset Value , 100—Medium Asset value , 150—High Asset Value, 200—Mission Critical Asset Value

The ASR is a user-modifiable weighted value that characterizes the damage potential of the suspect traffic. It is presented to the user in familiar, descriptive text tags—informational, low, medium, and high.

- An informational alert is based on commonly seen network traffic and has no particular security relevance when seen on most networks. It may be a violation of a policy on some networks, but it generally poses no immediate threat to network security.
- A low alert is also based on relatively benign network traffic, but is somewhat unusual on most networks. Also categorized as low would be overt scans, such as those commonly seen by network management devices. Although this type of scan could be a precursor to an attack, it is uncommon for an overt scan to be used for this purpose.
- A medium alert is based on traffic that generally should not be seen on the network. It is usually assigned to midlevel reconnaissance traffic, denial of service (DoS) attacks on self-healing services, and remote access of unexpected information or programs. This type of behavior warrants investigation or preventive actions, sometimes requiring policy decisions from the user.
- A high alert is based on traffic that is indicative of an active attack or an obvious precursor to an attack. This traffic should never be seen in a normal network. This rating is reserved for attacks that could result in serious compromise of the target, or for specific network traffic that is only seen in covert reconnaissance traffic.

The SFR is a user-modifiable weighted value that characterizes the fidelity of the signature that has detected the suspect activity. Several factors affect the fidelity of a signature. First, many vulnerabilities are only relevant for a particular OS, service, application, or even patch level. Without

this information, particularly in the classic IDS mode, the sensor may identify attempts that will ultimately fail as actual attacks, leading to wasted effort on the part of the security administrator investigating the alleged attack. Another issue that can cloud the fidelity of a signature is a legitimate application that produces traffic that mimics the behavior of an exploitation of a network vulnerability. The signature developer takes these factors into consideration when assigning the SFR for a particular signature.

The ARR is an internal weighted value that characterizes any additional knowledge that the sensor may have about the target of the event. This information is used to clarify some of the uncertainties related to signature fidelity. As the sensor builds a more definitive picture of the target host, the risk associated with the event can be better defined.

Finally, the TVR is a user-defined value that represents the user's perceived value of the target host. This allows the user to increase the risk of an event associated with a critical system and to de-emphasize the risk of an event on a low-value target.

In closing, risk rating provides the user with valuable insight into the overall risk of an event. This allows the user to develop policies for the prevention of network attacks or to better characterize events for prioritization of further investigation



Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel
Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R) 205391.B_ETMG_KL_9.05