Risk Rating and Threat Rating: Simplify IPS Policy Management

Introduction

Depending on the size of the enterprise and where an intrusion prevention system (IPS) is placed, your IPS may generate thousands to millions of alerts every day. Analyzing all these alerts can be a daunting task. Cisco® IPS Sensor Software Version 5.0 introduced risk rating and threat rating, two powerful features that greatly simplify IPS policy management and day-to-day operations. Risk rating is a quantitative measure of your network's threat level before IPS mitigation. Threat rating is a quantitative measure of your network's threat level after IPS mitigation.

Risk rating and threat rating can greatly enhance your productivity and increase the security of your network and assets. This white paper explains how risk rating and threat rating are calculated, and explains how to build policies with risk rating and threat rating.

Risk Rating Calculation

Risk rating is a quantitative measure of your network's threat level before IPS mitigation. For each event fired by IPS signatures, Cisco IPS Sensor Software calculates a risk rating number. The factors used to calculate risk rating are:

- Signature fidelity rating: This IPS-generated variable indicates the degree of attack certainty.
- Attack severity rating: This IPS-generated variable indicates the amount of damage an attack can cause.
- Target value rating: This user-defined variable indicates the criticality of the attack target. This is the only factor in risk rating that is routinely maintained by the user. You can assign a target value rating per IP address in Cisco IPS Device Manager or Cisco Security Manager. The target value rating can raise or lower the overall risk rating for a network device. You can assign the following target values:
  - 75: Low asset value
  - 100: Medium asset value
  - 200: Mission-critical asset value
- Attack relevancy rating: This IPS-generated value indicates the vulnerability of the attack target.
- Promiscuous delta: The risk rating of an IPS deployed in promiscuous mode is reduced by the promiscuous delta. This is because promiscuous sensing is less accurate than inline sensing. The promiscuous delta can be configured on a per-signature basis, with a value range of 0 to 30. (The promiscuous delta was introduced in Cisco IPS Sensor Software Version 6.0.)
- Watch list rating: This IPS-generated value is based on data found in the Cisco Security Agent watch list. The Cisco Security Agent watch list contains IP addresses of devices involved in network scans or possibly contaminated by viruses or worms. If an attacker is found on the watch list, the watch list rating for that attacker is added to the risk rating. The

value for this factor is between 0 and 35. (The watch list rating was introduced in Cisco IPS Sensor Software Version 6.0.)

The formula to calculate risk rating in Cisco IPS Sensor Software Version 6.0 is:

$$RR = \frac{ASR * TVR * SFR}{10000} + ARR - PD + WLR$$

Risk rating can help enhance your productivity as it intelligently assesses the level of risk of each event and helps you focus on high-risk events.

Threat Rating Calculation

Threat rating is a quantitative measure of your network's threat level after IPS mitigation. The formula for threat rating is:

```
Threat Rating = Risk Rating – Alert Rating
```

The values of the alert ratings are listed below.

- 45: deny-attacker-inline
- 40: deny-attacker-victim-pair-inline
- 40: deny-attacker-service-pair-inline
- 35: deny-connection-inline
- 35: deny-packet-inline
- 35: modify-packet-inline
- 20: request-block-host
- 20: request-block-connection
- 20: reset-tcp-connection
- 20: request-rate-limit

For example, if an alert had a risk rating of 100 and the IPS mitigates the event with a deny-attacker-inline action, the threat rating would be calculated as:

```
Threat Rating = Risk Rating – Alert Rating, or 100 – 45 = 55.
```

Threat rating brings the value of risk rating to a new level. By taking the IPS mitigation action into account, threat rating helps you further focus on the most important threats that have not been mitigated.

Policy Definition Based on Risk Rating and Threat Rating

Risk rating and threat rating allow you to easily build powerful policies with Cisco IPS Device Manager embedded in the IPS sensor, or Cisco Security Manager, an advanced multidevice policy management application. With Cisco IPS Device Manager or Cisco Security Manager event action override, you can apply policies based on risk rating. For example, you can build the following policy:

```
90 < risk rating < 100, deny packet inline
70 < risk rating < 89, produce verbose alert
59 < risk rating < 60, produce alert
```

You can easily tune your IPS by changing the risk rating thresholds for each action. Furthermore, you can create exceptions with the event action filters. For example, you can create an exception

to allow all management traffic, or all traffic from the CEO of your company. With one click, you can assign the event action override and event action filter to one sensor with Cisco IPS Device Manager, or to thousands of sensors with Cisco Security Manager.

With Cisco IPS Event Viewer, you can easily filter your alerts by risk rating or threat rating. You can configure your Cisco IPS Event Viewer to show only high risk rating events or high threat rating events, or sort events by risk rating or threat rating in descending or ascending order. Cisco IPS Event Viewer can also use third-party tools to send pages and e-mail. The intelligent processing within Cisco IPS Sensor Software allows you to focus on the most critical alerts and activities.

Summary

Cisco IPS risk rating and threat rating are intelligent processing features that simplify policy configuration and event monitoring. Instead of spending hours investigating low-risk alerts, you only analyze high-risk, critical events. Risk rating and threat rating allow you to increase your productivity and enhance the security of your network and assets.

Americas 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: 408 527-0883

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

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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

Printed in USA C11-436980-00 10/07

