Cisco IPS Tuning Overview

Overview

Increasingly sophisticated attacks on business networks can impede business productivity, obstruct access to applications and resources, and significantly disrupt communications. And because of compliance regulations and consumer privacy laws, business priorities now include minimizing legal liability, protecting brand reputation, and safeguarding intellectual property.

Cisco® Intrusion Prevention System (IPS) solutions are an integral part of the Cisco Self-Defending Network and Cisco Threat Control solutions, providing end-to-end protection for your network. This inline, network-based defense can identify, classify, and stop known and unknown threats, including worms, network viruses, application threats, system intrusion attempts, and application misuse. In addition, a Cisco IPS solution will protect against new day-zero threats, botnet data leakage, and security evasion attempts.

Cisco IPS 4200 Series Sensors and Cisco IPS Sensor Software deliver high-performance, intelligent detection with precision response, from the network edge to the data center. This technology evaluates metrics in both multimedia and transactional environments, so you can anticipate true IPS performance tailored to your business.

About This Paper

This paper explains the basics of IPS tuning and guides you through the tuning process to provide you with actionable information that you can research to help ensure the security of your network assets. This paper is geared toward Cisco partners, Cisco customers, or anyone who needs a basic understanding of Cisco IPS.

Tuning Step 1: Correct IPS Deployment

An IPS device should always be placed behind a perimeter filtering device such as a firewall or an adaptive security appliance (such as a Cisco 5500 Series Adaptive Security Appliance). The perimeter device will filter traffic to match your security policy, allowing only expected acceptable traffic into your network. Correct placement significantly reduces the number of alerts, thereby increasing actionable data that you can use to investigate security violations. Conversely, if you have an IPS device on the edge of your network in front of the firewall, your IPS would fire on every single scan and attempted attack even if there is no significance to your network implementation. This could result in hundreds, thousands, or—in the case of larger enterprises—possibly millions of alerts that are not considered critical or actionable in your environment. Wading through this data would be a costly and near-impossible process.

Step 2: The IPS Tuning Process

IPS tuning helps ensure that the alerts you are seeing are real, actionable information. Without tuning, you will potentially have thousands of benign events, making it difficult for you to conduct any security research or forensics on your network. Benign events, also known as false positives, exist in all IPS devices, but they happen much less in devices such as Cisco IPS devices, which are stateful and normalized, and use vulnerability signatures for attack evaluation. Additional Cisco

IPS features include risk rating, which identifies high-risk events, and policy-based management, which easily lets you deploy rules that enforce an IPS signature action based on risk rating.

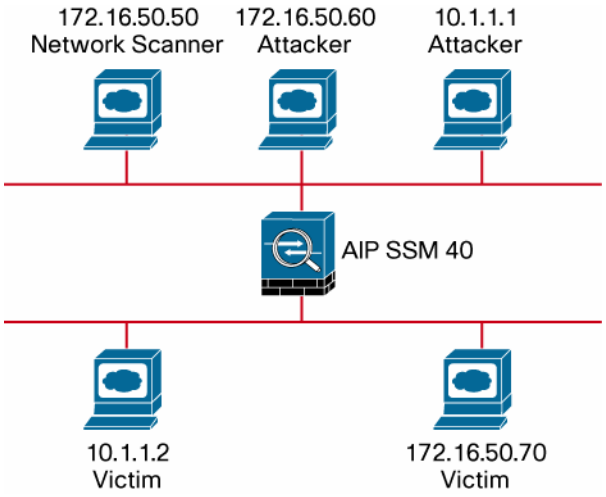
In the real-life case study and tuning process that follows, basic steps will be taken to reduce alerts. When finished, you will see that the remaining results are actionable IPS events that you can use to determine if a real attack has been attempted on your network.

The network topology for this case study includes six devices, each with a specific purpose.

1. A Cisco Advanced Inspection and Prevention Security Services Module 40 (AIP-SSM 40) protecting a data center server. The management IP address is 172.16.254.204. This device will detect and report all data traversing the network that matches a signature or threat protection algorithm used by the Cisco IPS.
2. A scanning device that is known to network and security administrators. This device is used by network and security administrators to find security holes (vulnerabilities) in their network devices. A scanning device like this is usually running 24x7; for simplicity in this case study, we are running it on demand so the alerts being tuned are manageable. The IP address is 172.16.50.40.
3. Two devices used to generate real attacks on the server. The IP addresses are 172.16.50.60 and 10.1.1.1.
4. Two data center servers that are being protected by the IPS. These servers are unpatched and the IP addresses are 172.16.50.70 and 10.1.1.2.

Following is the topology of the lab used in this case study.

Figure 1.



Following is a basic step-by-step process for tuning using Cisco IPS Manager Express, which is available in Cisco IPS Sensor Software v6.1 or later.

1. The first and most critical task for ensuring that the IPS does not overburden you with alerts is to place the IPS in your network behind a perimeter filtering device. This simple placement task may reduce the number of alerts that you need to filter by several thousand events per day.
2. Deploy your IPS with the default signatures in place. There are no specialized profiles or specialized parameters that need to be configured to deploy a Cisco IPS. The default

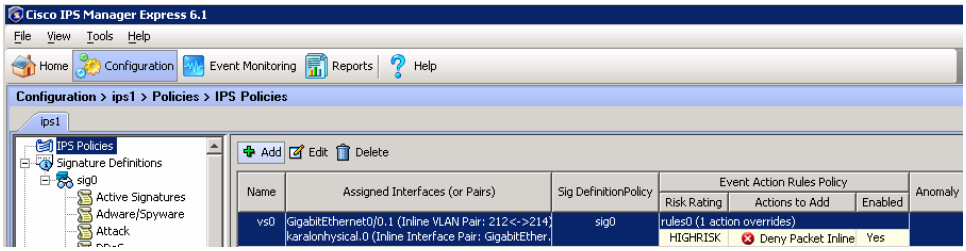
signature set will provide you with a high security protection posture. You can view all the IPS signatures on your sensor using Cisco IPS Manager Express and browsing to Configuration > IPS-Name > Policies > IPS Policies > All Signatures. You can view only your active signatures by browsing to Configuration > IPS-Name > Policies > IPS Policies > Active Signatures.

Note: This case study uses the default Cisco IPS signature set. The Cisco IPS signature team has spent thousands of person hours determining the most secure default signature settings. If you think you may have inadvertently changed some signature values, select all signatures, click the button “Restore default” and then click “Apply.”

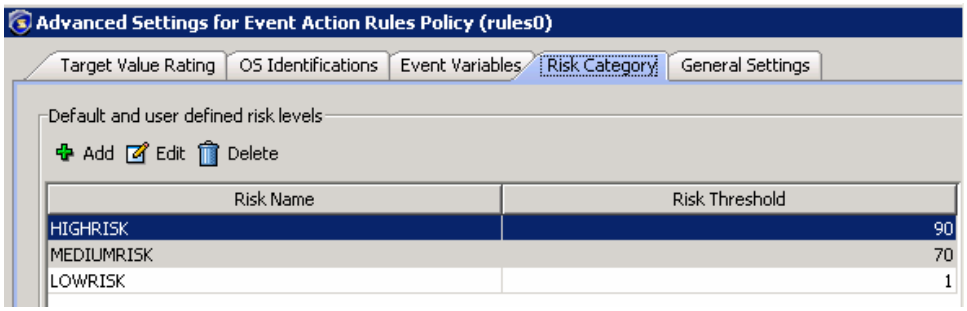
3. Set the event action override to drop packets with a risk rating greater than 90. This is the default configuration and will help ensure that high risk alerts will be stopped immediately.

Note: By default, the sophisticated Cisco IPS risk rating calculation feature will accurately identify risks and report a risk rating value for each alert that is fired. The higher the risk rating, the more dangerous the attack.

Check your default event action override by using Cisco IPS Manager Express and browsing to Configuration > IPS-Name > Policies > IPS Policies. Following is the screen capture for this case study.



Click the “Edit” icon and then the Advanced tab to view the current override settings. HIGHRISK should be set to 90.



4. Now that the IPS device is set to a default signature set located correctly in the network and overrides are set correctly, we can start the case study. The following steps will be taken to generate both benign and real alerts on the IPS device.
   - The scanning device (172.16.50.40) will run one NMAP scan to the data center server (172.16.50.70).
   - Using the same IP addresses, the scanning device will run one default Nessus scan to the data center server.
   - During these scans, the attack servers (172.16.50.60 and 10.1.1.1) will launch several real attacks against the data center servers.

- During the scans, the 10.1.1.1 or 10.1.1.2 attack devices will generate both high- and low-priority attacks to help demonstrate some high-level security analysis used to decide how to respond to these attacks.

5. After this scan and attack traffic is generated, there will be a few hundred alerts fired by the IPS. All of these alerts are not what would be considered actionable alerts, so harmless events need to be eliminated.

Begin the Filtering Process

The first step is to filter out known benign events from your network caused by specialized software such as vulnerability scanners and load balancers.

In this case study, we know the source IP address for our scanner is 172.16.50.40. The first thing you will probably notice when scrolling through the events is that there are 681 events.

Note: Just scanning a single target for three minutes generated almost 700 events. That's 233 events per minute per scanner on your network. It's not unusual for a company to run multiple scanners: consider that if you have five scanners on your network, you will generate 1,006,5560 benign events per day!

Using Cisco IPS solutions, it's easy to filter out these events. There are two methods you can use to achieve this.

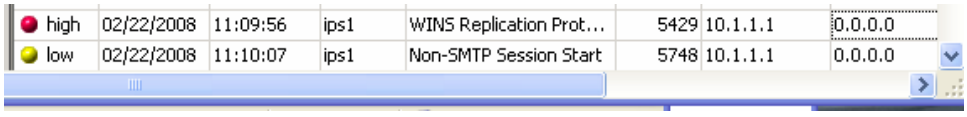
a. Configure the Cisco IPS device to ignore these alerts in the future.

b. Allow the Cisco IPS device to fire the alerts and then use Cisco IPS Manager Express to only filter the benign events.

There are legitimate reasons to use either method. Generally speaking, it's best to use Cisco IPS Manager Express to filter the events: you'll have a historical record to go back and view if you ever need to do backdated forensics. If your company is under any regulations to protect customer data or financial data, it's recommended to meet the compliance regulations that you do not filter the event from the IPS itself. In this case study, we have elected to use Cisco IPS Manager Express to filter benign events and research critical events.

Because you know your network, you will know the source IP addresses of these devices, and you can simply use a filter in the IPS device to create a policy whereby if scan data is sourced from these IP addresses, the alert should not be shown.

1. To filter all events from the scanner, enter (not equal) != 172.16.50.40 into the attacker IP address field. This will immediately get rid of all the primary alerts generated by the scanner and significantly reduce the number of alerts you need to work with. We've gone from 800 alerts to 14.
2. The next step is to look at the remaining attacks and see if anything jumps out. The most obvious is the attacks that are destined for an IP address of 0.0.0.0. Enter !=0.0.0.0 in the destination IP address field. We are now down to 7 alerts.



3. The next step is to filter attacks that have been dropped. Scroll though the list and you can easily see those alerts. Keep in mind that even though these are high-level alerts, they are not overly concerning because they have been blocked. No forensics need to be performed on these alerts unless you want to check the attacking IP address.

If the attacking address is outside your IP address range, you can contact the owner of the IP address range, which you can find by using the Cisco IPS Manager Express “whois” tool. To do this, highlight the event, click on the tool icon, and select “whois.” Results may vary because when you are attacked, the machine that attacked you has often been exploited and the operator of that machine may be unaware of any problems.

If it’s an internal address, you will want to run security scans to try and repair the infected machine or reinstall the OS and applications to fix the problem. It’s important to remember that there is an outside chance that the owner of the machine is responsible for the attack.

To filter dropped signatures, select the “Action” field, click on the popup button at the right, and select all the actions that drop or reset packets or flows.

4. The next step is to filter information alerts. Uncheck the box labeled “Informational.” Even though these events are filtered out, they could warrant investigation. In many cases, including this example, the low-priority events may indicate that another device is doing reconnaissance on a device protected by the IPS.. Network administrators should research these source addresses to see if the reconnaissance on those machines is being caused by malware or an employee. If it’s an infected machine, remove the malware or restore the infected device to a known good condition. There are now five alerts remaining.

Severity	Date	Time	Device	Sig. Name	Sig. ID	Attacker IP	Victim IP	Action...	Vicitm ...
high	02/22/2008	11:09:39	ips1	Cursor/Icon File Forma...	5442	10.1.1.2	10.1.1.1		1072
high	02/22/2008	11:09:40	ips1	Possible Heap Payload ...	5477	10.1.1.2	10.1.1.1		9112
high	02/22/2008	11:09:41	ips1	WINS Replication Prot...	5429	10.1.1.1	10.1.1.2		42
high	02/22/2008	11:09:43	ips1	WinZip ActiveX Control...	5876	10.1.1.2	10.1.1.1		4604
high	02/22/2008	11:09:45	ips1	Nmap UDP Port Sweep	4003	10.1.1.2	10.1.1.1		

5. At this point, the tuning process is essentially complete: all the benign scanning events, alerts for invalid destination address, informational alerts, and stopped attacks have been filtered. The remaining alerts are considered actionable information. They represent the greatest threat to your network and therefore must be analyzed. Researching these events with Cisco IPS Manager Express is a straightforward process.

Following is a step-by-step explanation of how to process the remaining events. In this case study, forensics analysis will be performed only on one of the remaining alerts. If this were a live network, you would take the same steps for the remaining events.

1. The event in the case study to be analyzed is Cisco sig ID 5867/0. The following steps must be taken.

   Research the alert: Right-click on the event and select the “Explanation” tab. The description says, “The signature fires on attempts to instantiate the WinZip ActiveX control. A vulnerability exists in the ActiveX control that was never intended to be used in Internet Explorer.” A second section in the explanation tab tells you if other actions besides an attack can cause this signature to fire. In this case, it says “Individuals browsing proof of concept code may cause this signature to trigger.” This description is telling us that either someone browsed to a Webpage and looked at proof of concept code or there was an actual attack. We are going to assume that an attack was attempted because if it was an incident during browsing, the port

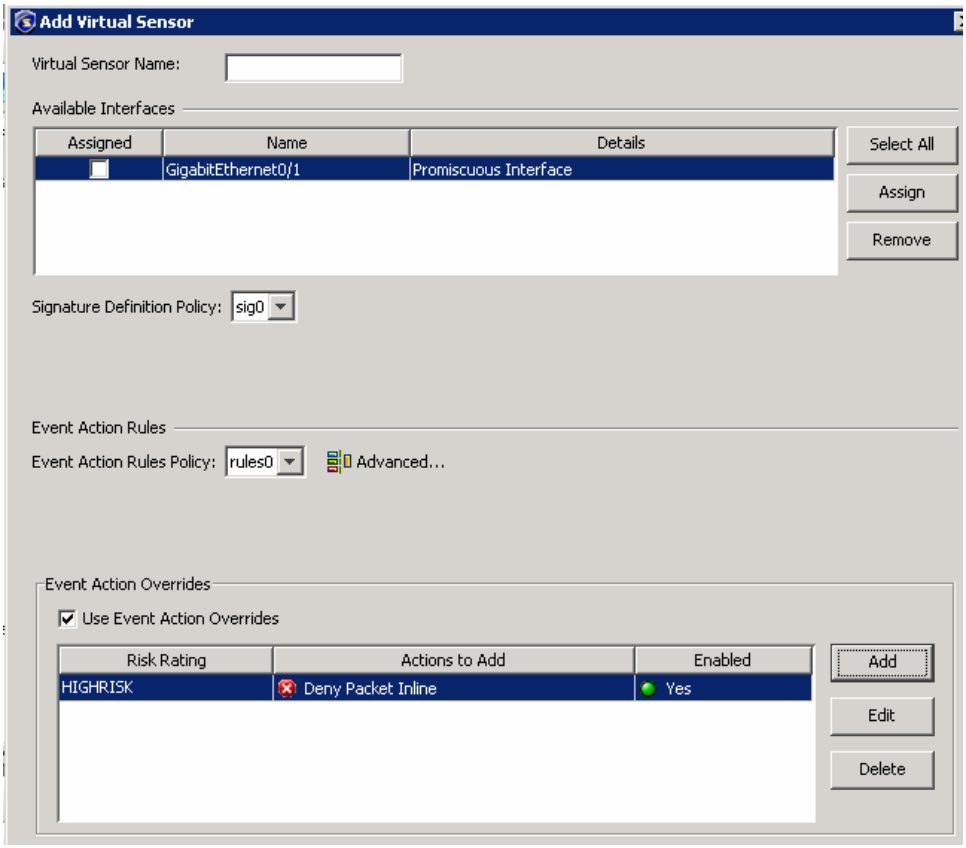
should have been HTTP TCP/80, but it was port 39630. There are a few steps you want to take because this may have been a successful attack.

Fix the attack source: If the attack originated from a device on your network, remove malware or reinstall the source OS, and install current security patches and applications. You may also want to take a look at the person who owns the machine. Keep in mind that another attacker may have exploited that machine; in other words, the machine owner may also be a victim.

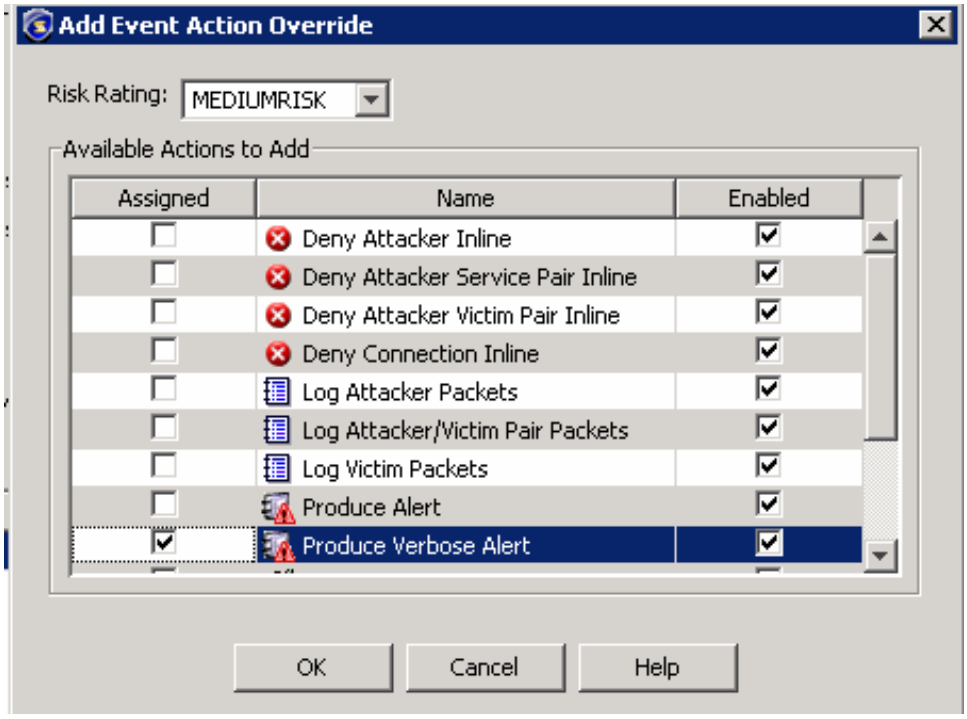
Fix the destination host: Use a vulnerability scanner and see if the destination host was vulnerable to the attack that was reported. If not, there is a good chance the machine has not been compromised. If the vulnerability does exist, take the same steps to restore the system: remove malware or reinstall the source OS, and install current security patches and applications.

Modify IPS policy to provide more information: It can sometimes be difficult to determine if an attack occurred. A best practice is to use verbose logging, which will capture the entire packet that triggers an alert. When an alert is triggered, you can view data in the packet; this provides you with more precise information to determine if an attack is successful.

- To globally enable verbose alert reporting and critical signatures, browse to Configuration > Policies > IPS Policies. Click “Edit” on the desired virtual sensor. See the following panel.



2. Click “Add” to define a new global action. For medium-risk attacks, create an action that will product verbose output for alerts that have a risk rating between 70 and 89. See the following panel for a configuration example.



Summary

Not all IPS alerts are actionable. Using Cisco IPS Manager Express, you can easily filter out benign alerts and focus on the alerts that could be attacks on your network. If you find an attack that wasn't dropped, you can use a single click to examine the intelligence about the alert, which will help you to decide if you need to take action on the victim or source host. You can also modify IPS policy to give you more information about alerts; this will give you more data to help your forensics investigation.

If you need assistance with tuning or forensics research, Cisco offers two options for customers: Cisco Professional Services and Cisco Remote Operation Services (http://www.cisco.com/go/ros).

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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 C17-464691-00 04/08