Snort: The World’s Most Widely Deployed IPS Technology

Overview

Martin Roesch, the founder of Sourcefire and chief security architect at Cisco, created Snort® in 1998. Snort is an open-source, rule-based, intrusion detection and prevention system. It combines the benefits of signature-, protocol-, and anomaly-based inspection methods to deliver flexible protection from malware attacks. Snort gained notoriety for being able to accurately detect threats at high speeds. With nearly 4 million downloads and hundreds of thousands of registered users, Snort is the most widely deployed IPS technology in the world.

Business Benefits

Snort’s open-source development methodology offers three main benefits:

- **Rapid response:** Protect your environment from emerging attacks quickly using Snort to customize and enforce your own security rules. Protect from threats you haven’t even seen through the Cisco® Talos Security Intelligence and Research Group (Talos). Talos writes Snort rules every hour of the day to combat new and evolving threats.

- **Greater accuracy:** Strengthen your security without doing a thing. The worldwide Snort community continually reviews, tests, and offers improvements to the Snort source code. Benefit from the collective knowledge of security teams around the world as they suggest changes.

- **High adaptability:** Employ the Snort system as a foundation for creating your own unique network security solutions. With ready access to source code and documentation, you can add your own functions to Snort.

Challenge

Even with these benefits, Snort can present limitations.

Snort was originally a fairly static system. Today’s networks are very dynamic, and keeping systems up to date can be challenging. Snort wasn’t programmed to create or use contextual awareness, which is key for next-generation security. Contextual awareness is built by compiling data about the composition and behavior of networks, applications, and users. The lack of contextual awareness makes reliable automation and rapid threat assessment more challenging. Without automation, you have to manually sort through alerts just to determine which are relevant before you can identify the ones that pose a legitimate risk.

These issues can prove challenging as you try to optimize security and reduce administrative overhead without discarding your Snort deployment and the many benefits it offers. Extend your Snort investment through a partnership with Cisco through one of three paths. These involve the Cisco Intrusion Agent, Cisco Intrusion Prevention System (IPS) solutions, and our next-generation intrusion prevention system (NGIPS). Table 1 shows the features that each of these paths offers.
Solution

Table 1. Snort and Three Paths to Enhanced Security and Lower Costs

<table>
<thead>
<tr>
<th>Features</th>
<th>Snort</th>
<th>Intrusion Agent</th>
<th>IPSx</th>
<th>IPS</th>
<th>NGIPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS detection and blocking</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Centralized event data</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Report, alerts, and dashboard</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Third-party integration</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco supported</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Pre-packaged hardware</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Policy management</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Up to 20 Gbps IPS inspection</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Interface modularity, expandability, and scalability options</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Automated impact assessment</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Automated tuning</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Host profiles and network map</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Network behavior analysis</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Application monitoring</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>User identity tracking</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Path 1: Cisco Intrusion Agent plus Cisco FireSIGHT Management Center

Reduce administrative overhead and manage your costs by adding centralized management.

What's Needed

Implement this option by adding just two Cisco FireSIGHT™ system components:

- **Cisco FireSIGHT Management Center**: Easily aggregate and monitor security events, generate reports, and configure alerts with the nerve center of the Cisco FireSIGHT system.

- **Cisco Intrusion Agent**: Collect security events from Snort sensors and use the Cisco FireSIGHT Management Center to combine them with your data from Cisco IPS sensors.

Benefits

This option delivers seven tangible benefits to enhance security and reduce the total cost of ownership.

- **Central event data**: Simplify all your future event-processing activities. The Cisco FireSIGHT Management Center (Management Center) compiles events from each Snort sensor rather than writing them to individual databases.

- **Real-time alerts**: Automate warnings by syslog, email, or the Simple Network Management Protocol (SNMP) through the Management Center. You no longer have to manually interrogate the Snort event database to discover what is happening in your network.

- **Powerful data analysis**: Access preconfigured and customizable workflows that make it easy to view and process large numbers of events. Quickly summarize security events through the Management Center and group them at a high level. Easily pivot the information in those groups to see the details of the events. The Management Center helps to identify long-term trends in your network to simplify your investigation process.
● **Real-time attack response**: Create event-focused rules and actions through the Management Center’s policy and response engine. Use these rules to block suspicious traffic and trigger inspections and remediation for a targeted system in your environment.

● **Comprehensive reporting**: Generate preconfigured and customized reports to support a full range of operational objectives such as troubleshooting, attack trending, and presentations.

● **Third-party integration tools**: Inform and engage other components in your organization’s network and security infrastructure through APIs. Our APIs can employ security information and event management systems (SIEMs), patch or configuration management systems, vulnerability-assessment scanners, firewalls, and routers.

● **Cisco support**: Obtain support for the Management Center and the Cisco Intrusion Agent directly from Cisco Technical Support.

Path 2: Cisco IPS Solution

The Cisco IPS solution is ideal for larger organizations who want more robust protection features without awareness.

What’s Needed

Add the Cisco FireSIGHT system to an existing Snort deployment.

● **Cisco FireSIGHT system**: Deploy a cost-effective, highly functional network security solution. We offer the widest range of throughput in the industry, with sensors ranging from 5 Mbps to 20 Gbps of IPS-inspected throughput. Deploy our sensors in inline or passive mode. We designed our system to adapt to your needs.

● **Cisco FireSIGHT Management Center**: Configure up to 150 individual sensors with the top-of-the-line Management Center. As part of our IPS solution, the Management Center supports event categorization, reporting, automated Snort rule updates, policy configuration, and customizable dashboards to quickly communicate sensor feedback.

Additional Benefits

● **Restoration and backup of configuration data**: Back up and restore sensor settings through the Management Center’s centralized backup mechanism. To achieve a similar capability using Snort without this mechanism, you would have to manually store the configuration file for each sensor.

● **“Zero-touch” upgrades for sensors**: Effortlessly schedule and implement updates through the Management Center. Our system automatically downloads and installs the required updates at an appropriate time. Updating Snort without the Management Center is a much more involved process, generally requiring a complete new installation that forces you to manually regenerate configuration files and rebuild all of the sensors each time an update is required.

● **Robust dashboards**: Easily monitor and manage security events on your network through your Management Center dashboard. Use a customizable library of interactive widgets to build them out. Widgets can be dragged from one column to another, saved, and shared throughout your organization.

● **Up to 20 Gbps of IPS inspection**: Get the fastest speeds in the industry with the new Cisco FirePOWER™ 8000 Series Appliances. Deploy Cisco FirePOWER acceleration technology to get up to 20 Gbps of IPS inspection.
- **Interface modularity, expandability, and scalability options:** Lower your total cost of ownership while deploying the number of ports and media types you need for your network. The Cisco FirePOWER 8000 Series Appliances are expandable to meet your needs as you grow. Swap out interface types and add future appliances to increase your processing power.

**Path 3: Cisco NGIPS Solution**
Upgrading from IPS to next-generation IPS (NGIPS) adds contextual awareness through Cisco FireSIGHT technology. Such awareness is crucial for reliable, automated responses to network security events.

**What’s Needed**
- **Cisco FireSIGHT sensors:** Take advantage of a wealth of network information gathered by our NGIPS. We give you information on the systems and applications deployed, the types of devices in use (including mobile systems), identification information for individual network users, and network behavior analysis based on traffic activity.
- **Cisco FireSIGHT awareness technologies:** Access unequaled contextual data from the real-time network- and user-awareness components of Cisco FireSIGHT. Network awareness provides continuous passive network monitoring. You get a real-time inventory of operating systems, services, applications, protocols, and potential vulnerabilities on the network. User awareness detects Active Directory and Lightweight Directory Access Protocol (LDAP) logins and pairs usernames with corresponding IP addresses. These technologies deliver the detailed information needed for contextual awareness.

**Additional Benefits**
- **Automated security impact assessment:** Avoid false positives and use your time better. We correlate security events against the profiles of targeted systems to prioritize events with impact flags.
- **Automated IPS tuning:** Automate and improve your IPS tuning and protection. We recommend only the Snort rules that pertain to a network’s operating systems and services.
- **Host profiles and network map:** Improve the method you use to evaluate and respond to security events. As the sensors gather network data, they display it in the form of information-rich network maps and host profiles. These help you see the problem areas right away.
- **Network behavior analysis:** Detect unauthorized hosts and communications taking place on your network. Network flow analysis is at the heart of what is commonly referred to as network behavior anomaly detection (NBAD). Our network behavior analysis delivers much more value. Our solution facilitates both security and network operations by supplying invaluable contextual information pertaining to network composition, specific events, and overall usage patterns.
- **Monitored applications:** Enforce compliance and policy initiatives across your organization. We lead the market in identifying the use of applications and in detecting operating systems, virtual machines, consumer devices like smartphones and tablet computers, VoIP systems, network devices, printers, and more. Prevent users from creating vulnerabilities in your network.
- **Tracked user identities:** Investigate incidents and threat warnings in just seconds. To quickly respond to threats, you need the identity of the individuals involved. Most network security systems provide only a network address or system name. Using our system, administrators get individual identities and contact information in automated alerts.
Other Extension Options

Virtual Networks
We are the only vendor to provide a complete virtual network security system. The solution comes with fully functional virtual sensors and Management Centers. For further flexibility, you can mix and match our virtual security offerings with physical products.

- **Cisco FireSIGHT Virtual Management Center**: Extend your investment in virtualization technology with a full-featured VMware- or Xen-based virtual implementation of our Management Center. This solution supports the operation of multiple Management Centers on a single physical host (particularly useful for managed security service providers).

- **Cisco NGIPSv sensor**: Get advanced protection in virtual environments and extend the deployment of Cisco FireSIGHT sensors across the entire network without increasing your costs. Get our complete VMware- or Xen-based virtual appliance implementation of a Cisco FireSIGHT sensor.

SSL Decryption
Encrypted network traffic is a fast-growing component of some networks. Ironically, encrypted traffic is a blind spot for traditional network security systems and provides attackers with a way to hide their activity. Decrypt Secure Sockets Layer (SSL) traffic for thorough inspection using our SSL Appliances. An SSL Appliance operates on the network and supports both passive and inline network configurations. Reduce deployments with our plug-and-protect approach and close the security loophole that SSL creates.

Summary
The options discussed in this technology brief deliver significant benefits while preserving an organization’s investments in Snort. They provide:

- **Optimized operational efficiency**: Experience a more focused workload thanks to the automation build into our solution. Take advantage of enhanced management capabilities, shared intelligence, and smooth integration with other components.

- **Enhanced security effectiveness**: Get better control and faster response times. Enjoy additional threat protection technologies and greater management capabilities.

- **Improved compliance status and readiness**: Show auditors a comprehensive approach to threat management with our fine-grained policy enforcement and compliance reporting capabilities.

- **Reduced or equivalent costs**: Get a faster return on investment (ROI) through significant time savings than you’ll get managing an open-source Snort environment.

- **Maintained Snort investment**: Import your existing Snort rules into the new system. After they’re imported, you maintain the ability to view, edit, and create new rules while gaining the distinct advantages of our appliances. Continue using your Snort expertise with Cisco’s innovative commercial offerings.
For More Information

To learn more, visit us at www.cisco.com or contact Cisco or a member of the Cisco channel partner team today.