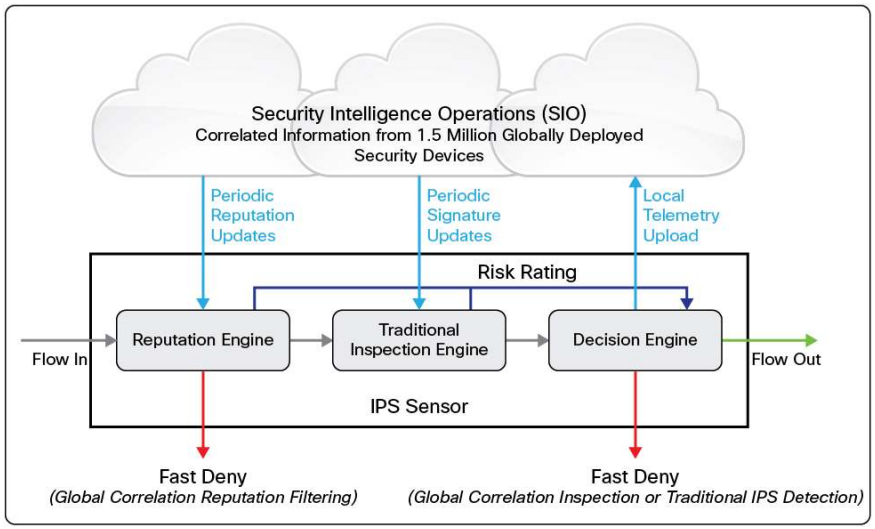
Global Correlation on Cisco IPS Sensors

Intrusion prevention systems (IPSs) use protocol-based decoding engines and regular-expression-based signatures to detect and stop incoming threats. These traditional techniques are the “workhorses” of the IPS sensor, but there are several deployment situations in which the techniques can be augmented to improve a sensor’s ability to detect threats. Cisco Remote Management Services’ experience has shown that network reputation can be combined with traditional IPS techniques to stop incoming threats effectively.

Cisco® IPS sensors are context-aware. They take into account the network reputation of the source of an incoming flow, the value to the organization of the target, the operating system of the target, and the user identity associated with the flow. The network reputation component of the context comes from Cisco Security Intelligence Operations (SIO), a cloud-based service that collects real-time flow telemetry from more than 1.5 million Cisco IPS sensors, firewalls, email gateways, and secure web gateways that are deployed worldwide. Cisco SIO produces reputation scores for various traffic sources (networks) and then downloads the scores to Cisco IPS sensors that have been configured to receive them. These scores form the basis of the Cisco IPS Global Correlation feature.

The Global Correlation feature uses network reputation scores in two different but complementary ways. First, the reputation of the source of a new flow is tested and the flow is denied without further processing if the reputation is bad. Second, the flow is passed through traditional IPS inspection engines. These engines determine the threat potential of the flow based on the sensor’s policy configuration, and assign a risk rating to the flow. The risk rating is then modified to take into account the reputation of the flow’s source. If the resultant risk rating is above a threshold, the flow is denied (or an alternate action is taken, depending on the policy configuration). This process is depicted in Figure 1.

Figure 1. Global Correlation on Cisco IPS



Thus, bad traffic denied by a Cisco IPS sensor falls into three categories:

- **Global Correlation Reputation Filtering:** Based on reputation alone. Flow is not passed to the traditional inspection engines.
- **Global Correlation Inspection:** Based on a combination of traditional inspection and network reputation information. The risk rating mechanism combines the two threat signals.
- **Traditional IPS Detection:** Based on traditional inspection techniques, including protocol decoding engines, signature based inspection, and anomaly detection via statistical analysis of network traffic. In this case, network reputation information for the traffic flow is not available or does not have an effect on the flow.

Customers deploying Cisco IPS can benefit from Global Correlation in multiple ways. First, bad traffic from known sources is stopped immediately. This includes zero-day attacks, for which no traditional threat prevention currently exists, advanced persistent threats (APTs), and botnet command and control traffic. Second, multiple signals are used to detect and stop incoming threats, enabling Cisco IPS sensors to stop a greater number of threats than would have been possible with traditional IPS mechanisms alone. Finally, a Cisco IPS sensor is able to inspect more traffic as traffic denied by Global Correlation Reputation Filtering is prevented from passing through the computationally intensive traditional IPS inspection process.

Global Correlation put to work by Cisco RMS

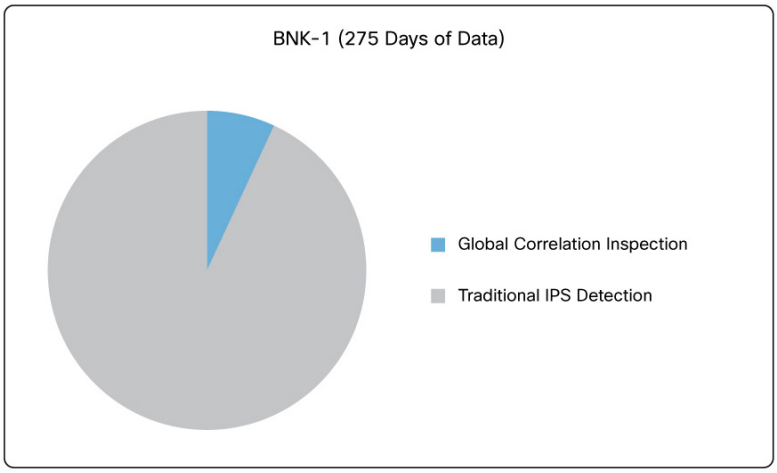
Cisco Remote Management Services (RMS) is a Cisco business unit that provides managed services. The security portion of these services includes monitoring and management of Cisco IPS sensors. Cisco RMS has more than a decade of experience deploying Cisco IPS across multiple industry segments, as well as first-hand experience with deploying the Global Correlation feature. We'll use this data and experience to demonstrate the effectiveness of Global Correlation.

As we will see, Global Correlation significantly augments traditional IPS techniques in most situations. In cases where a firewall with tight access control fronts an IPS sensor, the portion of bad traffic caught on the sensor attributable to Global Correlation is relatively small. However, in cases where such access control is more relaxed, Global Correlation stops a higher portion of bad traffic on the sensor.

Tight access control in front of sensor

Figure 2 shows data from a sensor at a bank in North America. The bank has a defensive security posture that includes multiple layers of security. It has a tight access control policy on the firewall, blocking the majority of known bad traffic. Thus, Global Correlation Reputation Filtering on the IPS sensor (BNK-1) denies a negligible portion of the bad traffic coming to the sensor. Global Correlation Inspection has a noticeable impact: 7% of bad traffic denied. However, the bulk of bad traffic coming to the IPS sensor is denied using traditional IPS techniques, since the firewall has stopped much of that which could be caught by Global Correlation.

Figure 2. Sensor at Bank (BNK-1)



Even though the influence of Global Correlation on the percentage of bad traffic stopped is small, it is important for the customer to deploy Global Correlation. First, given the assets at stake in a financial institution, letting even a single attack (that could have been stopped by Global Correlation) through can result in irreparable harm. Second, having Global Correlation turned on ensures updates to reputation information on the sensor every few minutes. As SIO identifies new bad sources, the customer's assets are automatically protected against attacks originating from these sources.

Moderate access control in front of sensor

Figure 3 and Figure 4 show data from two sensors at an industrial supplies distributor in North America. In this case, Global Correlation results in 26% (IND-1) to 35% (IND-2) of bad traffic being denied. Firewall-based access policies at the distributor, while reasonably maintained, are not as tight as the bank discussed in the previous example. Hence, Global Correlation has a more pronounced effect for the distributor than for the bank.

Figure 3. Sensor at Industrial Supplies Distributor (IND-1)

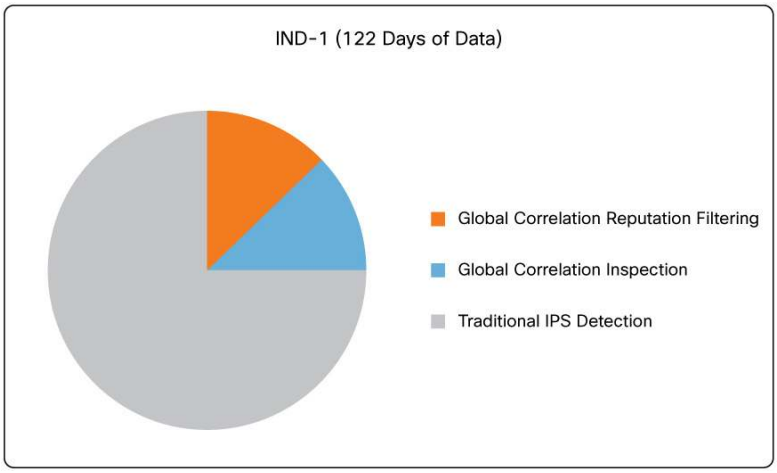
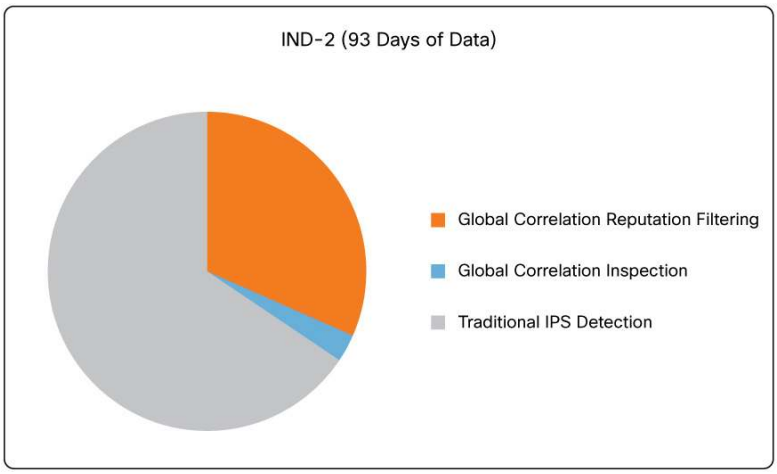


Figure 4. Sensor at Industrial Supplies Distributor (IND-2)



Permissive access control in front of sensor

Figure 5 and Figure 6 show data from two sensors at a professional services firm. One sensor (PRO-1) is in Europe and the other is in Asia (PRO-2). Both sensors have firewalls in front of them, but with relatively lax access controls. While PRO-1 has been undergoing a tightening of its access environment in recent weeks, PRO-2 has not yet benefitted from similar tightening. As a result of the lax access environment, Global Correlation plays a major role in denying bad traffic and the effect is more prominent in the case of PRO-2 (nearly 100% of bad traffic denied) than PRO-1 (43% of bad traffic denied). As it turns out for PRO-2, a significant portion of the malicious traffic originates at web-zero.net, a well-known bad traffic source.

Figure 5. Sensor at Professional Services Firm (PRO-1)

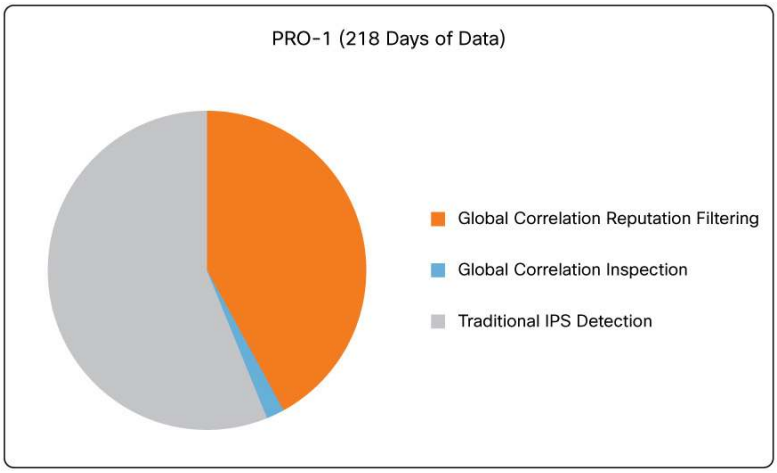


Figure 6. Sensor at Professional Services Firm (PRO-2)

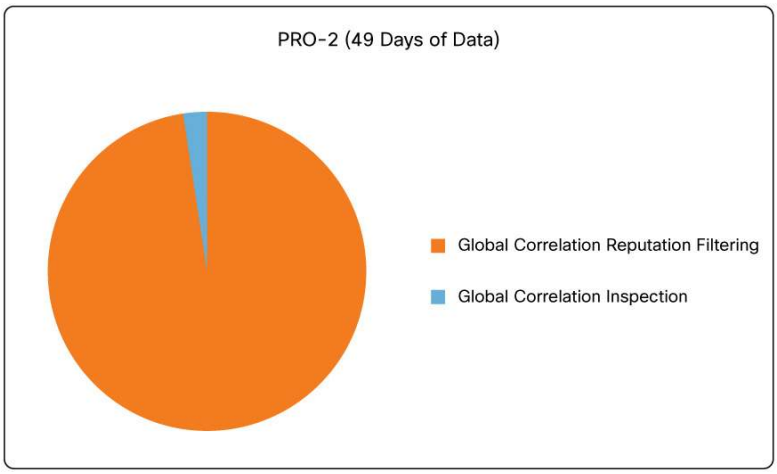
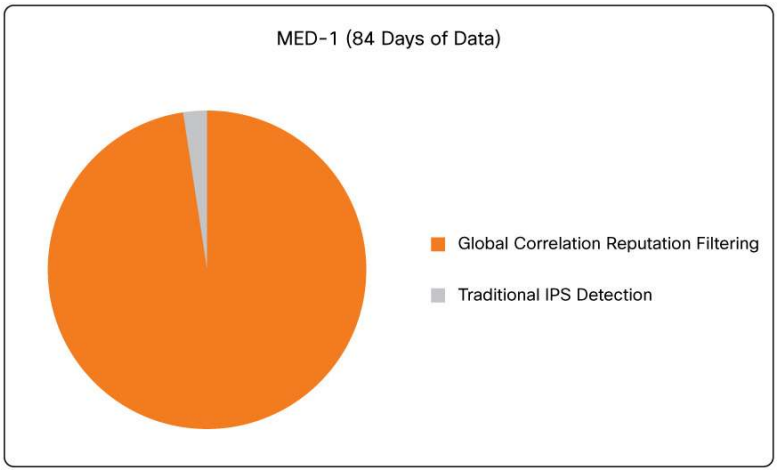


Figure 7 shows data from a medical school and hospital that, by policy, maintain a permissive access environment. The IPS sensor at this school (MED-1) sees a significant amount of peer-to-peer (P2P) and Internet Relay Chat (IRC) traffic, and some of this traffic contains embedded threats. In addition, the school has an inconsistently patched OS environment - a fact likely known to hackers. Since many of the networks originating bad traffic are known to Cisco SIO, the Reputation Filtering portion of Global Correlation on MED-1 denies the majority of bad traffic.

Figure 7. Sensor at Medical School and Hospital (MED-1)



Even though Global Correlation Inspection has a negligible impact on bad traffic on MED-1, the configuration related to the inspection should be left in place. The incoming traffic profile and the attacks they contain change from time to time. In addition, SIO updates the sensor with new signatures periodically. Over time, the balance of traffic blocked by Reputation Filtering versus Global Correlation Inspection versus Traditional IPS Detection may vary. However, once Global Correlation is properly configured on a sensor, a security administrator need not reconfigure this capability to accommodate a changing traffic profile or signature updates.

Summary

The results that an individual Cisco IPS customer sees on a particular sensor may differ from those analyzed here, depending on the access policy, geographical location, network topology (Internet edge versus network core), and configuration of the sensor. However, Global Correlation clearly offers significant additional protection in many situations. Cisco IPS customers who don't already have Global Correlation deployed on their sensors, should consider turning-on the feature or work with Cisco RMS to enable this capability.

About Cisco RMS

Cisco Remote Management Services (RMS) for Security provides 24/7/365 proactive threat monitoring and management services for advanced and emerging security technologies and network architectures. Utilizing a proven delivery methodology based on ITIL® while delivered within a co-managed framework, Cisco RMS for Security ensures operation excellence and complete customer control. Cisco RMS for Security provides a proactive, holistic approach to monitoring, managing and protecting critical network infrastructures ensuring business continuity. Built on an advanced, extensible Cisco Security Platform and embedded with real-time intelligence from Cisco Security Intelligence Operations, the Cisco RMS for Security architecture is a proven and unparalleled.

For more information on Cisco RMS, visit http://www.cisco.com/go/rms.

About Cisco IPS

Cisco IPS is the most widely deployed IPS solution in the market. Cisco's newly refreshed IPS portfolio includes the Cisco IPS 4500 Series, the Cisco IPS 4300 Series, and IPS modules integrated into Cisco ASA 5500-X Series Adaptive Security Appliances.

For more information on Cisco IPS and Global Correlation, visit http://www.cisco.com/go/ips.

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 C11-715386-00 08/12