

IP-to-ID Solution Brief



■ Problem Statement

As corporate networks have evolved, so have the threats. In recent years we have witnessed internally originated attacks as an increasing cause of network and PC issues resulting in productivity and opportunity costs.

Accuracy and a proactive approach to these issues have become essential to today's network and security professionals. Solutions need to be put in place to detect issues on the network, automatically mitigate the issues and provide root cause analysis of the issues. Complete root cause analysis is needed to ensure a correct view of the situation and ensure it does not reoccur.

Root cause analysis includes looking at the "what" and the "who" of the event. The "what" consists of information on the specific event and the scope. The "who" consists of the source, typically today, it is a machine IP address or machine host name. Often finding the username behind the action can take hours or days to find, if the logs are available. With hundreds to thousands of events this is typically not done.

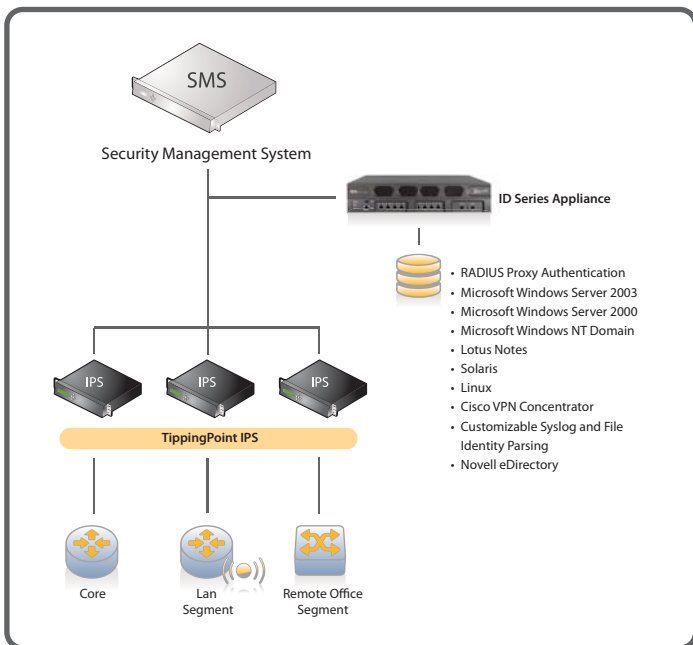
Traditional monitoring systems lack the ability to proactively correlate network activity with user identity and require the manual resolution of syslog events and alerts using multiple logs, often involving multiple departments and prolonging troubleshooting and forensic activities. With fast spreading worms, viruses, and zero-day attacks on the rise, isolating malicious traffic quickly and identifying the users responsible is critical to keeping the corporate network safe.

■ The Joint Solution

The TippingPoint® Intrusion Prevention System (IPS) delivers the most powerful network protection in the world. The TippingPoint IPS is an in-line device that is inserted seamlessly and transparently into the network. As packets pass through the IPS, they are fully inspected to determine whether they are legitimate or malicious. This instantaneous form of protection is the most effective means of preventing attacks from ever reaching their targets.

TippingPoint delivers best-of-breed management capabilities that are simple to use and extremely powerful. The TippingPoint Security Management System (SMS) is a hardened appliance that provides global vision and control for the TippingPoint IPS. The SMS is responsible for discovering, monitoring, configuring, diagnosing and reporting for multiple TippingPoint systems. The TippingPoint SMS is a rack mountable appliance that features a state-of-the-art secure Java client interface that enables "big picture" analysis with trending reports, correlation and real-time graphs on traffic statistics, filtered attacks, network hosts and services, as well as IPS inventory and health.

TippingPoint SMS customers can now leverage A10 Networks' ID Series of appliances with IP-to-ID technology which automates the process of identifying the activities of individual users, providing the ability to tie specific network events with actual user logins. This allows administrators to significantly improve audit controls and assure regulatory compliance by linking the event directly to an individual user. Quarantine and remediation efforts are streamlined by the immediate identification of the responsible party.



The SMS appliance has achieved the "IP-to-ID Enabled" designation* which means the IP-to-ID information is directly accessible from within the TippingPoint SMS management interface. Once installed a seamless connection, transparent to the network or security professional can be applied, allowing the XML API to query the A10 Networks ID Series on demand.

Administrators simply request the user name(s) and IP address associated with an event from the TippingPoint SMS management interface and the system returns the appropriate information in real time. Because multiple administrators can access this data simultaneously, the ID Series of appliances are an ideal tool for optimizing security and network operations across the enterprise.

Together, TippingPoint's SMS management console and A10's ID Series of appliances with IP-to-ID technology simplify critical network monitoring and identity correlation – streamlining the optimization of security and network operations into one process.

*Scheduled release for TippingPoint SMS 2.7.

■ About A10 Networks

A10 Networks was founded in Q4 2004 with a mission to provide innovative networking and security solutions. A10 Networks makes high-performance products that help organizations accelerate, optimize and secure their applications. A10 Networks is headquartered in Silicon Valley with offices in the United States, Japan, China, Korea and Taiwan. For more information, visit <http://www.a10networks.com>.

■ About TippingPoint

TippingPoint, a leader in intrusion prevention systems (IPS), provides the IPS-Secured Network, which delivers attack control, access control, and application control. Its foundation is the TippingPoint IPS, the most decorated in its industry with unparalleled performance and security, as evidenced by nearly 35 awards. For a full list, visit: http://www.tippingpoint.com/products_certifications.html. The IPS obtains evergreen protection from the Digital Vaccine® service, powered by DV Labs, the largest body of security researchers in the world. DV Labs is made up of expert internal researchers and over 600 Zero Day Initiative researchers. For more information on TippingPoint, please visit www.tippingpoint.com



■ The TippingPoint and A10 Networks Advantage

- Instant view of "What" is happening and "Who" is doing it
- Industry leading Intrusion Prevention System (IPS) and Response solution
- Integrated solution designed for fast and cost effective deployment
- Proactive network monitoring and analysis with real-time identity resolution
- Enhanced regulatory compliance and network visibility
- Popular data store support for maximum identity resolution