

## Profiler Overview

---

The Profiler is a network-analysis tool that helps you learn about your internal network so you can create effective security policies and minimize unnecessary log records. The Profiler queries and correlates information from multiple IDP appliances.

After you configure the Profiler, it automatically learns about your internal network and the elements that constitute it, including hosts, peers (which host is talking to which other host), ports (non-IP protocols, TCP/UDP ports, RPC programs), and Layer 7 data that uniquely identifies hosts, applications, commands, users, and filenames. You can use this data to investigate and analyze potential problems in the network and to resolve security incidents.

During profiling, the IDP appliance records network activity at Layer 3, Layer 4, and Layer 7 and stores this information in a searchable database called the Profiler DB. The Profiler uses session creation, session teardown, and protocol contexts to generate this database, which defines all unique activities occurring on your network. Unique activities include attempts, probes, and successful connections.

The device logs normal events only once, and it logs all unique events as often as they occur.

A *normal event* is an event that reoccurs frequently and does not change. For example, suppose Wendy holds a meeting every Tuesday at 4:00 PM in conference room A. Every meeting, she connects her laptop to the network and accesses documents on the primary fileserver. Because the same event occurs multiple times, the device logs the event once and includes a timestamp that indicates the first and last times Wendy accessed the network from conference room A.

A *unique event* is an event that is new, unexpected, or does not match the normal traffic patterns of your network. For example, suppose that in her weekly meeting, Wendy accesses documents from a different fileserver or has a colleague lead the meeting when she is on vacation. Because the network session information differs, the device logs these activities separately from the normal Tuesday afternoon meeting.

When you configure the Profiler, you can specify:

- General settings, such as whether to collect application volume data and whether to record the OS fingerprint of network hosts
- Network and host IP addresses to track in Profiler logs
- Network and host IP addresses to exclude in Profiler logs
- Contexts to retrieve additional data
- Alerts in cases where you want to track new hosts and applications

For complete procedures on setting Profiler options, see the *IDP Administration Guide*.

**Related Topics** The following related topics are included in the *IDP Concepts and Examples Guide*:

- Example: Using Profiler to Set a Baseline
- Example: Using Profiler to Alert You to New Hosts and Port Activity
- Example: Identifying Services That Use Nonstandard Ports
- Example: Responding to Vulnerability Announcements with Due Diligence
- Example: Using Profiler to Investigate Unanticipated Attacks
- Example: Using Profiler to Mitigate Risks from Laptops

The following related topic is included in the *IDP Administration Guide*:

- Profiler Task Summary

---

Published: 2010-01-12