

## Understanding the Traffic Anomalies Rulebase

The Traffic Anomalies rulebase employs a traffic flow analysis method to detect attacks that occur over multiple connections and sessions (such as scans).

A *traffic anomaly* is a pattern that indicates abnormal network activity. Traffic generated by automated port scanning tools trigger Traffic Anomalies rulebase rules. Attackers use automated port scanning tools to perform reconnaissance on your network. Typically, an automated port scanning tool attempts to connect to every port on a single machine (port scanning) or to connect to multiple IP addresses on a network (network scanning). Attackers do this to determine which services are allowed and responding on your network, so they can focus attacks on any vulnerabilities.

Traffic Anomalies rulebase rules count the number of ports scanned in a specified time period and use this traffic flow analysis to identify scans, as well as other attacks that occur over multiple connections and sessions. If the rule detects an attack, you can drop the connection and block the IP address that originated the attack. The IDP engine takes action against traffic that exceeds the thresholds you set.

Table 1 summarizes Traffic Anomalies rulebase detection settings. You can tune these parameters if safe traffic in your network triggers false positives.

**Table 1: Traffic Anomalies Rulebase Detection Settings**

Group	Description
TCP scans, UDP Port Scans	<p>Set a port count (number of ports scanned) and the time threshold (the time period that ports are counted) in seconds.</p> <p>The default port count is 20. The default time threshold is 120 seconds. The rule is matched if the same source scans 20 TCP ports on your internal network within 120 seconds or if the same source scans 20 UDP ports on your internal network within 120 seconds.</p>
Distributed Port Scan	<p>A distributed port scan is an attack that uses multiple source IP addresses to scan ports.</p> <p>Set a port count (number of ports scanned) and the time threshold (the time period that ports are counted) in seconds.</p> <p>The default IP count is 50. The default time threshold is 120 seconds. The rule is matched if 50 IP addresses attempt to scan ports on your internal network within 120 seconds.</p>
ICMP Sweep	<p>An ICMP sweep is an attack where a single source IP pings multiple IP addresses.</p> <p>Set a port count (number of ports scanned) and the time threshold (the time period that ports are counted) in seconds.</p> <p>The default IP count is 50. The default time threshold is 120 seconds. The rule is matched if the same source IP attempts to ping 50 IP addresses within 120 seconds.</p>

**Table 1: Traffic Anomalies Rulebase Detection Settings** (continued)

Group	Description
Network Scan	<p>A network scan is an attack where a single source IP scans multiple IP addresses.</p> <p>Set a port count (number of ports scanned) and the time threshold (the time period that ports are counted) in seconds.</p> <p>The default IP count is 50. The default time threshold is 120 seconds. The rule is matched if the same source IP attempts to scan 50 IP addresses within 120 seconds.</p>
Session Limit	<p>Set a threshold number of sessions allowed from a single host within a second. The default is 100 sessions.</p> <p>For example, assume your internal network typically has low volume traffic. To detect a sudden increase in traffic from a specific host (which might indicate a worm), configure a rule that matches traffic over your internal network and configure a limit of 200. To block traffic that exceeds the session limit, set an IP action of <b>IDP Block</b> and select <b>Source, Protocol</b> from the Blocking Options menu.</p>

In addition, you can tune runtime parameters for Traffic Signatures. Table 2 describes the runtime parameters associated with the Traffic Anomalies rulebase.

**Table 2: Traffic Signature Runtime Settings**

Setting	Description
Byte threshold for suspicious flows	Scans typically use small packets to access targets. You can exclude flows that contain large packets to reduce false positives. The default is to exclude flows where packet size exceeds 20 bytes.
Reporting frequency while scan in progress (seconds)	Specifies how frequently log messages are generated. Default is 30 seconds.
The number of IP addresses we track for session rate	Specifies the maximum number of source IP addresses for which session rate is calculated. Default is 32,767.

When you create rules for the Traffic Anomalies rulebase, you specify:

- A source/destination/service match condition
- Detection settings
- Response options
- Notification options

For complete procedures on configuring Traffic Anomalies rulebase rules, see the *IDP Administration Guide*.

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

- Understanding Traffic Anomalies Rulebase Match Conditions
- Understanding Traffic Anomalies Rulebase Detection Settings
- Understanding Traffic Anomalies Rulebase IP Actions
- Understanding Traffic Anomalies Rulebase Notification Options
- Understanding the Components of an IDP Security Policy

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

- Configuring Traffic Anomalies Rulebase Rules (NSM Procedure)

---

Published: 2010-01-12