

Attack Prevention Capabilities

Juniper Networks IDP delivers true attack prevention by dropping malicious traffic and connections during an attack thereby preventing attacks from ever reaching the target system. As a result, administrators may never need to investigate whether the attack successfully compromised the host or spend the money to recover from an attack again.

Juniper Networks IDP offers true protection as an in-line device

The Juniper Networks IDP can be deployed in-line as an active device that monitors all traffic and determines what constitutes an intrusion. If an intrusion or attack is found, IDP has a variety of response mechanisms that provide the ability to generate an alarm or drop the malicious traffic and the connection. The only way to drop malicious traffic to minimize the impact associated with an attack and eliminate the costs associated with security breaches is to operate as an in-line device

Passive responses do not protect the network

Some solutions claim prevention by using passive devices that send signal to other devices, such as a TCP Reset or Signal to the Firewall, to try to stop an attack. Passive responses are unable to prevent damages from occurring because they come after the attack reaches its victim. Unless the attack can be dropped during the detection process the attack will be investigated and any damages addressed.

TCP Reset

A TCP reset is a command sent to the client and/or the server associated with the attack, asking them to stop the connection. The latency involved in sending the reset **after the attack is detected allows the attack to reach the victim**. Besides the fact that the attack has already reached the victim, there is only a 10% range where the reset command works.

The TCP reset command only works if the IDS can pinpoint the sequence number of the attack at the time it reaches its victim. When an attack is detected, only the current sequence number (start of the 32,000 byte window) of the attack is known. For a reset to work, the IDS needs to send the victim the correct sequence number of when it will reach the victim. It must pick the sequence number from a changing 32,000-byte window, within a 4,000,000,000-byte range for any particular TCP session. The rate in which the window changes is controlled by the client (attacker) and affects the ability of another device to reset the connection. Basically, if the attacker doesn't want the reset to work, it will send a lot of traffic very fast. Even if mechanisms were in place to track how fast the connection is going, an attacker can vary the attack transmission speed to foil this type of response mechanism.

Firewall Signaling

Firewall signaling sends a signal to an access control device (like a firewall or router) to limit all future communications from the IP address of the attacker. This response introduces the latency involved in sending a "block all future traffic from this IP address" message from the detection device to the access control device. In addition, it occurs **after the attack is detected, allowing the attack to reach the victim**. This response is only designed to try to block future attacks. Besides the fact that the attack has already reached the victim, the blocking of future connections based on the source IP of an attack could form the basis of a crippling Denial-of-Service attack, which is a costly consequence that could be worse than the initial attack. All an attacker needs to do is use or spoof the IP address of a business partner, customer or service provider (such as AOL) during the attack, then when that IP address is blocked, legitimate traffic is stopped from accessing the network, creating a denial-of-service situation.

Juniper Networks IDP response mechanisms

To ensure enterprises have ultimate control and flexibility over the behavior of the system, IDP is built with a variety of response mechanisms. With multiple response mechanisms, an administrator has the ability to determine when to generate alarms, send e-mail alarms, generate an SNMP trap and - most importantly - drop the malicious traffic and the connection. The table below summarizes the response mechanisms supported by IDP.

Action	Description
Drop Connection	Drop the connection before the attack can cause harm to the network or system.
Close Connection	Close the connection by sending a message to both the client and server.
Session Packet Logging	Capture the packet that triggered the 'alarm.' A windowing option allows pre- and post- trigger packets to also be logged as part of the connection
Session Summary	Capture the session start, stop and overall statistics.
E-mail	Send an e-mail message to one or more recipient. Attachment options are available
Custom	Take a custom action, such as SNMP trap generation, defined by the administrator.
Logging	Log the connection for future forensic investigation.

Copyright © 2005 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, the NetScreen logo, NetScreen-Global Pro, ScreenOS, and GigaScreen are registered trademarks of Juniper Networks, Inc. in the United States and other countries.

The following are trademarks of Juniper Networks, Inc.: ERX, ESP, E-series, Instant Virtual Extranet, Internet Processor, J2300, J4300, J6300, J-Protect, J-series, J-Web, JUNOS, JUNOScope, JUNOScript, JUNOSe, M5, M7i, M10, M10i, M20, M40, M40e, M160, M320, M-series, MMD, NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-SA 1000 Series, NetScreen-SA 3000 Series, NetScreen-SA 5000 Series, NetScreen-SA Central Manager, NetScreen Secure Access, NetScreen-SM 3000, NetScreen-Security Manager, NMC-RX, SDX, Stateful Signature, T320, T640, and T-series. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. All specifications are subject to change without notice.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.