

IDP Series Features Overview

Table 1 briefly describes features of the standalone Juniper Networks IDP Series Intrusion Detection and Prevention Appliances.

Table 1: IDP Features

| Feature | Description | Documentation |
|---|--|---|
| Attack Detection and Prevention | | |
| Application identification | The application identification feature is used in the IDP rulebase and APE rulebase. The application identification feature parses protocol, context, and signature data to identify applications on any port. | ■ Using Application Identification |
| Application policy enforcement | The application policy enforcement (APE) rulebase enables you to set limits on available bandwidth for applications and/or user roles you specify. | ■ Understanding the APE Rulebase |
| Application volume tracking | The application volume tracking (AVT) feature leverages Profiler functionality to collect statistics about application usage over the network. | ■ Application Volume Tracking Overview |
| User role-based policies | When integrated with Juniper Networks IC Series Unified Access Control (UAC) appliance, the IDP Series appliance supports security policy rules based on UAC user roles. This feature enables you to more easily configure focused rules to implement your business security policy. | ■ User-Role-Based Policy Feature Overview |
| Multimethod attack detection | The IDP Series uses eight methods to detect malicious traffic. | See Table 2 for a description of detection methods. |
| Protocol decoding | Juniper Networks Security Center (J-Security Center) provides a robust protocol detection engine that can decode more than 60 protocols and analyze and enforce proper usage in more than 500 contexts. | ■ J-Security Center Updates Overview |
| Zero-day protection | J-Security Center attack updates provide same-day coverage for newly found vulnerabilities. The J-Security Center attack database includes more than 5500 signatures for identifying anomalies, attacks, spyware, and applications. | ■ J-Security Center Updates Overview |
| Recommended security policy and predefined attack objects | J-Security Center provides a robust default security policy (called Recommended) and a comprehensive set of predefined attack objects (including those flagged as Recommended for various categories of attacks). | ■ Using the Recommended Security Policy ■ Using Attack Objects |

Table 1: IDP Features (continued)

| Feature | Description | Documentation |
|---|---|---|
| User-defined security policies and attack objects | <p>If you choose, you can use the default security policy or other predefined templates as a basis for your own user-defined security policy.</p> <p>Similarly, you can use the predefined attack objects as a basis for your own user-defined attack objects.</p> | <ul style="list-style-type: none"> ■ Understanding the Components of an IDP Security Policy ■ Using Attack Objects |
| Active response methods | <p>J-Security Center attack objects are coded with recommended actions to take on the instant session, including drop packet, drop connection, close client, close server, and close client/server. You can rely on these or set your own.</p> <p>In addition, when the IDP appliance detects an attack from a particular IP address, it can block connections from the IP address for a configurable duration of time.</p> | <ul style="list-style-type: none"> ■ Understanding IDP Rulebase Actions |
| Passive response methods | The IDP Series supports several passive responses, including logging and TCP reset. | <ul style="list-style-type: none"> ■ Understanding IDP Rulebase Notification Options |
| Traffic decryption and decapsulation | The IDP Series can decapsulate or decrypt and inspect the payload of SSL, GRE, GTP, IPsec ESP NULL, and MPLS traffic. | <ul style="list-style-type: none"> ■ Inspection of SSL Traffic Overview ■ Inspection of GRE Traffic Overview ■ Inspection of GTP Traffic Overview ■ Inspection of IPsec VPN Traffic Overview ■ Inspection of MPLS Traffic Overview |
| Network profiling | The Profiler captures accurate and granular detail of your network traffic over time. | <ul style="list-style-type: none"> ■ Profiler Overview |
| Robust logging, reporting, and notification | The IDP Series includes useful predefined log views and reports and enables you to create custom views and reports. | <ul style="list-style-type: none"> ■ IDP Logs Overview ■ NSM Reports Overview ■ IDP Reporter Overview |
| Centralized management | The IDP Series is compatible with Juniper Networks Network and Security Manager (NSM). | <ul style="list-style-type: none"> ■ Centralized Management with NSM Overview |
| Coordinated threat control | The IDP Series is compatible with Juniper Networks SA Series SSL VPN appliances and IC Series devices. | <ul style="list-style-type: none"> ■ Coordinated Threat Control Overview |
| Bypass | <p>You can configure network interfaces to enter a bypass state in case of failure or graceful shutdown, or if the JNET driver encounters problems processing packets.</p> <p>The IDP Series also supports flow bypass to forward traffic when traffic exceeds IDP session capacity.</p> | <ul style="list-style-type: none"> ■ IDP Series Network Interfaces Overview ■ IDP Series Network Interfaces Overview ■ IDP Series Operating System Overview |
| Auto-recovery | If an IDP process engine experiences failure, the IDP appliance buffers the next packets in the flow and restarts the process engine. | <ul style="list-style-type: none"> ■ IDP Series Operating System Overview |

Table 2 briefly describes IDP detection methods and provides a reference to detailed information.

Table 2: Intrusion Detection Methods

| Feature | Description | Documentation |
|-------------------------|---|--|
| Stateful signature | The IDP rulebase attack object signatures are bound to protocol context. As a result, this detection method produces few false positives. | <ul style="list-style-type: none"> ■ Understanding the IDP Rulebase ■ Using Attack Objects |
| Protocol anomaly | The IDP rulebase attack objects detect protocol usages that violate published RFCs. This method protects your network from undiscovered vulnerabilities. | <ul style="list-style-type: none"> ■ Understanding the IDP Rulebase ■ Using Attack Objects |
| Traffic anomaly | The Traffic Anomalies rulebase uses heuristic rules to detect unexpected traffic patterns that might indicate reconnaissance or attacks. This method blocks distributed denial-of-service (DDoS) attacks and prevents reconnaissance activities. | <ul style="list-style-type: none"> ■ Understanding the Traffic Anomalies Rulebase |
| Backdoor | The Backdoor rulebase uses heuristic-based anomalous traffic patterns and packet analysis to detect Trojans and rootkits. These methods prevent proliferation of malware in case other security measures have been compromised. | <ul style="list-style-type: none"> ■ Understanding the Backdoor Rulebase |
| IP spoofing | The IDP appliance checks the validity of allowed addresses inside and outside the network, permitting only authentic traffic and blocking traffic with a disguised source. | <ul style="list-style-type: none"> ■ IP Spoof Attack Prevention Overview |
| Layer 2 attacks | The IDP appliance prevents Layer 2 attacks using rules for Address Resolution Protocol (ARP) tables, fragment handling, connection timeouts, and byte/length thresholds for packets. These methods prevent a compromised host from polluting an internal network using methods such as ARP cache poisoning. | <ul style="list-style-type: none"> ■ Layer 2 Attack Prevention Overview |
| Denial of service (DoS) | The SYN Protector rulebase provides two, alternative methods to prevent SYN-flood attacks. | <ul style="list-style-type: none"> ■ Understanding the SYN Protector Rulebase |
| Network honeypot | The IDP appliance impersonates vulnerable ports so you can track attacker reconnaissance activity. | <ul style="list-style-type: none"> ■ Understanding the Network Honeypot Rulebase |

Related Topics The following additional related topic is included in the *IDP Concepts and Examples Guide*:

- Juniper Networks IDP Solutions