

Accurate Attack Protection

Today's complex attacks manifest themselves differently in different customer environments. Juniper Networks IDP's advanced attack protection and customization helps accurately detect attacks and drop them from the network to prevent any damage. Juniper Networks IDP's advanced attack protection combines the following features:

- Multiple detection methods that include compound signatures, Stateful signatures, protocol anomaly and backdoor detection.
- An open signature format that allows administrators to view how the attack string matches the attack signature and edit the signature as needed. This level of understanding and customization allows administrators to tailor the attack signature to address unique attack requirements.
- Extensive signature customization improves the ability to detect unique attacks by providing an additional level of control needed to tailor the signature specific requirements.
 - Compound signatures: Improves speed of detection by proving the ability to combine Stateful signatures and protocol anomalies into a single attack object to detect complex attacks within a single session.
 - Over 400 customization parameters and Perl style regular expressions: Provides the ability to tailor signatures or create completely custom signatures

Multi-Method Attack Detection

Juniper Networks' Multi-Method Detection (MMD™) combines multiple detection mechanisms in a single product for comprehensive coverage. Because different types of attacks require different methods to identify them, products using only a few detection methods are incapable of detecting all attacks. Juniper Networks IDP's Multi-Method Detection maximizes the types of attacks detected, ensuring critical threats do not go undetected. The detection methods in MMD include:

Mechanism	Description
Stateful Signatures	Detect known attack patterns only in relevant traffic.
Protocol Anomaly	Detect unknown or permutated attacks.
Backdoor Detection	Detect unauthorized interactive backdoor traffic.
Traffic Anomaly	Detect attacks spanning multiple sessions and connections.
Network Honeypot	Detect attackers that are impersonating network resources and tracking attacks against them.
Layer-2 Detection	Detect layer-2 (ARP) attacks.
DOS Detection	Detect certain Denial of Service attacks.
Spoofing Detection	Detect IP spoofing attacks.
Compound Signatures	Combines stateful signatures and protocol anomalies to detect complex attacks in a single session.

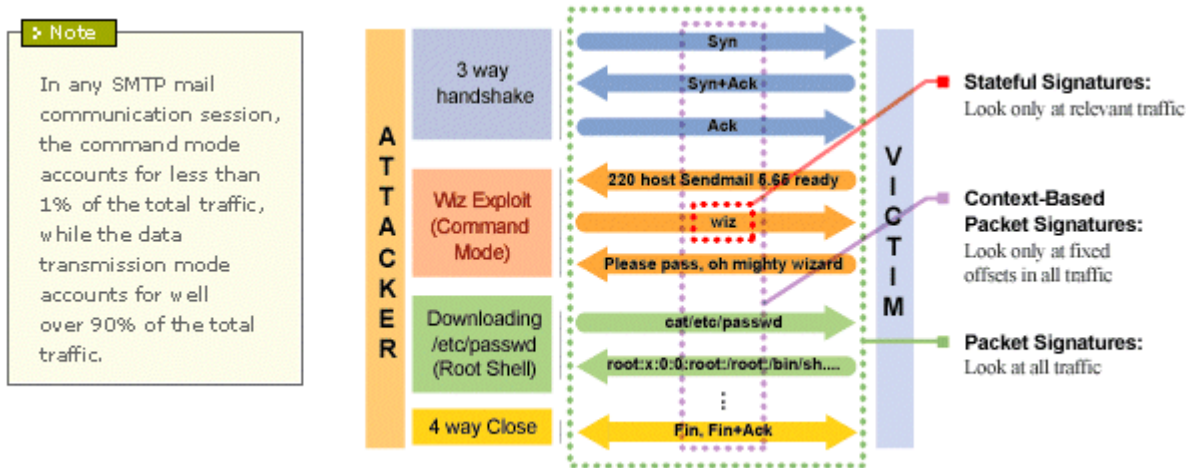
Stateful Signature Detection

There are certain attacks that can be identified using an attack signature, is the pattern of the attack that can be found in the network traffic. Stateful Signatures were developed to significantly increase detection performance and reduce the false alarms associated with signature-based intrusion detection systems currently on the market. Juniper Networks IDP tracks the state of a connection and looks for attack patterns in only the relevant portions of the traffic where these attacks can be perpetrated. Traditional signature-based intrusion detection systems look for attack patterns arbitrarily in the traffic stream, resulting in higher rates of false alarms.

For example, to determine if someone is attempting to login to a server as a root user, a traditional signature-based IDS would send an alarm any time the word "root" appears in the transmission, generating false alarms. Juniper Networks IDP, using Stateful Signature Detection, would only look for the string "root" in the login sequence, which is a way to accurately detect the attack.

All of Juniper Networks IDP's signatures are accessible via a simple, graphical user interface, making it easy to understand what the system is looking for in traffic. Additionally, an open signature format and signature editor provides the ability to quickly modify or add signatures. Both of these capabilities allow users to determine what is important to their environments and make sure the system identifies it.

Let's take a look at the Sendmail Wiz Attack, which tries to gain root access to a SMTP server. To perpetrate, an attacker initiates an SMTP connection and sends "wiz" during the control connection. An intrusion detection system needs to identify the "wiz" pattern to detect the attack.



Most IDSes look for attacks using packet-signature detection, which means they look for a pattern match in each and every packet, without regard to the state of the communication. As shown in the diagram above, a packet signature would look for the "wiz" pattern in the 3-way handshake, the command mode, the data transmission mode, and the 4-way close.

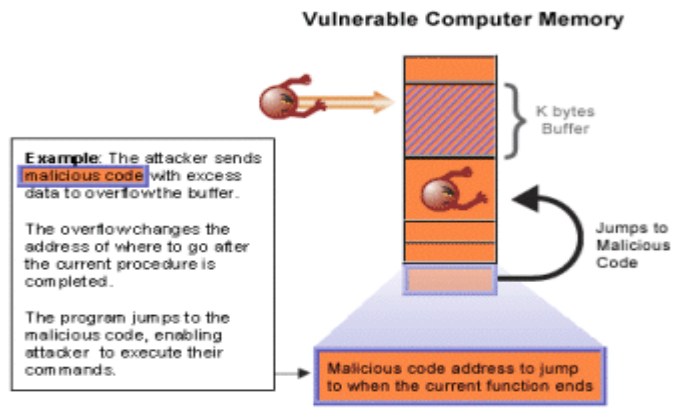
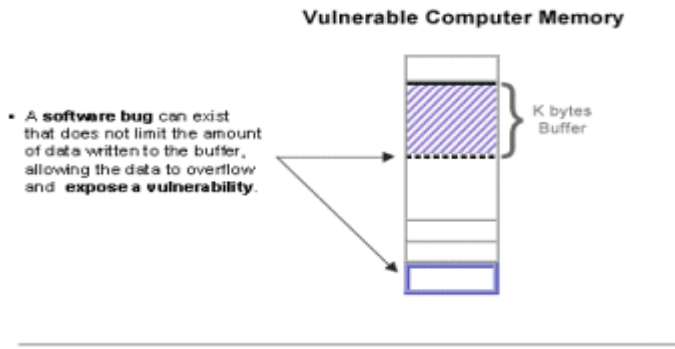
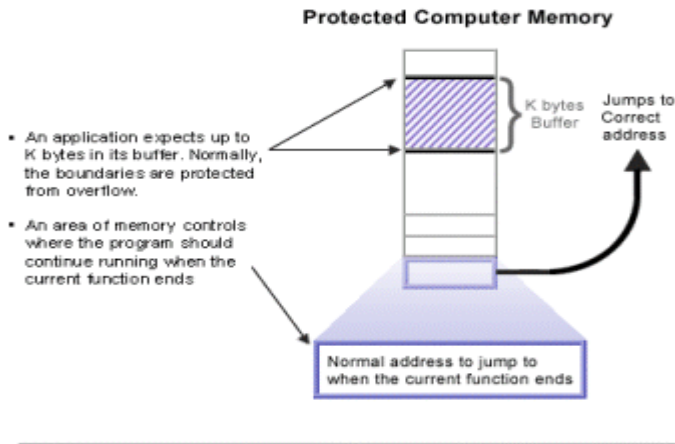
Because the packet signature looks for the attack in all of this unrelated traffic, it wastes resources processing unnecessary information and generates lots of false alarms. This is because SMTP data transmissions are random and use a base64 encoding mechanism that results in the manifestation of the "wiz" pattern at least once in every 32,000 characters.

A few IDS products have tried to improve their packet signature detection implementation by looking for patterns at fixed offsets within each packet. This method is sometimes referred to as context-based signature detection. Systems that use this method still do not understand the communication flows and continue to generate false alarms, as seen in the diagram, by either picking up the pattern across all packets or missing attacks because the attack has permuted the attack pattern.

However, Stateful Signatures track and understand the state of the communication and, therefore, narrow down the pattern matching to the exact location (communication mode and flow direction - meaning client to server or server to client traffic flow) where the attack can be perpetrated. As seen in the diagram, Stateful Signatures only perform signature pattern matching on relevant traffic where an attack can be perpetrated. As a result, performance is greatly improved and the occurrence of false positives significantly reduced.

Protocol Anomaly Detection

Attackers are constantly evolving, launching new or sophisticated attacks that don't follow a pattern. Protocol anomaly detection can be used to identify the attacks that deviate from the protocols that "normal" traffic follows. For instance, it would identify attacks that use ambiguous traffic to try to evade detection and compromise a network and/or host. Using a buffer overflow as an example (below), an attacker gains full access of a machine by making the server run the attacker's code under the server's permissions.

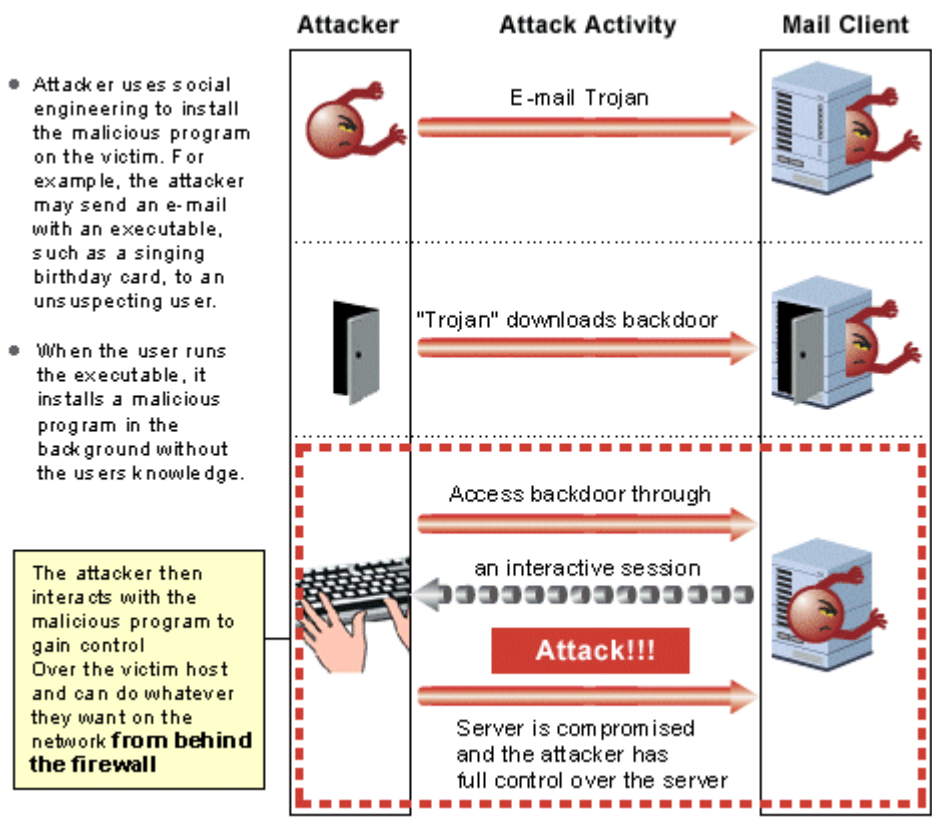


Protocol Anomaly Detection compares the amount of data allowed by the buffer with the amount of data sent and alarms on traffic sent in excess of the allowed amount. Protocol anomaly detection is as effective as the number of protocols it supports. If a protocol is not supported, then attacks exploiting that protocol will go undetected in the network. Juniper Networks IDP is the first to support such a broad range of protocols, including SNMP (to protect against more than 60,000 vulnerabilities) and SMB (to protect against Windows-based vulnerabilities running on internal systems).

Backdoor Detection

Juniper Networks was the first product capable of identifying and protecting against backdoor attacks. Backdoor attacks enter a network and allow an attacker to take complete control of a system, often resulting in a loss of data. For example, an attacker can exploit a vulnerability to load a Trojan onto a network resource, and then interact with that system to control it. The attacker continues can then try different commands in an effort to launch attacks from that system or compromise other systems. Juniper Networks IDP identifies the unique characteristics of the interactive traffic and sends an alarm for unexpected activity.

Example: Trojan Attack

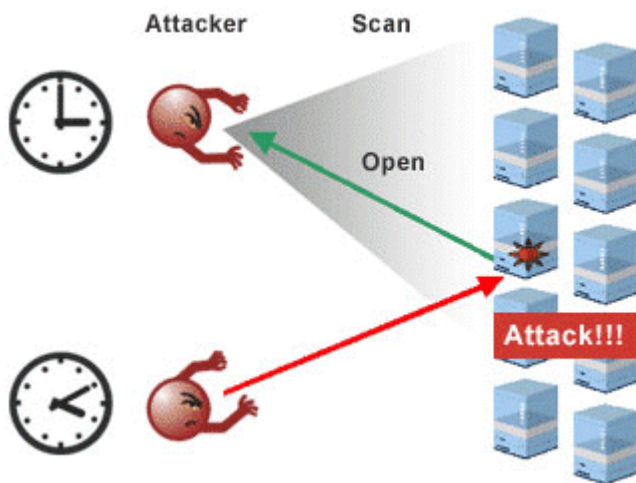


Backdoor Detection is the only way to detect Worms and Trojans

- Looks for interactive traffic
- Detects unauthorized interactive traffic, based on what the administrator defines is allowed
- Detects virtually any backdoor, even if the traffic is encrypted and the protocol is unknown

Traffic Anomaly Detection

Some attacks are not contained within a single session, rather they span a number of connections. Often these attacks are reconnaissance missions, gathering information on the network for future attacks. Traffic anomaly detection can identify this activity by comparing incoming traffic to "normal" traffic patterns and identifying deviations. This method allows Juniper Networks IDP to detect intrusion attempts that span multiple connections, by defining and applying thresholds and triggers. Network probes and port scans are examples of attacks that can be detected by traffic anomaly detection. In the Reconnaissance Attack example below, an attacker scans for open ports on the network and then returns to exploit any discovered vulnerabilities.

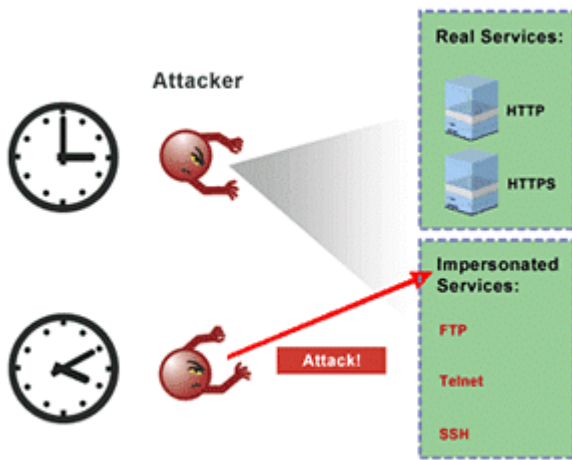


While not an attack in and of itself, network and port scans are indicative of someone trying to get the information they need to launch a future attack. If an administrator is aware of network and port scans, then they can be on the look out for future attacks from that IP address.

Network Honeypot

There are a lot of attackers out there exploring networks to see what they can get away with. A Network Honeypot is a good way to filter out some of the "noise" created by the less sophisticated attackers. By impersonating services that don't exist, the Network Honeypot sends fake information to people scanning the network to try and entice attackers to access the non-existent services. It identifies the attacker when they attempt to connect to the service. There is no reason for legitimate traffic to access these resources because they don't exist; therefore any attempt to access them constitutes an attack.

The Network Honeypot impersonates services, sending fake information in response to scans to try and entice attackers to access the non-existent services. An attack is identified when the attacker returns and tries to access the impersonated resources. There is no reason for legitimate traffic to access these resources because they don't exist, so any attempt to connect constitutes an attack. This is a good way to stop the "noise" created by "script kiddies" and unsophisticated attackers.



Organizations are unique and each has specialized security needs. Juniper Networks IDP's Multi-Method Detection gives organizations maximum coverage, while allowing them to control what to look for and how to respond.

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.